# "Примеры настройки PIX, TACACS+ и RADIUS: 4.2. x

## Содержание



## Введение

RADIUS и TACACS + аутентификация могут быть сделаны для FTP, Telnet и соединений HTTP. TACACS + авторизация поддерживается; Авторизация RADIUS не поддерживается.

Синтаксис для аутентификации изменился немного в программном обеспечении PIX 4.2.2. Этот документ использует синтаксис для версий программного обеспечения 4.2.2.

# Предварительные условия

## Требования

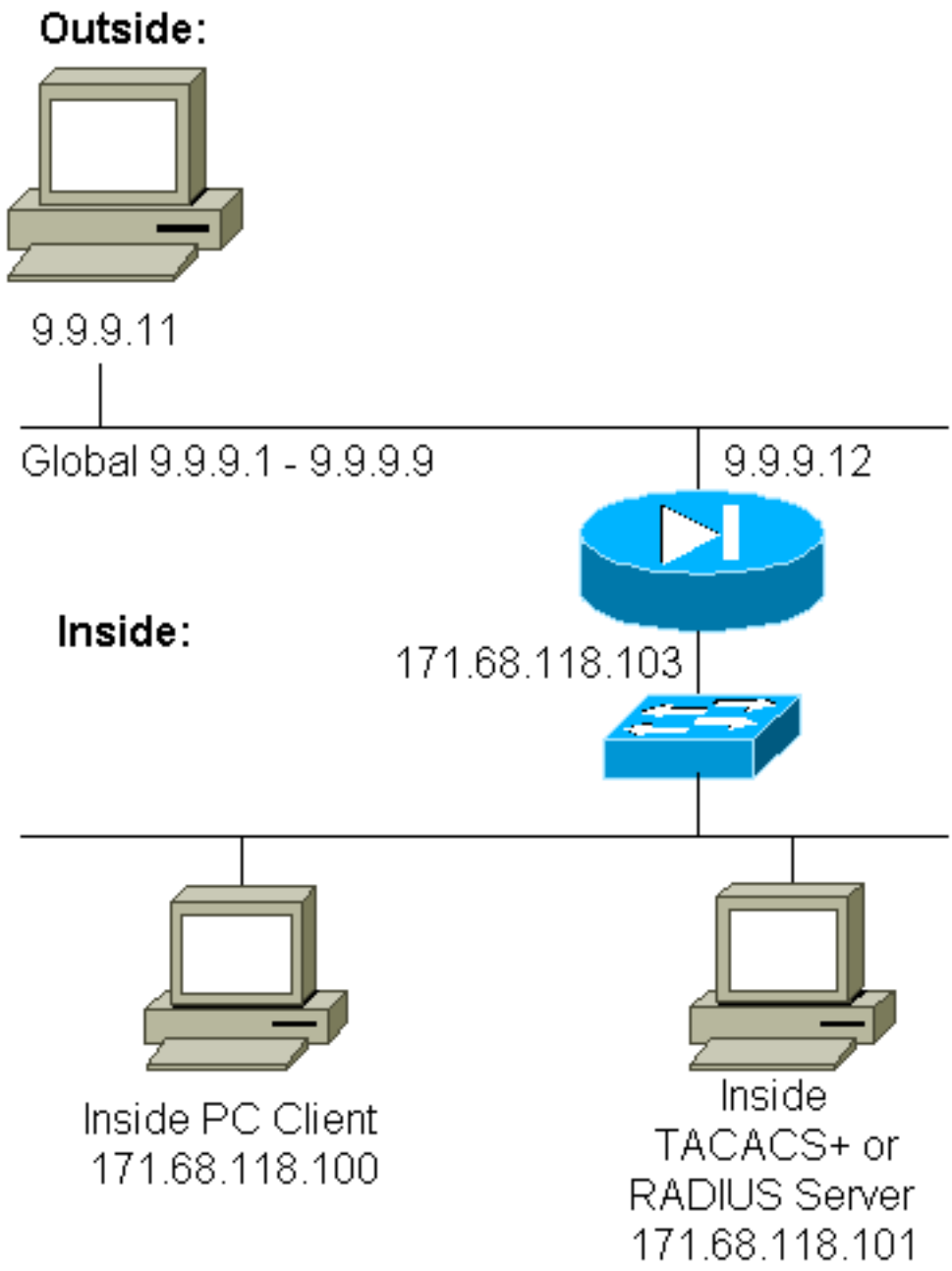
Для этого документа отсутствуют особые требования.

## Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

## Схема сети

В настоящем документе используется следующая схема сети:




| Конфигурация PIX |
| --- |
| pix2# **write terminal** Building configuration : Saved : PIX Version 4.2(2) nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd OnTrBUG1Tp0edmkr encrypted hostname pix2 fixup protocol http 80 fixup protocol smtp 25 no fixup protocol ftp 21 no fixup protocol h323 1720 no fixup protocol rsh 514 no fixup protocol sqlnet 1521 no failover failover timeout 0:00:00 failover ip address outside 0.0.0.0 failover ip address inside 0.0.0.0 failover ip address 0.0.0.0 names pager lines 24 logging console debugging no logging monitor logging buffered debugging logging trap debugging logging facility 20 interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto ip address outside 9.9.9.12 255.255.255.0 ip address inside 171.68.118.103 255.255.255.0 ip address 0.0.0.0 0.0.0.0 arp timeout 14400 global (outside) 1 9.9.9.1-9.9.9.9 netmask 255.0.0.0 static (inside,outside) 9.9.9.10 171.68.118.100 netmask 255.255.255.255 0 0 conduit permit icmp any any conduit permit tcp host 9.9.9.10 eq |

```
telnet any no rip outside passive no rip outside default
no rip inside passive no rip inside default timeout
xlate 3:00:00 conn 1:00:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:00:00 absolute ! !-
-- The next entry depends on whether TACACS+ or RADIUS
is used. ! tacacs-server (inside) host 171.68.118.101
cisco timeout 5 radius-server (inside) host
171.68.118.101 cisco timeout 10 ! !--- The focus of
concern is with hosts on the inside network !---
accessing a particular outside host. ! aaa
authentication any outbound 171.68.118.0 255.255.255.0
9.9.9.11 255.255.255.255 tacacs+|radius ! !--- It is
possible to be less granular and authenticate !--- all
outbound FTP, HTTP, Telnet traffic with: aaa
authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius aaa authentication http outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius ! !--- Accounting records are
sent for !--- successful authentications to the TACACS+
or RADIUS server. ! aaa accounting any outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius ! no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps telnet 171.68.118.100
255.255.255.255 mtu outside 1500 mtu inside 1500 mtu
1500 Smallest mtu: 1500 floodguard 0 tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0 : end
[OK]
```

## Условные обозначения

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

# Аутентификация и авторизация

- Аутентификация состоит в том, *кто* пользователь.
- Авторизация - *то, что* может сделать пользователь.
- *Аутентификация допустима без авторизации.*
- *Авторизация недопустима без аутентификации.*

Как как пример, предположите, что у вас есть пользователи сто внутри, и вы только хотите, чтобы шесть из этих пользователей были в состоянии сделать FTP, Telnet или HTTP вне сети. Скажите PIX аутентифицировать исходящий трафик и давать все шесть идентификаторов пользователей на TACACS +/RADIUS сервер безопасности. С простой проверкой подлинности эти шесть пользователей могут аутентифицироваться с именем пользователя и паролем, затем выйти. Другие девяносто четыре пользователя не могут выйти. PIX побуждает пользователей для имени пользователя/пароля, затем передает их имя пользователя и пароль к TACACS +/RADIUS сервер безопасности. Кроме того, в зависимости от ответа это открывает или запрещает соединение. Эти шесть пользователей могли сделать FTP, Telnet или HTTP.

Однако предположите, что нельзя доверять одному из этих трех пользователей, "Терри". Требуется позволить Терри делать FTP, но не HTTP или Telnet к внешней стороне. Это означает, что необходимо добавить авторизацию. Т.е. авторизация, что пользователи могут сделать в дополнение к аутентификации, кто они. Когда вы добавляете авторизацию к PIX,

PIX сначала передает имя пользователя и пароль Терри к серверу безопасности, затем передает запрос авторизации, который говорит сервер безопасности, что "команда" Терри пытается сделать. С настройкой сервера должным образом, Терри можно разрешить "FTP 1.2.3.4", но запрещают способность к "HTTP" или "Telnet" где угодно.

