Настройка PIX 5.0.x: TACACS+ и RADIUS

Содержание

Введение

RADIUS и TACACS + аутентификация могут быть сделаны для FTP, Telnet и соединений HTTP. Аутентификация для другого меньшего количества обычных протоколов TCP может обычно делаться работать.

TACACS + авторизация поддерживается. Авторизация RADIUS не поддерживается. Изменения в аутентификации, авторизации и учете (AAA) PIX 5.0 по предыдущей версии включают учет AAA для трафика кроме HTTP, FTP и Telnet.

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.

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 пример, предположите, что у вас есть пользователи сто внутри, и вы хотите, только хотят, 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 неспособны выйти. PIX побуждает пользователей для имени пользователя/пароля, затем передает их имя пользователя и пароль к TACACS +/RADIUS сервер безопасности. В зависимости от ответа это открывает или запрещает соединение. Эти шесть пользователей могут сделать FTP, Telnet или HTTP.

С другой стороны, 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, говоря 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 -** который окно отобразило 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 блокировать по времени HTTP подключение, но не делает это, вероятно, что в данный момент производится заново подтверждение подлинности, браузер «выстреливает» кэшированные имя пользователя и пароль на PIX, который затем направляет их на сервер проверки подлинности. Данное событие будет отображено в системном журнале PIX и/или при отладке сервера. Это является причиной в ситуациях, когда Telnet и FTP функционируют нормально, а соединения HTTP – нет.

Настройки сервера безопасности для всех сценариев

Конфигурация сервера CiscoSecure UNIX TACACS

Удостоверьтесь, что у вас есть IP-адрес PIX или полное доменное имя и ключ в файле CSU.cfg.

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

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

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

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

Конфигурация сервера CiscoSecure UNIX RADIUS

Используйте графический пользовательский интерфейс (GUI) для добавления IP PIX и ключа к списку сервера доступа к сети (NAS).

```
user=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
```

Windows 2.x RADIUS Cisco Secure

Выполните следующие действия:

1. Получите пароль в Разделе ГИП настройки пользователя.
2. От Раздела графического интерфейса пользователя Настройки групп, атрибут набора 6 (Service-Type) для Входа в систему или Административный.
3. Добавьте IP PIX в GUI конфигурации NAS.

EasyACS TACACS+

Документация по открытому доступу описывает настройку.

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 новая команда** для каждой команды, которую вы хотите позволить (например, Telnet).
4. Если вы хотите позволить Telnet определенным узлам, войдите, IP в разделе аргумента в форме "разрешают #.#.#.#". Для разрешения Telnet всем узлам нажмите **Allow все не включенные в список аргумент**.
5. **Нажать Finish editing command**.
6. Выполните шаги 1 - 5 для каждой из позволенных команд (например, Telnet, HTTP или FTP).
7. Добавьте IP PIX в Разделе графического интерфейса пользователя Конфигурации NAS.

CiscoSecure 2.x TACACS+

Пользователь получает пароль в Разделе ГИП настройки пользователя.

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 новая команда** для каждой команды, которую вы хотите позволить (например, Telnet).
4. Если вы хотите позволить Telnet определенным узлам, введите IP разрешения в поле для ввода аргумента (например, "разрешите 1.2.3.4"). Для разрешения Telnet всем узлам нажмите **Allow все не включенные в список аргумент**.
5. **Нажать Finish editing command**.
6. Выполните предыдущие шаги для каждой из позволенных команд (например, Telnet,

HTTP и/или FTP).
7. Добавьте IP PIX в Разделе графического интерфейса пользователя Конфигурации NAS.

Конфигурация сервера Livingston RADIUS

Добавьте IP PIX и ключ к файлу клиентов.

