Аутентификация, авторизация и учет пользователей с помощью PIX версии 5.2 и более поздних версий

Содержание

Введение

RADIUS и TACACS + аутентификация могут быть сделаны для FTP, Telnet и соединений HTTP через межсетевой экран Cisco Secure PIX. Аутентификация для другого меньшего количества част используемых протокол обычно делается работать. TACACS + авторизация поддерживается. Проверка подлинности RADIUS не поддерживается. Изменения в аутентификации, авторизации и учете (AAA) PIX 5.2 по более ранней версии включают поддержку списка AAA (проверка подлинности, авторизация и учет) для управления, кто аутентифицируется и к каким ресурсам пользователь обращается. В PIX 5.3 и позже, переключается аутентификация, авторизация и учет (AAA), более ранние версии кода то, что Порты RADIUS конфигурируемы.

Примечание: PIX 6.x может сделать составление сквозного трафика прохода, но не для трафика destinated к PIX.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Программное обеспечение межсетевого экрана Cisco Secure PIX версий 5.2.0.205 и 5.2.0.207

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Примечание: При выполнении версии программного обеспечения 7.x PIX/ASA и позже обратитесь к AAA-серверам Настройки и Локальной базе данных.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Аутентификация, авторизация и учет

Вот описание проверки подлинности, Авторизация и Учет:

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

Что видит пользователь при включенной аутентификации/авторизации

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

- **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 передает "local_username" и "local_password" к локальному серверу безопасности. Если аутентификация (и авторизация) успешна в PIX/server, "remote_username" и "remote_password" передают к конечному серверу FTP вне.
- **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 вызвать таймаут соединения HTTP, но не делает так, вероятно, что повторная проверка подлинности фактически имеет место с браузером, "стреляющим" в кэшированное имя пользователя и пароль к PIX. PIX Вперед это к серверу проверки подлинности. Системный журнал PIX и/или серверная отладка показывают это явление. Если Telnet и FTP, кажется, "обычно" работают, но соединения HTTP не делают, это - причина.

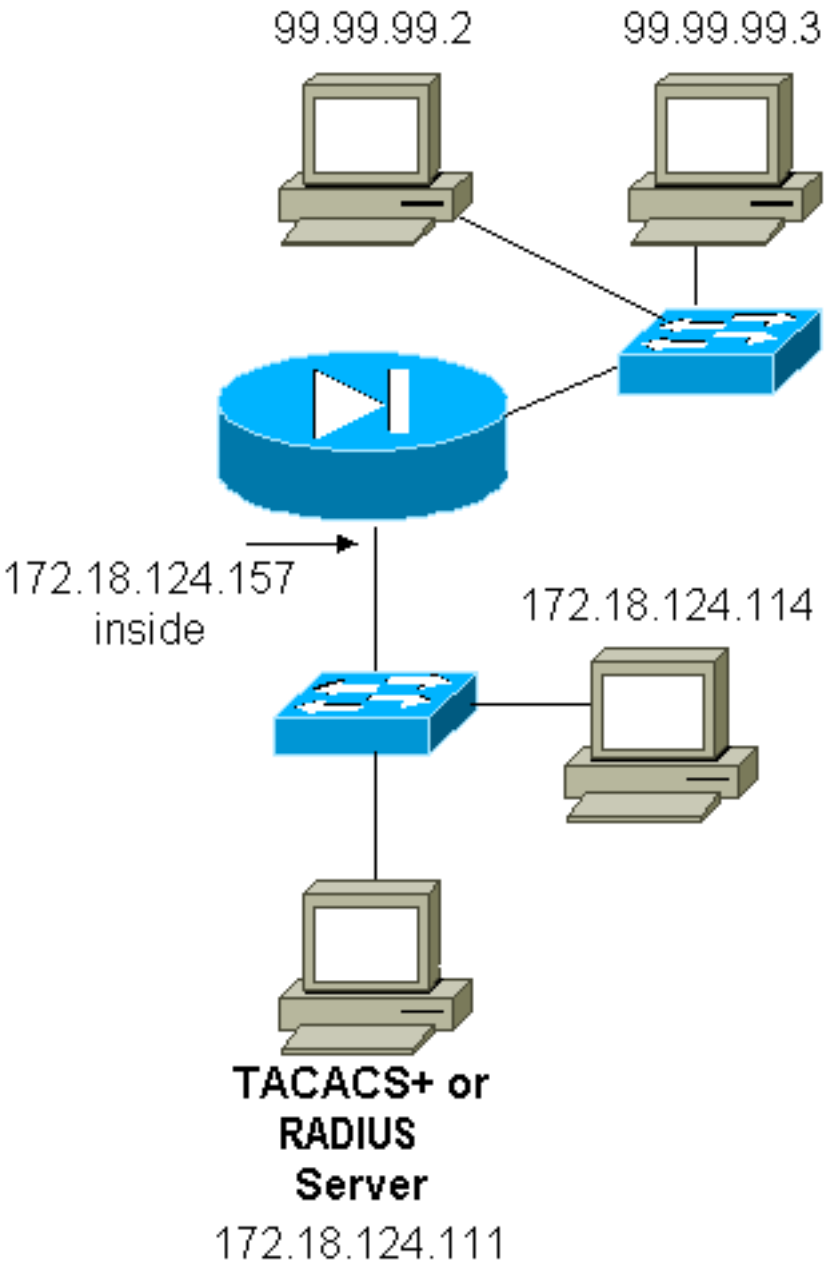
Шаги отладки

- Удостоверьтесь, что конфигурация PIX работает перед добавлением аутентификации AAA (проверка подлинности, авторизация и учет) и авторизации. Если вы неспособны передать трафик перед учреждением проверки подлинности и авторизация вы неспособны сделать так впоследствии.
- Включите регистрацию в PIX.Выполните **команду logging console debug** для включения отладки консоли регистрации.**Примечание:** Не используйте отладку консоли регистрации на в большой степени загружаемая система.**Используйте команду logging monitor debug для регистрации сеанса Telnet.Можно использовать команду отладки logging buffered, а затем выполнить команду show logging.**Регистрация может быть

отправлена на сервер системных журналов для дальнейшего изучения.
- Включить отладку на серверах TACACS+ или RADIUS.

Только аутентификация

Схема сети



Настройка сервера - только аутентификация

Конфигурация сервера CiscoSecure UNIX TACACS

```
User = cse {
password = clear "cse"
default service = permit
}
```

Конфигурация сервера CiscoSecure UNIX RADIUS

Примечание: Добавьте IP-адрес PIX и ключ к списку Сервера доступа к сети (NAS) с помощью расширенного ГИПа.

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
}
reply_attributes= {
6=6
}
}
}
```

Windows RADIUS Cisco Secure

Использование эти шаги для устанавливания Windows RADIUS Cisco Secure Разъединяет.

1. Получите пароль в **Разделе настройки пользователя**.
2. **В разделе Group Setup установите атрибут 6 (Service-Type) на Login или Administrative.**
3. **Добавьте IP-адрес PIX в раздел конфигурации NAS графического интерфейса пользователя.**

Windows TACACS Cisco Secure +

Пользователь получает пароль в разделе настройки пользователя.

Конфигурация сервера Livingston RADIUS

Примечание: Добавьте IP-адрес PIX и ключ к файлу *клиентов*.

- счет Пароль = User-service-type "foo" = Shell-User

Конфигурация сервера Merit RADIUS

Примечание: Добавьте IP-адрес PIX и ключ к файлу *клиентов*.

- bill пароль ="foo" Тип сервиса = Пользователь оболочки

Конфигурация свободно распространяемого сервера TACACS+

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

Первоначальная конфигурация PIX - только аутентификация

Первоначальная конфигурация PIX - только аутентификация
`PIX Version 5.2(0)205` `nameif ethernet0 outside security0`