## Что видит пользователь при включенной аутентификации/авторизации

Когда вы пытаетесь пойти изнутри во внешнюю сторону (или наоборот) с аутентификацией/авторизацией на:

- **Telnet** - Пользователь видит отображение подсказки для ввода имени пользователя, придерживавшееся запросом о пароле. Если аутентификация (и авторизация) прошли успешно на PIX/сервере, пользователь должен ввести имя и пароль в командной строке узла назначения.
- **FTP - пользователь видит имя пользователя, которое появляется в командной строке.** Пользователь должен ввести "local_username@remote_username" в качестве имени пользователя и "local_password@remote_password" в качестве пароля. PIX посылает "локальное_имя_пользователя" и "локальный_пароль" на локальный сервер безопасности, и в случае успешной аутентификации (и авторизации) на PIX/сервере "локальное_имя_пользователя" и "локальный_пароль" пропускаются далее к FTP-серверу назначения.
- **HTTP -** окно отображено в браузере, который запрашивает имя пользователя и пароль. Если аутентификация (и авторизация) прошли успешно, веб-узел назначения появляется в другом окне. **Не забывайте, что браузеры кэшируют имена пользователей и пароли**. Если кажется, что PIX должен вызывать таймаут соединения HTTP, но не делает так, вероятно, что повторная проверка подлинности фактически имеет место с браузером, "стреляющим" в кэшированное имя пользователя и пароль к PIX. Это тогда вперед это к серверу проверки подлинности. Системный журнал PIX и/или серверные отладки показывают это явление. Если Telnet и FTP, кажется, обычно работают, но соединения HTTP не делают, это - причина.

## Конфигурации сервера, используемые для всех сценариев

В TACACS + Примеры конфигураций сервера, если только аутентификация идет, пользователи "все", "telnetonly", "httponly", и "ftponly", все работают. В примерах Конфигурации сервера RADIUS пользователь "все" работает.

Когда авторизация добавлена к PIX, в дополнение к передаче имени пользователя и пароля к TACACS + сервер проверки подлинности, PIX передает команды (Telnet, HTTP или FTP) к TACACS + сервер. TACACS + сервер тогда проверяет, чтобы видеть, авторизуется ли тот пользователь для той команды.

В более позднем примере, пользователе в 171.68.118.100 проблемах **команда telnet 9.9.9.11**. Когда это получено в PIX, PIX передает имя пользователя, пароль и команду к TACACS + сервер для обработки.

Таким образом с авторизацией на в дополнение к аутентификации, пользователь "telnetonly"

может выполнить Операции Telnet через PIX. Однако пользователи "httponly" и "ftponly" не могут выполнить Операции Telnet через PIX.

(Снова, авторизация не поддерживается с RADIUS к природе спецификации протокола).

## TACACS Cisco Secure UNIX + конфигурация сервера

### Cisco Secure 2. x

- Строфы пользователя отображены здесь.
- Добавьте IP-адрес PIX или полное доменное имя и ключ к CSU.cfg.

```
user = all {
password = clear "all"
default service = permit
}

user = telnetonly {
password = clear "telnetonly"
service = shell {
cmd = telnet {
permit .*
}
}
}

user = ftponly {
password = clear "ftponly"
service = shell {
cmd = ftp {
permit .*
}
}
}

user = httponly {
password = clear "httponly"
service = shell {
cmd = http {
permit .*
}
}
}
```

## Конфигурация сервера CiscoSecure UNIX RADIUS

Используйте усовершенствованный пользовательский графический интерфейс (GUI) для добавления IP PIX и ключа к списку сервера доступа к сети (NAS). Строфа пользователя появляется, как замечено здесь:

```
all Password="all"
User-Service-Type = Shell-User
```

## CiscoSecure NT 2.x RADIUS

Раздел Примеров конфигурации CiscoSecure 2.1 онлайн и веба - документации описывает настройку; атрибут 6 (Service-Type) был бы Входом в систему или Административный.

Добавьте IP PIX в разделе Конфигурации NAS с помощью GUI.

## EasyACS TACACS+

Документация по открытому доступу предоставляет сведения о программе установки.

1. В разделе группы нажмите **exec Shell** (для предоставления привилегий exec).
2. Для добавления авторизации к PIX нажмите **Deny несопоставленные команды IOS** у основания настройки групп.
3. Выберите **Add/Edit** для каждой команды, которую вы хотите позволить (Telnet, например).
4. Если вы хотите позволить Telnet определенным узлам, введите IP в раздел аргумента. Для разрешения Telnet всем узлам нажмите **Allow все не включенные в список аргумент**.
5. **Нажать Finish editing command**.
6. Выполните шаги 1through 5 для каждой из позволенных команд (Telnet, HTTP и/или FTP, например).
7. Добавьте IP PIX в разделе Конфигурации NAS с помощью GUI.

