Настройка PIX 5.1.x: TACACS+ и RADIUS

Содержание

Введение

RADIUS и TACACS + аутентификация могут быть сделаны для FTP, Telnet и соединений HTTP. Можно выполнить аутентификацию других менее распространенных протоколов. TACACS + авторизация поддерживается; Авторизация RADIUS не поддерживается. Изменения в аутентификации, авторизации и учете (AAA) PIX 5.1 по предыдущей версии включают расширенную проверку подлинности (XAUTH) - аутентификация Туннелей IPSec от Cisco Secure VPN Client 1.1.

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.

Общие сведения

Аутентификация и авторизация

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

Предположим, 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. Вы сказали бы PIX аутентифицировать исходящий трафик и давать все шесть идентификаторов пользователей на TACACS +/RADIUS сервер безопасности. С простой проверкой подлинности эти шесть пользователей могли аутентифицироваться с именем пользователя и паролем, затем выйти. Другие девяносто четыре пользователя не могли выйти. PIX побуждает пользователей для имени пользователя/пароля, затем передает их имя пользователя и пароль к TACACS +/RADIUS сервер безопасности, и в зависимости от

ответа, открывает или запрещает соединение. Эти шесть пользователей могли сделать FTP, Telnet или HTTP.

Но предположите, что нельзя доверять *одному* из этих шести пользователей, "Феста". Требуется позволить Фестусу делать FTP, но не HTTP или Telnet к внешней стороне. Это означает иметь необходимость добавить *авторизацию*, т.е. авторизуя *то, что* пользователи могут сделать в дополнение к аутентификации, кто они. Это только допустимо с TACACS +. Когда мы добавляем *авторизацию* к PIX, PIX сначала передает имя пользователя и пароль Фестуса к серверу безопасности, затем передает запрос авторизации, говоря сервер безопасности, что *"команда"* Фестус пытается сделать. С настройкой сервера должным образом, Фестуса можно было разрешить "ftp 1.2.3.4", но запретят способность к HTTP или Telnet где угодно.

Что видит пользователь при включенной аутентификации/авторизации

В случае попытки доступа пользователя изнутри системы безопасности наружу (или наоборот) при включенной аутентификации/авторизации происходит следующее:

- **Telnet - На экране появляется запрос имени пользователя подошла, затем запрос пароля.** 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 отображен в браузере, запрашивающем 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. Системный журнал PIX и/или серверная отладка показывают это явление. Это является причиной в ситуациях, когда Telnet и FTP функционируют нормально, а соединения HTTP – нет.
- **Tunnel** - При попытке туннелировать Трафик IPSec в сеть с Клиентом VPN и xauth на, серая коробка для "Проверки подлинности пользователя для Нового соединения" отображена для имени пользователя/пароля.**Примечание:** Эта аутентификация поддерживается, начинаясь с Cisco Secure VPN Client 1.1. Если меню **Help> About** не делает show version 2.1.x или позже, это не работает.

Настройки сервера безопасности для всех сценариев

Конфигурация сервера CiscoSecure UNIX TACACS

В этом разделе вам предоставляют информацию по настройке ваш сервер безопасности.

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 GUI для добавления IP-адреса PIX и ключа к списку Сервера доступа к сети (NAS).

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

Cisco Secure ACS для Windows 2.x RADIUS

Используйте эти шаги для настройки Cisco Secure ACS для Windows 2.x RADIUS.

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-адрес PIX в GUI раздела 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 щелкните **по 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 Telnet - сеанс к определенным узлам позволен, заполните IP-адрес (IP-адреса) в разделе аргумента в форме, "разрешают #.#.#.#". В противном случае, для разрешения Telnet - сеанса 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 щелкните **по exec Shell** для предоставления привилегий exec.
2. Для добавления авторизации к PIX, у основания настройки групп, нажимают **Deny несопоставленные команды IOS**.
3. Выберите **Add/Edit новая команда** для каждой команды, которую вы хотите позволить (например, **Telnet**).
4. Для разрешения Telnet - сеанса определенным узлам войдите, IP-адрес в разделе аргумента в форме "разрешают #.#.#.#". Для разрешения Telnet - сеанса любому узлу 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. Гарантируйте, что IP-адрес PIX добавлен в Разделе графического интерфейса пользователя Конфигурации NAS.

Конфигурация сервера Livingston RADIUS

Добавьте IP-адрес PIX и ключ к файлу Клиентов.

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

Конфигурация сервера Merit RADIUS

Добавьте IP-адрес PIX и ключ к файлу Клиентов.