```
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet access-list 101 permit tcp
any any eq ftp access-list 101 permit tcp any any eq www
! pager lines 24 logging on no logging timestamp no
logging standby logging console debugging no logging
monitor no logging buffered logging trap debugging no
logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 10baset mtu
outside 1500 mtu inside 1500 ip address outside
99.99.99.1 255.255.255.0 ip address inside
172.18.124.157 255.255.255.0 ip audit info action alarm
ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0 arp
timeout 14400 global (outside) 1 99.99.99.10-99.99.99.20
netmask 255.255.255.0 nat (inside) 1 172.18.124.0
255.255.255.0 0 0 static (inside,outside) 99.99.99.99
172.18.124.114 netmask 255.255.255.255 0 0 conduit
permit tcp any any conduit permit udp any any conduit
permit icmp any any route inside 172.18.0.0 255.255.0.0
172.18.124.1 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 si p 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute ! !--- For the purposes of
illustration, the TACACS+ process is used !--- to
authenticate inbound users and RADIUS is used to
authenticate outbound users. aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius aaa-server
AuthInbound protocol tacacs+ aaa-server AuthInbound
(inside) host 172.18.124.111 cisco timeout 5 aaa-server
AuthOutbound protocol radius aaa-server AuthOutbound
(inside) host 172.18.124.111 cisco timeout 5 ! !--- The
next six statements are used to authenticate all inbound
!--- and outbound FTP, Telnet, and HTTP traffic. aaa
authentication include ftp outside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound aaa authentication include
telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound aaa authentication include http outside
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authentication include http inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
telnet inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound aaa authentication include ftp inside
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound ! !--- OR
the new 5.2 feature allows these two statements in !---
conjunction with access-list 101 to replace the previous
six statements. !--- Note: Do not mix the old and new
verbiage. aaa authentication match 101 outside
AuthInbound aaa authentication match 101 inside
```

```
AuthOutbound no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable no sysopt route dnat
isakmp identity hostname telnet timeout 5 ssh timeout 5
terminal width 80
Cryptochecksum:5882f514247589d784a0d74c800907b8 : end
```

Настраиваемые порты RADIUS (5.3 и более поздние версии)

Некоторые серверы RADIUS используют порты RADIUS, отличные от 1645 или 1646 (обычно 1812 или 1813). В PIX 5.3 и позже, Проверка подлинности RADIUS и порты учета могут быть изменены на что-то другое, чем по умолчанию 1645/1646 с этими командами:

aaa-server radius-authport # aaa-server radius-acctport #

Примеры отладки аутентификации PIX

Посмотрите Действия по отладке для получения информации о том, как включить отладку. Это примеры пользователя в 99.99.99.2, который инициирует трафик к внутреннему 172.18.124.114 (99.99.99.99) и наоборот. Входящий трафик аутентифицируется на TACACS и исходящий, аутентифицируется на RADIUS.

Успешная аутентификация – TACACS+ (входящая)

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
  to 99.99. 99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
  gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse)
```

Попытка аутентификации завершилась неудачей из-за неправильного имени пользователя/пароля - TACACS+ (входящая). Пользователь видит "Ошибку: Максимальное число попыток превысило".

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1004 on interface outside
```

Сервер не отвечает PIX – TACACS+ (входящий). Пользователь видит имя пользователя только один раз, и межсетевой экран PIX никогда не спрашивает пароль (это касается Telnet). Пользователь видит "Ошибку: Максимальное число попыток превысило".

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1005 on interface outside
```

Успешная аутентификация – RADIUS (исходящая)

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
```

```
  to 99 .99.99.2/23 on interface inside
```

Ошибка аутентификации (в имени пользователя или пароле) – RADIUS (исходящий). Пользователь видит запрос об Имени пользователя, затем Пароль, имеет три возможности ввести их, и, если неуспешный, видеть "Ошибку: Максимальное число попыток превысило".

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
  to 99.99.99. 2/23 on interface inside
```

Сервер отвечает на команду ping, но недоступен демон, недоступен сервер или ключ не соответствует клиенту, поэтому нет связи с PIX - RADIUS (исходящие). Пользователь видит Имя пользователя, затем пароль, тогда "подведенный сервер RADIUS", и затем наконец "Ошибка: Максимальное число попыток превысило".

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
  to 99.99.99. 2/23 on interface inside
```

Проверка подлинности плюс авторизация

Если вы хотите позволить всем проверенным пользователям выполнять все операции (HTTP, FTP и Telnet) через PIX, то аутентификация достаточна, и авторизация не необходима. Однако, если вы хотите позволить некоторое подмножество сервисов некоторым пользователям или ограничить пользователей от того, чтобы переходить к определенным сайтам, авторизация необходима. Проверка подлинности RADIUS не допустима для трафика через PIX. TACACS + авторизация допустим в этом случае.

Если опознавательные проходы и авторизация идут, PIX передает команду, которую пользователь делает к серверу. Например, "http 1.2.3.4". В версии 5.2 PIX TACACS + авторизация используется в сочетании со списками доступа для управления, куда идут пользователи.

Если вы хотите внедрить авторизацию для HTTP (веб-сайты, которые посещают), используйте программное обеспечение, такое как Websense, так как одиночный веб-сайт может иметь большое число IP-адресов, привязанных к нему.

Установка сервера - проверка подлинности плюс авторизация

Конфигурация сервера CiscoSecure UNIX TACACS

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

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

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

Windows TACACS Cisco Secure +

Выполните эти шаги для устанавливания Windows TACACS Cisco Secure + сервер.

1. Нажмите **Deny несопоставленные команды IOS** у основания Настройки групп.
2. Нажмите **Add/Edit New Command (FTP, HTTP, Telnet)**.Например, если вы хотите позволить Telnet определенному узлу ("telnet 1.2.3.4"), команда является **telnet**. Аргумент *1.2.3.4*. **После ввода "command=telnet" введите IP-адреса разрешения в поле ввода аргумента (например "permit 1.2.3.4"). Если необходимо разрешить все операции Telnet, используется по-прежнему команда telnet, но следует выбрать Allow all unlisted arguments (Разрешить все не указанные аргументы)**. Затем **нажмите Finish editing command**.
3. Выполните шаг 2 для каждой из позволенных команд (например, Telnet, HTTP и FTP).
4. Добавьте IP-адрес PIX в разделе Конфигурации NAS с помощью GUI.

Конфигурация свободно распространяемого сервера TACACS+

```
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 .*
   }
   }
```

Конфигурация PIX – добавление авторизации

Команды Add для требования авторизации:

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization
include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Новые 5.2 функций позволяют этому оператору в сочетании с ранее определенным списком доступа 101 заменять предыдущие три оператора. Не следует смешивать прежние и новые формулировки.

```
aaa authorization match 101 outside AuthInbound
```

Примеры отладки аутентификации и авторизации PIX

Успешная проверка подлинности и авторизация успешно выполняются - TACACS +

```
109001: Auth start for user '???' from
   99.99.99.2/11010 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 3
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to 99.99.99.2/11010
   on interface outside
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
   from 99.99.99.2/11010 to 172.18.1  24.114/23
   on interface outside
302001: Built inbound TCP connection 2 for faddr
   99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
   172.18.124.114/23 (cse)
```

Успешная аутентификация, но сбой при авторизации - TACACS+. Пользователь также видит сообщение "Ошибка: Запрещенная Авторизация".

```
109001: Auth start for user '???' from
   99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
   from 172.18.124.114/23 to  9 9.99.99.2/11011
   on interface outside
109008: Authorization denied for user 'httponly'
   from 172.18.124.114/23 to 99.99.99.2/11011
   on interface outside
```

Новая функция списка доступа

В релизе программного обеспечения PIX 5.2 и позже, определите списки доступа на PIX. Примените их на основе для каждого пользователя на основе профиля пользователя на сервере. TACACS+ требует проверки подлинности и авторизации. Сервер RADIUS требует только аутентификации. В данном примере изменены исходящая аутентификация и авторизация к TACACS +. Список доступа на PIX установлен.

Примечание: В Версии PIX 6.0.1 и позже при использовании RADIUS списки доступа внедрены путем ввода списка в стандартном атрибуте RADIUS, утвержденный IETF 11 (Filter-Id) [CSCdt50422]. В данном примере припишите 11, установлен в 115 вместо выполнения определяемой поставщиком "acl=115" формулировки.

Конфигурация PIX

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet access-list 115 permit tcp any host
99.99.99.2 eq www access-list 115 permit tcp any host 99.99.99.2 eq ftp access-list 115 deny tcp
any host 99.99.99.3 eq www access-list 115 deny tcp any host 99.99.99.3 eq ftp access-list 115
deny tcp any host 99.99.99.3 eq telnet
```

Профили сервера

Примечание: В версии 2.1 свободно распространяемого программного обеспечения TACACS+ не поддерживается формулировка "acl".

TACACS Cisco Secure UNIX + конфигурация сервера

```
user = pixa{
  password = clear "********"
  service=shell {
  set acl=115
  }
  }
```

Windows TACACS Cisco Secure +

Для добавления авторизации к PIX для управления, куда пользователь идет со списками доступа, проверьте **оболочку/exec**, проверьте **Поле со списком контроля доступа** и заполните номер (совпадает с номером списка доступа на PIX).

Cisco Secure UNIX RADIUS

```
user = pixa{
  password = clear "********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
```

Windows RADIUS Cisco Secure

Сервис удаленной аутентификации по телефонной линии (RADIUS)/Cisco — тип устройства. "pixa" пользователю нужны имя пользователя, пароль, и проверка и "acl=115" в Прямоугольнике Cisco/RADIUS, где это говорит 009\001 (определяемую поставщиком) пару значение-атрибут.

