PIX/ASA 7.X : Пример настройки SSH/Telnet на внутреннем и внешнем интерфейсах

Содержание

Введение

Этот документ содержит пример конфигурации защищенного интерпретатора SSH на внутренних и внешних интерфейсах устройства защиты Cisco версий 7.x и выше. Конфигурация Устройства безопасности Серии удаленно с командной строкой включает использование или Telnet или SSH. Поскольку связи Telnet передаются в открытом тексте, который включает пароли, SSH настоятельно рекомендован. Трафик SSH зашифрован в туннеле и таким образом помогает защищать пароли и другие команды настройки от перехвата.

Устройство безопасности позволяет SSH - подключения устройству безопасности для целей управления. Устройство безопасности позволяет максимум пяти параллельных SSH - подключений для каждого контекста безопасности, при наличии, и общее максимальное

количество 100 соединений для всех объединенных контекстов.

В этом примере конфигурации Устройство безопасности PIX, как полагают, является сервером SSH. Трафик от Клиентов SSH (10.1.1.2/24 и 172.16.1.1/16) к серверу SSH зашифрован. Устройство безопасности поддерживает SSH удаленная функциональность оболочки, предоставленная в версиях SSH 1 и 2, и поддерживает шифры 3DES и Стандарт шифрования данных (DES). Версии SSH 1 и 2 являются другими и не являются совместимыми.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на версии 7.1 и 8.0 программного обеспечения Cisco PIX Firewall.

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: SSHv2 поддерживается в версии 7.x PIX/ASA и позже и не поддерживаемый в версиях ранее к 7. x.

Родственные продукты

Эта конфигурация может также использоваться с Устройством безопасности серии 5500 Cisco ASA с версиями программного обеспечения 7.x и позже.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

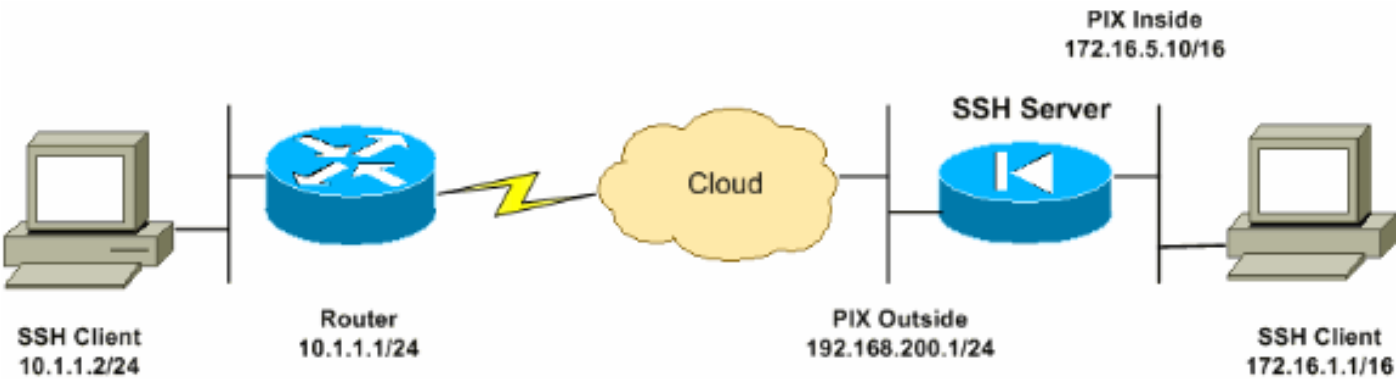
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Каждому действию настройки предоставляют необходимую информацию для использования командной строки или Менеджера устройств адаптивной безопасности (ASDM) (ASDM).

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации SSH

Эти конфигурации используются в данном документе:

- Доступ SSH к устройству безопасности
- Как использовать Клиента SSH
- Конфигурация PIX

Доступ SSH к устройству безопасности

Выполните эти шаги для настройки доступа SSH к устройству безопасности:

1. Сеансы SSH всегда требуют имени пользователя и пароля для аутентификации. Существует два способа удовлетворить это требование.Настройте имя пользователя и пароль и используйте AAA:Синтаксис:`pix(config)#`**`username`** *`username`* **`password`** *`password`*
`pix(config)#`**`aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]}`** **Примечание:** Если AAA-сервер недоступен, при использовании TACACS + или группа сервера RADIUS для аутентификации можно настроить устройство безопасности для использования локальной базы данных в качестве метода нейтрализации. Задайте имя серверной группы, и затем ЛОКАЛЬНЫЙ (ЛОКАЛЬНЫЙ учитывает регистр). Мы рекомендуем использовать то же имя пользователя и пароль в локальной базе данных как AAA-сервер, потому что приглашение устройства безопасности не дает индикации, какой метод используется.**Примечание:** Пример:`pix(config)#`**`aaa authentication ssh console TACACS+ LOCAL`** **Примечание:** Можно альтернативно использовать локальную базу данных в качестве основного способа аутентификации без нейтрализации. Чтобы сделать это, войдите ЛОКАЛЬНЫЙ один.Пример:`pix(config)#`**`aaa authentication ssh console LOCAL`**
ИлиИспользуйте имя пользователя по умолчанию **pix** и Пароль Telnet по умолчанию **Cisco**. Можно изменить Пароль Telnet с этой командой:`pix(config)#`**`passwd`** *`password`*
Примечание: Команда **пароля** может также использоваться в этой ситуации. Обе команды делают ту же вещь.
2. Генерируйте Открытые и секретные ключи криптосистемы RSA для Межсетевого экрана PIX, который требуется для SSH:`pix(config)#`**`crypto key generate rsa modulus`** *`modulus_size`* **Примечание:** `modulus_size` (в битах) может быть 512, 768, 1024, или 2048.

Чем больше ключевой размер модуля, который вы задаете, тем дольше он берет для генерации Открытых и секретных ключей криптосистемы RSA. Значение 1024 рекомендуется.**Примечание:** Команда, используемая для генерации Открытых и секретных ключей криптосистемы RSA, является другой для Версий ПО PIX ранее, чем 7. x. В более ранних версиях должно быть установлено доменное имя, прежде чем можно будет создать ключи.**Примечание:** В многоконтекстном режиме необходимо генерировать ключи RSA для каждого контексты. Кроме того, крипто-команды не поддерживаются в системном режиме контекста.

3. Укажите, что хосты позволили соединяться с устройством безопасности.Эта команда задает адрес источника, маска подсети и интерфейс хоста (хостов) позволили соединяться с SSH. Это может быть введено многократно для множественных хостов, сетей или интерфейсов. В данном примере разрешены один хост на внутренней части и один хост на внешней стороне.`pix(config)#`**`ssh 172.16.1.1 255.255.255.255 inside`**
`pix(config)#`**`ssh 10.1.1.2 255.255.255.255 outside`**
4. **Дополнительно:** По умолчанию устройство безопасности позволяет и версию SSH 1 и версию 2. Введите эту команду для ограничения соединений с определенной версией:`pix(config)#` **`ssh version`** *<version_number>* **Примечание:** `version_number` может быть 1 или 2.
5. **Дополнительно:** По умолчанию Сеансы SSH закрыты после пяти минут бездействия. Этот таймаут может быть настроен для длительности между 1 и 60 минутами.`pix(config)#`**`ssh timeout`** *minutes*

Как использовать Клиента SSH

Введите имя пользователя и пароль для входа устройства защиты PIX 500 Series при открытии Сеанса SSH. При начале Сеанса SSH точка (.) отображается на консоли устройства безопасности, прежде чем появится приглашение аутентификации пользователя SSH:

```
hostname(config)# .
```

Показ точки не влияет на функциональность SSH. Точка появляется в консоли, когда серверный ключ генерируется, или сообщение дешифровано с секретными ключами во время обмена SSH-ключа, прежде чем произойдет проверка подлинности пользователя. Эти задачи могут занять до двух минут или дольше. Точка является индикатором хода выполнения, который проверяет, что устройство безопасности занято и не "зависло".