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

Конфигурация сервера Merit RADIUS

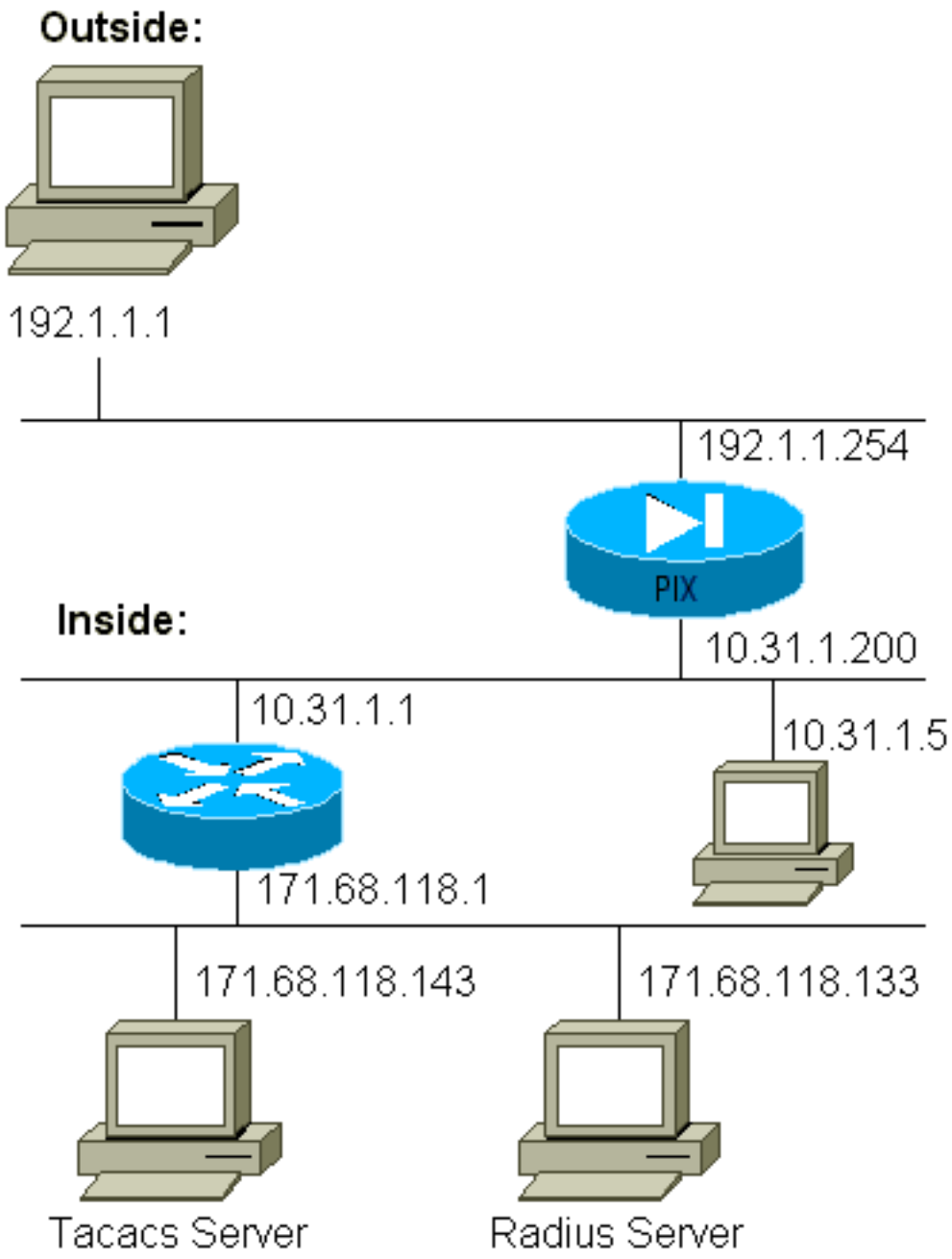
Добавьте IP PIX и ключ к файлу клиентов.

```
adminuser Password="all"
Service-Type = Shell-User  key = "cisco"

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

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

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

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

Шаги отладки

- Удостоверьтесь, что конфигурации PIX работают перед добавлением AAA.Если трафик нельзя передать до аутентификации и авторизации, этого нельзя будет сделать и впоследствие.
- Enable logging в PIX**Команда отладки консоли регистрации не должна использоваться в системе с высокой нагрузкой.Может использоваться команда отладки "buffered debugging".** Выходные данные от **show logging** или команд **регистрации** могут быть переданы серверу системного журнала и исследованы.
- Удостоверьтесь, что отладка идет для TACACS + или серверы RADIUS. На всех серверах есть данный параметр.

Схема сети



Конфигурация PIX
pix-5# **write terminal** nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pixfirewall fixup protocol ftp 21 fixup protocol http 80 fixup protocol smtp 25 fixup protocol h323 1720 fixup protocol rsh 514 fixup protocol sqlnet 1521 names name 1.1.1.1 abcd name 1.1.1.2 a123456789 name 1.1.1.3 a123456789123456 pager lines 24 logging timestamp no logging standby logging console debugging no logging monitor logging buffered debugging no logging trap logging facility 20 logging queue 512 interface ethernet0 auto interface ethernet1 auto mtu outside 1500 mtu inside 1500 ip address outside 192.1.1.254 255.255.255.0 ip address inside 10.31.1.200 255.255.255.0 no failover failover timeout 0:00:00 failover ip address outside 0.0.0.0 failover ip address inside 0.0.0.0 arp timeout 14400 global (outside) 1

```
192.1.1.10-192.1.1.20 netmask 255.255.255.0 static
(inside,outside) 192.1.1.25 171.68.118.143 netmask
255.255.255.255 0 0 static (inside,outside) 192.1.1.30
10.31.1.5 netmask 255.255.255.255 0 0 conduit permit tcp
any any conduit permit icmp any any conduit permit udp
any any no rip outside passive no rip outside default no
rip inside passive no rip inside default route inside
171.68.118.0 255.255.255.0 10.31.1.1 1 timeout xlate
3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00 timeout uauth 0:00:00
absolute aaa-server TACACS+ protocol tacacs+ aaa-server
RADIUS protocol radius aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host
171.68.118.143 cisco timeout 5 aaa-server AuthOutbound
protocol radius aaa-server AuthOutbound (inside) host
171.68.118.133 cisco timeout 5 aaa authentication telnet
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication telnet inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa
authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound no snmp-server location no snmp-
server contact snmp-server community public no snmp-
server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b : end
```

Опознавательные примеры отладки от примеров отладки PIXAuthentication от PIX

В этих примерах отладки:

Исходящий

Внутренний пользователь в 10.31.1.5 инициирует трафик к внешним 192.1.1.1 и аутентифицируется через TACACS +. Исходящий трафик использует список серверов "AuthOutbound", который включает сервер RADIUS 171.68.118.133.

Входящий

Внешний пользователь в 192.1.1.1 инициирует трафик к внутреннему 10.31.1.5 (192.1.1.30) и аутентифицируется через TACACS. Входящий трафик использует список серверов "AuthInbound", который включает Сервер tacacs 171.68.118.143).

Отладка PIX - успешная проверка подлинности - TACACS +

Данный пример показывает отладку PIX с успешной проверкой подлинности:

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
    to 10.31.1.5/23
 109011: Authen Session Start: user 'pixuser', sid 6
 109005: Authentication succeeded for user 'pixuser' from 10.31.1.5/23
    to 192.1.1.1/13155
 109012: Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds
```

```
 302001: Built inbound TCP connection 6 for faddr 192.1.1.1/13155
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

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

Данный пример показывает отладку PIX с неправильной проверкой подлинности (имя пользователя или пароль). Пользователь видит четыре установки имени/пароля пользователя и сообщение "`Error: max number of tries exceeded`".

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
    to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13157
```