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

Конфигурация свободно распространяемого сервера TACACS+

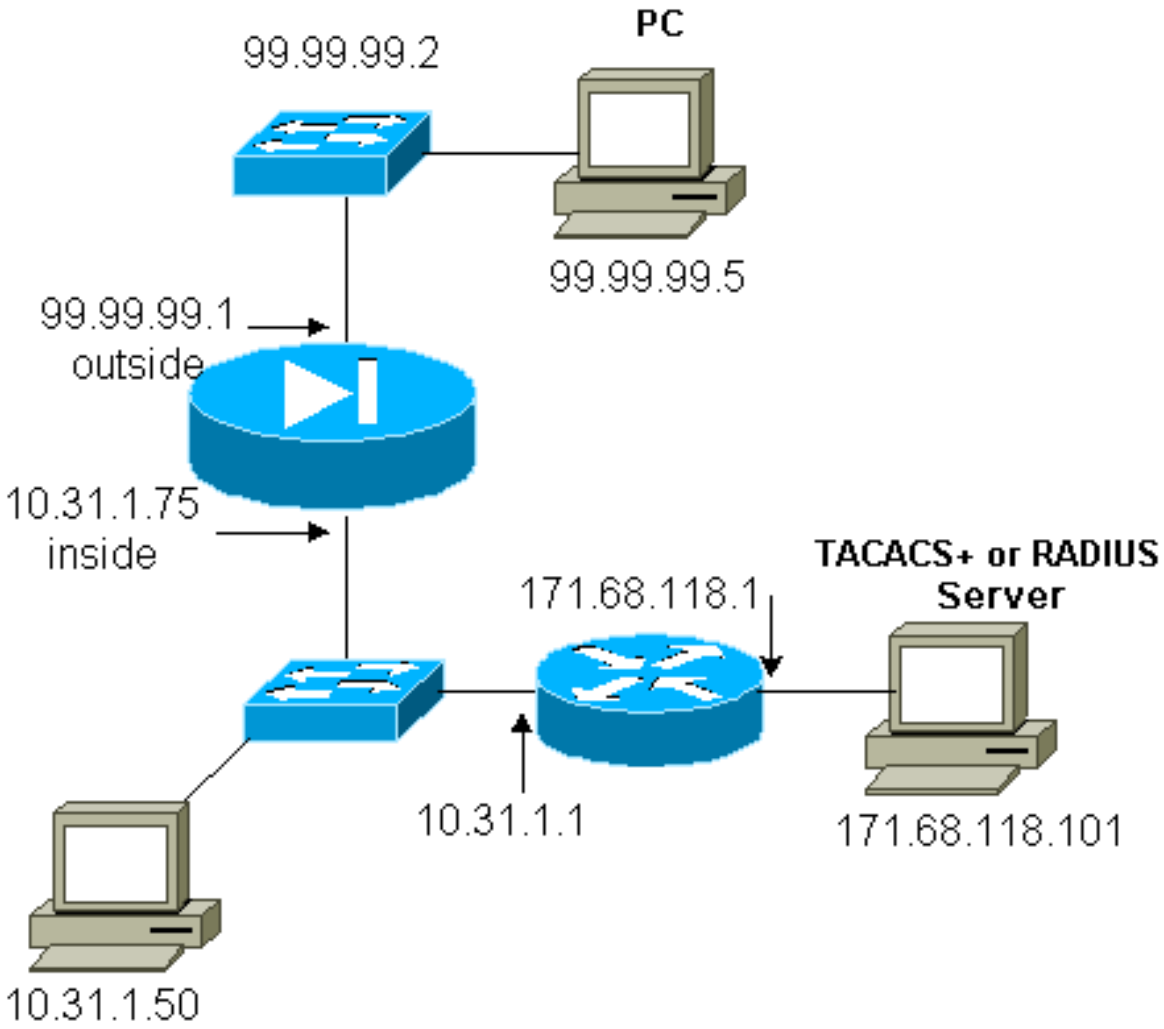
```
key = "cisco"
user = adminuser {
login = cleartext "all"
default service = permit
}

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

Примечание: Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- Удостоверьтесь, что конфигурация PIX работает перед добавляющим AAA. Если вы не можете передать трафик до учреждения проверки подлинности и авторизация, вы не будете в состоянии сделать так впоследствии.
- Enable logging в PIX.Отладка консоли регистрации не должна использоваться на в большой степени загружаемая система.**Можно использовать команду отладки logging buffered, а затем выполнить команду show logging.**Регистрация может быть отправлена на сервер системных журналов для дальнейшего изучения.
- Включите отладку на TACACS +, или серверы RADIUS (все серверы имеют эту опцию).

Схема сети



Конфигурация PIX
PIX Version 5.1(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 pix/intf2 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pix3 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 pager lines 24 no logging timestamp no logging standby **logging console debugging** no logging monitor no logging buffered no logging trap no logging history logging facility 20 logging queue 512 interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto shutdown mtu outside 1500 mtu inside 1500 mtu pix/intf2 1500 **ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0** ip address pix/intf2 127.0.0.1 255.255.255.255 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 pix/intf2 0.0.0.0 arp timeout 14400 **global (outside) 1**