Версии SSH 1.x и 2 являются совершенно другими протоколами и не совместимы. Загрузите совместимого клиента. См. Получение раздела Клиента SSH Усовершенствованных конфигураций для получения дополнительной информации.

Конфигурация PIX

В данном документе используется следующая конфигурация:

Конфигурация PIX

```
PIX Version 7.1(1)
!
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
```

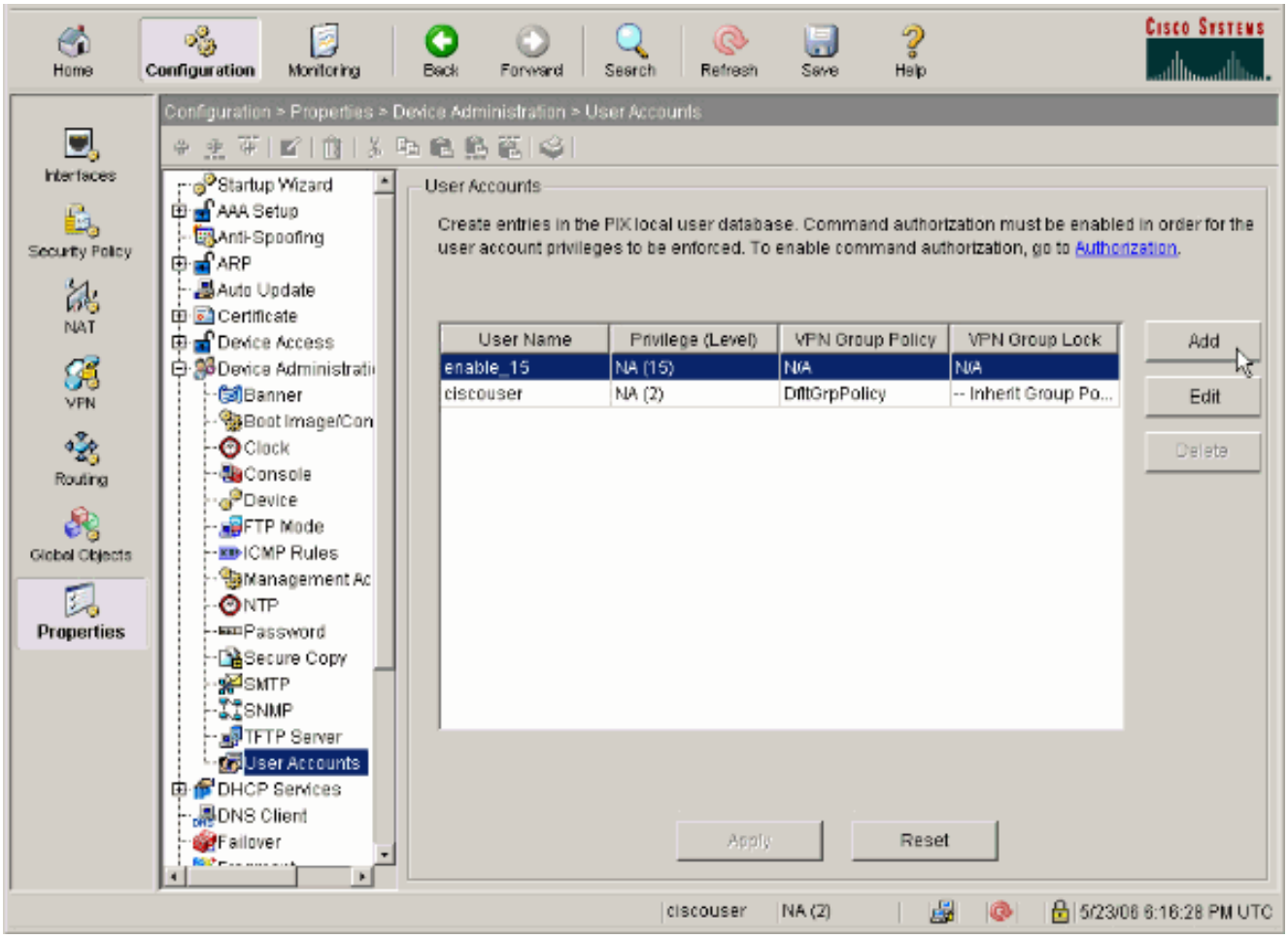
```
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp permit any outside
no asdm history enable
arp timeout 14400
route outside 10.1.1.0 255.255.255.0 192.168.200.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- AAA for the SSH configuration username ciscouser
password 3USUcOPFUiMCO4Jk encrypted aaa authentication
ssh console LOCAL http server enable http 172.16.0.0
255.255.0.0 inside no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstar telnet timeout 5
!--- Enter this command for each address or subnet !---
to identify the IP addresses from which !--- the
security appliance accepts connections. !--- The
security appliance accepts SSH connections from all
interfaces. ssh 10.1.1.2 255.255.255.255 outside !---
Allows the users on the host 172.161.1.1 !--- to access
the security appliance !--- on the inside interface. ssh
172.16.1.1 255.255.255.255 inside !--- Sets the duration
from 1 to 60 minutes !--- (default 5 minutes) that the
SSH session can be idle, !--- before the security
appliance disconnects the session. ssh timeout 60
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:a6b05fd04f9fbd0a39f1ca7328de91f7 : end
```

Примечание: Для доступа к интерфейсу управления ASA/PIX с помощью SSH выполните эту команду: `ssh 172.16.16.160 255.255.255.255`