Отладка PIX - Может Пропинговать Сервер, Никакой Ответ - TACACS +

Данный пример показывает отладку PIX, где сервер может быть пропингован, но не говорит с PIX. Пользователь видит имя пользователя однажды, но PIX никогда не просит пароль (это находится на Telnet). Пользователь видит "`Error: Max number of tries exceeded.`"

```
Auth start for user '???' from 192.1.1.1/13159 to
    10.31.1.5/23
 pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
    failed (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13159
```

Отладка PIX - неспособный пропинговать сервер - TACACS +

Данный пример показывает отладку PIX, где сервер не является отвечающим на команду ping. Пользователь видит имя пользователя однажды, но PIX никогда не просит пароль (это находится на Telnet). Эти сообщения отображены: "`Timeout to TACACS+ server`" и "`Error: Max number of tries exceeded`" (мы загрузили фиктивный сервер в конфигурации).

```
109001: Auth start for user '???' from 192.1.1.1/13158
    to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13158
```

Отладка PIX - успешная проверка подлинности - RADIUS

Данный пример показывает отладку PIX с успешной проверкой подлинности:

```
109001: Auth start for user '???' from 10.31.1.5/11074
    to 192.1.1.1/23
 109011: Authen Session Start: user 'pixuser', Sid 7
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.5/11074 to 192.1.1.1/23
 109012: Authen Session End: user 'pixuser', Sid 7,
```

```
    elapsed 1 seconds
 302001: Built outbound TCP connection 7 for faddr 192.1.1.1/23
    gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (pixuser)
```

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

Данный пример показывает отладку PIX с неправильной проверкой подлинности (имя пользователя или пароль). Пользователь видит запрос об Имени пользователя и пароле. У пользователя есть три возможности для успешного Имени пользователя/Ввода пароля.

```
- 'Error: max number of tries exceeded'
 pixfirewall# 109001: Auth start for user '???' from
    192.1.1.1/13157 to 10.31.1.5/23
 109001: Auth start for user '???' from 10.31.1.5/11075
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11075
    to 192.1.1.1/23
```

Отладка эхо-запроса - может пропинговать сервер, Выключенный демон - RADIUS

Данный пример показывает отладку PIX, где сервер является отвечающим на команду ping, но демон не работает и не свяжется с PIX. Пользователь видит Имя пользователя, пароль и сообщения "`RADIUS server failed`" и "`Error: Max number of tries exceeded.`"

```
pixfirewall# 109001: Auth start for user '???'
    from 10.31.1.5/11076 to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11076
    to 192.1.1.1/23
```

Отладка PIX - Неспособный Пропинговать Сервер или Несогласованность ключа/клиента - RADIUS

Обувь данного примера отладка PIX, где сервер не является отвечающим на команду ping или существует несогласованность ключа/клиента. Пользователь видит Имя пользователя, пароль и сообщения "`Timeout to RADIUS server`" и "`Error: Max number of tries exceeded`" (фиктивный сервер был подкачан в конфигурации).

```
109001: Auth start for user '???' from 10.31.1.5/11077
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11077
```

```
    to 192.1.1.1/23
```

Добавление авторизации

Если вы решите добавить авторизацию, то вы потребуете авторизации для того же исходного и конечного диапазона (так как авторизация не допустима без аутентификации):

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization
HTTP inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Обратите внимание на то, что авторизация не добавлена для "выхода", потому что исходящий поток данных аутентифицируется с RADIUS, и Проверка подлинности RADIUS не допустима.

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

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

Данный пример показывает отладку PIX с успешной проверкой подлинности и успешной авторизацией:

```
109011: Authen Session Start: user 'pixuser', Sid 8
 109007: Authorization permitted for user 'pixuser'
    from 192.1.1.1/13160 to 10.31.1.5/23
 109012: Authen Session End: user 'pixuser', Sid 8,
    elapsed 1 seconds
 302001: Built inbound TCP connection 8 for faddr 192.1.1.1/13160
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

Отладка PIX - успешная проверка подлинности, сбой проверки подлинности - TACACS +

Данный пример показывает отладку PIX с успешной проверкой подлинности, но со сбоем проверки подлинности. Здесь пользователь также видит сообщение "`Error: Authorization Denied.`"

```
109001: Auth start for user '???' from 192.1.1.1/13162
    to 10.31.1.5/23
 109011: Authen Session Start: user 'userhttp', Sid 10
 109005: Authentication succeeded for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109008: Authorization denied for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109012: Authen Session End: user 'userhttp', Sid 10,
    elapsed 1 seconds
 302010: 0 in use, 2 most used
```

Добавление учета

TACACS +

aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

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

TACACS + учетные записи похожи на эти выходные данные (это от Cisco Secure NT, следовательно разделенный запятой формат):

```
04/26/2000,01:31:22,pixuser,Default Group,192.1.1.1,
  start,,,,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1,
  ,, ,,,,,,,,,zekie,,,,,,,,^
04/26/2000,01:31:26,pixuser,Default Group,192.1.1.1,stop,4,
  ,36,82,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1,
  ,,,,,,,,,,,zekie,,,,,,,,
```

RADIUS

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound

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

Учетные записи RADIUS похожи на эти выходные данные (это от Cisco Secure UNIX; в Cisco Secure NT могут быть разделены запятой вместо этого):