## Cisco Secure NT 2.x TACACS +

Cisco Secure 2.x документация предоставляет сведения о программе установки.

1. В разделе группы нажмите **exec Shell** (для предоставления привилегий exec).
2. Для добавления авторизации к PIX нажмите **Deny несопоставленные команды IOS** у основания настройки групп.
3. Установите флажок **команды** в нижней части и введите команду, которую вы хотите позволить (Telnet, например).
4. Если вы хотите позволить Telnet определенным узлам, введите IP в раздел аргумента (например, "разрешите 1.2.3.4"). Для разрешения Telnet всем узлам нажмите **не включенных в список аргумент Permit**.
5. **Нажмите кнопку Submit (Отправить).**
6. Выполните шаги 1through 5 для каждой из позволенных команд (Telnet, FTP и/или HTTP, например).
7. Добавьте IP PIX в разделе Конфигурации NAS с помощью GUI.

## Конфигурация сервера Livingston RADIUS

Добавьте IP PIX и ключ к файлу клиентов.

```
all Password="all"
User-Service-Type = Shell-User
```

## Конфигурация сервера Merit RADIUS

Добавьте IP PIX и ключ к файлу клиентов.

```
all Password="all"
Service-Type = Shell-User
```

## Конфигурация свободно распространяемого сервера TACACS+

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
```

```
key = "cisco"

user = all {
default service = permit
login = cleartext "all"
}

user = telnetonly {
login = cleartext "telnetonly"
cmd = telnet {
permit .*
}
}

user = httponly {
login = cleartext "httponly"
cmd = http {
permit .*
}
}

user = ftponly {
login = cleartext "ftponly"
cmd = ftp {
permit .*
}
}
```

## Шаги отладки

- Удостоверьтесь, что конфигурации PIX работают перед добавляющей аутентификацией, авторизацией и учетом (AAA).Если вы не можете передать трафик прежде, чем установить AAA, вы не будете в состоянии сделать так впоследствии.
- Enable logging в PIX:**Команда logging console debugging** не должна использоваться на в большой степени загружаемая система.**Может использоваться команда отладки "buffered debugging".** Выходные данные от **show logging** или команд **регистрации** могут тогда быть переданы серверу системного журнала и исследованы.
- Удостоверьтесь, что отладка идет для TACACS + или серверы RADIUS. На всех серверах есть данный параметр.

## Примеры отладки аутентификации от PIX

### Отладка PIX - успешная проверка подлинности - RADIUS

Это - пример отладки PIX с успешной проверкой подлинности:

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

### Отладка PIX - неправильная проверка подлинности (имя пользователя или пароль) - RADIUS

Это - пример отладки PIX с неправильной проверкой подлинности (имя пользователя или пароль). Пользователь видит четыре установки имени/пароля пользователя. "Ошибка: максимальное число повторных попыток, превышенных" сообщение, отображено.

**Примечание:** Если это - попытка FTP, одна попытка позволена. Для HTTP позволены бесконечные количества повторов.

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

### Отладка PIX - Выключенный сервер - RADIUS

Это - пример отладки PIX с сервером вниз. Пользователь видит имя пользователя однажды. Сервер тогда "зависает" и просит пароль (три раза).

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

### Отладка PIX - успешная проверка подлинности - TACACS +

Это - пример отладки PIX с успешной проверкой подлинности:

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
  laddr 171.68.118.100/1200 (cse)
```

### Отладка PIX - неправильная проверка подлинности (имя пользователя или пароль) - TACACS +

Это - пример отладки PIX с неправильной проверкой подлинности (имя пользователя или пароль). Пользователь видит четыре установки имени/пароля пользователя. "Ошибка: максимальное число повторных попыток, превышенных" сообщение, отображено.

**Примечание:** Если это - попытка FTP, одна попытка позволена. Для HTTP позволены бесконечные количества повторов.

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

### Отладка PIX - Выключенный сервер - TACACS +

Это - пример отладки PIX с сервером вниз. Пользователь видит имя пользователя однажды. Сразу, "Ошибка: Максимальное число попыток, превышенных" сообщение, отображено.