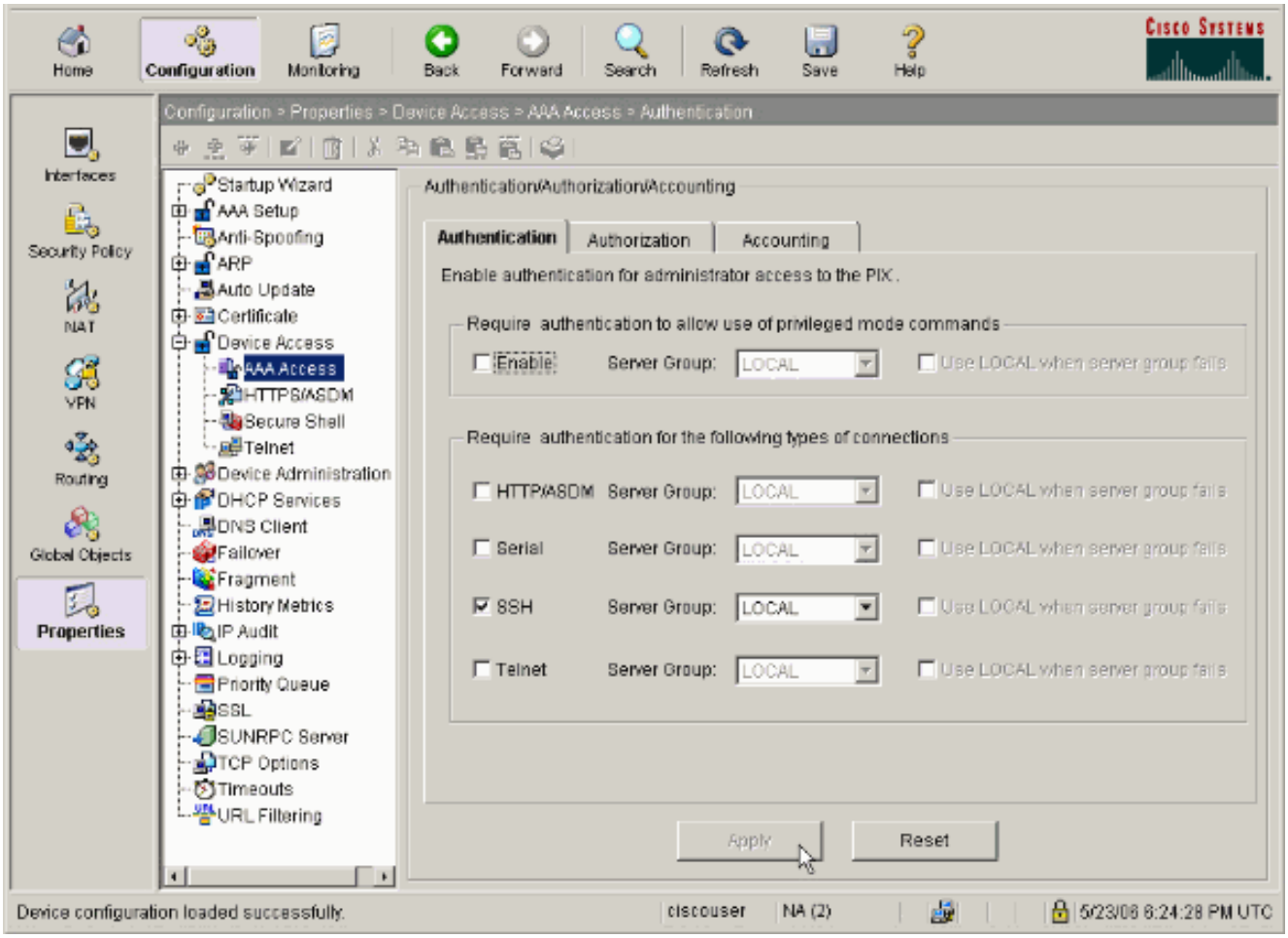
Конфигурация с ASDM 5. x

Выполните эти шаги для настройки устройства для SSH с помощью ASDM:

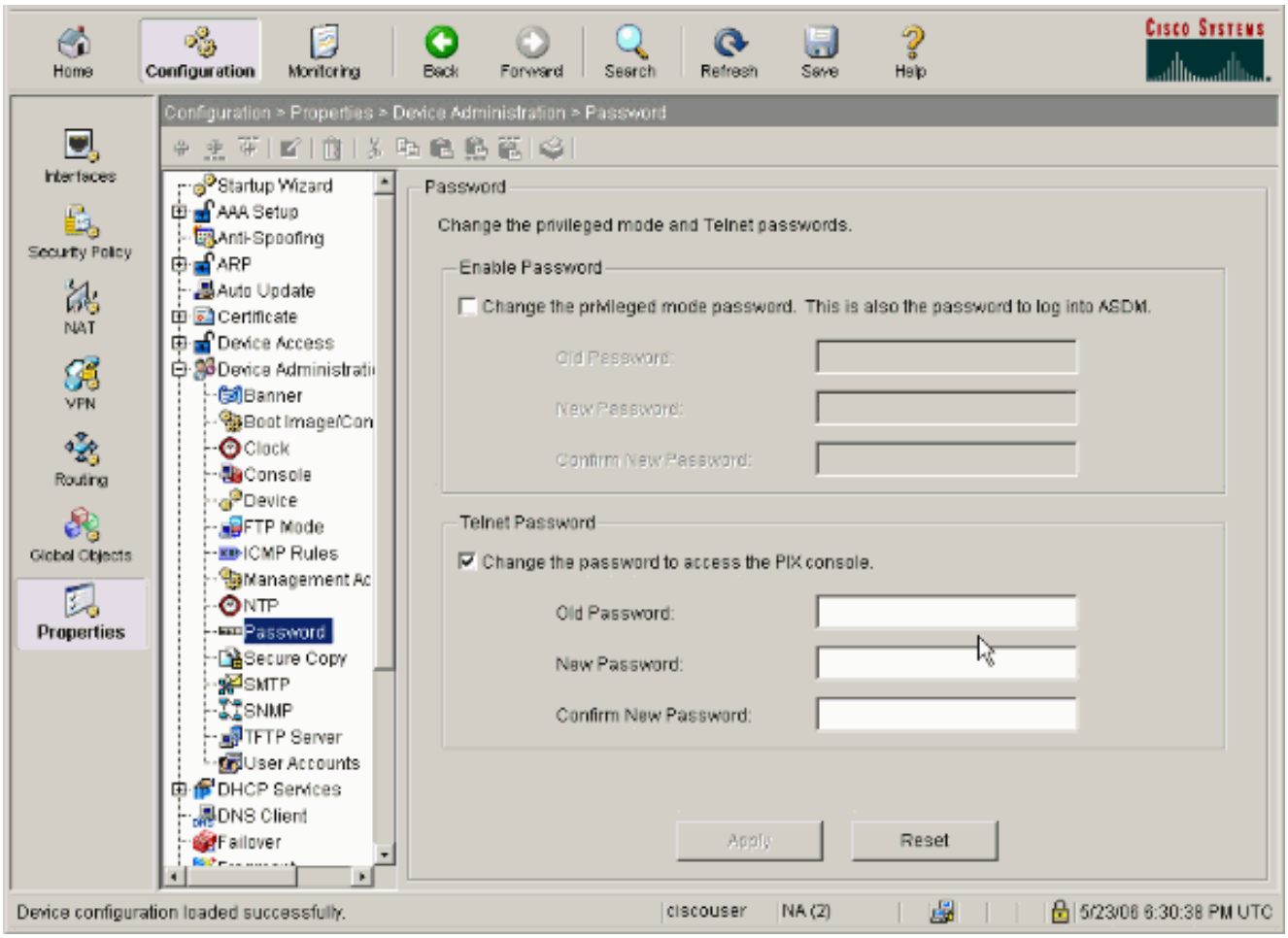
1. Выберите **Configuration> Properties> Device Administration> User Accounts** для добавления пользователя с
ASDM.



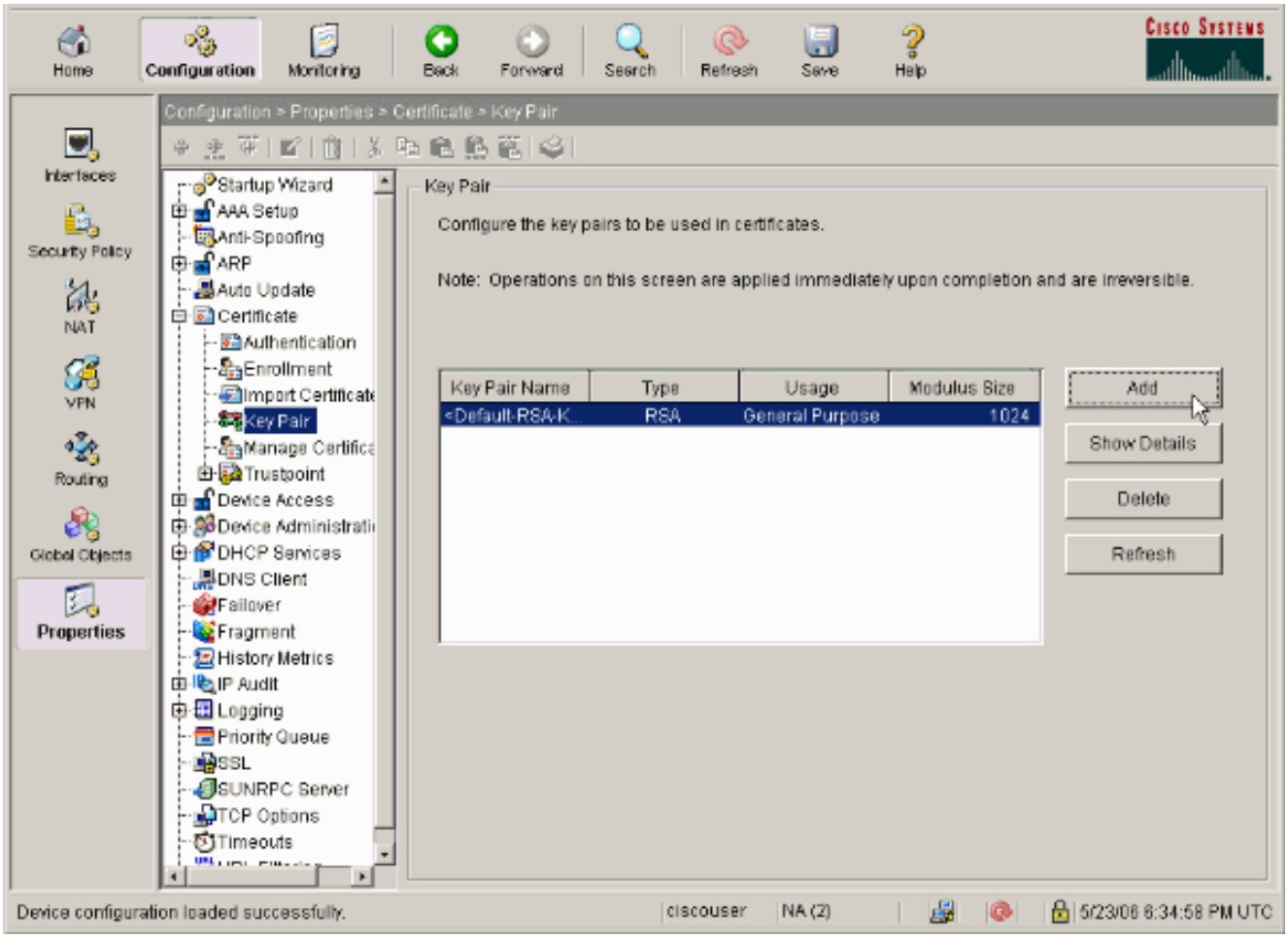
2. Выберите **Configuration> Properties> Device Access> AAA Access> Authentication** для устанавливания аутентификации AAA (проверка подлинности, авторизация и учет) для SSH с
ASDM.



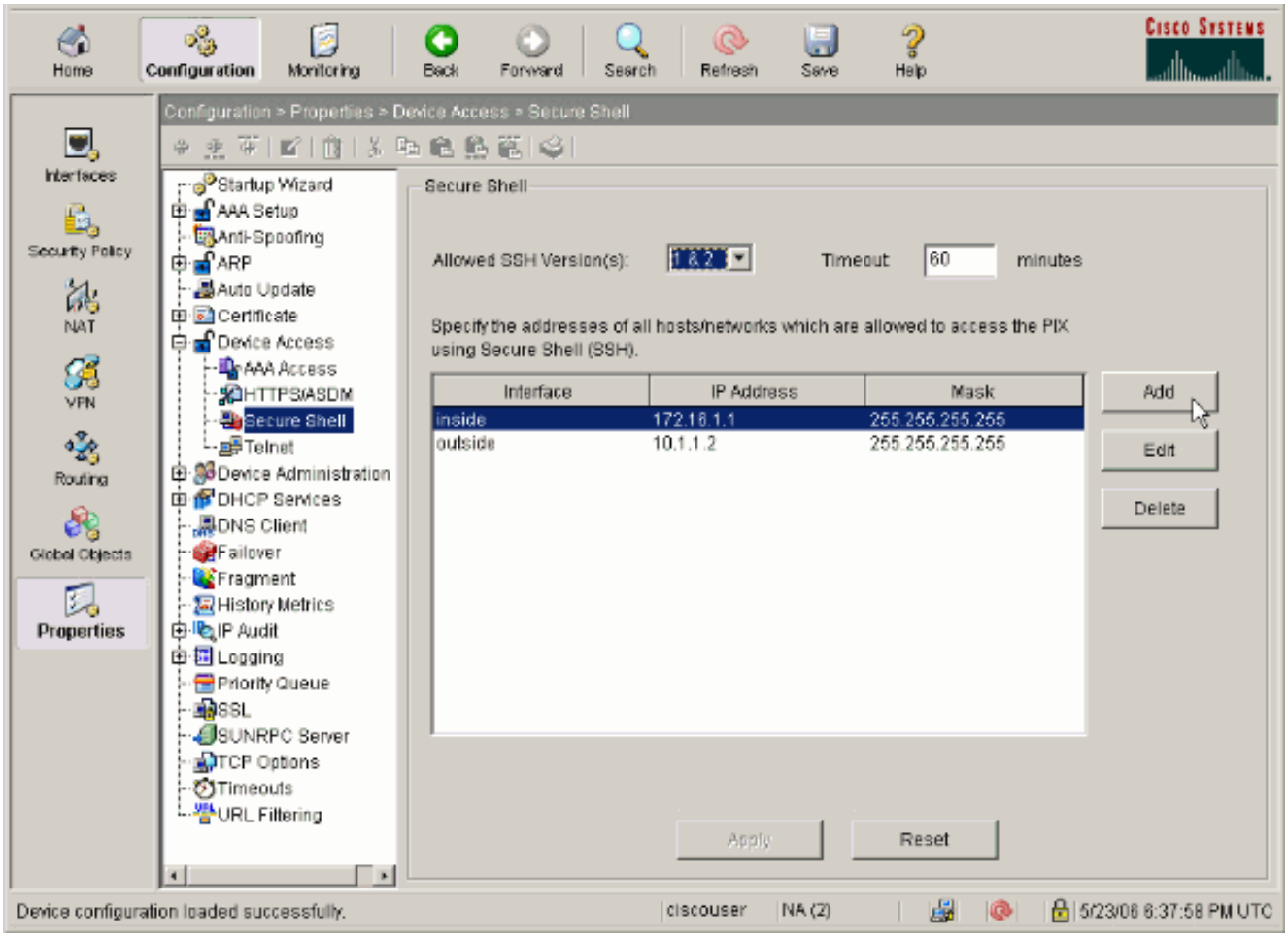
3. Выберите **Configuration> Properties> Device Administration> Password** для изменения Пароля Telnet с
ASDM.



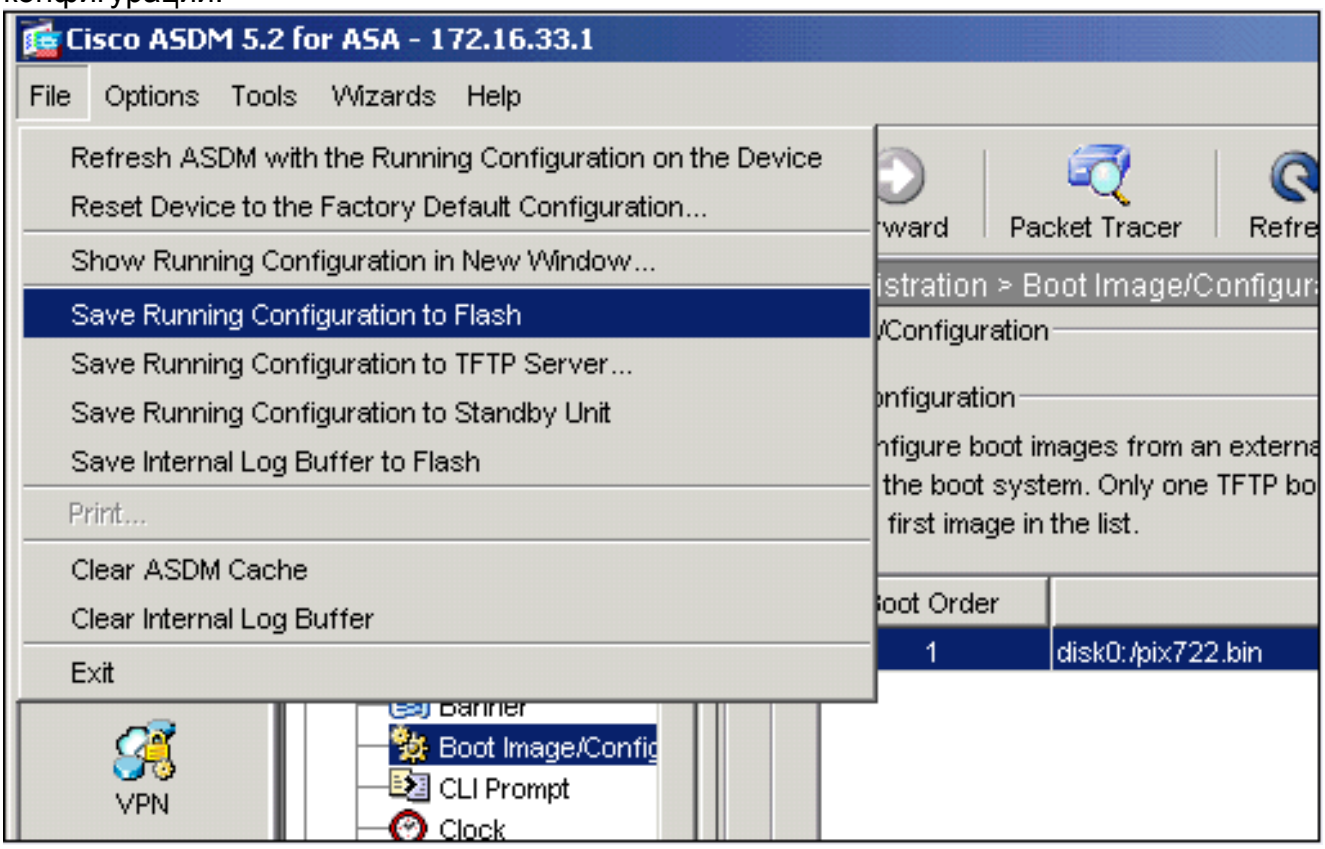
4. Выберите **Configuration> Properties> Certificate> Key Pair**, **нажмите Add** и используйте параметры по умолчанию, представленные для генерации тех же ключей RSA с ASDM.



5. Выберите **Configuration> Properties> Device Access> Secure Shell** для использования ASDM, чтобы указать, что хосты позволили соединяться с SSH и задавать версию и параметры
таймаута.



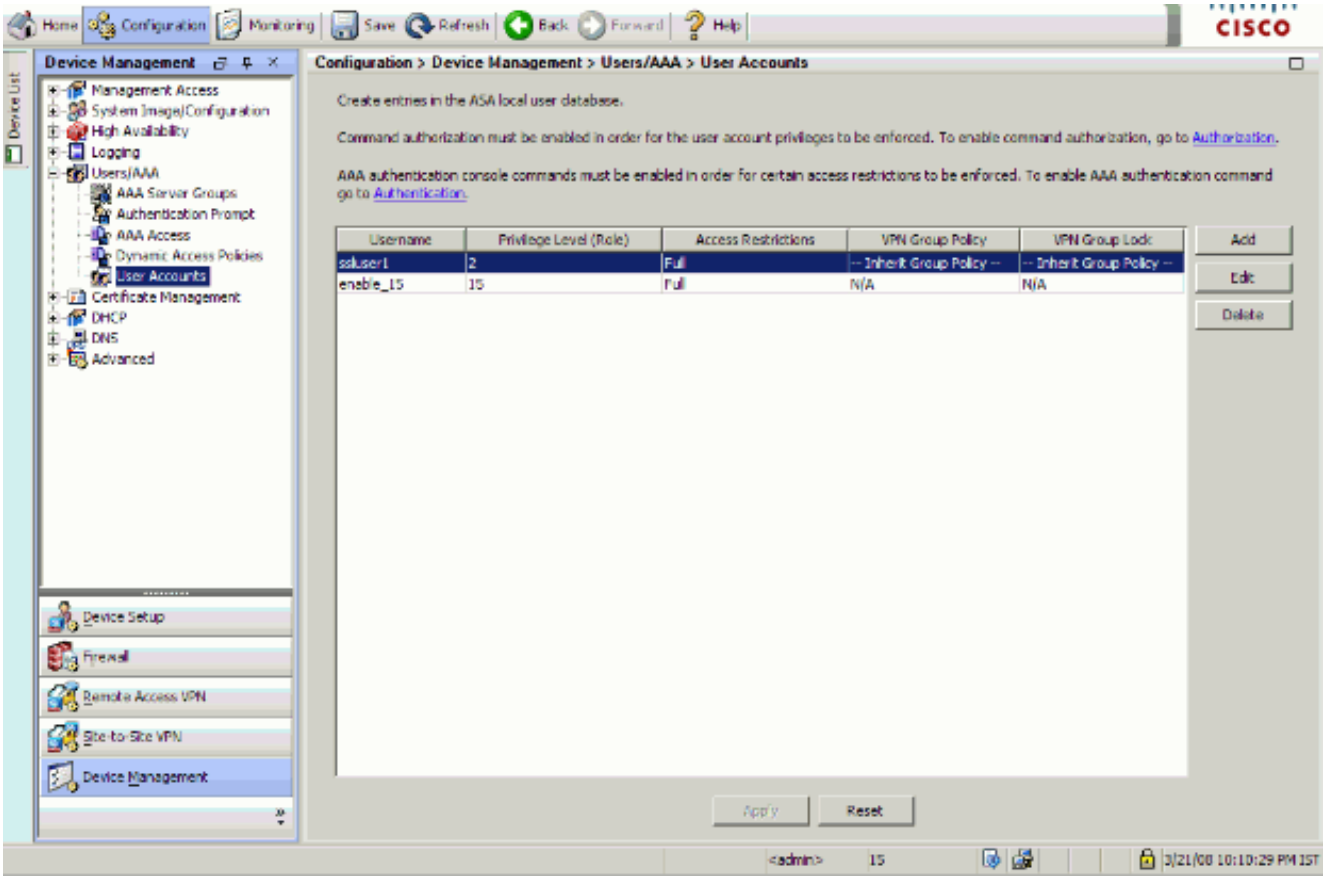
6. Нажмите **File> Save Running Configuration to Flash** для сохранения конфигурации.



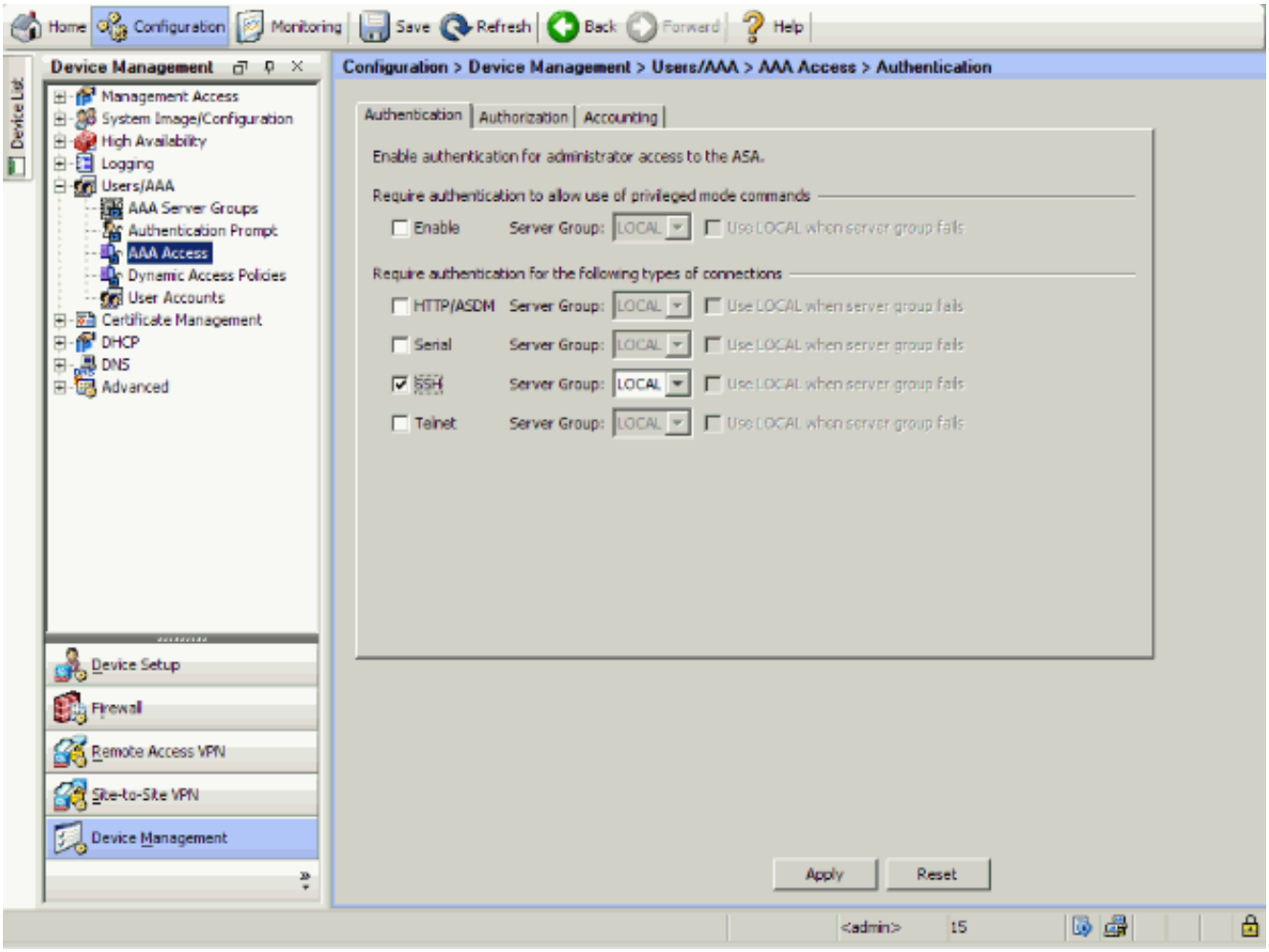
Конфигурация с ASDM 6. x

Выполните следующие действия:

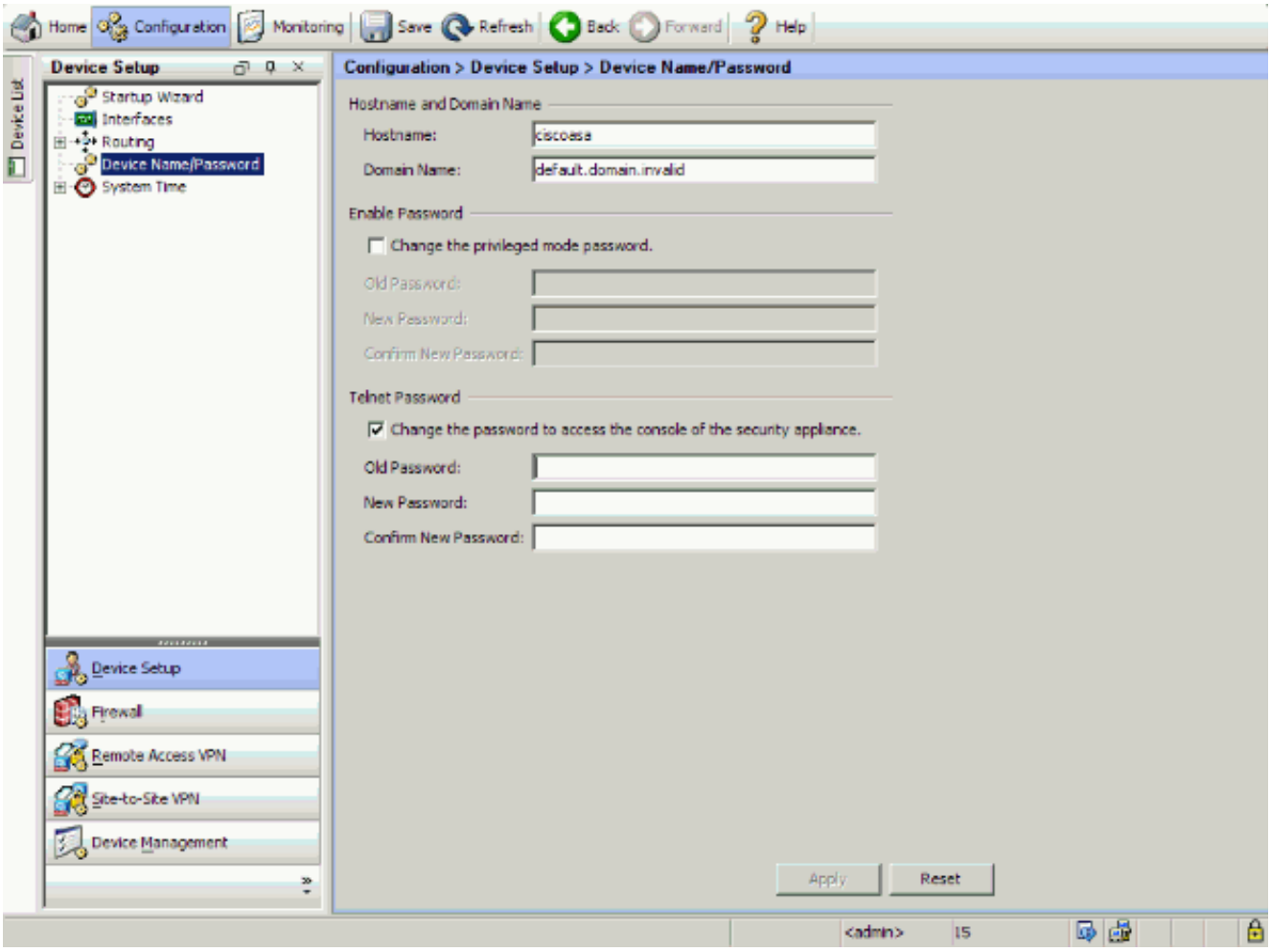
1. Выберите **Configuration>> Users Device Management / AAA> Учетные записи пользователя** для добавления пользователя с ASDM.



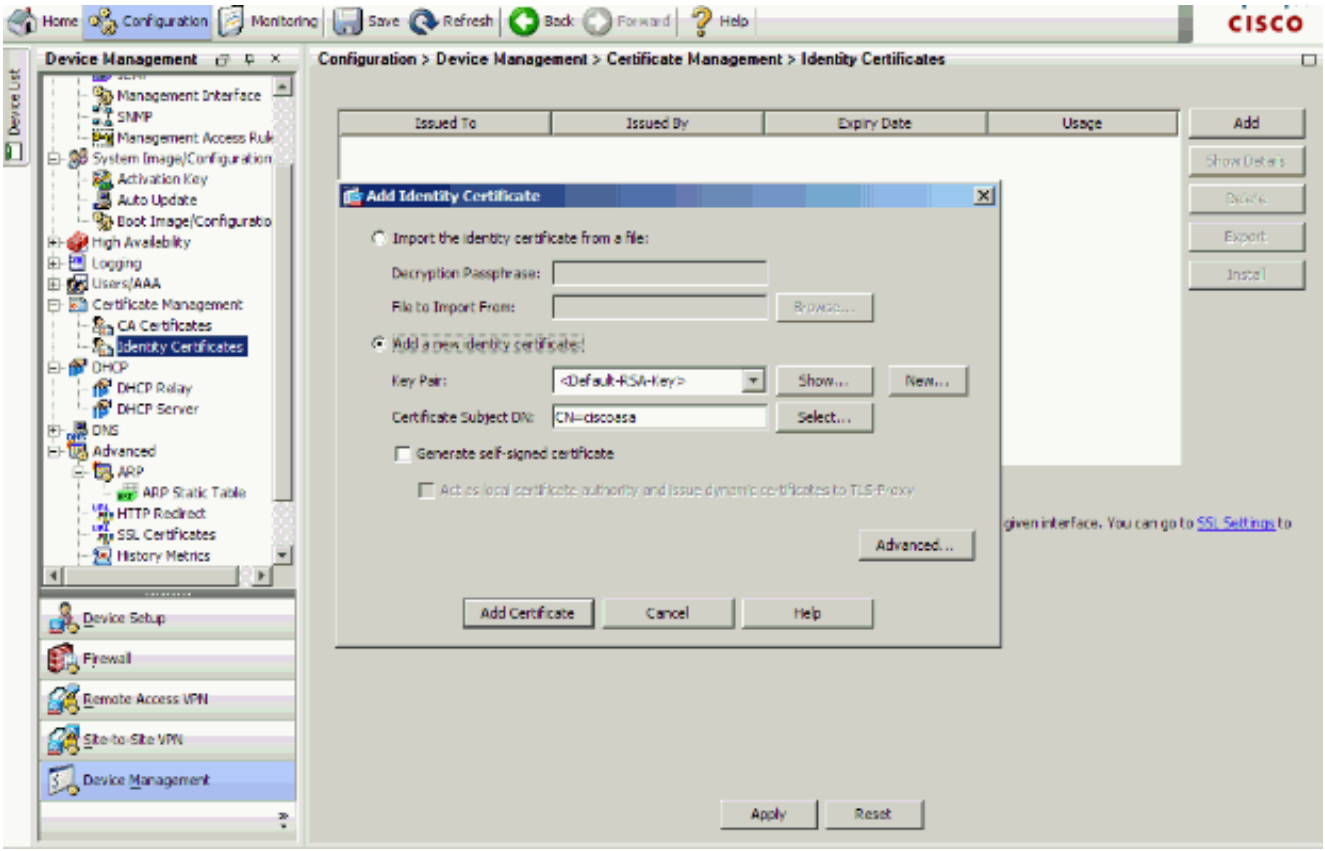
2. Выберите **Configuration>> Users Device Management / AAA> Доступ AAA> Аутентификация** для устанавливания аутентификации AAA (проверка подлинности, авторизация и учет) для SSH с ASDM.



3. Выберите **Configuration> Device Setup> Device Name / Пароль** для изменения Пароля Telnet с
ASDM.

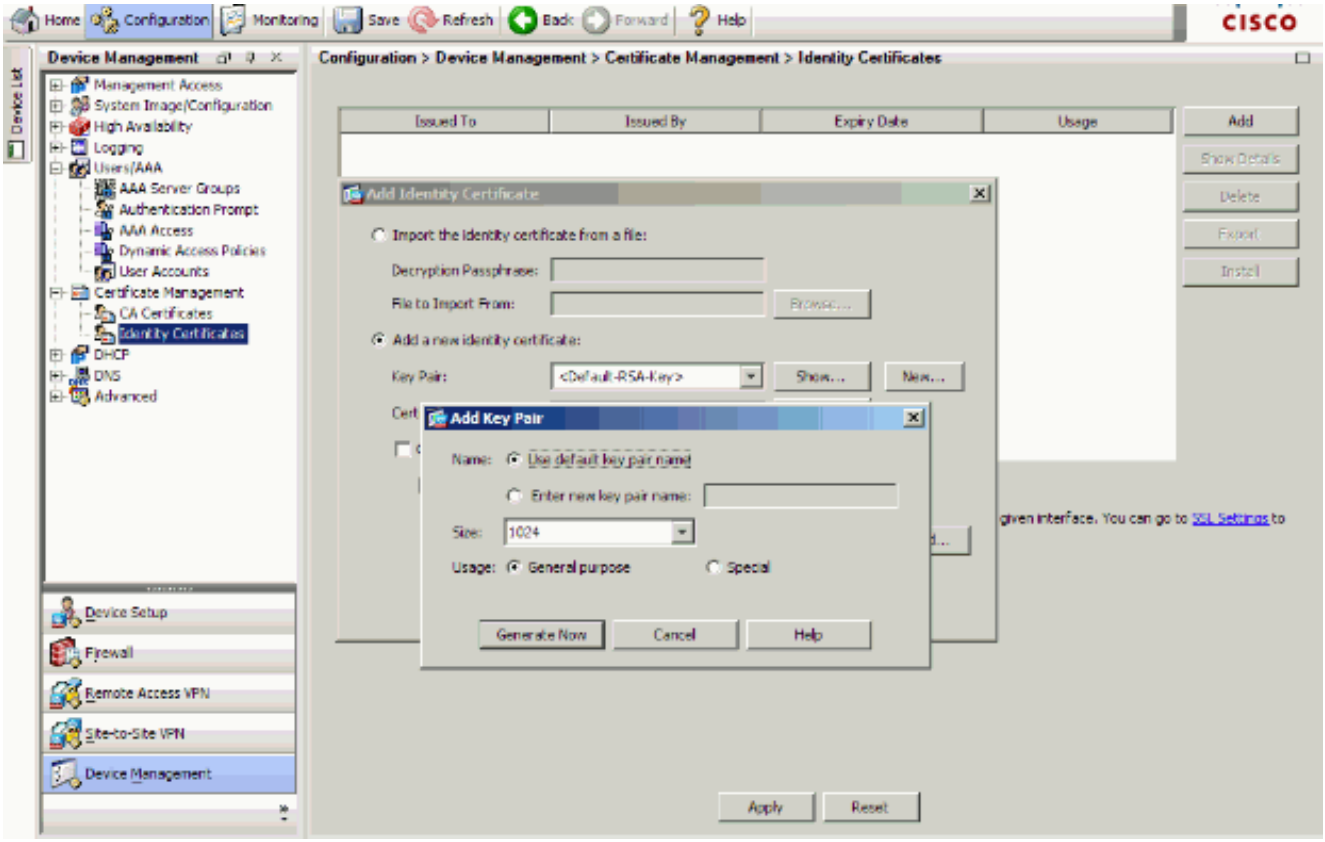


4. Выберите **Configuration>> Certificate Management Device Management> Сертификаты идентификации**, **нажмите Add** и используйте параметры по умолчанию, представленные для генерации тех же ключей RSA с ASDM.

