

Восстановление пароля Cisco PIX

Вступление

В данном документе описывается, как восстановить пароль Cisco PIX для программного обеспечения PIX версии 7.0.

Примечание: В данном примере описан метод, который позволит стереть только пароль для Cisco PIX, не затрагивая конфигурацию. Если версия ПО на Cisco PIX 6.2 и ниже, то команда **aaa authentication** на консоли или в сессии Telnet так же предложит стереть конфигурацию.

Примечание: Если вы настроили AAA на Cisco Pix Firewall и сервер AAA недоступен, то вы можете ввести пароль для Cisco PIX руками, а затем войти в привилегированный режим, используя имя пользователя **pix** и пароль **password**. Если пароль не был задан в конфигурации, то введите имя пользователя **pix** и нажмите Enter. Если данные пара логин/пароль не подойдут, то воспользуйтесь шагами, которые будут описаны ниже.

Программное обеспечение PIX Password Lockout Utility базируется на версии ПО Cisco PIX, которое у вас есть. Используйте команду **show version** для определения своей версии PIX/ASA Security appliance.

Примечание: Процедура сброса пароля для Cisco ASA 5500 Series Adaptive Security Appliance описана на сайте производителя по ссылке [Performing Password Recovery for the ASA 5500 Series Adaptive Security Appliance](#).

Используемые компоненты

Информация, представленная в данном документе, основана на использовании следующего:

- Компьютер
- Работоспособный терминал линии либо его эмулятор
- Возможность отключить Cisco PIX от сети на 10 минут

Примечание: Вам потребуется не менее 10 минут, во время которых Cisco PIX не будет полноценно функционировать, иными словами трафик через него проходить не будет. .

Вам потребуется утилита PIX Password Lockout Utility для восстановления пароля Cisco PIX, включая следующие файлы:

- Файл нужно выбрать исходя из версии ПО на вашем Cisco PIX:

[np70.bin](#) (релиз 7.x и 8.0)

[np63.bin](#) (6.3 релиз)

[np62.bin](#) (6.2 релиз)

[np61.bin](#) (6.1 релиз)

[np60.bin](#) (6.0 релиз)

[np53.bin](#) (5.3 релиз)

[np52.bin](#) (5.2 релиз)

[np51.bin](#) (5.1 релиз)

[np50.bin](#) (5.0 релиз)

[np44.bin](#) (4.4 релиз)

[nppix.bin](#) (4.3 и более поздние релизы)

- [rawrite.exe](#) (данная утилита cisco необходима только для Cisco PIX с floppy драйвом)

- TFTP сервер (нужен в случае, если Cisco PIX без floppy драйва) — TFTP сервер с некоторых пор не доступен для загрузки с сайта Cisco.com, но вы сможете найти его используя фразу "tftp server" в различных поисковых системах. Компания Cisco не предъявляет требований к вариациям TFTP сервера.

Пошаговая инструкция

- Для Cisco PIX с Floppy приводом

Выполните следующие шаги для восстановления пароля Cisco PIX:

1. Запустите утилиту **rawrite.exe** на вашем ПК и следуйте инструкциям мастера.
2. Установите серийный терминал или эмулятор терминала на вашем ПК для подключения к консольному порту Cisco PIX.
3. Проверьте, что установилась связь между терминалом и Cisco PIX (нажмите пару любых клавиш).

Примечание: Так как пароля вы не знаете, то вам будет доступен только диалог на ввод пароля.

4. Вставьте диск Cisco PIX Password Lockout Utility disk в floppy драйв Cisco PIX.
5. Нажмите кнопку **Reset** на передней панели Cisco PIX. Оборудование Cisco PIX перезагрузится с floppy и выдаст следующее сообщение:

```
Erasing Flash Password. Please eject diskette  
and reboot.
```

6. Выньте диск из дисководов floppy и нажмите снова кнопку **Reset** на передней панели. Теперь вы сможете зайти на Cisco PIX без пароля. Нажмите клавишу **ENTER** при запросе пароля.
7. По умолчанию для Telnet сессии пароль "cisco" (без кавычек). Пароля для enable по умолчанию нет. Перейдите в режим конфигурирования и выполните команду **passwd ваш_Telnet_пароль** для смены пароля Telnet и команду **enable password**

ваш_пароль_enable для смены соответственно пароля enable, после чего сохраните конфигурацию.

- Для Cisco PIX без Floppy дисководов

Выполните следующие шаги для восстановления пароля Cisco PIX:

1. Установите серийный терминал или эмулятор терминала на вашем ПК для подключения к консольному порту Cisco PIX.
2. Проверьте, что установилась связь между терминалом и Cisco PIX (нажмите пару любых клавиш).

Примечание: Так как пароля вы не знаете, то вам будет доступен только диалог на ввод пароля.

3. Выключите Cisco PIX.
4. Включите Cisco PIX и сразу же, после того как будет загружаться ПО Cisco PIX Firewall и появится окно начальной инициализации, нажимайте клавишу **BREAK** или клавишу **ESC**. Если вы всё сделали правильно, то появится приглашение `monitor>`. Если необходимо, то можно нажать? (знак вопроса) для просмотра доступных команд.
5. Используйте команду **interface** для определения интерфейса, через который будет проходить ping (icmp) трафик. Cisco PIX с floppy имеет только два интерфейса, и в режиме **monitor** по умолчанию используется внутренний интерфейс.
6. Используйте команду **address** для задания IP адреса для интерфейса PIX Firewall.
7. Команда **server** задает IP адрес удалённого TFTP сервера, который содержит файл для восстановления пароля Cisco PIX.
8. Командой **file** нужно задать имя файла для восстановления пароля Cisco PIX. К примеру для релиза 5.1 файл будет называться **np51.bin**.
9. Если TFTP сервер находится в подсети, отличной от той в которой находится Cisco PIX, то соответственно нужно указать шлюз. Делается это командой **gateway** – задаём IP адрес шлюза, через который можно попасть в подсеть, где находится удалённый TFTP сервер.
10. При необходимости воспользуйтесь командой **ping** для проверки связи между Cisco PIX и TFTP сервером. Если пинги не проходят, то нужно локализовать проблему и только после этого приступить к процедуре восстановления пароля Cisco PIX.
11. Используйте команду **tftp** для начала загрузки файла восстановления пароля Cisco PIX.
12. После того, как файл будет загружен на Cisco PIX появится сообщение:

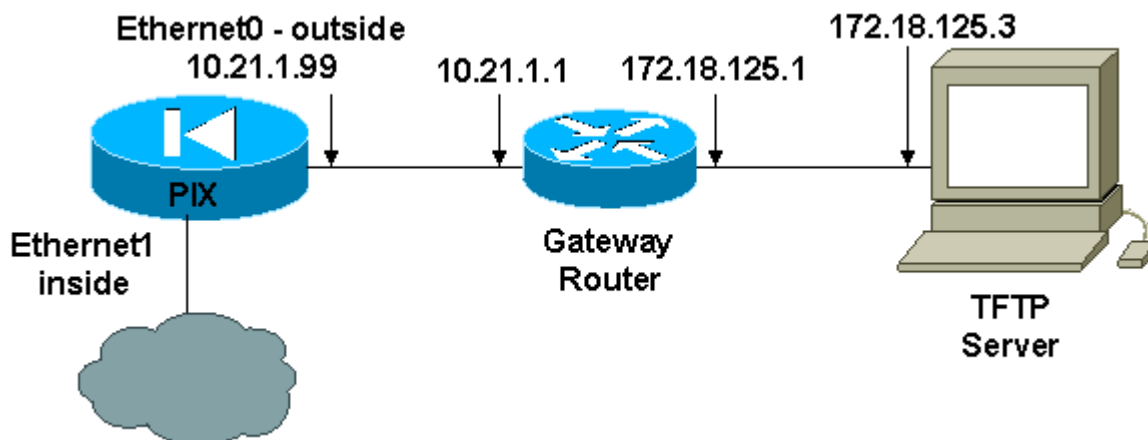
```
Do you wish to erase the passwords? [yn] y  
Passwords have been erased.
```

13. По умолчанию для Telnet сессии пароль "cisco" (без кавычек). Пароля для enable по умолчанию нет. Перейдите в режим конфигурирования и выполните команду **passwd** *ваш_Telnet_пароль* для смены пароля Telnet и команду **enable password** *ваш_пароль_enable* для смены соответственно пароля enable, после чего сохраните конфигурацию.

Примеры

Рассмотрим пример, в котором есть Cisco PIX с floppy приводом, TFTP сервер, который расположен в отличии от Cisco PIX подсети и продемонстрируем как можно восстановить пароль.

Сетевая диаграмма



```
monitor>interface 0
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7 )

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10), MAC:
0050.54ff.82b9
monitor>address 10.21.1.99
address 10.21.1.99
monitor>server 172.18.125.3
server 172.18.125.3
monitor>file np52.bin
file np52.bin
monitor>gateway 10.21.1.1
gateway 10.21.1.1
monitor>ping 172.18.125.3
Sending 5, 100-byte 0xf8d3 ICMP Echoes to
172.18.125.3, timeout is 4 seconds:
!!!!!
Success rate is 100 percent (5/5)
monitor>tftp
tftp np52.bin@172.18.125.3 via
10.21.1.1.....
Received 73728 bytes

Cisco Secure PIX Firewall password tool (3.0) #0:
Tue Aug 22 23:22:19 PDT 2000
```

```
Flash=i28F640J5 @ 0x300  
BIOS Flash=AT29C257 @ 0xd8000
```

```
Do you wish to erase the passwords? [yn] y  
Passwords have been erased.
```

```
Rebooting....
```

Более подробную информацию о восстановлении паролей Cisco PIX читайте на сайте производителя по ссылке
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_password_recovery09186a008009478b.shtml.