Как провести аутентификацию и включение на межсетевом экране Cisco Secure PIX (версии с 5.2 до 6.2)

Содержание

Введение

В этом документе поясняется настройка доступа с аутентификацией AAA на межсетевом экране PIX, работающем под управлением версии ПО PIX 5.2 до 6.2, а также описывается

включение аутентификации, ведение системного журнала и получение доступа, при неработающем сервере AAA (проверка подлинности, авторизация и учет). В PIX 5.3 и более поздних версий аутентификация, авторизация и учет (AAA) были изменены; в новых версиях порты RADIUS можно настраивать.

Программное обеспечение PIX версии 5.2 и более поздней предусматривает создание прав доступа к PIX с аутентификацией AAA пятью различными способами:

- Аутентификация Telnet - внутренний интерфейс
- Аутентификация порта консоли
- Проверенный клиент Cisco Secure VPN Client 1.1 - внешний
- VPN - соединение с аутентификацией 3000 2.5 - снаружи
- Аутентифицированный протокол Secure Shell (SSH) - Внутри или снаружи

Примечание: DES или 3DES должен быть включен на PIX (выдайте команду show version для подтверждения) для последних 3 методов. В версии ПО PIX 6.0 и более поздних, можно также загрузить PIX Device Manager (PDM) для того, чтобы включить управление GUI. Вопрос о PDM выходит за рамки этого документа.

Для получения дополнительной информации о команде проверки подлинности и авторизация для PIX 6.2, обратитесь к PIX 6.2: Пример настройки команды проверки подлинности и авторизация.

Для создания АУТЕНТИФИЦИРУЕМЫЙ НА AAA (Сквозной Прокси) обращаются к Межсетевому экрану PIX, который выполняет Версии ПО PIX 6.3 и позже, обратитесь к PIX/ASA: Пример настройки сетевого доступа через Cut-through прокси с использованием серверов проверки подлинности TACACS+ и RADIUS.

Предварительные условия

Требования

Выполните эти задачи перед добавлением аутентификации AAA (проверка подлинности, авторизация и учет):

- Выполните эти команды для добавления пароля для PIX:**passwd wwtelnet <local_ip> [<mask>] [<if_name>]**PIX автоматически шифрует этот пароль для формирования зашифрованной строки с **зашифрованным** ключевым словом, как в данном примере:`passwd OnTrBUG1Tp0edmkr encrypted` **Добавление зашифрованного ключевого слова необязательно.**
- Удостоверьтесь, что вы можете Telnet от внутренней сети до внутреннего интерфейса PIX *без* аутентификации AAA (проверка подлинности, авторизация и учет) после добавления этих операторов.
- Всегда имейте соединение, открытое для PIX, в то время как вы добавляете объявления проверки подлинности, если отступление команды необходимо.

На аутентификации AAA (проверка подлинности, авторизация и учет) (кроме SSH, где последовательность зависит от клиента), пользователь видит запрос о пароле PIX (как в *passwd <вообще>*), затем запрос об Имени пользователя и пароль RADIUS или TACACS.

Примечание: Вы не можете Telnet к внешнему интерфейсу PIX. SSH может использоваться на внешнем интерфейсе, если связано от внешнего Клиента SSH.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия ПО PIX 5.2, 5.3, 6.0, 6.1, или 6.2
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client 2.5
- Cisco VPN Client 3.0.x (требуемый код PIX 6.0)

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.

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 Проверка подлинности RADIUS и порты учета могут быть изменены на кроме по умолчанию 1645/1646 с этими командами:

aaa-server radius-authport #

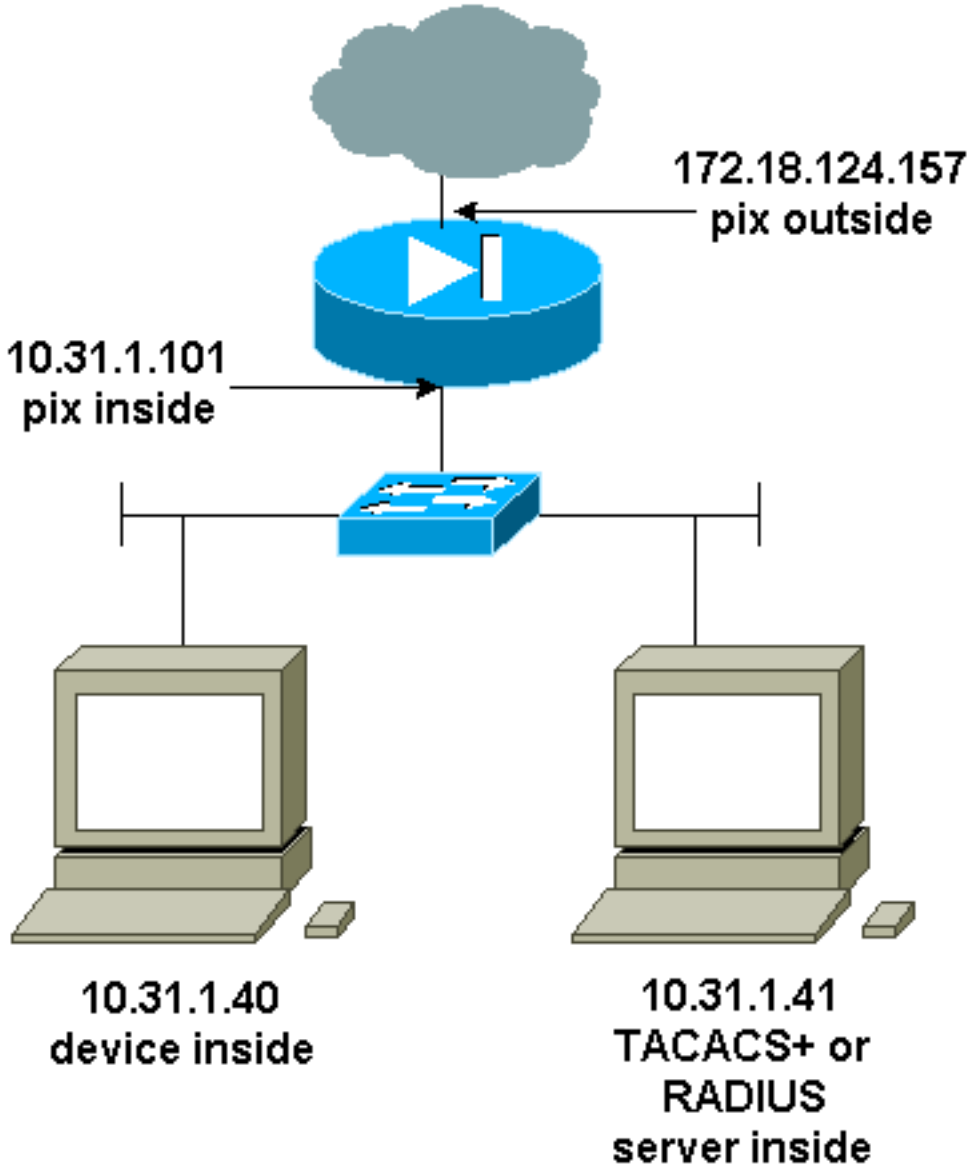
aaa-server radius-acctport #

Условные обозначения

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

Аутентификация Telnet - внутренний интерфейс

Схема сети



Команды, добавленные к конфигурации PIX

Добавьте эти команды к своей конфигурации:

aaa-server topix protocol tacacs +

aaa-server topix host 10.31.1.41 таймаута Cisco 5

TOPIX Telnet-консоля аутентификации AAA

Пользователь видит запрос о пароле PIX (как в `passwd <whatever>`), и затем запрос об Имени пользователя и пароль RADIUS или TACACS (сохраненный на 10.31.1.41 TACACS или сервере RADIUS).