```
radrecv: Request from host a1f01c8 code=4, id=18, length=65
Acct-Status-Type = Start
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
User-Name = "pixuser"
Sending Accounting Ack of id 18 to a1f01c8 (10.31.1.200)
radrecv: Request from host a1f01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
Username = "pixuser"
Acct-Session-Time = 7
```

Использование команды "except"

В нашей сети, если мы решаем, что конкретному источнику и/или назначению не нужны аутентификация, авторизация или учет, мы можем сделать что-то вроде этого выходные данные:

aaa authentication except inbound 192.1.1.1 255.255.255.255 0.0.0.0 0.0.0.0 AuthInbound

Если вы "исключаете" коробку из аутентификации и имеете авторизацию на, вы должны также кроме коробки из авторизации.

Максимальное количество сеансов и просмотров авторизованными пользователями

На некоторых серверах TACACS+ и RADIUS есть функции установки максимального количества соединений и просмотра зарегистрированных пользователей в сети. Возможность выполнения команды max-sessions и просмотра пользователей, вошедших в систему, зависит от учетных записей. То, когда существует бухгалтерская генерируемая запись "запуска", но никакие не "останавливают" запись, TACACS + или сервер RADIUS предполагает, что в человека все еще входят (имеет сеанс через PIX).

Такая ситуация годится для соединений Telnet и FTP благодаря типу этих соединений. Для протокола HTTP это работает некорректно в связи с особенностями подключения. В выходных данных данного примера используется другая конфигурация сети, но понятия являются тем же.

Пользовательские Telnet 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
```

Так как 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 (принимающий max-sessions поддержек сервера), соединению отказывает сервер.

Пользователь продолжает Telnet или FTP - бизнес 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 (аутентифицируйтесь каждый раз), или больше (аутентифицируются однажды и не снова во время периода проверки подлинности (uauth)), учетная запись вырезано для каждого узла, к которому обращаются.

HTTP работает по-другому вследствие типа протокола. Эти выходные данные показывают пример HTTP:

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 просматривает загруженную веб-страницу.

Начальная запись, зарегистрированная в 16:35:34, и запись остановки, зарегистрированная в 16:35:35. Эта загрузка продолжалась 1 секунду (т. е. между записью начала и записью остановки прошло менее секунды). В пользователя все еще входят к веб-сайту, и соединение все еще открываются, когда они читают веб-страницу? Нет. Есть ли здесь возможность установки максимального количества сеансов или просмотра зарегистрированных в сети пользователей? Нет, поскольку время подключения (интервал времени между установлением соединения и освобождением канала) для протокола HTTP слишком мало. Интервал между состояниями "start" (начало) и "stop" (окончание) составляет менее одной секунды. 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 работают из-за природы соединений HTTP.

Аутентификация и включение в самом PIX

Предыдущее обсуждение описало аутентифицирующуюся Telnet (и HTTP, FTP) трафик *через* PIX. Мы удостоверяемся, что Telnet *к* PIX работает *без* аутентификации на:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
aaa authentication telnet console AuthInbound
```

Когда подключение пользователей посредством Telnet к PIX, им предлагают для Пароля Telnet **(ww)**. Затем PIX также запрашивает TACACS + (в этом случае, так как список серверов "AuthInbound" используется), или Имя пользователя RADIUS и пароль. Если сервер не работает, можно войти в PIX путем ввода **pix** для имени пользователя, и затем enable password (**enable password** *вообще*) для получения доступа.

С этой командой:

```
aaa authentication enable console AuthInbound
```

пользователю предлагают для имени пользователя и пароля, которое передается TACACS (в этом случае, так как список серверов "AuthInbound" используется, запрос переходит к Серверу tacacs), или сервер RADIUS. Поскольку пакет аутентификации для включения представляет собой то же, что и пакет аутентификации для входа, если пользователь может

войти в PIX с аутентификацией TACACS или RADIUS, он также может выполнить включение с помощью аутентификации TACACS или RADIUS с тем же именем пользователя и паролем. Этой проблемой был назначенный идентификатор ошибки Cisco CSCdm47044 (только зарегистрированные клиенты).

Аутентификация в последовательной консоли

Команда aaa authentication serial console AuthInbound требует проверки для проверки подлинности для доступа к последовательной консоли PIX.

Когда пользователь выполняет команды настройки от консоли, сообщения системного журнала вырезаны (предположение, что PIX настроен для передачи системного журнала в уровне отладки к узлу системного журнала). Это - пример того, что отображено на сервере системного журнала:

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
 03:21:14: %PIX-5-111008: User 'pixuser' executed the 'logging' command.
```

Измените Приглашение, которое Видят Пользователи

Если у вас есть **команда auth-prompt PIX_PIX_PIX**, пользователи, которые проходят PIX, видят эту последовательность:

```
PIX_PIX_PIX [at which point one would enter the username]
Password:[at which point one would enter the password]
```

По прибытию в последнее поле назначения, "Имя пользователя": и "Пароль": приглашение отображено. Это приглашение влияет только на пользователей, *проходящих* PIX, не *к* PIX.

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

Настройте пользователей сообщения, посмотрите на успехе/Сбое

Если у вас есть команды:

```
auth-prompt accept "GOOD_AUTH" auth-prompt reject "BAD_AUTH"
```

пользователи видят эту последовательность на неудачной/удачной попытке входа через PIX:

```
PIX_PIX_PIX
 Username: asjdkl
 Password:
 "BAD_AUTH"
 "PIX_PIX_PIX"
 Username: cse
 Password:
 "GOOD_AUTH"
```

Простой по числу пользователей и абсолютное время простоя

Простаивающий и абсолютные времена ожидания uauth может быть передан вниз от TACACS + сервер на основе для каждого пользователя. Если у всех пользователей в вашей сети должно быть то же "время ожидания, указанное в uauth '", не внедряйте это! Но если вы нуждаетесь в другом uauths для каждого пользователя, продолжаете читать.

В данном примере используется **команда timeout uauth 3:00:00**. Как только человек аутентифицируется, они не должны проходить повторную проверку подлинности в течение трех часов. Однако, если вы устанавливаете пользователя с этим профилем и имеете *авторизацию AAA* TACACS на в PIX, простаивающее и абсолютные времена ожидания в профиле пользователя отвергают время ожидания, указанное в uauth ' в PIX для того пользователя. Это не означает, что сеанс Telnet через PIX разъединен после простаивающего / абсолютного времени ожидания. Это просто управляет, имеет ли повторная проверка подлинности место.