```
99.99.99.7-99.99.99.10 netmask 255.255.255.0 nat
(inside) 1 10.31.1.0 255.255.255.0 0 0 static
(inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0 conduit permit icmp any any conduit
permit tcp any any conduit permit udp any any route
outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route inside
171.68.118.0 255.255.255.0 10.31.1.1 1 route inside
171.68.120.0 255.255.255.0 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 0:05:00
absolute aaa-server TACACS+ protocol tacacs+ aaa-server
RADIUS protocol radius aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host
171.68.118.101 cisco timeout 5 aaa-server AuthOutbound
protocol radius aaa-server AuthOutbound (inside) host
171.68.118.101 cisco timeout 5 aaa authentication
include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound aaa authentication include telnet inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
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
floodguard enable telnet timeout 5 terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca : end
[OK]
```

Примеры отладки аутентификации от PIX

Этот раздел показывает выборки опознавательных отладок для различных сценариев.

Входящий

Внешний пользователь в 99.99.99.2 инициирует трафик к внутреннему 10.31.1.50 (99.99.99.99) и аутентифицируется через TACACS (т.е. входящий трафик использует список серверов "AuthInbound", который включает Сервер tacacs 171.68.118.101).

Отладка PIX - успешная проверка подлинности - TACACS +

Пример ниже показов отладка PIX с успешной проверкой подлинности:

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

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

Пример ниже показов отладка PIX с неправильной проверкой подлинности (имя

пользователя или пароль). Пользователь видит три установки имени/пароля пользователя, придерживавшиеся этим сообщением: `Error: max number of tries exceeded`.

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

Отладка PIX - может пропинговать сервер, никакой ответ - TACACS +

Пример ниже показов отладка PIX, где сервер является отвечающим на команду ping, но не говорящий 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`.

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

Отладка PIX - неспособный пропинговать сервер - TACACS +

Пример ниже показов отладка PIX, где сервер не является отвечающим на команду ping. Пользователь видит имя пользователя однажды, но PIX никогда не просит пароль (это находится на Telnet). Следующие сообщения отображены: `Timeout to TACACS+ server` и `Error: Max number of tries exceeded` (фиктивный сервер был подкачан в конфигурации).

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

Отладка PIX - успешная проверка подлинности - RADIUS

Пример ниже показов отладка PIX с успешной проверкой подлинности:

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

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

RADIUS

Пример ниже показов отладка PIX с неправильной проверкой подлинности (имя пользователя или пароль). Пользователь видит запрос об имени пользователя и пароле и имеет три возможности ввести их. Когда запись неуспешна, следующее сообщение отображено: `Error: max number of tries exceeded.`

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

Отладка PIX - может пропинговать сервер, Выключенный демон - RADIUS

Пример ниже показов отладка PIX, где сервер является отвечающим на команду ping, но демон не работает и не свяжется с PIX. Пользователь видит имя пользователя, затем пароль, сообщение `RADIUS server failed` и `Error: Max number of tries exceeded.`.

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

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

Пример ниже показов отладка PIX, где сервер не является отвечающим на команду ping или существует Клиент/основная несогласованность. Пользователь видит имя пользователя, пароль, сообщение `Timeout to RADIUS server`, и `Error: Max number of tries exceeded` обменивается сообщениями, фиктивный сервер был подкачан в конфигурации).

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

Добавление авторизации

Если вы решаете добавить авторизацию, так как авторизация не допустима без аутентификации, необходимо потребовать авторизации для того же исходного и конечного диапазона.

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 вы не добавляете авторизацию 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 +

Пример ниже показов отладка PIX с успешной проверкой подлинности и успешной авторизацией:

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

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

Пример ниже показов отладка PIX с успешной проверкой подлинности, но сбоем проверки подлинности. Здесь пользователь также видит сообщение `Error: Authorization Denied`.

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

Добавление автоматического учета

TACACS +

aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

TACACS + бесплатное программное обеспечение выводят:

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
```

```
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

aaa accounting include any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound

Выходные данные Merit RADIUS:

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

Использование команды исключения "Exclude"

Если мы добавляем другой хост снаружи (в 99.99.99.100) к нашей сети, и этому хосту доверяют, можно исключить их из проверки подлинности и авторизация со следующими командами:

aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255 AuthInbound aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255 AuthInbound

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. Если запись начала учета создана, а запись остановки отсутствует, сервер TACACS+ или RADIUS полагает, что данное лицо по-прежнему в системе (т. е. пользователь установил 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 следующем примере используется другая конфигурация сети, но понятия являются тем же.

Пользователь устанавливает сеанс Telnet через PIX и проходит аутентификацию:

```
   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 начальную запись, 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 идет об их Telnet или FTP - бизнесе на конечном узле, затем выходит (проводит десять 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
```

Если значение uath равно 0 (аутентификация выполняется каждый раз) или больше (аутентификация выполняется только один раз за сеанс uaoth), учетная запись отсекается для каждого посещенного узла.

HTTP работает по-другому вследствие типа протокола. Ниже 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.

Стартовая запись зарегистрирована в 16:35:34, а запись остановки в 16:35:35. Эта загрузка продолжалась 1 секунду (т. е. между записью начала и записью остановки прошло менее секунды). Когда пользователь читает веб-страницу, он по-прежнему остается на веб-узле, а подключение сохраняется открытым? 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. Нет начальной записи 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). Функции контроля максимального числа сеансов и просмотра зарегистрированных пользователей не будут действовать в силу особенностей соединений HTTP.

Аутентификация и включение в самом PIX

Проблемы предыдущего обсуждения, аутентифицирующие Telnet (и HTTP, FTP) трафик через PIX. Гарантируйте, что Telnet к PIX работает без аутентификации на:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

Затем добавьте команду для аутентификации пользовательского Telnet - сеанса на PIX:

```
aaa authentication telnet console AuthInbound
```

Когда подключение пользователей посредством Telnet к PIX, им предлагают для Пароля Telnet **(WW)**. PIX также запрашивает TACACS + или Имя пользователя RADIUS и пароль. В этом случае, так как список серверов AuthInbound используется, PIX запрашивает TACACS + имя пользователя и пароль.

Если сервер не работает, можно обратиться к PIX путем ввода **pix** для имени пользователя, и затем enable password (**enable password** *вообще*). С помощью команды:

```
aaa authentication enable console AuthInbound
```

Пользователю предлагают для имени пользователя и пароля, которое передается TACACS или серверу RADIUS. В этом случае, так как список серверов AuthInbound используется, PIX запрашивает TACACS + имя пользователя и пароль.

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).

Если сервер не работает, можно обратиться к режиму включения PIX путем ввода **pix** для имени пользователя и обычного enable password от PIX (**enable password** *вообще*). *Если разрешающего пароля нет в конфигурации PIX, введите имя пользователя "pix" и нажмите клавишу Enter*. Если enable password установлен, но не известен, диск для восстановления пароля должен быть создан для изменения пароля.

Изменение приглашения для пользователя

Если у вас есть команда:

```
auth-prompt PIX_PIX_PIX
```

пользователи, проходящие PIX, видят следующую последовательность:

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

По прибытии в конечный пункт назначения пользователи видели бы Имя пользователя: и Пароль: приглашение, отображенное полем назначения. Это приглашение только влияет на пользователей*, проходящих* PIX, не к PIX.

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

Настройка сообщения, отображаемого для пользователей при успешном или неуспешном выполнении

Если youh имеют команды:

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

тогда пользователи видят следующую 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

Эта функция в настоящее время не работает, и проблемой был назначенный идентификатор ошибки Cisco CSCdp93492 (только зарегистрированные клиенты).

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.

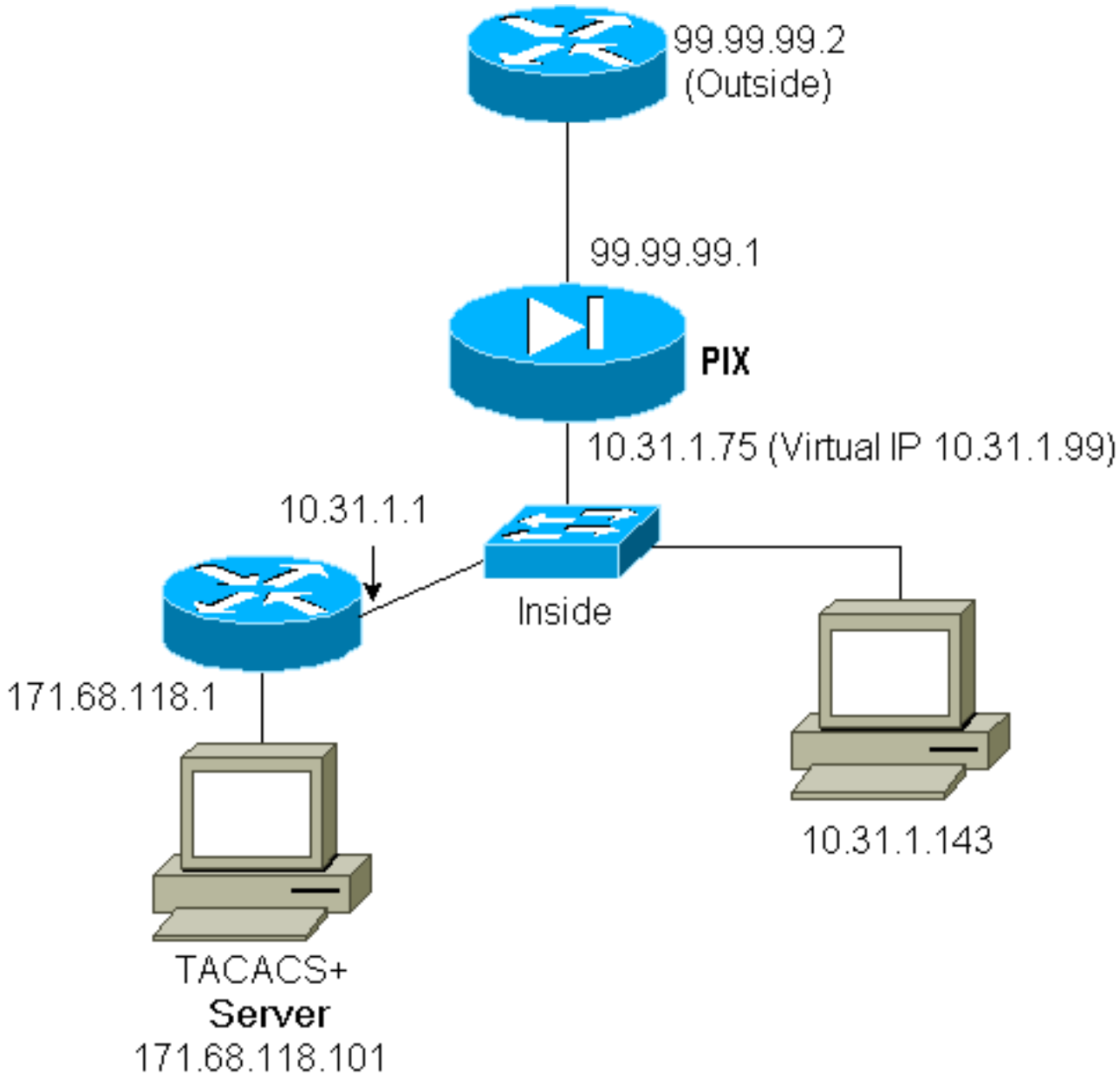
Для предотвращения этого можно внедрить действительный HTTP путем добавления адреса RFC 1918 (т.е. адрес, который немаршрутизуем в Интернете, но допустим и уникален для внутренней сети PIX) к конфигурации PIX с помощью следующей команды:

```
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.

Пример исходящего трафика виртуального HTTP



Выходная данные виртуального HTTP конфигурация PIX:

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 01:00:00 aaa
authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa-server
RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound (inside)
host 171.68.118.101 cisco timeout 5 virtual http 10.31.1.99
```

Виртуальный протокол Telnet

Возможно настроить PIX для аутентификации всех входящих и исходящих, но это не хорошая идея, потому что легко не аутентифицируются некоторые протоколы, такие как почта. Когда почтовый сервер и Клиент пытаются связаться через PIX, когда весь трафик

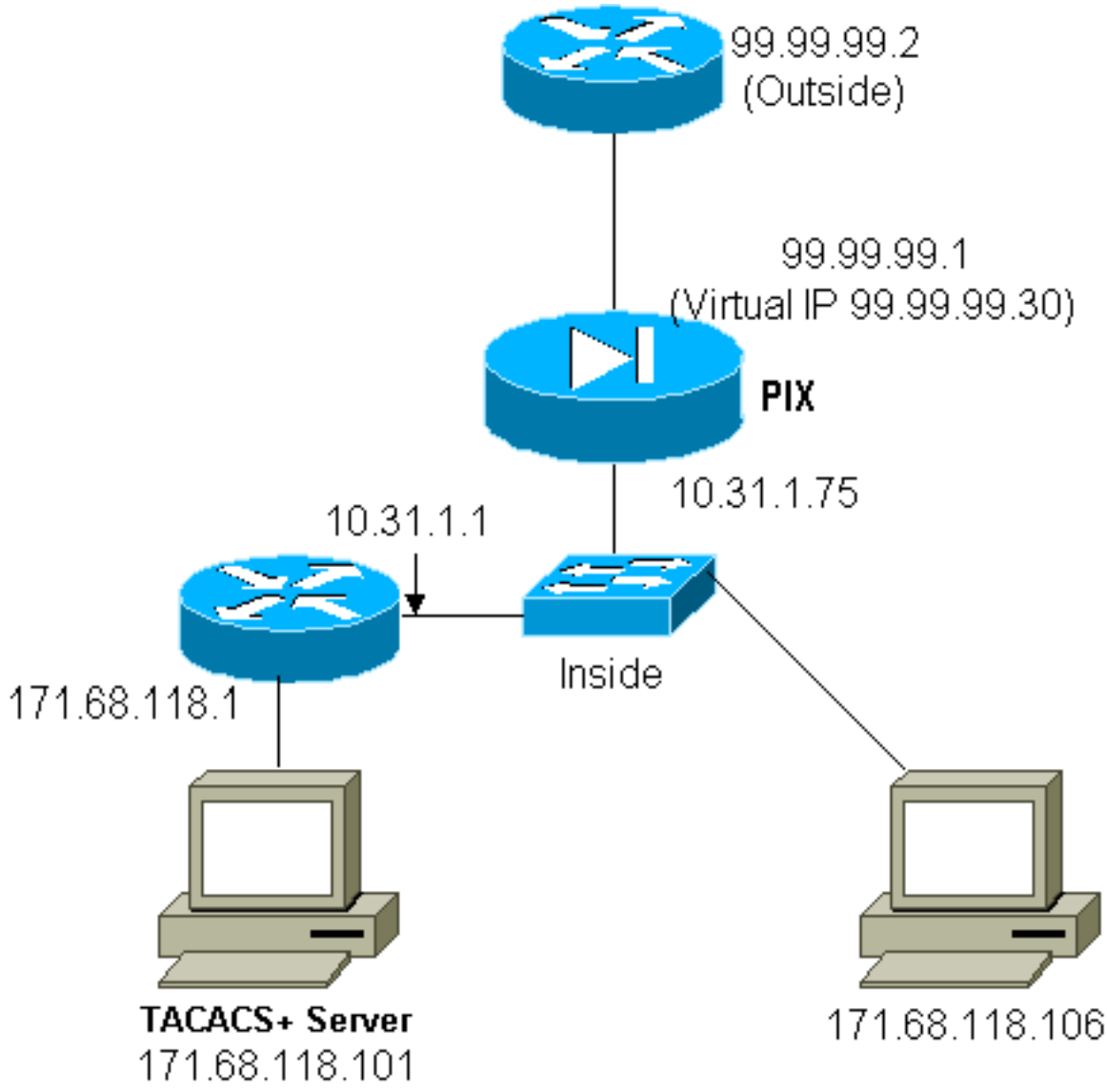
через PIX аутентифицируется, системный журнал PIX для протоколов без возможности проверки подлинности показывает сообщения, такие как:

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

Однако, если существует действительно потребность аутентифицировать некоторый необычный сервис, это может быть сделано при помощи команды **виртуального протокола Telnet**. Эта команда позволяет аутентификации происходить с IP - адресом по виртуальному протоколу Telnet. После этой аутентификации трафик для необычного сервиса может перейти к реальному серверу.

В данном примере вы хотите, чтобы порт TCP 49 трафиков вытекал из внешнего хоста 99.99.99.2 к внутреннему хосту 171.68.118.106. Так как этот трафик не действительно authenticatable, установите виртуальный протокол Telnet. Для виртуального протокола Telnet должны быть связанные помехи. Здесь, и 99.99.99.20 и 171.68.118.20 виртуальные адреса.

Входящие данные протокола Virtual Telnet



Входящий виртуальный протокол Telnet конфигурации PIX

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 static
(inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0 static (inside,outside)
99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0 conduit permit tcp host 99.99.99.20 eq
telnet any conduit permit tcp host 99.99.99.30 eq tacacs any aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+ aaa-server Incoming (inside) host 171.68.118.101 cisco
timeout 5 aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming virtual telnet
99.99.99.20
```

Входящий виртуальный протокол Telnet отладки PIX

Пользователь в 99.99.99.2 должен сначала аутентифицироваться Telnet - сеансом на этих 99.99.99.20 адресах на PIX:

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

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

```
pixfirewall# show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'cse' at 99.99.99.2, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

И когда устройство в 99.99.99.2 хочет передать трафик TCP/49 к устройству в 171.68.118.106:

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

Авторизация может быть добавлена:

```
aaa authorization include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

так, чтобы, когда трафик TCP/49 предпринят через PIX, PIX также передал запрос авторизации к серверу:

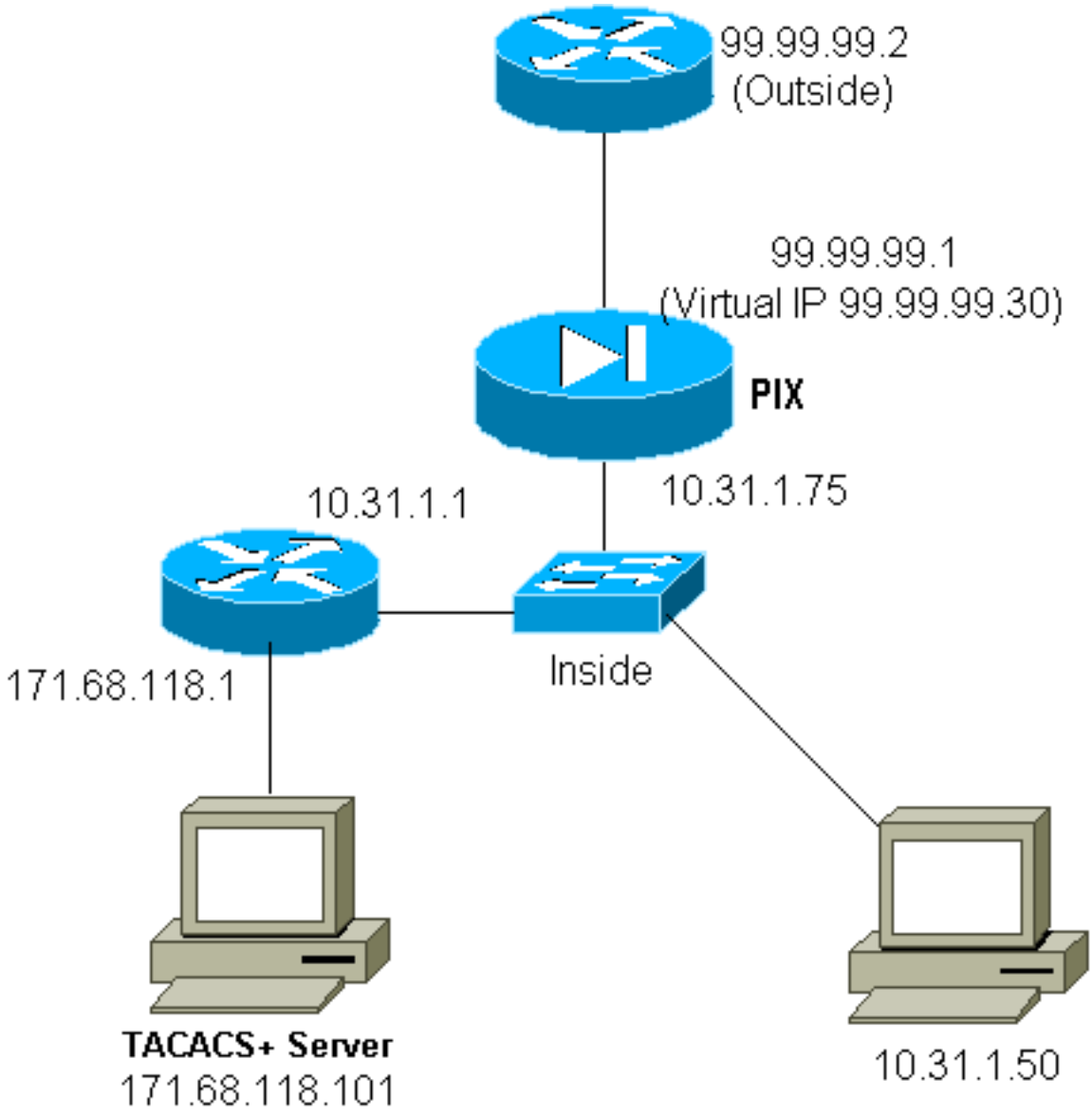
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

На TACACS + сервер, это замечено как:

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

Исходящие данные протокола Virtual Telnet

Так как исходящий трафик позволен по умолчанию, никакие помехи не требуются для использования исходящих данных протокола Virtual Telnet. В следующем примере, внутреннем пользователе в 10.31.1.50 Telnet к действительным 99.99.99.30 и аутентифицируется; Telnet - подключение сразу отброшен. После того, как аутентифицируемый, Трафик TCP позволен с 10.31.1.50 на сервер в 99.99.99.2:



Исходящие данные протокола Virtual Telnet конфигурации PIX:

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 0:05:00 absolute aaa-
server RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound
(inside) host 171.68.118.101 cisco timeout 5 aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound virtual telnet 99.99.99.30
```

Примечание: Нет никакой авторизации, так как это - RADIUS.

Исходящие данные протокола Virtual Telnet отладки PIX:

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
 109011: Authen Session Start: user 'pixuser', Sid 16
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11034 to 99.99.99.30/23 on interface
    inside
 302001: Built outbound TCP connection 18 for faddr
    99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
    10.31.1.50/11036 (pixuser)
 302002: Teardown TCP connection 18 faddr 99.99.99.2/49
```

```
    gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
    duration 0:00:02 bytes 0 (pixuser)
```

Выход из виртуального сеанса Telnet

Когда подключение пользователей посредством Telnet к IP - адресу по виртуальному протоколу Telnet, **команда show uauth** показывает их uauth. Если пользователи хотят препятствовать тому, чтобы трафик прошел после того, как их сеансы закончены, когда там время оставленный в uauth, им нужно к Telnet к IP - адресу по виртуальному протоколу Telnet снова. В результате этих действий сеанс заканчивается.

После первой аутентификации:

```
 pix3# show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'pixuser' at 10.31.1.50, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
pix3# 109001: Auth start for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 109005:
Authentication succeeded for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 on interface
inside
```

После второй аутентификации (т.е. дыра переключена закрытая):

```
 pix3# show uauth Current Most Seen Authenticated Users 0 2 Authen In Progress 0 1
```

Авторизация порта

Авторизация позволена для диапазонов портов (как TCP/30-100). Если виртуальный протокол Telnet настроен на PIX и авторизации для диапазона портов, когда-то дыра открыта с виртуальным протоколом Telnet, PIX выходит **tcp/30-100** команда к TACACS + сервер для авторизации:

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0 conduit permit tcp
host 99.99.99.75 host 99.99.99.2 static (inside,outside) 99.99.99.75 10.31.1.50 netmask
255.255.255.255 0 0 virtual telnet 99.99.99.75 aaa authentication include any inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound virtual telnet 99.99.99.30
```

Конфигурация свободно распространяемого сервера TACACS+:

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

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

После виртуального протокола Telnet проверки, работавшего для разрешения трафика TCP/49 хосту в сети, мы решили, что хотели объяснить это, таким образом, мы добавили:

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Это приводит к вырезке учетной записи, когда трафик tcp/49 проходит (данный пример от TACACS + бесплатное программное обеспечение):

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

Расширенная аутентификация (Xauth)

Примеры конфигураций

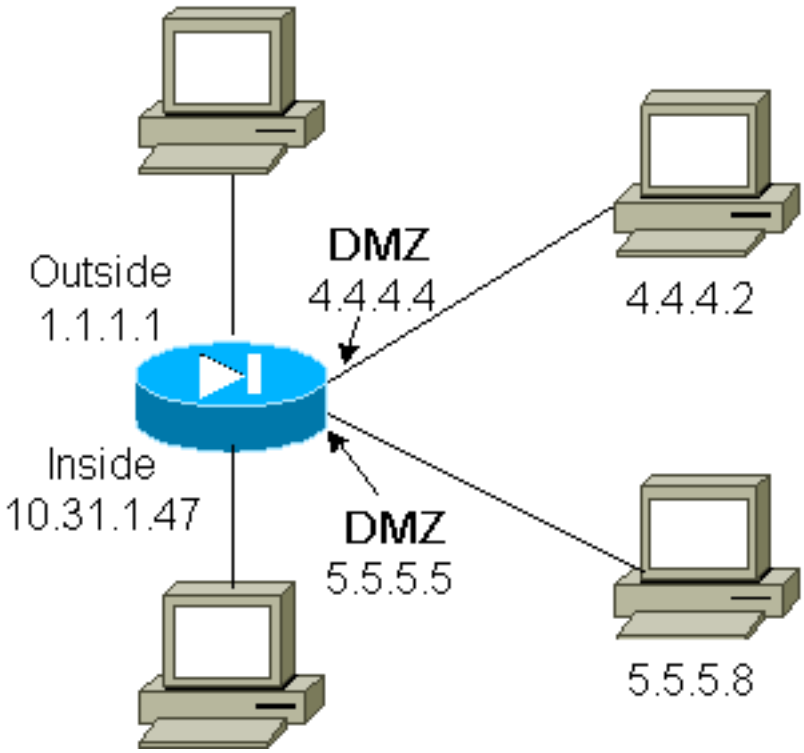
- Разъединение туннелей IPSec на нескольких интерфейсах межсетевого экрана Cisco Secure PIX с Xauth
- IPSec между межсетевым экраном Cisco Secure PIX и клиентом VPN с расширенной проверкой подлинности

Аутентификация в демилитаризованной зоне DMZ

Для аутентификации пользователей, идущих от одного интерфейса DMZ до другого, скажите PIX аутентифицировать трафик для именованных интерфейсов. На нашем PIX расположение:

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

 most secure
```

Схема сети



Конфигурация PIX

Мы хотим аутентифицировать трафик Telnet между pix/intf4 и pix/intf5:

```
nameif ethernet0 outside security0 nameif ethernet1 inside security100 (nameif ethernet2
pix/intf2 security10 nameif ethernet3 pix/intf3 security15) nameif ethernet4 pix/intf4
security20 nameif ethernet5 pix/intf5 security25 ip address outside 1.1.1.1 255.255.255.0 ip
address inside 10.31.1.47 255.255.255.0 (ip address pix/intf2 127.0.0.1 255.255.255.255 ip
address pix/intf3 127.0.0.1 255.255.255.255) ip address pix/intf4 4.4.4.4 255.255.255.0 ip
address pix/intf5 5.5.5.5 255.255.255.0 static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask
255.255.255.255 0 0 aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa-server TACACS+ protocol tacacs+ aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Учет Xauth

Если команда **sysopt connection permit-ipsec**, не **команда sysopt ipsec pl-compatible**, настроена в PIX с xauth, учет допустим для TCP - подключений, но не ICMP или UDP.

Дополнительные сведения

- Страница поддержки продуктов PIX
- Справочник по командам PIX
- Страница поддержки RADIUS
- Запросы комментариев (RFC)
- Страница поддержки Cisco Secure UNIX
- Страница поддержки Cisco Secure ACS для Windows
- Техническая поддержка - Cisco Systems