Аутентификация порта консоли

Добавьте эти команды к своей конфигурации:

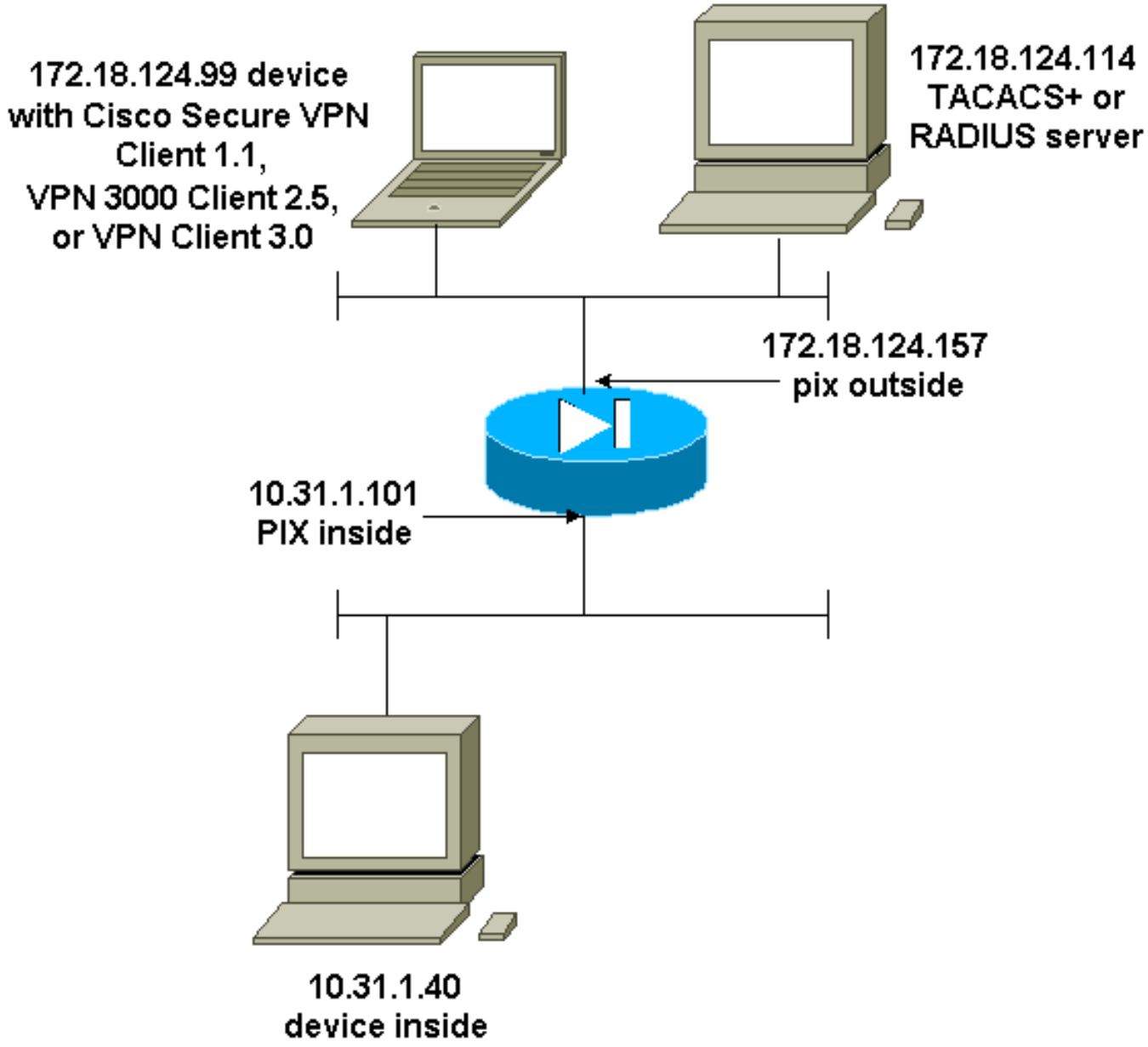
aaa-server topix protocol tacacs +

aaa-server topix host 10.31.1.41 таймаута Cisco 5

последовательная консоль аутентификации AAA Topix

Пользователь видит запрос о пароле PIX (как в `passwd <whatever>`), затем запрос об имени пользователя/пароле RADIUS/TACACS (сохраненный на RADIUS или TACACS 10.31.1.41 сервера).