Этот профиль прибывает из TACACS + бесплатное программное обеспечение:

```
user = timeout {
default service = permit
login = cleartext "timeout"
service = exec {
timeout = 2
idletime = 1
}
}
```

После аутентификации выполните **команду show uauth** на PIX:

```
pix-5# show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user
'timeout' at 10.31.1.5, authorized to: port 11.11.11.15/telnet absolute timeout: 0:02:00
inactivity timeout: 0:01:00
```

После того, как пользователь сидит сложа руки в течение одной минуты, отладка на PIX показывает:

```
109012: Authen Session End: user 'timeout', Sid 19, elapsed 91 seconds
```

Пользователь должен пройти повторную проверку подлинности, когда это возвращается к тому же конечному узлу или другому хосту.

Виртуальный HTTP

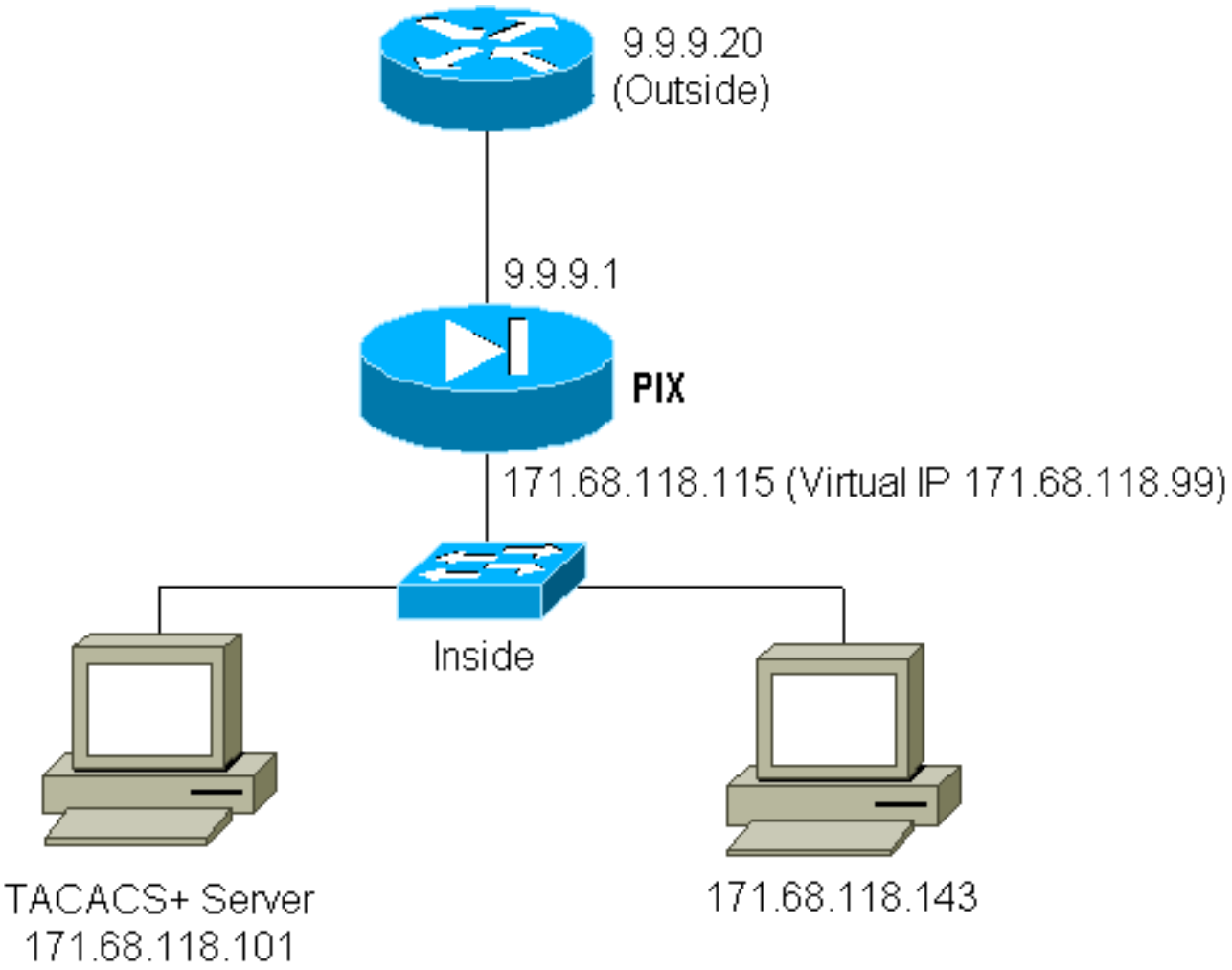
Если для узлов PIX, а также вне PIX необходима аутентификация, пользователь может столкнуться с необычным поведением браузера, поскольку браузеры помещают в кэш имя пользователя и пароль.

Для предотвращения этого можно внедрить действительный HTTP путем добавления адреса RFC 1918 (адрес, который немаршрутизуем в Интернете, но допустим и уникален для внутренней сети PIX) к конфигурации PIX с помощью этой команды:

```
virtual http #.#.#.# [warn]
```

Аутентификация требуется при попытке пользователя выйти из PIX. При наличии параметра предупреждения пользователь получает переадресованное сообщение. Аутентификация проводится для периода времени, указанного в "uauth". Как обозначено в документации, сделайте "not set" продолжительность команды **времени ожидания, указанное в uauth '** к 0 секундам с действительным HTTP. Это не позволит устанавливать подключения по HTTP к реальному веб-серверу.