Выходные данные

Исходящий пользователь "pixa" с "acl=115" в профиле аутентифицирует и авторизует. Сервер передает acl=115 к PIX, и PIX показывает это:

```
pixfirewall#show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 2 user
'pixa' at 172.18.124.114, authenticated access-list 115 absolute timeout: 0:05:00 inactivity
timeout: 0:00:00
```

Когда пользователь "pixa" пытается перейти 99.99.99.3 (или любой IP-адрес кроме 99.99.99.2, потому что существует неявное, запрещают), пользователь видит это:

```
Error: acl authorization denied
```

Новый загружаемый список доступа для каждого пользователя в версии 6.2

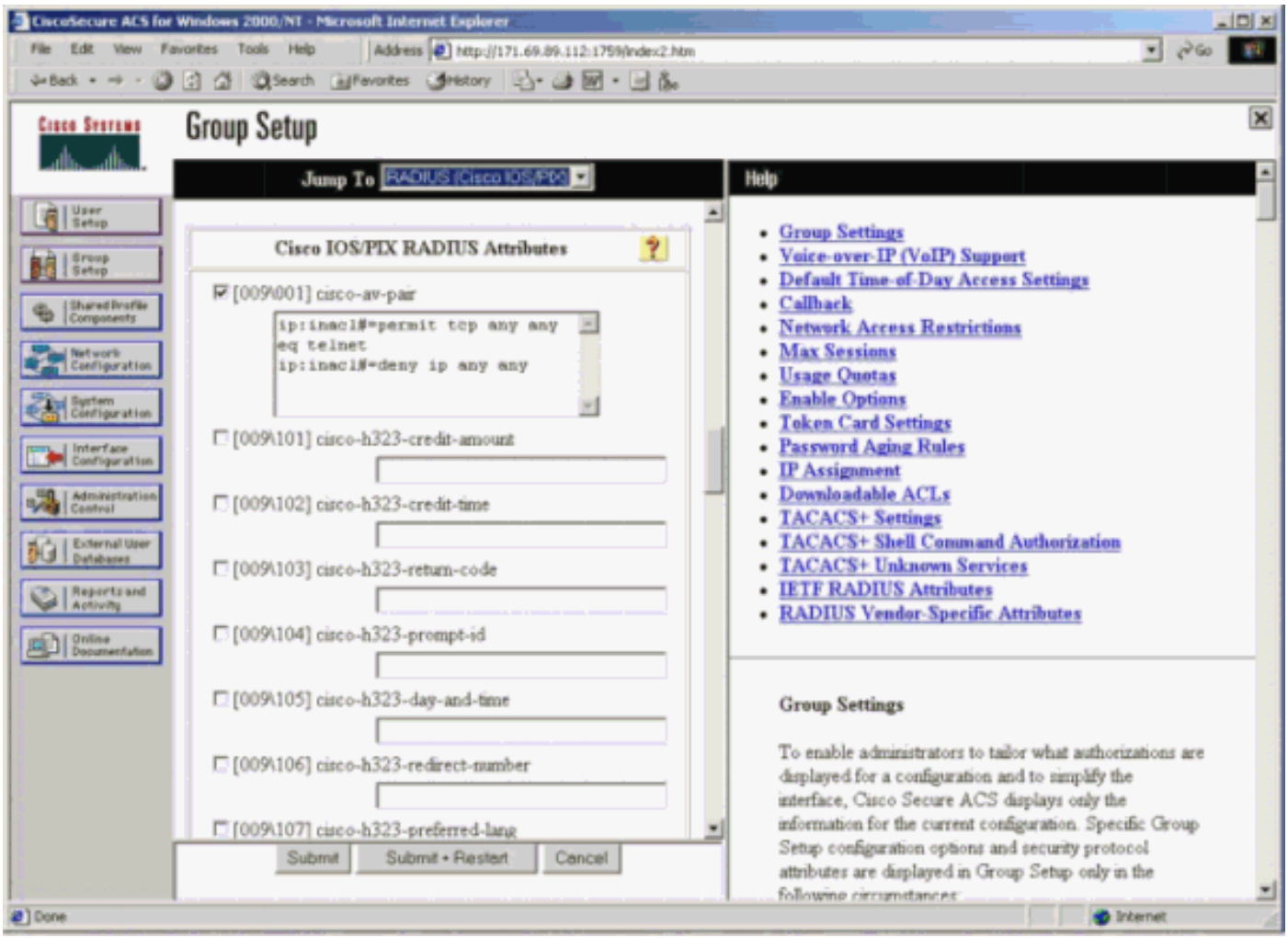
В выпуске ПО 6.2 и позже Межсетевого экрана PIX, списки доступа определены на Access Control Server (ACS) для загрузки к PIX после аутентификации. Это работает только с Протоколом RADIUS. Нет необходимости настраивать список доступа на самом PIX. Шаблон группы применен к нескольким пользователей.

В более ранних версиях список доступа определен на PIX. На аутентификацию ACS выдвинул название списка доступа к PIX. Новая версия позволяет ACS выдвигать список доступа непосредственно к PIX.

Примечание: Если аварийное переключение происходит, uauth таблица не является скопированными Пользователями, повторно аутентифицируются. Список доступа загружен снова.

Настройка ACS

Нажмите **Group Setup** и выберите **RADIUS (Cisco IOS / PIX)** тип устройства для устанавливания учетной записи пользователя. Назначьте имя пользователя ("cse" в данном примере) и пароль для пользователя. Из списка Атрибутов выберите опцию для настройки **[009\001]** ***vendor-av-pair***. Определите список доступа, как проиллюстрировано в данном примере:



Отладки PIX: Достоверная аутентификация и загруженный список доступа

- Позволяет только Telnet и запрещает другой трафик.
```
pix# 305011: Built dynamic TCP translation from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
   to 172.16.171.202/23 on interface inside

302013: Built outbound TCP connection 123 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11063 (172.16.171.201/1049) (cse)
```
Выходные данные от **команды show uauth**.
```
pix#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user 'cse' at 172.16.171.33, authenticated access-list AAA-user-cse absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```
Выходные данные от команды **show access-list**.
```
pix#show access-list access-list AAA-user-cse; 2 elements access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1) access-list AAA-user-cse deny ip any any (hitcnt=0)
```
- Запрещает только Telnet и позволяет другой трафик.
```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11064
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
  from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```
Выходные данные от **команды show uauth**.
```
pix#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user 'cse' at 172.16.171.33, authenticated access-list AAA-user-cse absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```
Выходные данные от команды **show access-list**.
```
pix#show access-list access-list AAA-user-cse; 2 elements access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1) access-list AAA-user-cse permit ip any any (hitcnt=0)
```

Новый загружаемый список доступа, использующий ACS 3.0, для каждого пользователя

В ACS версии 3.0 компонент общего профиля позволяет пользователю создавать шаблон списка доступа и определять имя шаблона для специализированных пользователей или групп. Имя шаблона может использоваться с в качестве многих пользователей или групп по мере необходимости. Это избавляет от необходимости настраивать идентичные списки доступа для каждого пользователя.

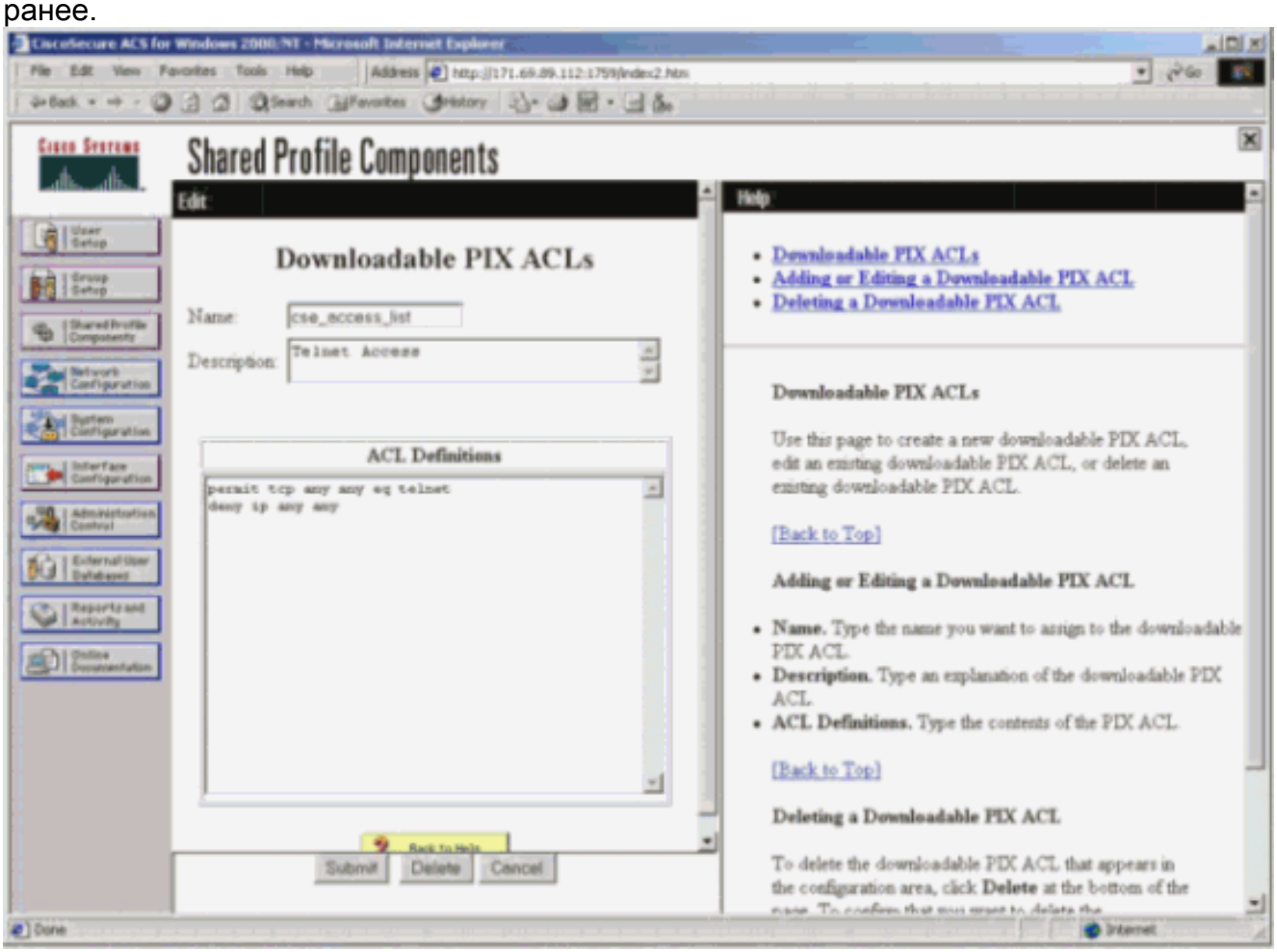
Примечание: Если аварийное переключение происходит, uauth не скопирован к вторичному межсетевому экрану (PIX). В перехвате управления при отказе с синхронизацией состояния поддержан сеанс. Однако новое соединение должно повторно аутентифицироваться, и список доступа должен быть загружен снова.

Использование общих профилей

Выполните эти шаги при использовании разделенных профилей.

1. **Нажмите " Interface Configuration " (Настройка интерфейса).**
2. Проверьте **Загружаемые списки ACL Пользовательского уровня** и/или **Загружаемые списки ACL Уровня Группы**.

3. Нажмите **Shared Profile Components**. Нажмите **User-Level Downloadable ACLs**.
4. Определите загружаемые списки ACL.
5. **Щелкните на отцию Group Setup.** Под Загружаемыми списками ACL назначьте список доступа PIX на список доступа, созданный ранее.



[Отладки PIX: Проверенная аутентификация и загруженный список доступа Использование совместно используемых профилей]

- Позволяет только Telnet и запрещает другой трафик.
```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11065 to outside:172.16.171.201/1051
109001: Auth start for user '???' from 172.16.171.33/11065 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 12
109005: Authentication succeeded for user 'cse' from
   172.16.171.33/11065 to 172.16.171.202/23 on interface inside
302013: Built outbound TCP connection 124 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11065 (172.16.171.201/1051) (cse)
```
Выходные данные от **команды show uauth**.
```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```
Выходные данные от команды **show access-list**.
```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3 permit tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3 deny ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-list
```
- Запрещает только Telnet и позволяет другой трафик.
```
pix# 305011: Built dynamic TCP
```

```
translation from inside:
   172.16.171.33/11066 to outside:172.16.171.201/1052
109001: Auth start for user '???' from 172.16.171.33/11066 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 13
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
   for user 'cse' from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
```

Выходные данные от **команды show uauth**.

```
pix#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user
'cse' at 172.16.171.33, authenticated access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00 inactivity timeout: 0:00:00 pix# 111009: User 'enable_15' executed
cmd: show uauth
```

Выходные данные от команды **show access-list**.

```
pix#show access-list access-
list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements access-list #ACSACL#-PIX-
cse_access_list-3cff1dd6 deny tcp any any eq telnet (hitcnt=1) access-list #ACSACL#-PIX-
cse_access_list-3cff1dd6 permit ip any any (hitcnt=0) pix# 111009: User 'enable_15' executed
cmd: show access-listpix#
```

Добавление учета

Конфигурация PIX - добавляет учет

TACACS (AuthInbound=tacacs)

Добавьте эту команду.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Или используйте новую характеристику в 5.2 для определения то, что должно считаться списками доступа.

```
aaa accounting match 101 outside AuthInbound
```

Примечание: Список доступа 101 определен отдельно.

RADIUS (AuthOutbound=radius)

Добавьте эту команду.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

Или используйте новую характеристику в 5.2 для определения то, что должно считаться списками доступа.

```
aaa accounting match 101 outside AuthOutbound
```

Примечание: Список доступа 101 определен отдельно.

Примечание: Учетные записи могут генерироваться для административных сеансов на PIX, запускающемся с кода PIX 7.0.

Примера учета

- Пример учета TACACS для Telnet от 99.99.99.2 внешней стороны до 172.18.124.114 внутренних (99.99.99.99).
```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
   time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
   time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114
   cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```
- Пример использования средств учета RADIUS для соединения от 172.18.124.114 внутренней части до 99.99.99.2 внешних (Telnet) и 99.99.99.3 внешних (HTTP).
```
Sun Aug  6 03:59:28 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
        User-Name = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
        Acct-Input-Octets = 101
        Acct-Output-Octets = 143
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 04:05:02 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 80
        Username = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35949
        Vendor-Specific = Destination-IP=99.99.99.3
        Vendor-Specific = Destination-Port=80

Sun Aug  6 04:05:02 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 80
        Acct-Session-Id = 0x0000000a
        Username = cse
        Acct-Session-Time = 0
        Acct-Input-Octets = 1277
        Acct-Output-Octets = 310
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35949
        Vendor-Specific = Destination-IP=99.99.99.3
        Vendor-Specific = Destination-Port=80
```

Использование команды exclude

В этой сети, если вы решаете, что конкретному источнику или назначению не нужна аутентификация, авторизация или учет, выполняет эти команды.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255 99.99.99.3
255.255.255.255 AuthInbound aaa authorization exclude telnet outside 172.18.124.114
255.255.255.255 99.99.99.3 255.255.255.255 AuthInbound aaa accounting exclude telnet outside
172.18.124.114 255.255.255.255 99.99.99.3 255.255.255.255 AuthInbound
```

Примечание: У вас уже есть **включать** команды.

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

Или, с новой характеристикой в 5.2, определите то, что вы хотите исключить.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet access-list 101 deny tcp
host 99.99.99.3 host 172.18.124.114 eq ftp access-list 101 deny tcp host 99.99.99.3 host
172.18.124.114 eq www access-list 101 permit tcp any any eq telnet access-list 101 permit tcp
any any eq www access-list 101 permit tcp any any eq ftp aaa authentication match 101 outside
AuthInbound aaa authorization match 101 outside AuthInbound aaa accounting match 101 outside
AuthInbound
```

Примечание: Если вы исключаете коробку из аутентификации, и у вас есть авторизация на, необходимо также исключить коробку из авторизации.

Max-sessions и обзорные вошедшии в систему пользователь

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. Однако это не работает хорошо для HTTP. В данном примере используется другая конфигурация сети, но понятия являются тем же.

Пользователь устанавливает сеанс Telnet через PIX и проходит аутентификацию.

```
(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 171.68.118.100/1200 to 9.9.9.25/23
    (pix) 302001: Built TCP connection 5 for
        faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 laddr
        171.68.118.100/1200 (cse)
    (server start account) Sun Nov 8 16:31:10 1998
        rtp-pinecone.rtp.cisco.com cse
        PIX 171.68.118.100 start task_id=0x3
        foreign_ip=9.9.9.25
        local_ip=171.68.118.100 cmd=telnet
```

Поскольку сервер видел запись "запуска", но никакие не "останавливают" запись, в данный момент, сервер показывает, что входят в пользователя "Telnet". Если пользователь делает

попытку другого соединения, которое требует аутентификации (возможно, от другого ПК), и если max-sessions установлен в "1" на сервере для этого пользователя (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. Вот пример HTTP, где 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). В пользователя не входят к веб-сайту. Когда пользователь читает веб-страницу, соединение не открыто. Max-sessions или обзорные вошедшии в систему пользователь не работают здесь. Это вызвано тем, что время соединения (время между "Созданным" и "Разрушением") в HTTP слишком коротко. Интервал между состояниями "start" (начало) и "stop" (окончание) составляет менее одной секунды. Нет никаких, "запускают" запись без записи "остановки", так как записи происходят в фактически тот же момент. Существует все еще "запуск", и "остановите" запись, передаваемую серверу для каждой транзакции, установлен ли uauth для 0 или что-то большее. Однако max-sessions и обзорные вошедшии в систему пользователь не работают из-за природы соединений HTTP.

Пользовательский интерфейс

Изменитесь быстрые пользователи видят

Если у вас есть команда:

```
auth-prompt prompt PIX515B
```

тогда пользователи, проходящие PIX, видят это приглашение.

```
PIX515B
```

Настройте пользователей сообщения, посмотрите

Если у вас есть команды:

```
auth-prompt accept "GOOD_AUTHENTICATION" auth-prompt reject "BAD_AUTHENTICATION"
```

тогда пользователи видят сообщение о статусе проверки подлинности на неудачной/удачной попытке входа.

```
  PIX515B
  Username: junk Password: "BAD_AUTHENTICATION" PIX515B Username: cse Password:
"GOOD_AUTHENTICATION"
```

Простой по числу пользователей и абсолютное время простоя

Команда PIX timeout uauth управляет частотой повторной аутентификации. Если TACACS + аутентификация/авторизация идет, это управляется на основе для каждого пользователя. Этот профиль пользователя установлен для управления таймаутом (это находится на TACACS +, бесплатный сервер и таймауты находятся в минутах).

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

После проверки подлинности/авторизации:

```
show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user 'cse' at
99.99.99.3, authorized to: port 172.18.124.114/telnet absolute timeout: 0:02:00 inactivity
timeout: 0:01:00
```

В конце двух минут:

Абсолютное время ожидания - сеанс разъединен:

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025
   gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
   bytes 7547 (TCP FINs)
```

Исходящий трафик виртуального HTTP

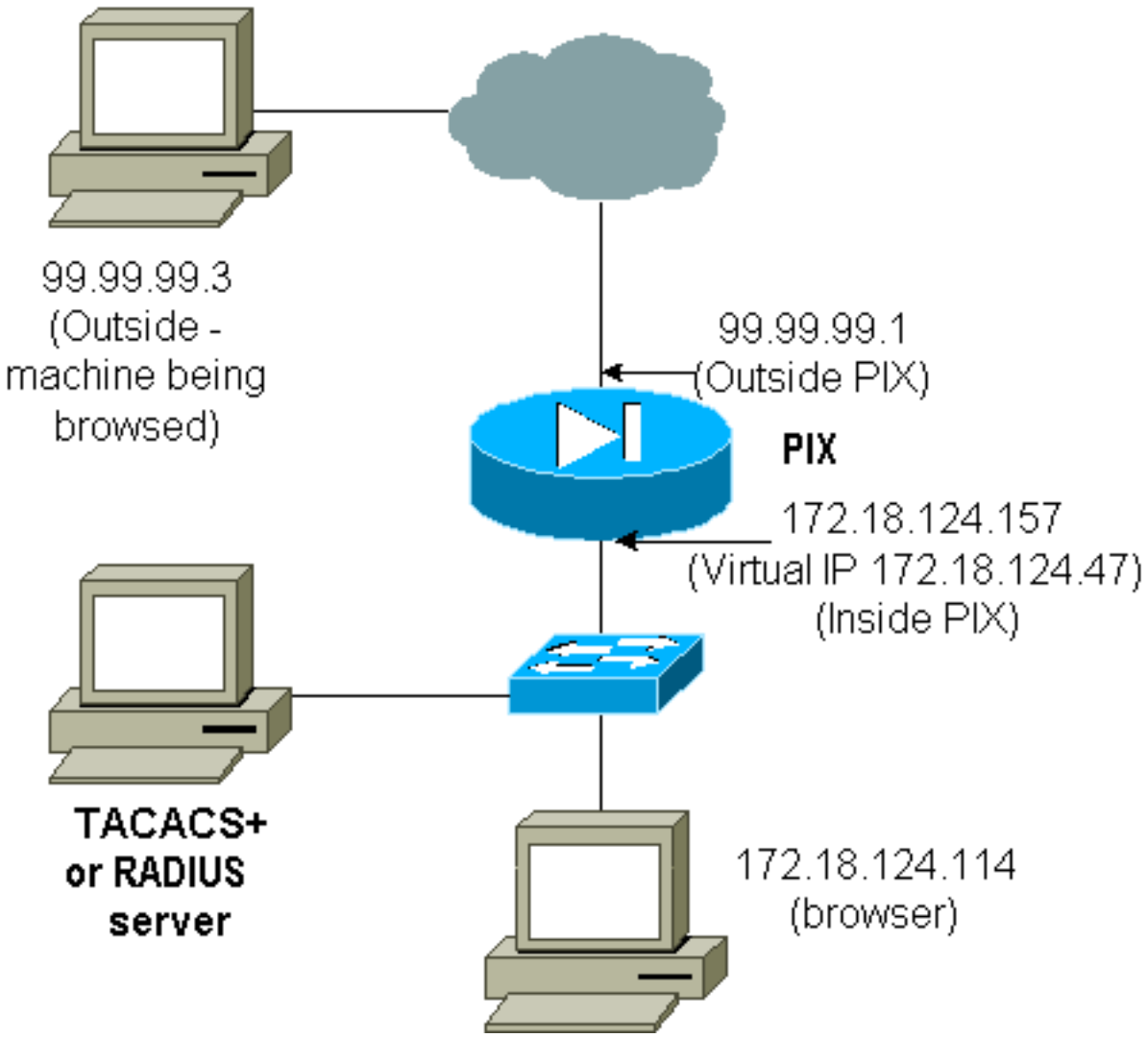
Если аутентификация требуется на узлах вне PIX, а также на самом PIX, необычное поведение обозревателя иногда наблюдается, так как браузеры кэшируют имя пользователя и пароль.

Во избежание этого внедрите действительный HTTP путем добавления адреса RFC 1918 (немаршрутизируемый адрес в Интернете, но допустимый и уникальный для внутренней сети PIX) к конфигурации PIX в формате.

```
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.

Примечание: Действительный HTTP и IP - адреса по виртуальному протоколу Telnet должны быть включены в **операторы aaa authentication**. В данном примере, задавая 0.0.0.0 действительно включает эти адреса.



В конфигурации PIX добавляют эту команду.

```
virtual http 172.18.124.47
```

Пользователь указывает браузер в 99.99.99.3. Это сообщение отображено.

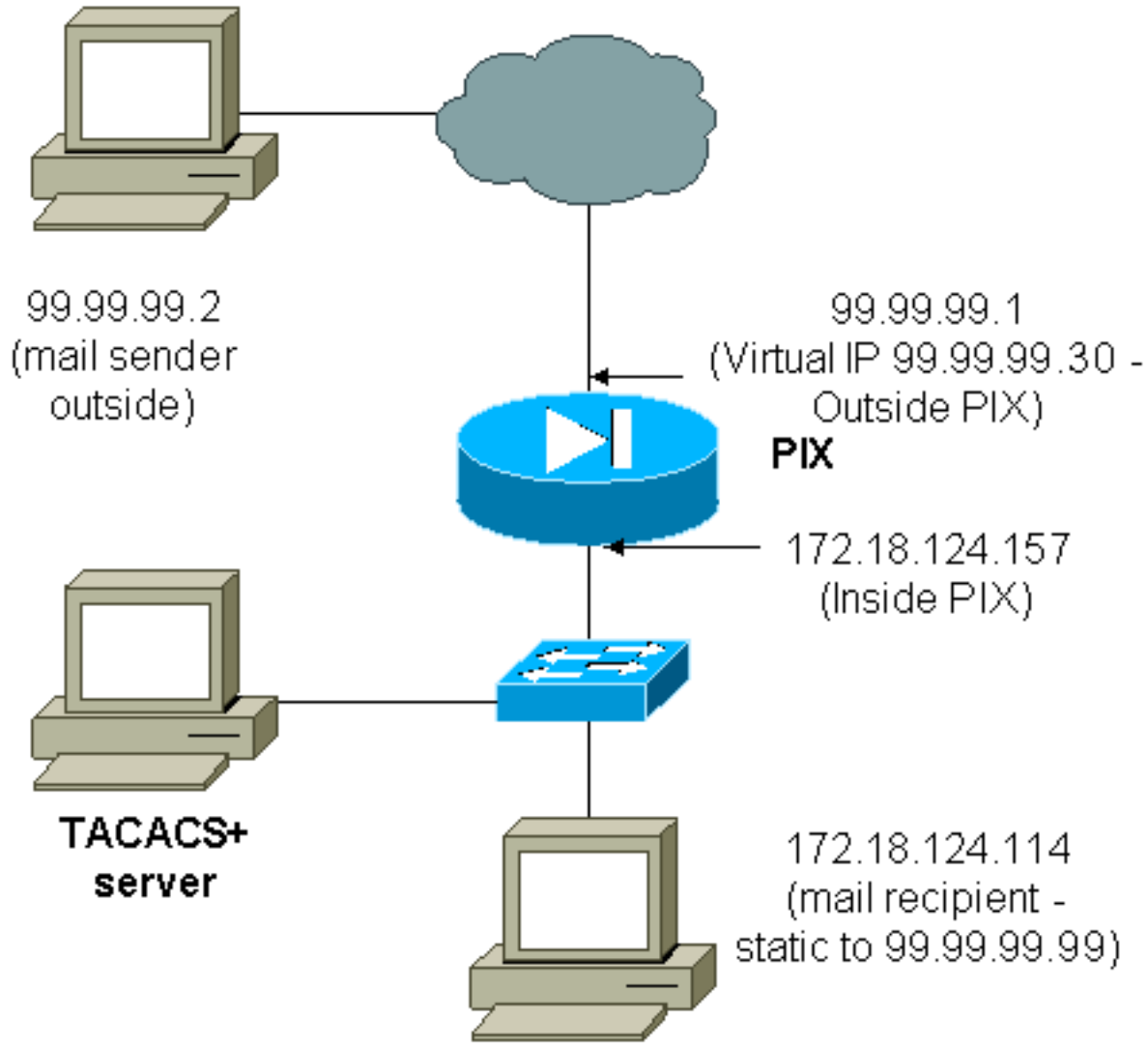
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

После аутентификации трафик перенаправлен к 99.99.99.3.

Виртуальный протокол Telnet

Примечание: Действительный HTTP и IP - адреса по виртуальному протоколу Telnet должны быть включены в **операторы aaa authentication**. В данном примере, задавая 0.0.0.0 действительно включает эти адреса.

Входящие данные протокола Virtual Telnet



Это не хорошая идея для аутентификации почты, входящей, так как окно не отображено для почты, которая будет передаваться входящее. Используйте **команду exclude** вместо этого. Но для цели иллюстрации, добавлены эти команды.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound !--- OR the new
5.2 feature allows these !--- four statements to perform the same function. !--- Note: The old
and new verbiage should not be mixed. access-list 101 permit tcp any any eq smtp !--- The "mail"
```

was a Telnet to port 25. **access-list 101 permit tcp any any eq telnet aaa authentication match 101 outside AuthInbound aaa authorization match 101 outside AuthInbound** ! *!--- plus* ! **virtual telnet 99.99.99.30 static (inside,outside) 99.99.99.30 172.18.124.30 netmask 255.255.255.255 0 0 static (inside,outside) 99.99.99.99 172.18.124.114 netmask 255.255.255.255 0 0 conduit permit tcp host 99.99.99.30 eq telnet any conduit permit tcp host 99.99.99.99 eq telnet any conduit permit tcp host 99.99.99.99 eq smtp any**

Пользователи (это - TACACS + бесплатное программное обеспечение):

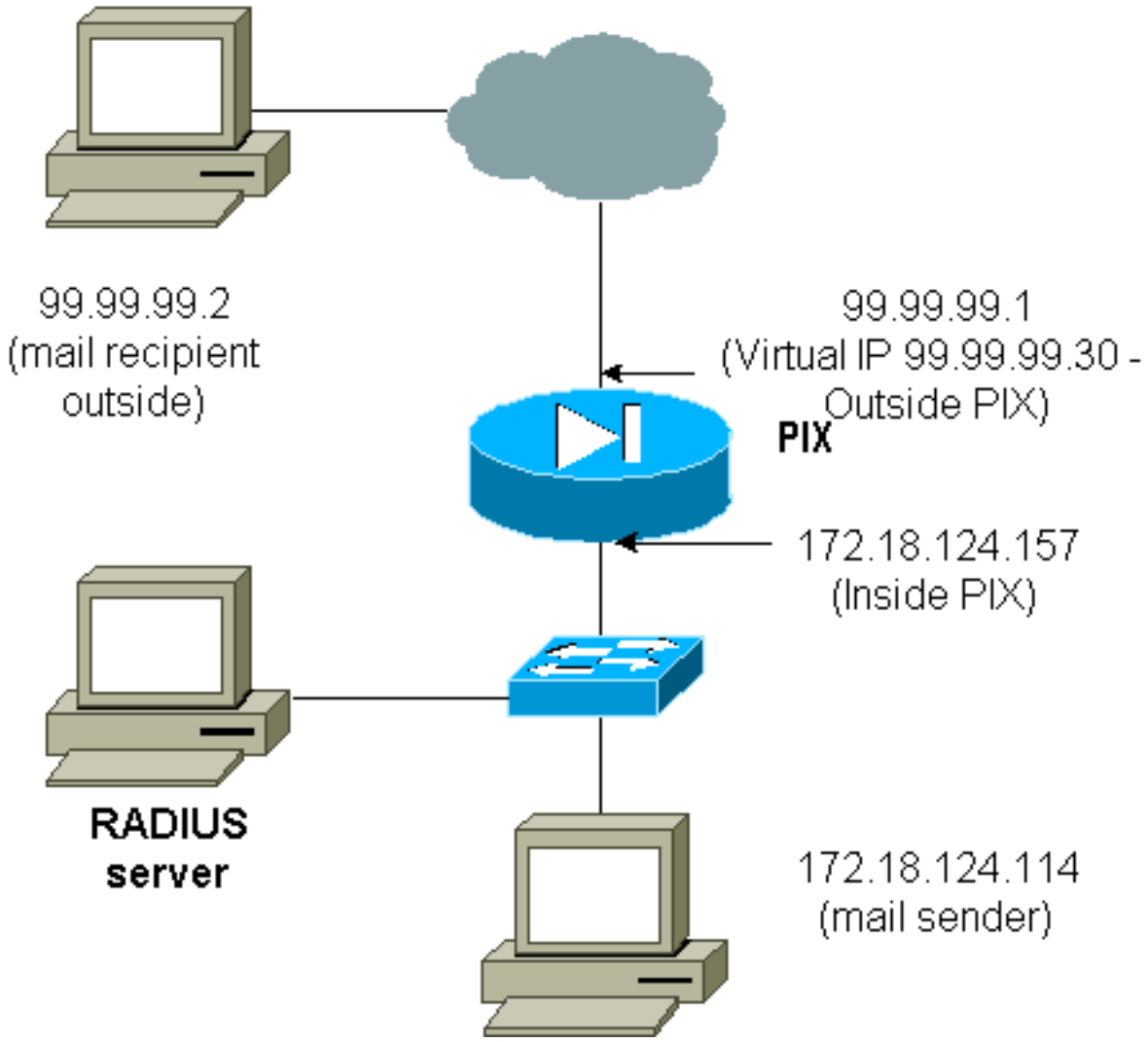
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


  user = pixuser {
  login = cleartext "pixuser"
  service = exec {
  }
  cmd = telnet {
  permit .*
  }
  }
```

Если только аутентификация идет, оба пользователя передают почту, входящую после аутентификации на Telnet к IP-адресу 99.99.99.30. Если авторизация включена, пользовательские Telnet "cse" к 99.99.99.30, и вводит TACACS + имя пользователя/пароль. Отбрасывания Telnet - подключения. Пользователь "cse" тогда передает почту к 99.99.99.99 (172.18.124.114). Аутентификация успешно выполняется для пользователя "pixuser". Однако, когда PIX передает запрос авторизации за cmd=tcp/25 и cmd-arg=172.18.124.114, сбои запроса, как показано в этих выходных данных.

```
109001: Auth start for user '???' from
   99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to
   99.99.99.2/11036 on interface outside
```

```
pixfirewall#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user
'cse' at 99.99.99.2, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11173 to 172.18.124.30/23 109011:
Authen Session Start: user 'cse', sid 10 109005: Authentication succeeded for user 'cse' from
99.99.99.2/23 to 172.18.124.30/11173 on interface outside 109011: Authen Session Start: user
'cse', sid 10 109007: Authorization permitted for user 'cse' from 99.99.99.2/11173 to
172.18.124.30/23 on interface outside 109001: Auth start for user 'cse' from 99.99.99.2/11174 to
172.18.124.114/25 109011: Authen Session Start: user 'cse', sid 10 109007: Authorization
permitted for user 'cse' from 99.99.99.2/11174 to 172.18.124.114/25 on interface outside 302001:
Built inbound TCP connection 5 for faddr 99.99.99.2/11174 gaddr 99.99.99.99/25 laddr
172.18.124.114/25 (cse) pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175 to
172.18.124.30/23 109011: Authen Session Start: user 'pixuser', sid 11 109005: Authentication
succeeded for user 'pixuser' from 99.99.99.2/23 to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11 109007: Authorization permitted for user
'pixuser' from 99.99.99.2/11175 to 172.18.124.30/23 on interface outside 109001: Auth start for
user 'pixuser' from 99.99.99.2/11176 to 172.18.124.114/25 109008: Authorization denied for user
'pixuser' from 99.99.99.2/25 to 172.18.124.114/11176 on interface outside
```

Исходящие данные протокола Virtual Telnet



Это не хорошая идея для аутентификации почты, входящей, так как окно не отображено для почты, которая будет передаваться входящее. Используйте **команду exclude** вместо этого. Но для цели иллюстрации, добавлены эти команды.

Это не хорошая идея для аутентификации почты, исходящей, так как окно не отображено для почты, которая будет передаваться исходящее. Используйте **команду exclude** вместо этого. Но для целей иллюстрации, добавлены эти команды.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound !--- OR
the new 5.2 feature allows these three statements !--- to replace the previous statements. !---
Note: Do not mix the old and new verbiage. access-list 101 permit tcp any any eq smtp access-
list 101 permit tcp any any eq telnet aaa authentication match 101 inside AuthOutbound ! !---
plus ! virtual telnet 99.99.99.30 !--- The IP address on the outside of PIX is not used for
anything else.
```

Для передачи почты изнутри к внешней стороне, переведите командную строку в рабочее состояние на почтовом узле и Telnet к 99.99.99.30. Это открывает дыру для почты для прохождения через. Почта передается от 172.18.124.114 до 99.99.99.2:

```
305002: Translation built for gaddr 99.99.99.99
   to laddr 172.18.124.114
109001: Auth start for user '???' from
   172.18.124.114/32860 to 99.99.99.30/23
109011: Authen Session Start: user 'cse', Sid 14
109005: Authentication succeeded for user 'cse'
   from 172.18.124.114/32860 to    99.99.99.30/23
   on interface inside
```

```
   302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)

pixfirewall#show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'cse' at 172.18.124.114, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

Выход из виртуального сеанса Telnet

Когда пользователи Telnet обращаются к виртуальному IP-адресу Telnet, команда show uauth показывает время, в течение которого "дыра" открыта. Если пользователям нужно предотвратить прохождение трафика после окончания их сеансов (время сохраняется в "uauth"), им необходимо снова подключиться с помощью Telnet к Telnet IP-адресу. В результате этих действий сеанс заканчивается. Это проиллюстрировано данным примером.

Первая аутентификация

```
 109001: Auth start for user '???'
    from 172.18.124.114/32862 to 99.99.99.30/23
 109011: Authen Session Start: user 'cse', Sid 15
 109005: Authentication succeeded for user
    'cse' from 172.18.124.114/32862 to
    99.99.99.30/23 on interface inside
```

После первой аутентификации

```
pixfirewall#show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'cse' at 172.18.124.114, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

Вторая аутентификация

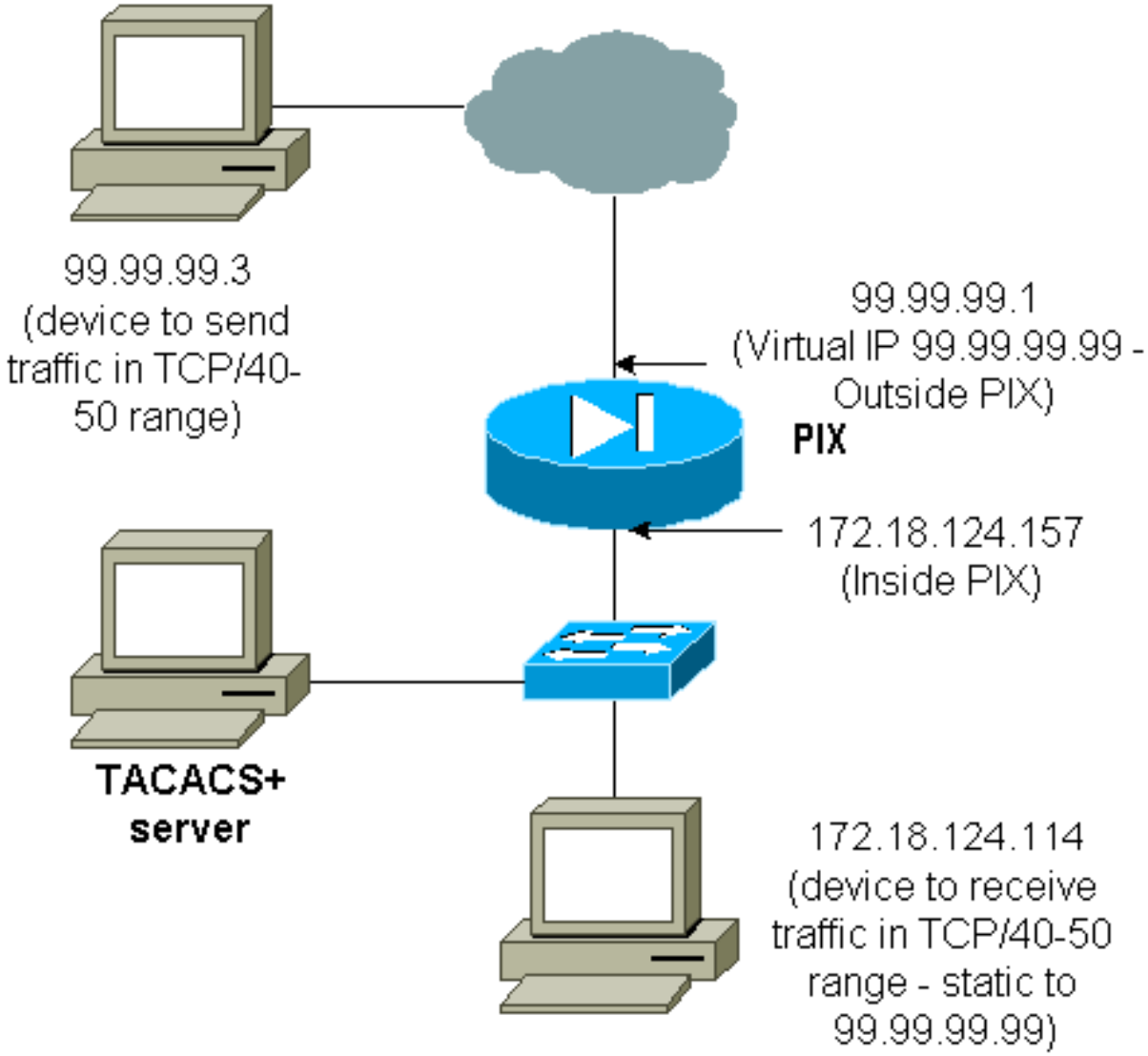
```
   pixfirewall#109001: Auth start for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23
109005: Authentication succeeded for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23 on
interface inside
```

После второй аутентификации

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

Авторизация порта

Схема сети



Для диапазона портов разрешена авторизация. Если виртуальный протокол Telnet настроен на PIX, и авторизация настроена для диапазона портов, пользователь открывает дыру с виртуальным протоколом Telnet. Затем, если авторизация для диапазона портов включена, и трафик в этом диапазоне совпадает с PIX, то PIX посылает команду серверу TACACS+ для авторизации. Данный пример показывает авторизацию для входящих вызовов на диапазоне портов.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound !--- OR the
new 5.2 feature allows these three statements !--- to perform the same function as the previous
two statements. !--- Note: The old and new verbiage should not be mixed. access-list 116 permit
tcp any any range 40 50 aaa authentication match 116 outside AuthInbound aaa authorization match
116 outside AuthInbound ! !--- plus ! static (inside,outside) 99.99.99.99 172.18.124.114 netmask
255.255.255.255 0 0 conduit permit tcp any any virtual telnet 99.99.99.99
```

TACACS + Примеры конфигураций сервера (бесплатное программное обеспечение):