Диаграмма - VPN Client 1.1, VPN 3000 2.5 или VPN Client 3.0 - внешний



Проверенный клиент Cisco Secure VPN Client 1.1 - внешний

Проверенный клиент Cisco Secure VPN Client 1.1 - Внешний - Конфигурация клиента
1- Myconn My Identity Connection security: Secure Remote Party Identity and addressing ID Type: IP address Port all Protocol all Pre-shared key (matches that on PIX)

```
    Connect using secure tunnel
         ID Type: IP address
         172.18.124.157

    Authentication (Phase 1)
    Proposal 1

        Authentication method: Preshared key
        Encryp Alg: DES
        Hash Alg: MD5
        SA life:  Unspecified
        Key Group: DH 1

    Key exchange (Phase 2)
    Proposal 1
        Encapsulation ESP
        Encrypt Alg: DES
        Hash Alg: MD5
        Encap: tunnel
        SA life: Unspecified
        no AH

 2- Other Connections
       Connection security: Non-secure
       Local Network Interface
         Name: Any
         IP Addr: Any
         Port: All
```

Авторизованный клиент Cisco Secure VPN версии 1.1 - внешний - частичная конфигурация PIX

```
ip address outside 172.18.124.157 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
!--- If you know the IP address of the outside client,
use that !--- IP address in this statement. isakmp key
******** address 0.0.0.0 netmask 0.0.0.0 ! isakmp
identity address isakmp policy 10 authentication pre-
share isakmp policy 10 encryption des isakmp policy 10
hash md5 isakmp policy 10 group 1 isakmp policy 10
lifetime 86400 !--- We knew our client would access the
PIX from this !--- network. If you know the IP address
of the client, use that IP address !--- in this
statement. telnet 172.18.124.0 255.255.255.0 outside
```

Авторизованный VPN 3000 2.5 или VPN Client 3.0 - внешний

Авторизованный VPN 3000 2.5 или VPN Client 3.0 – внешний – конфигурация клиента

1. Выберите **VPN Dialer> Properties> Name соединение** от VPN 3000.

2. Выберите **Authentication> Group Access Information**. Имя группы и пароль должны совпасть с тем, что находится на PIX в **vpngroup** *<group_name>* **пароль** ******** оператор.

Когда нажимается кнопка Connect, запускается зашифрованный туннель и PIX присваивает IP-адрес из тестового пула (клиентом VPN 3000 поддерживается только режим настройки). Затем можно извлечь окно терминала, получить сетевой теледоступ к 172.18.124.157 и пройти аутентификацию AAA. **Команда telnet 192.168.1.x на PIX позволяет пользователям в пуле подключаться к внешнему интерфейсу.**

VPN - соединение с аутентификацией 3000 2.5 - снаружи - частичная конфигурация PIX

```
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.31.1.101 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
!!--- ISAKMP Policy for VPN 3000 Client runs 2.5 code.
isakmp policy 10 authentication pre-share isakmp policy
10 encryption des isakmp policy 10 hash md5 !--- The 2.5
client uses group 1 policy (PIX default). isakmp policy
10 group 1 isakmp policy 10 lifetime 86400 !--- ISAKMP
Policy for VPN Client runs 3.0 code. isakmp policy 20
authentication pre-share isakmp policy 20 encryption des
isakmp policy 20 hash md5 !--- The 3.0 clients use D-H
group 2 policy and require PIX 6.0 code. isakmp policy
20 group 2 isakmp policy 20 lifetime 86400 ! vpngroup
vpn3000 address-pool test vpngroup vpn3000 idle-time
1800 vpngroup vpn3000 password ******** telnet
192.168.1.0 255.255.255.0 outside
```

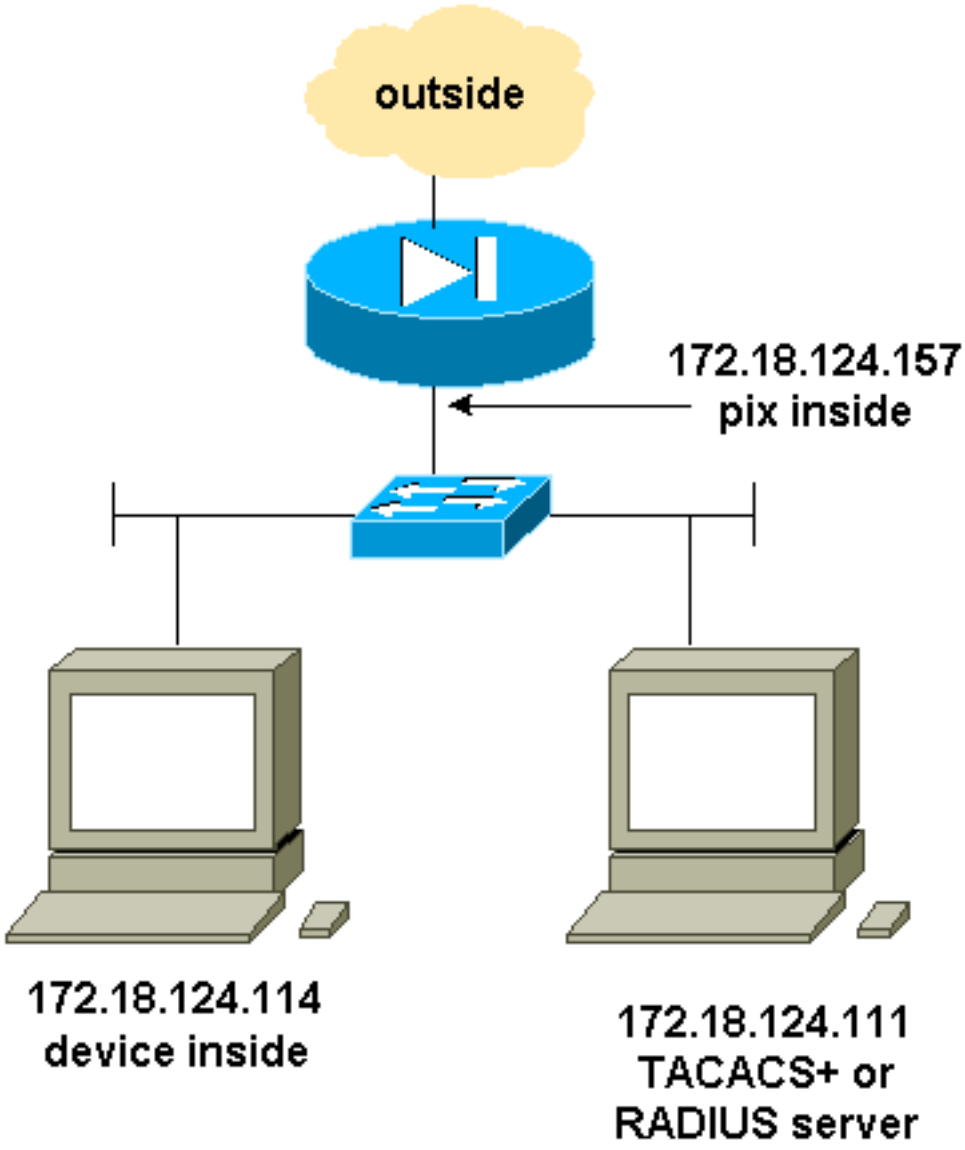
SSH - внутренний или внешний интерфейс

В PIX 5.2 была добавлена поддержка протокола Secure Shell (SSH) 1-й версии. Протокол SSH-1 основан на проекте группы IETF от ноября 1995 г. Версия SSH 1 и 2 не совместима друг с другом. См. Часто задаваемые вопросы Secure Shell (SSH) для получения дополнительной информации о SSH.

PIX считается SSH-сервером. Трафик от SSH-клиентов (устройств, использующих протокол SSH) к SSH-серверу (PIX) зашифрован. Некоторые SSH-1 клиенты перечислены в сопроводительных документах к PIX 5.2. Проверки в нашей лаборатории выполнялись с использованием F-secure SSH 1.1 на NT и версии 1.2.26 для Solaris.

Примечание: Для PIX 7.x, обратитесь к разделу Доступа SSH Разрешения Управляющего Системного доступа.

Схема сети



Настройте SSH удостоверенный AAA (проверка подлинности, авторизация и учет)

Выполните эти шаги для настройки SSH удостоверенного AAA (проверка подлинности, авторизация и учет):

1. Убедитесь, что возможно telnet-соединение с PIX с включенным AAA, но без SSH:`aaa-server AuthOutbound protocol radius (or tacacs+)`
   `aaa authentication telnet console AuthOutbound`
   `aaa-server AuthOutbound host 172.18.124.111 cisco` **Примечание:** Когда SSH настроен, **команда telnet 172.18.124.114 255.255.255.255** не необходима, потому что **ssh 172.18.124.114 255.255.255.255 внутри** выполнен на PIX. Обе команды включенны для целей тестирования.
2. Добавьте SSH с помощью этих команд:`hostname goss-d3-pix515b`
   `domain-name rtp.cisco.com`
   `ca gen rsa key 1024`*!--- **Caution:** The RSA key is not be saved without !--- the **ca save all** command. !--- The **write mem** command does not save it. !--- In addition, if the PIX has undergone a **write erase** !--- or has been replaced, then cutting and pasting !--- the old configuration does not generate the key. !--- You must re-enter the **ca gen rsa key** command. !--- If there is a secondary PIX in a failover pair, the **write standby** !--- command does*

not copy the key from the primary to the secondary. !--- You must also generate and save the key on the secondary device. ssh 172.18.124.114 255.255.255.255 inside ssh timeout 60 aaa authen ssh console AuthOutbound logging trap debug logging console debug

3. **Введите команду show ca mypubkey rsa в режиме настройки.**goss-d3-pix(config)#**show ca mypubkey rsa** % Key pair was generated at: 08:22:25 Aug 14 2000 Key name: goss-d3-pix.rtp.cisco.com Usage: General Purpose Key Key Data: 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ad4bcb e9c174d5 0657a0f3 c94e4b6d 32ac8500 6b84e754 59e20df4 f28c257d 131af21d 4c0a8f4c e79d8b6d a3520faa 1a42d577 c6adfe51 9d96fa62 f3be07fb 01e082d7 133cecff bf24f653 bc690b11 ee222070 413c1920 d02321f8 4fc3c5f1 f0c6e077 81e93184 af55438b dcdcda34 c0a5f5ad 87c435ef 67170674 4d5ba51e 6d020301 0001 % Key pair was generated at: 08:27:18 Aug 14 2000 Key name: goss-d3-pix.rtp.cisco.com.server Usage: Encryption Key Key Data: 307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00d4f61b ec45843a 4ad9266d b125ee26 efc63cc4 e5e9cda4 9418ee53 6e4d16cf 3d0dc864 4d4830c8 fa7f110e 8a5761ed 4ca73ea7 5d405862 6f3150df 9eb0d11e 9c4d3563 95ff51ae 6711d60b 9a1415e4 19201d3f 03b455ea c1df9a41 b3a5a73f 4f020301 0001
4. Попробуйте Telnet от станции Solaris:rtp-evergreen#**./ssh -c 3des -l cisco -v 172.18.124.157** **Примечание:** "cisco" – это имя пользователя на сервере RADIUS/TACACS+, а 172.18.124.157 – пункт назначения.

Настройте локальный SSH (никакая аутентификация AAA (проверка подлинности, авторизация и учет))

Также возможно установить SSH - подключение к PIX с локальной проверкой подлинности и никаким AAA-сервером. Однако нет никакого отдельного имени пользователя для каждого пользователя. Имя пользователя всегда имеет значение "pix"."

Используйте эти команды для настройки локального SSH на PIX:

```
hostname goss-d3-pix515b
domain-name rtp.cisco.com
ca gen rsa key 1024!--- Caution: The RSA key is not saved without !--- the ca save all command. !--- The write mem command does not save it. !--- In addition, if the PIX has undergone a write erase !--- or has been replaced, then cutting and pasting !--- the old configuration does not generate the key. !--- You must re-enter the ca gen rsa key command. !--- If there is a secondary PIX in a failover pair, a write standby !--- command does not copy the key from the primary to the secondary. !--- You must also generate and save the key on the secondary device.
ssh 172.18.124.114 255.255.255.255 inside ssh timeout 60 passwd cisco123
```

Поскольку имя пользователя по умолчанию в этом расположении всегда "pix", то команда для подключения к PIX (использовался 3DES из Solaris box) будет следующей:

```
./ssh -c 3des -1 pix -v <ip_of_pix>
```