Выходная данные виртуального HTTP схема



Выходная данные виртуального HTTP конфигурация PIX

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

Виртуальный протокол Telnet

Возможно настроить PIX для аутентификации всего входящего и исходящего трафика, но это не хорошая идея сделать так. Это вызвано тем, что некоторые протоколы, такие как "почта", легко не аутентифицируются. Когда весь трафик через PIX аутентифицируется, системный журнал PIX для сообщений протоколов, не допускающих аутентификацию, таких как, когда почтовый сервер и клиент пытаются связаться через PIX:

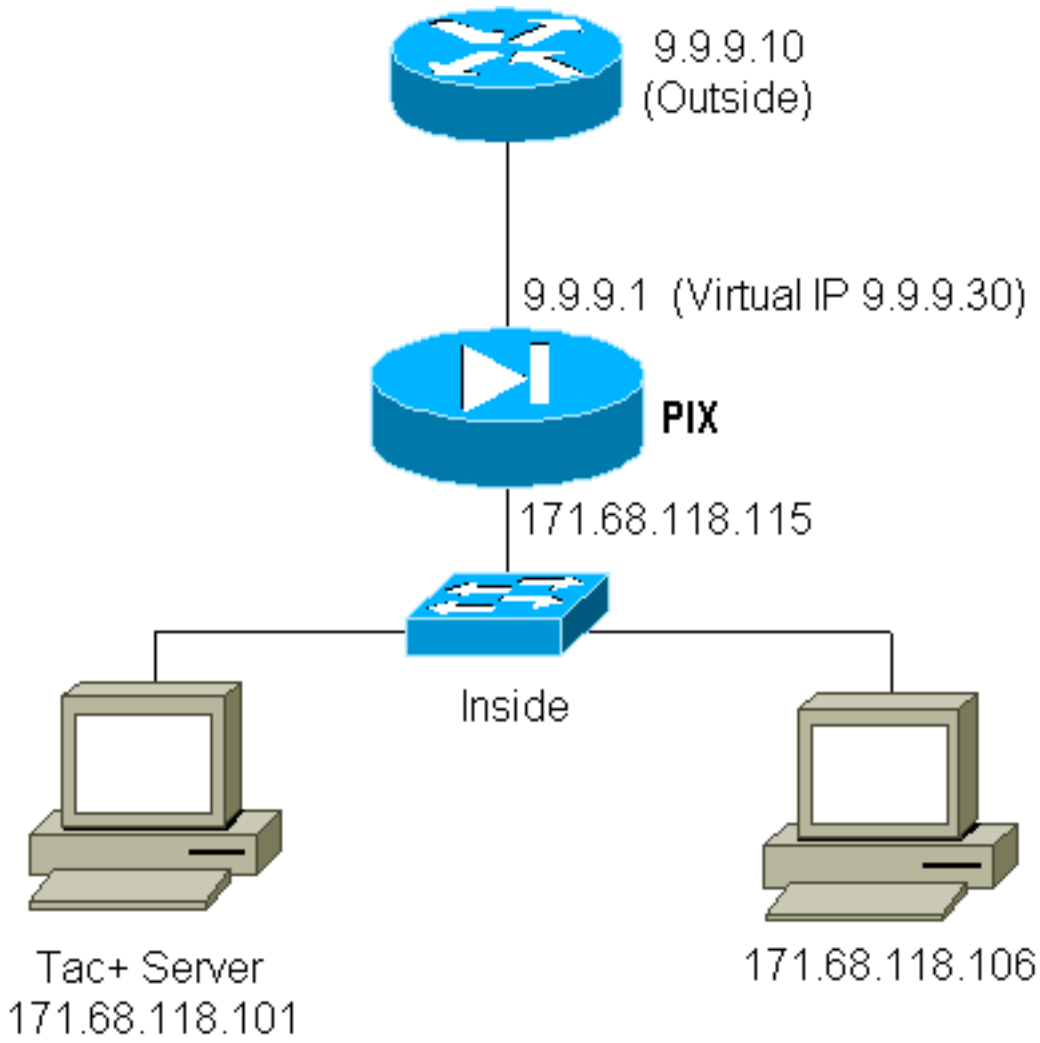
```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
 109009: Authorization denied from 171.68.118.106/49 to
    9.9.9.10/11094 (not authenticated
```

Так как почта и некоторые другие сервисы не являются достаточно интерактивными для аутентификации, одно решение состоит в том, чтобы использовать **кроме** команды для аутентификации/авторизации (аутентифицируйте все за исключением источника/назначения почтового сервера / клиент).

Если существует реальная потребность аутентифицировать некоторый необычный сервис, это может быть сделано при помощи команды **виртуального протокола Telnet**. Эта команда позволяет аутентификации происходить с IP для виртуального протокола Telnet. После этой аутентификации трафик для необычного сервиса может перейти к реальному серверу.

В данном примере мы хотим, чтобы порт TCP 49 трафиков вытекал из внешнего хоста 9.9.9.10 к внутреннему хосту 171.68.118.106. Так как этот трафик не действительно authenticatable, мы устанавливаем виртуальный протокол Telnet. Для входящего виртуального протокола Telnet должны быть связанные помехи. Здесь, и 9.9.9.20 и 171.68.118.20 виртуальные адреса.