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

## Добавление авторизации

Поскольку авторизация не допустима без аутентификации, авторизация требуется для того же источника и назначения:

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11 255.255.255.255
tacacs+|radius
```

Или, если первоначально аутентифицировались все три исходящих сервиса:

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa authorization
ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa authorization telnet outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius
```

## Примеры отладки процессов проверки подлинности и полномочий из межсетевого экрана Private Internet Exchange (PIX)

### Отладка PIX - успешная проверка подлинности и авторизация - TACACS +

Это - пример отладки PIX с успешной проверкой подлинности и авторизацией:

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

### Отладка PIX - успешная проверка подлинности, но сбой в авторизации - TACACS +

Это - пример отладки PIX с успешной проверкой подлинности, но сбоем в авторизации:

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
```

### Отладка PIX - неправильная проверка подлинности, авторизация, не предпринятая - TACACS +

Это - пример отладки PIX с проверкой подлинности и авторизация, но авторизацией, не предпринятой из-за неправильной проверки подлинности (имя пользователя или пароль). Пользователь видит четыре установки имени/пароля пользователя. "Ошибка: максимальное число повторных попыток превысило". сообщение отображено

**Примечание:** Если это - попытка FTP, одна попытка позволена. Для HTTP позволены бесконечные количества повторов.

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
```

```
 109006: Authentication failed for user '' from 171.68.118.100/1228
   to 9.9.9.11/23
```

### Отладка PIX - Аутентификация/Авторизация, Выключенный Сервер - TACACS +

Это - пример отладки PIX с проверкой подлинности и авторизация. Сервер не работает. Пользователь видит имя пользователя однажды. Сразу, "Ошибка: Максимальное число попыток превысило". отображен.

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

## Добавление учета

### TACACS +

**aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+**

Отладка выглядит одинаково, идет ли учет или прочь. Однако во время "Созданного", учетная запись "запуска" передается. Кроме того, во время "Разрушения" передается учетная запись "остановки":

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

TACACS + учетные записи похожи на эти выходные данные (это от CiscoSecure UNIX; записи в Windows Cisco Secure могут быть разделены запятой вместо этого):

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

Поля ломаются, как замечено здесь:

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
```

```
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

## RADIUS

**aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius**

Отладка выглядит одинаково, идет ли учет или прочь. Однако во время "Созданного", учетная запись "запуска" передается. Кроме того, во время "Разрушения" передается учетная запись "остановки":

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

Учетные записи RADIUS похожи на эти выходные данные (это от Cisco Secure UNIX; те в Windows Cisco Secure разделены запятой):

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```

Поля ломаются, как замечено здесь:

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
<Acct-Session-Time = #>
```

# Максимальное количество сеансов и просмотров авторизованными пользователями

Некоторый TACACS и серверы RADIUS имеют max-session, или "просматривают вошедшии в систему пользователь" функции. Возможность выполнения команды max-sessions и просмотра пользователей, вошедших в систему, зависит от учетных записей. Когда существует бухгалтерская генерируемая запись "запуска", но никакие не "останавливают" запись, TACACS или сервер RADIUS предполагают, что в человека все еще входят (который является; имеет сеанс через PIX). Такая ситуация годится для соединений Telnet и

FTP благодаря типу этих соединений. Пример:

Пользовательские Telnet от 171.68.118.100 до 9.9.9.25 через PIX, аутентифицирующийся на пути:

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1200
   to 9.9.9.25/23
(pix) 109011: Authen Session Start: user 'cse', sid 3
(pix) 109005: Authentication succeeded for user 'cse' from 171.68.118.100/12
00 to 9.9.9.25/23
(pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23 gaddr 9.9.9.10/12
00 laddr 171.68.118.100/1200 (cse)
(server start account) Sun Nov  8 16:31:10 1998 rtp-pinecone.rtp.cisco.com
    cse PIX     171.68.118.100  start   task_id=0x3     foreign_ip=9.9.9.25
    local_ip=171.68.118.100     cmd=telnet
```

Поскольку сервер видел запись "запуска", но никакие не "останавливают" запись (в данный момент), сервер показывает, что входят в пользователя "Telnet". Если пользователь делает попытку другого соединения, которое требует аутентификации (возможно, от другого ПК) и если max-sessions установлен в "1" на сервере для этого пользователя, соединению отказывает сервер.