Отладка SSH

Отладка без команды debug ssh - 3DES и с 512 шифрами

```
109005: Authentication succeeded for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
109011: Authen Session Start: user 'cse', sid 0
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
315011: SSH session from 172.18.124.114 on interface inside
   for user "cse" terminated normally
```

Отладка с командой debug ssh - 3DES и с 512 шифрами

```
goss-d3-pix#debug ssh SSH debugging on goss-d3-pix# Device opened successfully. SSH: host key initialised. SSH: SSH client: IP = '172.18.124.114' interface # = 1 SSH1: starting SSH control process SSH1: Exchanging versions - SSH-1.5-Cisco-1.25 SSH1: client version is - SSH-1.5-1.2.26
```

```
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c SSH1: SSH_SMSG_PUBLIC_KEY message
sent SSH1: SSH_CMSG_SESSION_KEY message received - msg type 0x03, length 112 SSH1: client
requests 3DES cipher: 3 SSH1: keys exchanged and encryption on SSH1: authentication request for
userid cse SSH(cse): user authen method is 'use AAA', aaa server group ID = 3 SSH(cse): starting
user authentication request, and waiting for reply from AAA server SSH(cse): user 'cse' is
authenticated SSH(cse): user authentication request completed SSH1: authentication successful
for cse109005: SSH1: starting exec shellAuthentication succeeded for user 'cse' from 0.0.0.0/0
to 172.18.124.114/0 on interface SSH 315002: Permitted SSH session from 172.18.124.114 on
interface inside for user "cse"
```

Отладка - 3DES и с 1024 шифрами

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

Отладка - DES и с 1024 шифрами

Примечание: Эти выходные данные получены на ПК с SSH, а не Solaris.

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.99' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-W1.0
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests DES cipher: 2
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid ssh
SSH(ssh): user authen method is 'use AAA', aaa server group ID = 4
SSH(ssh): starting user authentication request,
   and waiting for reply from AAA server
SSH(ssh): user 'ssh' is authenticated
SSH(ssh): user authentication request completed
SSH0: authentication successful for ssh109
SSH0: invalid request - 0x2500
SSH0: starting exec shell5: Authentication succeeded for user 'ssh'
   from 0.0.0.0/0 to 172.18.124.99/0 on interface SSH
109011: Authen Session Start: user 'ssh', sid 1
315002: Permitted SSH session from 172.18.124.99 on interface outside
   for user "ssh"
```

Отладка - 3DES и с 2048 шифрами

Примечание: Эти выходные данные получены на ПК с SSH, а не Solaris.

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3.
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse10900
SSH1: invalid request - 0x255:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
109011: Authen Session Start: user 'cse', Sid 2
315002: Permitted SSH session from 161.44.17.151 on interface inside
   for user "cse"
```

Возможные проблемы

Отладка Solaris - с 2048 шифрами и SSH Solaris

Примечание: Solaris не может обработать 2048-шифр.

```
rtp-evergreen.cisco.com: Initializing random;
seed file /export/home/cse/.ssh/random_seed
RSA key has too many bits for RSAREF to handle (max 1024).
```

Неверный пароль или имя пользователя на сервере RADIUS/TACACS+

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA serverss-d3-pix#
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH1: password authentication failed for cse
109006: Authentication failed for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
```

Доступ пользователя запрещается следующей командой:

ssh 172.18.124.114 255.255.255.255 inside

Попытки соединиться:

315001: Запрещенный сеанс SSH из 161.44.17.151 на внутренний интерфейс

Если ключ удален из PIX (командой ca zero rsa) или не сохранен командой ca save all

```
Device opened successfully.
SSH: unable to retrieve host public key for 'goss-d3-pix.rtp.cisco.com',
   terminate SSH connection.
SSH-2145462416: Session disconnected by SSH server - error 0x00 "Internal error"
315004: Fail to establish SSH session because PIX RSA host key retrieval failed.
315011: SSH session from 0.0.0.0 on interface outside for user ""
   disconnected by SSH server, reason: "Internal error" (0x00)
```

AAA-сервер не работает:

```
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH0: SSH_SMSG_PUBLIC_KEY message sent302010: 0 in use, 0 most used
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests 3DES cipher: 3
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server1090
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH0: password authentication failed for cse0
SSH0: authentication failed for cse
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
2: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109006: Authentication failed for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
315003: SSH login session failed from 172.18.124.114 (1 attempts)
   on interface outside by user "cse"
315011: SSH session from 172.18.124.114 on interface outside for user "cse"
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
109012: Authen Session End: user 'cse', Sid 0, elapsed 352 seconds
```

Клиент устанавливается для 3DES, но в PIX есть только ключ DES:

Примечание: Клиентом был Solaris, не поддерживающий DES.

```
GOSS-PIX# Device opened successfully.
SSH: host key initialised
SSH: license supports DES: 1.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
```

```
315011: SSH session from 172.18.124.114 on interface outside for user ""
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
```

и на нашем CLI Solaris:

```
Selected cipher type 3DES not supported by server.
```

Удаление ключа RSA из частного обмена данными через Internet

ca zero rsa

Как сохранить RSA-ключ в PIX

ca save all

Как разрешить безопасный командный процессор (SSH) из внешнего клиента SSH

ssh outside_ip 255.255.255.255 outside

Включение аутентификации

С помощью команды:

aaa authentication включает консоль Topix

(где topix — список упомянутых серверов) пользователю предлагается ввести имя пользователя и пароль, которые оправляются на сервер TACACS или RADIUS. Поскольку пакет аутентификации для включения представляет собой то же, что и пакет аутентификации для входа, если пользователь может войти в PIX с аутентификацией TACACS или RADIUS, он также может выполнить включение с помощью аутентификации TACACS или RADIUS с тем же именем пользователя и паролем.

Дополнительные сведения об этих проблемах доступны в идентификаторе ошибки Cisco CSCdm47044 (только зарегистрированные клиенты).

Информация о Syslogg

Пока учет по схеме AAA действителен только для соединений, идущих через PIX, а не к PIX, если настроен учет на syslog-сервере, то информация о действиях аутентифицированного пользователя отправляется на syslog-сервер (и на сервер управления сетью, если он настроен, через базу данных MIB для syslog).

Если запись в системный журнал установлена, то сообщения, такие как они отображены в сервере системного журнала:

Уровень уведомления о прерывании регистрации:

```
111006: Console Login from pixuser at console
111007: Begin configuration: 10.31.1.40 reading from terminal
111008: User 'pixuser' executed the 'conf' command.
111008: User 'pixuser' executed the 'hostname' command.
```

Запись нформационного уровня ловушки (который включает уровень уведомления):

307002: Permitted Telnet login session from 10.31.1.40 (Разрешен сеанс входа в Telnet из 10.31.1.40)

Получение доступа, когда сервер AAA (проверки подлинности, авторизации и учета) не функционирует

Если AAA-сервер не работает, можно войти, Пароль Telnet обращаются к PIX первоначально, то **производят пробу монет** для имени пользователя, и затем enable password (**enable password** *вообще*) для пароля. *Если разрешающего пароля нет в конфигурации PIX, введите имя пользователя "pix" и нажмите клавишу Enter*. Если enable password установлен, но не известен, вам нужен диск для восстановления пароля для изменения пароля.

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 следующую информацию.
• Описание проблемы и соответствующие сведения о топологии • Меры по устранению неполадок, предпринятые до оформления запроса • **Выходные данные команды show tech-support** • **Выходные данные команды show log после выполнения команды logging buffered debugging или снимки консоли, демонстрирующие проблему (при их наличии)** Приложите собранные сведения по вашей ситуации в простом незаархивированном текстовом файле (.txt). Можно приложить эти сведения, загрузив их с помощью средства Case Query Tool (только для зарегистрированных клиентов). Если средство Case Query недоступно, необходимые данные можно отправить как вложение в электронное сообщение по адресу attach@cisco.com, указав в теме сообщения номер обращения.

Дополнительные сведения

- Справочники по командам для межсетевого экрана PIX Cisco Secure
- PIX RADIUS TACACS +
- Запросы комментариев (RFC)

- Cisco Systems – техническая поддержка и документация