Схема входящего виртуального протокола Telnet



Входящий виртуальный протокол Telnet конфигурации PIX

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
```

```
 conduit permit tcp host 9.9.9.20 eq telnet any
 conduit permit tcp host 9.9.9.30 eq tacacs any
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
 AAA authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 virtual telnet 9.9.9.20
```

TACACS + входящий виртуальный telnet пользовательской конфигурации сервера

```
user = pinecone {
default service = permit
        login = cleartext "pinecone"
service = exec {
        timeout = 10
        idletime = 10
        }
}
```

Входящий виртуальный протокол Telnet отладки PIX

Пользователь в 9.9.9.10 должен сначала аутентифицироваться Telnet - сеансом на этих 9.9.9.20 адресах на PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
    to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 13
 109005: Authentication succeeded for user 'pinecone'
    from 171.68.118.20/23 to 9.9.9.10/1470
```

После успешной аутентификации **команда show uauth** показывает, что у пользователя есть "время на метре":

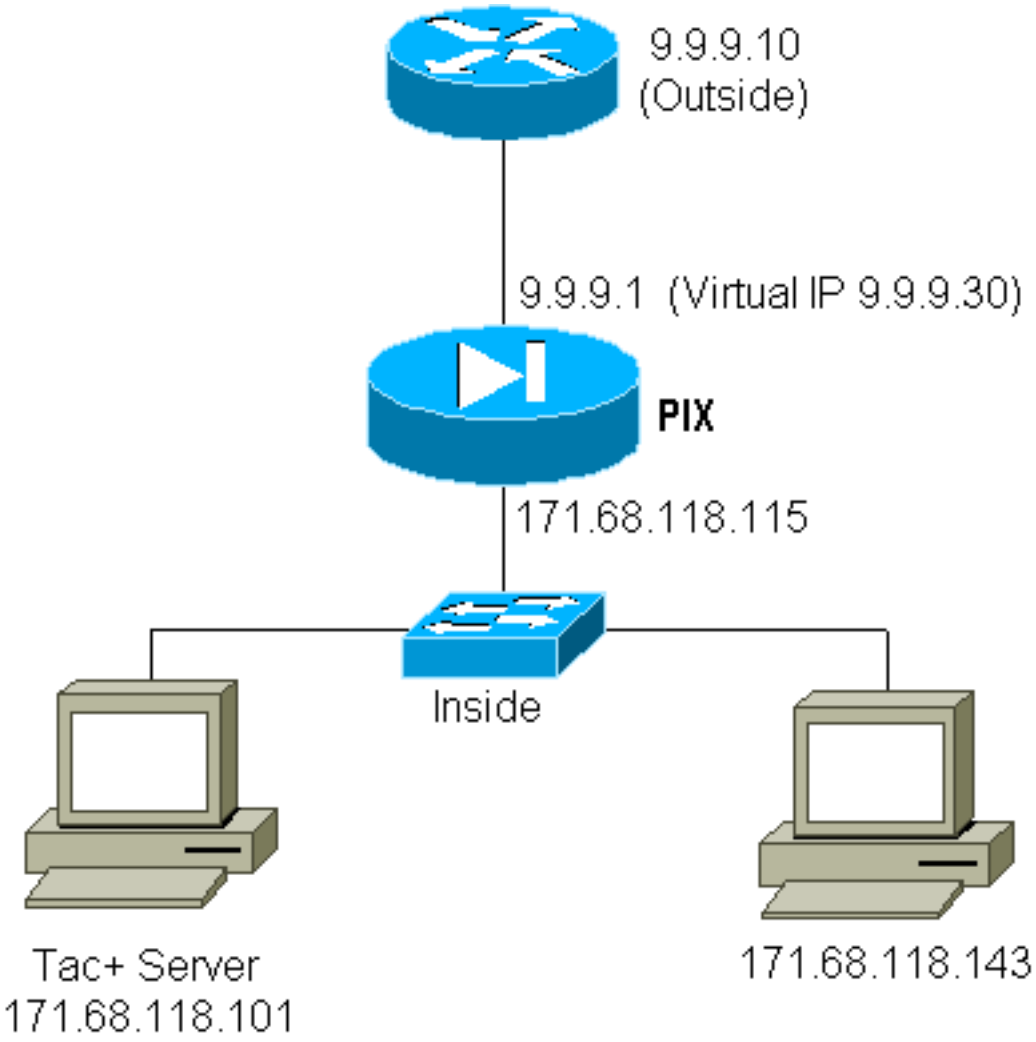
```
pixfirewall# show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user
'pinecone' at 9.9.9.10, authenticated absolute timeout: 0:10:00 inactivity timeout: 0:10:00
```

Здесь, устройство в 9.9.9.10 хочет передать трафик TCP/49 к устройству в 171.68.118.106:

```
pixfirewall# 109001: Auth start for user 'pinecone' from 9.9.9.10/11104
     to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 14
 109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
     to 9.9.9.10/1470
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

Исходящие данные протокола Virtual Telnet

Так как исходящий трафик позволен по умолчанию, никакие помехи не требуются для использования исходящих данных протокола Virtual Telnet. В данном примере, внутреннем пользователе в 171.68.118.143 Telnet к действительным 9.9.9.30 и аутентифицируется. Telnet - подключение сразу отброшен. После того, как аутентифицируемый, Трафик TCP позволен с 171.68.118.143 на сервер в 9.9.9.10:



Исходящие данные протокола Virtual Telnet конфигурации PIX

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 00:05:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual telnet 9.9.9.30
```

Исходящие данные протокола Virtual Telnet отладки PIX

```
109001: Auth start for user '???' from 171.68.118.143/1536
     to 9.9.9.30/23
 109011: Authen Session Start: user 'timeout_143', Sid 25
 109005: Authentication succeeded for user 'timeout_143' from
    171.68.118.143/1536 to 9. 9.9.30/23
 302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68 .118.143/1537 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1538 laddr 171.68 .118.143/1538 (timeout_143)
 302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68. 118.143/1537 duration 0:00:03
    bytes 625 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr
```

```
    9.9.9.30/1538 laddr 171.68. 118.143/1538 duration 0:00:01
    bytes 2281 (timeout_143)
 302009: 0 in use, 1 most used
```

Выход из виртуального сеанса Telnet

Когда пользовательские Telnet к IP для виртуального протокола Telnet, **команда show uauth** показывает uauth.

Если пользователь хочет препятствовать тому, чтобы трафик прошел после того, как сеанс закончен (когда там время оставленный в uauth), пользователю нужно к Telnet к IP для виртуального протокола Telnet снова. В результате этих действий сеанс заканчивается.

Авторизация порта

Можно потребовать авторизации на диапазоне портов. В данном примере аутентификация все еще требовалась для всех исходящих, но только авторизация требовалась для портов TCP 23-49.

Конфигурация PIX

AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound

Когда Telnet была сделана от 171.68.118.143 до 9.9.9.10, проверка подлинности и авторизация произошла, потому что порт 23 Telnet находится в диапазоне 23-49.

Когда сеанс HTTP сделан от 171.68.118.143 до 9.9.9.10, все еще необходимо аутентифицироваться, но PIX не просит, чтобы TACACS + сервер авторизовал HTTP, потому что 80 не находится в диапазоне 23-49.

Конфигурация свободно распространяемого сервера TACACS+

```
user = telnetrange {
        login = cleartext "telnetrange"
        cmd = tcp/23-49 {
        permit 9.9.9.10
        }
        }
```

Обратите внимание на то, что PIX передает "`cmd=tcp/23-49`" и "`cmd-arg=9.9.9.10`" к TACACS + сервер.

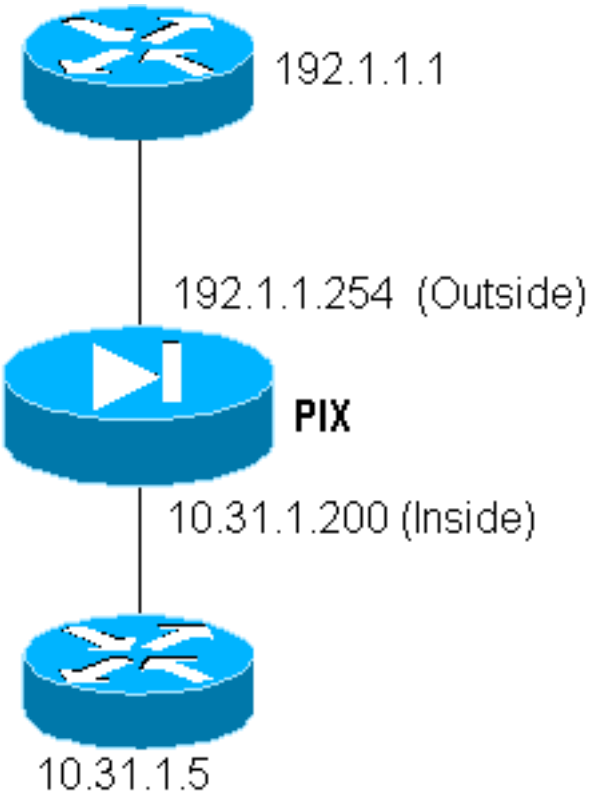
Отладка на PIX

```
109001: Auth start for user '???' from 171.68.118.143/1051
    to 9.9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109005: Authentication succeeded for user 'telnetrange'
    from 171.68.118.143/1051 to 9. 9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109007: Authorization permitted for user 'telnetrange'
    from 171.68.118.143/1051 to 9.9 .9.10/23
 302001: Built TCP connection 0 for faddr 9.9.9.10/23
    gaddr 9.9.9.5/1051 laddr 171.68.1 18.143/1051 (telnetrange)
```

```
109001: Auth start for user '???' from 171.68.118.143/1105
   to 9.9.9.10/80
109001: Auth start for user '???' from 171.68.118.143/1110
   to 9.9.9.10/80
109011: Authen Session Start: user 'telnetrange', Sid 1
109005: Authentication succeeded for user 'telnetrange'
   from 171.68.118.143/1110 to 9. 9.9.10/80
302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.1 18.143/1110 (telnetrange)
302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.1 18.143/1111 (telnetrange)
302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

Учет использования ресурсов AAA для трафика, отличного от HTTP, FTP и Telnet

Версия ПО PIX 5.0 изменяет трафик бухгалтерская функциональность. Учетные записи могут теперь быть вырезаны для трафика кроме HTTP, FTP и Telnet, как только завершена аутентификация.



К копии TFTP файл от внешнего маршрутизатора (192.1.1.1) к внутреннему маршрутизатору (10.31.1.5), добавьте виртуальный протокол Telnet для открытия дыры для процесса TFTP:

```
virtual telnet 192.1.1.30 static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0
0 conduit permit udp any any AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound AAA
accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Затем, Telnet от внешнего маршрутизатора в 192.1.1.1 к виртуальным IP 192.1.1.30 и

аутентифицируется на виртуальном адресе, который позволяет UDP пересекать PIX. В данном примере процесс **флэш-памяти tftp copy tftp** был запущен снаружи к внутренней части:

```
302006: Teardown UDP connection for faddr 192.1.1.1/7680
    gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

Для каждой **флэш-памяти copy tftp** на PIX (были три во время этой копии IOS), учетная запись вырезана и передана серверу проверки подлинности. Придерживающееся является примером записи TACACS на Windows Cisco Secure):

```
Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time,
    service,bytes_in,bytes_out,paks_in,paks_out,
    task_id,addr,NAS-Portname,NAS-IP-Address,cmd
 04/28/2000,03:08:26,pixuser,Default Group,192.1.1.1,start,,,,,,,
    0x3c,,PIX,10.31.1.200,udp/69
```

Дополнительные сведения

- Справочник по командам PIX
- Страница поддержки продуктов PIX
- Запросы комментариев (RFC)
- Техническая поддержка - Cisco Systems