```
user = cse {
login = cleartext "numeric"
cmd = tcp/40-50 {
permit 172.18.124.114
}
}
```

Пользователь сначала должен установить сеанс Telnet с виртуальным IP-адресом 99.99.99.99. После аутентификации, когда пользователь попытки выдвинуть Трафик TCP в

диапазоне порта 40-50 через PIX к 99.99.99.99 (172.18.124.114), cmd=tcp/40-50 передается TACACS + сервер с cmd-arg=172.18.124.114, как проиллюстрировано сюда:

```
109001: Auth start for user '???' from 99.99.99.3/11075
    to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 13
109005: Authentication succeeded for user 'cse'
    from 172.18.124.114/23 to 99.99.99.3/11075
    on interface outside
109001: Auth start for user 'cse' from 99.99.99.3/11077
    to 172.18.124.114/49
109011: Authen Session Start: user 'cse', Sid 13
109007: Authorization permitted for user 'cse'
    from 99.99.99.3/11077 to 172.18.124.114/49
    on interface outside
```

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

После того, как вы удостоверитесь, что виртуальный протокол Telnet работает, чтобы позволить трафик TCP/40-50 хосту в сети, добавить составление этого трафика с этими командами.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound !--- OR the new 5.2 feature allows these !--- two statements to replace the previous statement. !--- Note: Do not mix the old and new verbiage. aaa accounting match 116 outside AuthInbound access-list 116 permit ip any any
```

Пример записей учета TACACS+

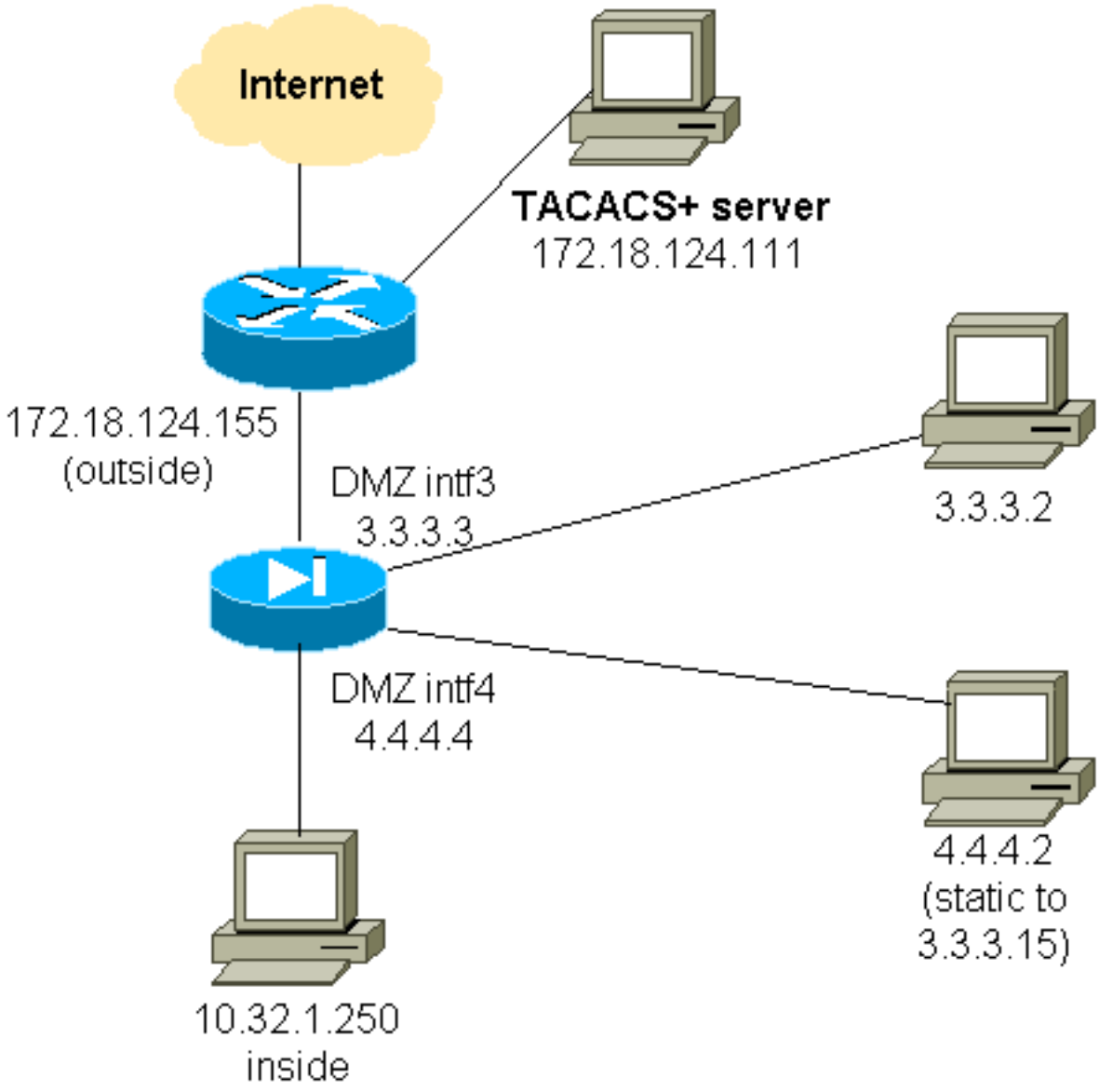
```
   Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
   start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50
   Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
   stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

Аутентификация в демилитаризованной зоне DMZ

Для аутентификации пользователей, которые идут от одного интерфейса DMZ до другого, говорят PIX аутентифицировать трафик для именованных интерфейсов. На PIX расположение походит на это:

```
least secure
PIX outside (security0) = 172.18.124.155
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)
PIX inside (security100) = 10.32.1.250
most secure
```

Схема сети



Частичная конфигурация PIX

Аутентифицируйте трафик Telnet между pix/intf3 и pix/intf4, как продемонстрировано здесь.

Частичная конфигурация PIX
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) interface ethernet0 auto interface ethernet1 auto (interface ethernet2 auto shutdown) interface ethernet3 auto interface ethernet4 auto (interface ethernet5 auto shutdown) ip address outside 172.18.124.155 255.255.255.0 ip address inside 10.32.1.250 255.255.255.0 **ip address pix/intf3 3.3.3.3 255.255.255.0 ip address pix/intf4 4.4.4.4 255.255.255.0 static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask 255.255.255.255 0 0 conduit permit tcp host 3.3.3.15 host 3.3.3.2 aaa-server xway protocol tacacs+ aaa-server**

```
xway (outside) host 172.18.124.111 timeout 5 aaa
authentication include telnet pix/intf4 4.4.4.0
255.255.255.0 3.3.3.0 255.255.255.0 3.3.3.0
255.255.255.0 xway aaa authentication include telnet
pix/intf3 4.4.4.0 255.255.255.0 3.3.3.0 255.255.255.0
3.3.3.0 255.255.255.0 xway !--- OR the new 5.2 feature
allows these four statements !--- to replace the
previous two statements. !--- Note: Do not mix the old
and new verbiage. access-list 103 permit tcp 3.3.3.0
255.255.255.0 4.4.4.0 255.255.255.0 eq telnet access-
list 104 permit tcp 4.4.4.0 255.255.255.0 3.3.3.0
255.255.255.0 eq telnet aaa authentication match 103
pix/intf3 xway aaa authentication match 104 pix/intf4
xway
```

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

Если вы все еще нуждаетесь в помощи после того, чтобы придерживаться действий по устранению проблем выше и хотите открыть случай с Центром технической поддержки Cisco, несомненно, будут включать эту информацию для устранения проблем вашего Межсетевого экрана PIX.

- Описание проблемы и соответствующие сведения о топологии
- Устранение неполадок перед открытием случая
- **Выходные данные команды show tech-support**
- Выходные данные от **команды show log** после выполнения с командой **отладки буферированной регистрации** или снимками консоли, которые демонстрируют проблему (при наличии)

Присоедините собранные данные к запросу в простом текстовом формате (.txt), не архивируя файл. Информация о присоединении к вашему случаю путем загрузки его с помощью Программного средства Case Query (только зарегистрированные клиенты). Если вы неспособны обратиться к Программному средству Case Query, передайте информацию во вложении электронной почты к attach@cisco.com с вашим номером заявки в строке темы вашего сообщения.

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Secure Access Control Server for Windows
- Cisco Secure Access Control Server for Unix

- Terminal Access Controller Access Control System (TACACS+)
- Служба удаленной аутентификации пользователей коммутируемого доступа (RADIUS)
- Cisco Systems – техническая поддержка и документация