Пользователь идет о бизнесе на конечном узле, затем выходит (проводит 10 минут там).

```
(pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr 9.9.9.10/128 1
  laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)

 (server stop account) Sun Nov  8 16:41:17 1998
   rtp-pinecone.rtp.cisco.com cse PIX
   171.68.118.100  stop task_id=0x3 foreign_ip=9.9.9.25
   local_ip=171.68.118.100
   cmd=telnet elapsed_time=5  bytes_in=98 bytes_out=36
```

Является ли uauth 0 (который является; аутентифицируйтесь каждый раз), или больше (аутентифицируйтесь однажды и не снова во время периода проверки подлинности (uauth)), будет вырезка учетной записи для каждого узла, к которому обращаются.

Но HTTP работает по-другому из-за природы протокола. Ниже представлен пример:

Пользователь просматривает от 171.68.118.100 до 9.9.9.25 через PIX.

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1281
   to 9.9.9.25 /80 (pix) 109011: Authen Session Start: user 'cse', sid 5

 (pix) 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/12 81 to 9.9.9.25/80

 (pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/80 gaddr 9.9.9.10/12 81
   laddr 171.68.118.100/1281 (cse)

 (server start account) Sun Nov  8 16:35:34 1998 rtp-pinecone.rtp.cisco.com
   cse PIX     171.68.118.100  start   task_id=0x9     foreign_ip=9.9.9.25
   local_ip=171.68.118.100     cmd=http

 (pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr 9.9.9.10/128 1
   laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)

 (server stop account) Sun Nov  8 16:35.35 1998 rtp-pinecone.rtp.cisco .com
   cse     PIX     171.68.118.100  stop  task_id=0x9   foreign_ip =9.9.9.25

   local_ip=171.68.118.100 cmd=http   elapsed_time=0
```

```
      bytes_ in=1907   bytes_out=223
```
Пользователь читает загруженную веб-страницу.

Обратите внимание на время. Эта загрузка взяла одну секунду (были меньше, чем одна секунда между запуском и записью остановки). В пользователя все еще входят к веб-сайту, и соединение все еще открываются? Нет.

Есть ли здесь возможность установки максимального количества сеансов или просмотра зарегистрированных в сети пользователей? Нет, потому что время соединения в HTTP слишком коротко. Время между "Созданным" и "Разрушением" ("запуск" и "останавливают" запись) является подвторым. Не будет записи "запуска" без записи "остановки", так как записи происходят в фактически тот же момент. Сервер получит записи "start" и "stop" для каждой транзакции вне зависимости от значения "uauth" (0 или больше). Однако max-sessions и обзорные вошедшии в систему пользователь не будут работать из-за природы соединений HTTP.

## Использование команды except

В нашей сети, если мы решаем, что один исходящий пользователь (171.68.118.100) не должен аутентифицироваться, мы можем сделать это:

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11 255.255.255.255 tacacs+ aaa
authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11 255.255.255.255 tacacs+
```

## Аутентификация в PIX

Предыдущее обсуждение имеет аутентифицирующуюся Telnet (и HTTP, FTP) трафик через PIX. С 4.2.2, могут также аутентифицироваться Telnet - подключения к PIX. Здесь, мы определяем IPs коробок, которые могут Telnet к PIX:

```
telnet 171.68.118.100 255.255.255.255
```
Затем предоставьте Пароль Telnet: **passwd ww**.

Добавьте новую команду для аутентификации пользовательского Telnet - сеанса на PIX:

```
aaa authentication telnet console tacacs+|radius
```
Когда подключение пользователей посредством Telnet к PIX, им предлагают для Пароля Telnet ("ww"). PIX также запрашивает TACACS + или Имя пользователя RADIUS и пароль.

## Изменение приглашения, показываемого пользователям

Если вы добавляете команду: **подлинное приглашение YOU_ARE_AT_THE_PIX**, пользователи, проходящие PIX, будет видеть последовательность:

```
YOU_ARE_AT_THE_PIX [at which point you enter the username] Password:[at which point you enter
the password]
```
По прибытию в конечный пункт назначения, "Имя пользователя": и "Пароль": приглашения будут отображены. Это приглашение только влияет на пользователей, проходящих PIX, не к PIX.

**Примечание:** Нет никакой вырезки учетных записей для доступа к PIX.

## Дополнительные сведения

- Поддержка продуктов программного обеспечения Cisco PIX Firewall
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация