"Примеры настройки PIX, TACACS+ и RADIUS: 4.4. x

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 PIX 4.4.1 аутентификации, авторизации и учета (AAA) по предыдущей версии включают: Группы AAA-серверов и аварийное переключение, аутентификация для включает и доступ последовательной консоли, и принимает и отклоняет подсказки.

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.

Предположим, что у вас есть 100 пользователей внутри, и вы хотите, только хотят, чтобы 6 из этих пользователей были в состоянии сделать FTP, Telnet или HTTP вне сети. Вы сказали бы PIX аутентифицировать исходящий трафик и давать все 6 идентификаторов пользователей на TACACS +/RADIUS сервер безопасности. С простой проверкой подлинности эти 6 пользователей могли аутентифицироваться с именем пользователя и паролем, затем выйти. Другие 94 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 6 пользователей могли сделать FTP, Telnet или HTTP.

Но 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 иметь необходимость добавить авторизацию, т.е. авторизуя то, что пользователи могут сделать в дополнение к аутентификации, кто они. Когда мы добавляем авторизацию к PIX, PIX сначала передал бы имя пользователя и пароль Терри к серверу безопасности, затем передать запрос авторизации, говоря сервер безопасности, что "команда" Терри пытается сделать. С настройкой сервера должным образом, Терри можно было разрешить "FTP 1.2.3.4", но будете, запретил 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** - 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 – в браузере отображается окно для ввода имени пользователя и пароля. 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 усовершенствованный пользовательский графический 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
}
}
```

CiscoSecure NT 2.x RADIUS

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 щелкните **по exec Shell** (для предоставления привилегий exec).
2. К добавить авторизацию 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 и/или FTP).
7. Добавьте IP PIX в Разделе графического интерфейса пользователя Конфигурации NAS.

CiscoSecure 2.x TACACS+

Пользователь получает пароль в Разделе настройки пользователя GUI.

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 (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 шаги 1 - 5 для каждой из позволенных команд (например, Telnet, HTTP 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
```

Конфигурация свободно распространяемого сервера TACACS+

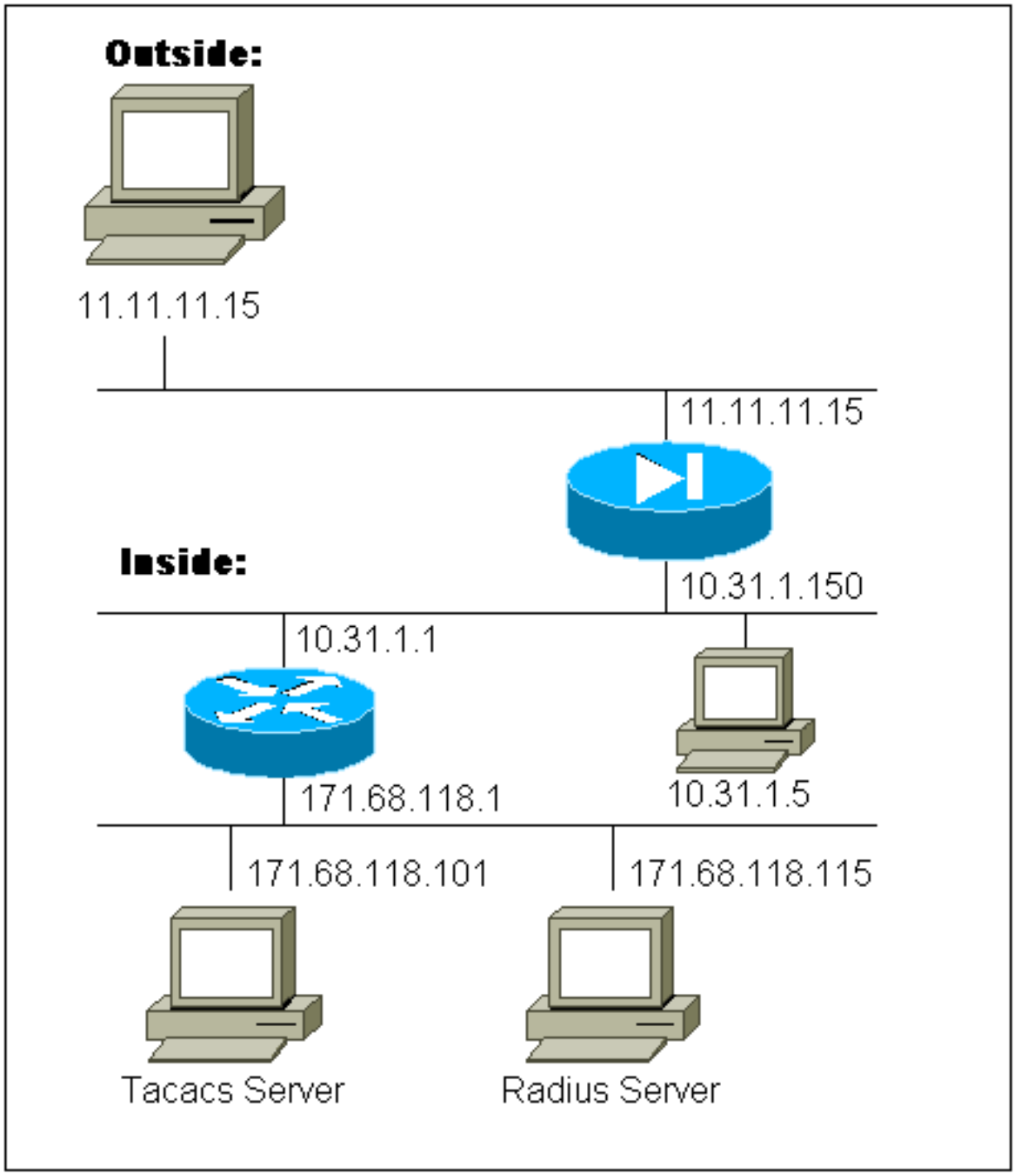
```
key = "cisco"

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

- Удостоверьтесь, что конфигурации PIX работают перед добавляющей аутентификацией, авторизацией и учетом (AAA).Если трафик нельзя передать до аутентификации и авторизации, этого нельзя будет сделать и впоследствие.
- 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 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** Building configuration... : Saved : PIX Version 4.4(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 pix/intf2 security10 nameif ethernet3 pix/intf3 security15 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pix-5 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 logging console debugging no logging monitor no logging buffered logging trap debugging logging facility 20 interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto interface ethernet3 auto mtu outside 1500 mtu inside 1500 mtu pix/intf2 1500 mtu pix/intf3 1500 ip address outside 11.11.11.1 255.255.255.0 ip address inside 10.31.1.150 255.255.255.0 ip address pix/intf2 127.0.0.1

```
255.255.255.255 ip address pix/intf3 127.0.0.1
255.255.255.255 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
failover ip address pix/intf3 0.0.0.0 arp timeout 14400
global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0 static (inside,outside) 11.11.11.20
171.68.118.115 netmask 255.255.255.255 0 0 static
(inside,outside) 11.11.11.21 171.68.118.101 netmask
255.255.255.255 0 0 static (inside,outside) 11.11.11.22
10.31.1.5 netmask 255.255.255.255 0 0 conduit permit
icmp any any conduit permit tcp any any no rip outside
passive no rip outside default no rip inside passive no
rip inside default no rip pix/intf2 passive no rip
pix/intf2 default no rip pix/intf3 passive no rip
pix/intf3 default route inside 0.0.0.0 0.0.0.0 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 ! !--- For any
given list, multiple AAA servers can !--- be configured.
They will be !--- tried sequentially if any one of them
is down. ! aaa-server Outgoing protocol tacacs+ aaa-
server Outgoing (inside) host 171.68.118.101 cisco
timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

Примеры отладки аутентификации от PIX

В этих примерах отладки:

Исходящий

Внутренний пользователь в 10.31.1.5 инициирует трафик к внешним 11.11.11.15 и аутентифицируется через TACACS + (исходящий трафик использует список серверов "Выход", который включает Сервер tacacs 171.68.118.101).

Входящий

Внешний пользователь в 11.11.11.15 инициирует трафик к внутреннему 10.31.1.5 (11.11.11.22) и аутентифицируется через RADIUS (входящий трафик использует список серверов "Поступление", которое включает сервер RADIUS 171.68.118.115).

Отладка PIX - успешная проверка подлинности - TACACS +

Пример ниже отладки PIX показов с успешной проверкой подлинности:

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
 109011: Authen Session Start: user 'ddunlap', sid 3
 109005: Authentication succeeded for user 'ddunlap'
 from 10.31.1.5/11004 to 11.11.11.15/23
 109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
 302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

Отладка PIX - Неправильная проверка подлинности (Имя пользователя или пароль) - TACACS +

Пример ниже отладки PIX показов с неправильной проверкой подлинности (имя пользователя или пароль). Пользователь видит четыре установки имени/пароля пользователя. Показы следующего сообщения: Ошибка: максимальное число попыток превысило".

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
 109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

Отладка PIX - Может Пропинговать, но никакой Ответ - TACACS +

Пример ниже отладки PIX показов для сервера доступный по эхо-тесту, который не говорит с PIX. Пользователь видит имя пользователя однажды, и PIX никогда не просит пароль (это находится на Telnet).

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

Отладка PIX - не может пропинговать сервер - TACACS +

Пример ниже отладки PIX показов для сервера, который не является отвечающим на команду ping. Пользователь видит имя пользователя однажды. PIX никогда не просит пароль (это находится на Telnet). Показы следующего сообщения: "Таймаут к TACACS + сервер" и "Ошибка: Максимальное число попыток превысило" (конфигурация в данном примере отражает фиктивный сервер).

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

Отладка PIX - успешная проверка подлинности - RADIUS

Пример ниже отладки PIX показа с успешной проверкой подлинности:

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
```

```
 109011: Authen Session Start: user 'adminuser', sid 4
 109005: Authentication succeeded for user 'adminuser'
 from 10.31.1.5/23 to 11.11.11.15/11003
 109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
 302001: Built inbound TCP connection 5 for faddr
 11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

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

Пример ниже отладки PIX показов с неправильной проверкой подлинности (имя пользователя или пароль). Пользователь видит запрос об Имени пользователя и пароле. Если любой неправ, сообщение "Неверный пароль" отображается четыре раза. Затем пользователь разъединен. Этой проблемой был назначенный идентификатор ошибки #CSCdm46934.

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

Отладка PIX - Выключенный Deamon, не свяжется с PIX - RADIUS

Пример ниже отладки PIX показов с сервером доступный по эхо-тесту, но демон не работает. Сервер не свяжется с PIX. Пользователь видит Имя пользователя, придерживавшееся паролем. Показ следующих сообщений: "Сервер RADIUS отказал" и "Ошибка: Максимальное число попыток превысило".

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

Отладка PIX - не Может Пропинговать Сервер или Несогласованность ключа/клиента - RADIUS

Пример ниже отладки PIX показов для сервера, который не является отвечающим на команду ping или где существует несогласованность ключа/клиента. Пользователь видит Имя пользователя и пароль. Показ следующих сообщений: "Таймаут к серверу RADIUS" и "Ошибке: Максимальное число попыток превысило" (сервер в конфигурации является, например, только целями).

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

Добавление авторизации

Поскольку авторизация не допустима без аутентификации, мы потребуем авторизации для того же исходного и конечного диапазона:

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 aaa authorization http outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0
```

Выход

Обратите внимание на то, что мы не добавляем авторизацию для "поступления", потому что входящий трафик 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 с успешной проверкой подлинности и успешной авторизацией - TACACS +

Пример ниже отладки PIX показа с успешной проверкой подлинности и успешной авторизацией:

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109005: Authentication succeeded for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109007: Authorization permitted for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_telnet', sid 7,
 elapsed 1 seconds
 302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
 gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

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

Пример ниже отладки PIX показов с успешной проверкой подлинности, но сбой проверки подлинности:

Здесь пользователь также видит сообщение "Ошибка: Запрещенная Авторизация"

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_ftp', sid 5
 109005: Authentication succeeded for user 'can_only_do_ftp'
 from 10.31.1.5/11000 to 11.11.11.15/23
 109008: Authorization denied for user 'can_only_do_ftp' from
 10.31.1.5/11000 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

Добавление автоматического учета

TACACS +

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing

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

TACACS + учетные записи похожи на следующее (это от CiscoSecure UNIX; те в CiscoSecure NT могут быть разделены запятой вместо этого):

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
 PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
 stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming

Отладка будет выглядеть 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 придерживающееся: (это от CiscoSecure UNIX; те в CiscoSecure NT могут быть разделены запятой вместо этого):

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
 Thu Jun  3 15:53:11 1999
         Acct-Status-Type = Start
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
 10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
 Thu Jun  3 15:54:24 1999
         Acct-Status-Type = Stop
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
         Acct-Session-Time = 73
         Acct-Input-Octets = 27
         Acct-Output-Octets = 73
```

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 как придерживающееся:

aaa authentication except outbound 10.31.1.60 255.255.255.255 11.11.11.15 255.255.255.255 Outgoing aaa authorization except outbound 10.31.1.60 255.255.255.255 11.11.11.15 255.255.255.255 Outgoing

Если вы "исключаете" IP-адреса из аутентификации и имеете авторизацию на, вы должны также кроме них 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 (т.е. 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 следующем примере 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
```

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

Пользователь продолжает ее 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.

Однако HTTP работает по-другому из-за природы 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.

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). Функции контроля максимального числа сеансов и просмотра зарегистрированных пользователей не будут действовать в силу особенностей соединений HTTP.

Аутентификация и включение в самом PIX

Предыдущее обсуждение имело аутентифицирующуюся Telnet (и HTTP, FTP) трафик через PIX. В примере ниже, мы удостоверяемся, что Telnet к pix работает без аутентификации на:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

Затем мы добавляем команду для аутентификации пользовательского Telnet - сеанса на PIX:

```
aaa authentication telnet console Outgoing
```

Когда подключение пользователей посредством Telnet к PIX, им предлагают для Пароля Telnet ("ww"). PIX также запрашивает TACACS + в этом случае (так как "Исходящий" список серверов используется), или Имя пользователя RADIUS и пароль.

```
aaa authentication enable console Outgoing
```

С этой командой пользователю предлагают для имени пользователя и пароля, которое передается TACACS или серверу RADIUS. В этом случае, так как "Исходящий" список серверов используется, запрос переходит к Серверу tacacs. Так как пакет проверки подлинности для включает, совпадает с пакетом проверки подлинности для входа в систему, пользователь может включить через TACACS или RADIUS с том же имя пользователя / пароль, предположив, что пользователь может войти к PIX с TACACS или RADIUS. Этой проблемой был назначенный идентификатор ошибки #CSCdm47044.

Если сервер не работает, пользователь может получить доступ к режиму включения PIX путем ввода "PIX" для имени пользователя и обычного enable password от PIX ("enable

password безотносительно"). Если "enable password безотносительно" не находится в конфигурации PIX, пользователь должен ввести "PIX" для имени пользователя и нажать Клавишу Enter. Если enable password будет установлен, но не известен, то диск для восстановления пароля будет требоваться для сброса.

Аутентификация в последовательной консоли

Команда aaa authentication serial console требует проверки для проверки подлинности для доступа к последовательной консоли PIX. Когда пользователь выполнит команды настройки от консоли, сообщения системного журнала будут вырезаны (если PIX будет настроен для передачи системного журнала в уровне отладки к узлу системного журнала). Ниже пример от сервера системного журнала:

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

Изменение приглашения для пользователя

Если имеется команда:

auth-prompt THIS_IS_PIX_5

пользователи, проходящие PIX, видят последовательность:

```
THIS_IS_PIX_5 [at which point one would enter the username]
 Password:[at which point one would enter the password]
```

и затем, по прибытии в последнее поле назначения, "Имя пользователя": и "Пароль": приглашение поле назначения представлено.

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 имеются команды:

auth-prompt accept "You're allowed through the pix" auth-prompt reject "You blew it"

Пользователи будут видеть следование неудачной/удачной попытки входа через PIX:

```
THIS_IS_PIX_5
 Username: asjdkl
 Password:
 "You blew it"
 "THIS_IS_PIX_5"
 Username: cse
 Password:
 "You're allowed through the pix"
```

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 '", то не внедряйте это! Но при необходимости в другом uauths для каждого пользователя продолжать читать.

В нашем примере на PIX мы используем **команду timeout uauth 3:00:00**. Это означает, что, как только человек аутентифицируется, они не должны будут повторно аутентифицироваться в течение 3 часов. Но если мы устанавливаем пользователя со следующим профилем и имеем 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.

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

После аутентификации, проблема **команда 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 будет пройти повторную проверку подлинности при возврате 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.

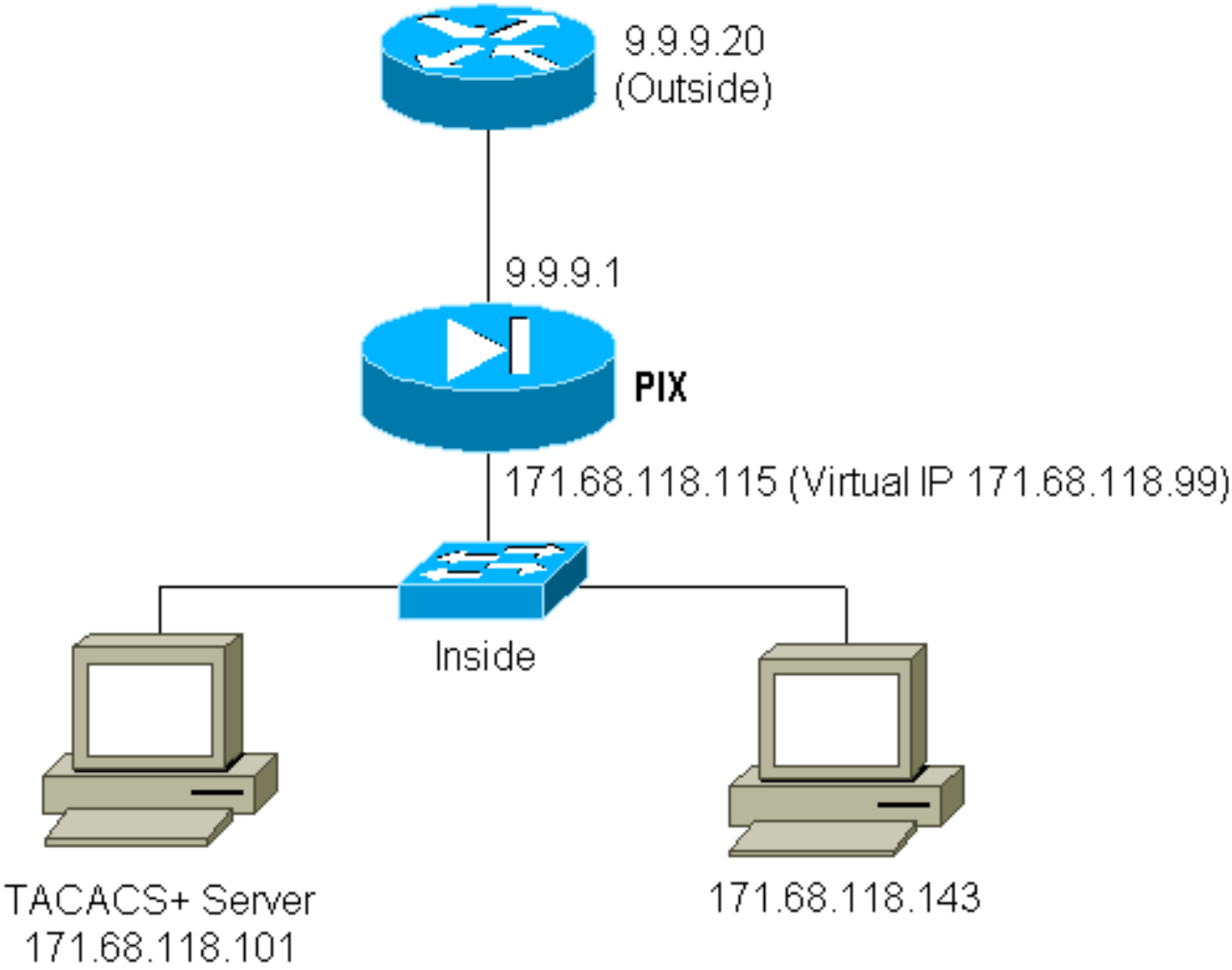
Для предотвращения этого можно внедрить действительный HTTP путем добавления адреса RFC 1918 (т.е. адрес, который немаршрутизуем в Интернете, но допустим и уникален для внутренней сети PIX) к конфигурации PIX с помощью следующей команды:

```
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 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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

Виртуальный протокол Telnet

Настройка PIX для аутентификации всего входящего и исходящего трафика не является хорошей идеей, потому что легко не аутентифицируются некоторые протоколы, такие как "почта". Когда почтовый сервер и клиент пытаются связаться через PIX, когда весь трафик через PIX будет аутентифицироваться, системный журнал PIX для протоколов без возможности проверки подлинности покажет сообщения, такие как:

```
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
```

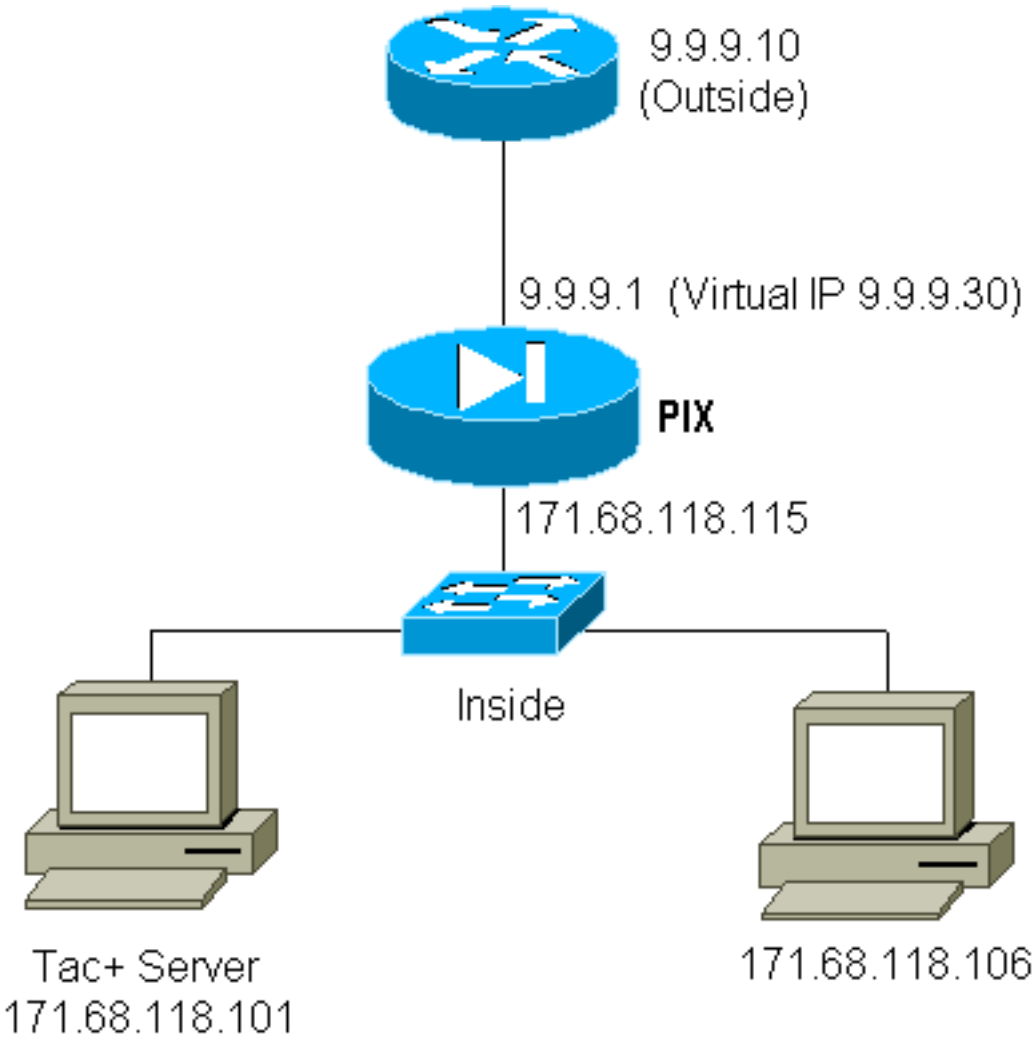
```
(not authenticated
```

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).

Но 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 для виртуального протокола Telnet. После этой аутентификации трафик для необычного сервиса может перейти к реальному серверу, который связан к виртуальному IP.

В нашем примере мы хотим позволить порту TCP 49 трафиков, чтобы вытекать из внешнего хоста 9.9.9.10 к внутреннему хосту 171.68.118.106. Поскольку этот трафик не действительно authenticatable, мы устанавливаем виртуальный протокол Telnet.

Входящие данные протокола Virtual 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) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.30 host 9.9.9.10
 aaa-server TACACS+ protocol tacacs+
 aaa-server Incoming protocol tacacs+
```

```
 aaa-server Incoming (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 Incoming
 virtual telnet 9.9.9.30
```

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 telnetting на этих 9.9.9.30 адресах на PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
 to 171.68.118.106/23
 109011: Authen Session Start: user 'pinecone', sid 13
 109005: Authentication succeeded for user 'pinecone' from
 171.68.118.106/23 to 9.9.9.10/11099
```

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
```

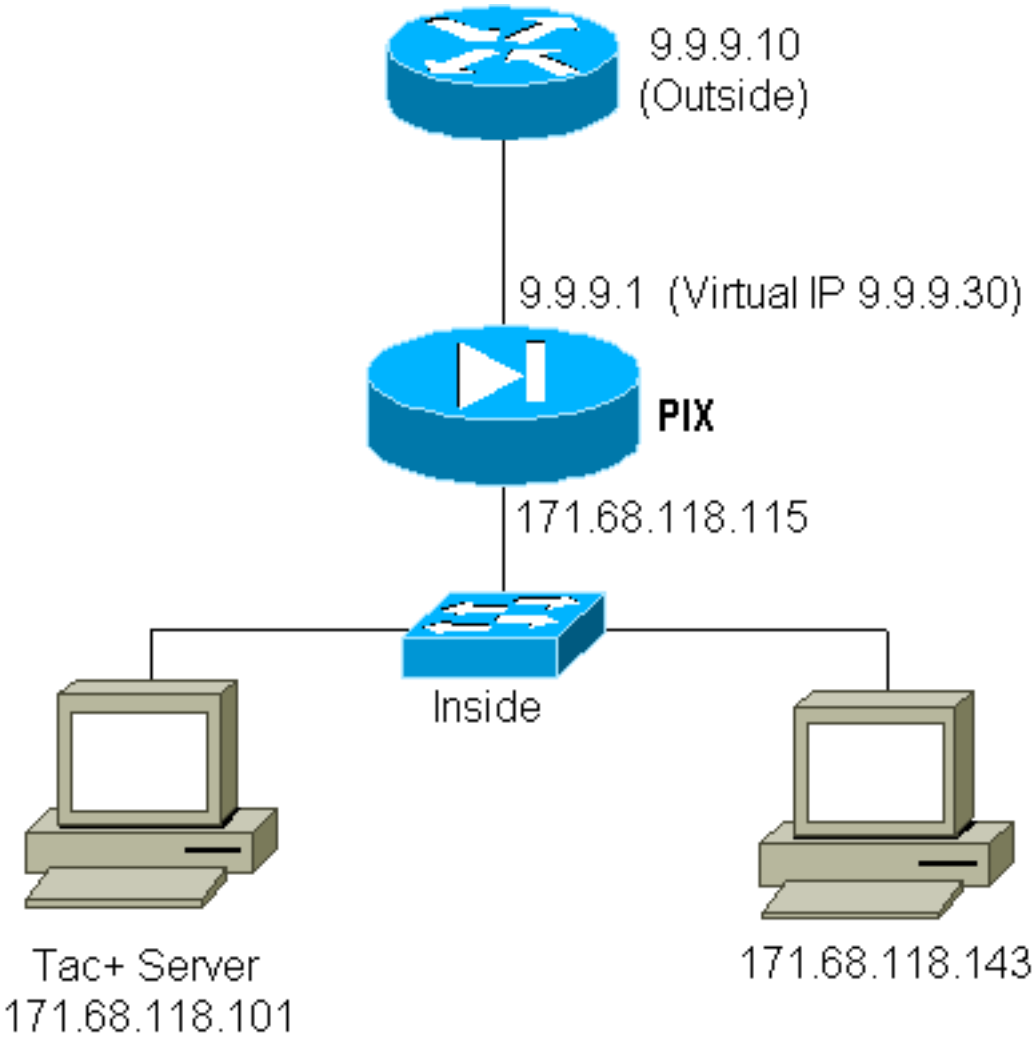
И когда устройство в 9.9.9.10 хочет передать трафик TCP/49 к устройству в 171.68.118.106:

```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 109011: Authen Session Start: user 'pinecone', sid 14
 109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
 to 171.68.118.106/49
 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 следующем примере внутренний пользователь в 171.68.118.143 будет Telnet к действительным 9.9.9.30 и аутентифицироваться. 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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 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 его uauth. Если пользователь хочет препятствовать тому, чтобы трафик прошел после того, как его сеанс закончен (когда там время оставленный в uauth), ему 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 следующем примере аутентификация все еще требовалась для всех исходящих, но авторизация только требуется 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 Outgoing aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing

Так, когда мы, Telnet 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 мы делаем сеанс HTTP от 171.68.118.143 до 9.9.9.10, мы все еще должны 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)
```

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