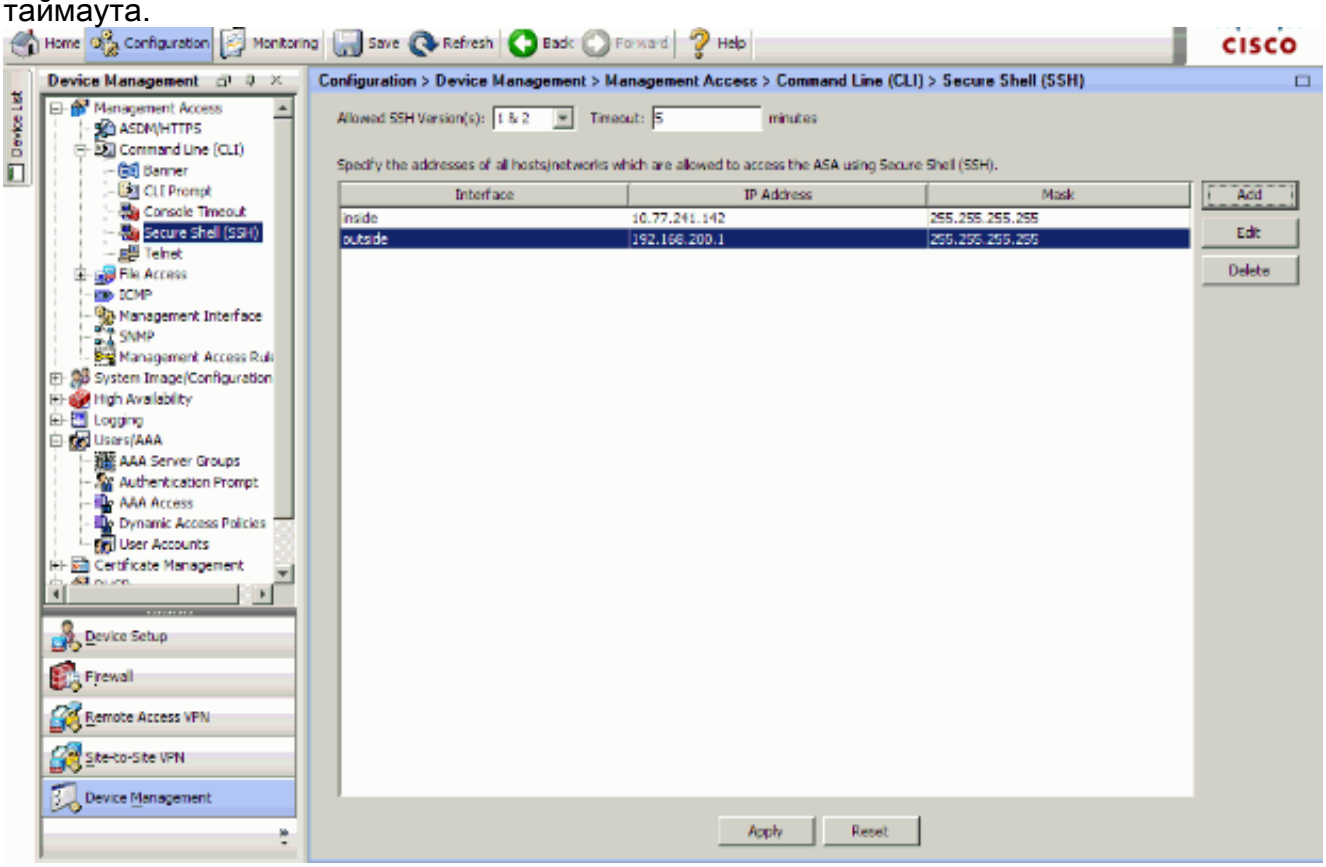


5. Под **Добавляют, что новый Сертификат идентификации** нажимает **New** для добавления

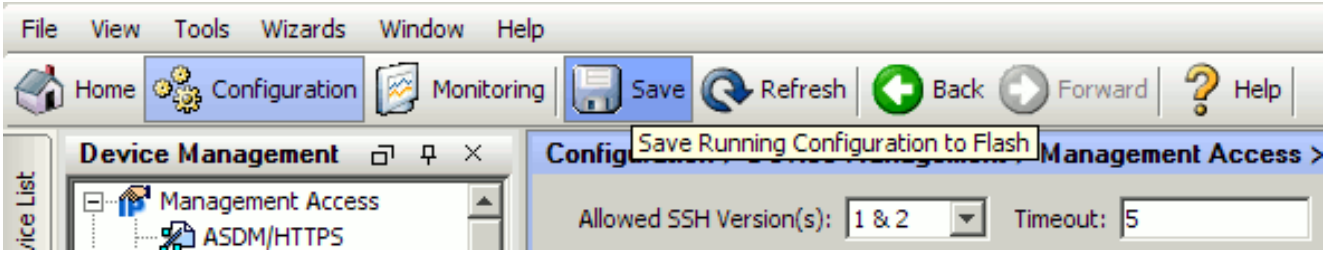
пары ключа по умолчанию, если вы не делаете существует. Затем нажмите **Generate Now**.



6. Выберите **Configuration> Device Management> Management Access> Command Line (CLI)> Secure Shell (SSH)** для использования ASDM, чтобы указать, что хосты позволили соединяться с SSH и задавать версию и параметры таймаута.



7. Нажмите **Save** на вершине окна для сохранения конфигурации.



8. Когда предложено сохранить конфигурацию на флэш-памяти, выберите **Apply** для сохранения конфигурации.

Конфигурация telnet

Чтобы добавить доступ Telnet к консоли и установить время простоя, выполняет **команду telnet** в режиме глобальной конфигурации. По умолчанию сеансы Telnet, которые оставляют простаивающими в течение пяти минут, закрыты устройством безопасности. Для удаления доступа Telnet из ранее IP-адрес набора, используйте *эту команду с параметром по*.

```
telnet {{hostname | IP_address mask interface_name} | {IPv6_address interface_name} | {timeout number}} no telnet {{hostname | IP_address mask interface_name} | {IPv6_address interface_name} | {timeout number}}
```

Команда telnet позволяет вам задать, какие хосты могут обратиться к консоли устройства безопасности с Telnet.

Примечание: Можно включить Telnet к устройству безопасности на всех интерфейсах. Однако устройство безопасности принуждает тот весь трафик Telnet к внешнему интерфейсу быть защищенным IPsec. Для включения сеанса Telnet к внешнему интерфейсу настройте IPsec на внешнем интерфейсе для включения IP - трафика, который генерируется устройством безопасности, и включите Telnet на внешнем интерфейсе.

Примечание: . в целом, если какой-либо интерфейс Telnet тому интерфейсу, который имеет уровень безопасности 0 или ниже, чем какой-либо другой интерфейс, тогда PIX/ASA не позволяет

Примечание: Не рекомендуется обратиться к устройству безопасности через сеанс Telnet. Информация об учетных данных для аутентификации, такая как пароль, передается как открытый текст. Сервер Telnet и связь с клиентом происходят только с открытым текстом. Cisco рекомендует использовать SSH для большего количества связи защищенных данных.

При вводе IP-адреса необходимо также ввести маску подсети. Нет никакой маски подсети по умолчанию. Не используйте маску подсети внутренней сети. Маска подсети является только небольшим количеством маски для IP-адреса. Для ограничения доступа к одному IP-адресу используйте 255 в каждом октете; например, 255.255.255.255.

Если IPsec работает, можно задать небезопасное имя интерфейса, которое, как правило, является внешним интерфейсом. Как минимум можно настроить команду **криптокарты** для определения имени интерфейса с **командой telnet**.

Выполните команду **пароля** для установки пароля для доступа Telnet к консоли. По умолчанию является Cisco. Выйдите**, кто** дает команду для просмотра, какие IP-адреса в настоящее время обращаются к консоли устройства безопасности. Выполните команду **уничтожения** для завершения активного сеанса консоли Telnet.

Для включения сеанса Telnet к внутреннему интерфейсу рассмотрите эти примеры:

Пример 1

Данный пример разрешает только хосту 10.1.1.1 получать доступ к консоли устройства безопасности через Telnet:

```
pix(config)#telnet 10.1.1.1 255.255.255.255 inside
```

Пример 2

Данный пример разрешает только сети 10.0.0.0/8 получать доступ к консоли устройства безопасности через Telnet:

```
pix(config)#telnet 10.0.0.0 255.0.0.0 inside
```

Пример 3

Данный пример позволяет всем сетям получать доступ к консоли устройства безопасности через Telnet:

```
pix(config)#telnet 0.0.0.0 0.0.0.0 inside
```

При использовании **команды aaa** с консольным ключевым словом консольный доступ Telnet должен аутентифицироваться с сервером проверки подлинности.

Примечание: При настройке **команды aaa** для требования аутентификации для консольного доступа Telnet устройства безопасности и таймаутов запроса регистрационного имени консоли, можно получить доступ к устройству безопасности от последовательной консоли. Чтобы сделать это, поступите в устройство безопасности имя пользователя и пароль, который установлен с **командой enable password**.

Выполните команду **истечения времени telnet-сеанса** для установки максимального времени, когда консольный сеанс Telnet может быть простаивающим, прежде чем это выйдется из системы устройством безопасности. Вы не можете использовать **команду telnet** с командой **истечения времени telnet-сеанса**.

Данный пример показывает, как изменить максимальную пропускную способность для сеанса простаивающая продолжительность:

```
hostname(config)#telnet timeout 10 hostname(config)#show running-config telnet timeout telnet timeout 10 minutes
```

Поддержка SSH/Telnet в ACS 4. x

При рассмотрении функций RADIUS можно использовать RADIUS для функциональности SSH.

Когда попытка предпринята для доступа к устройству безопасности с Telnet, SSH, HTTP, или подключение последовательной консоли и трафик совпадают с объявлением проверки подлинности, устройство безопасности запрашивает имя пользователя и пароль. Это тогда передает эти учетные данные к RADIUS (ACS) сервер, и предоставляет или запрещает доступ CLI на основе ответа от сервера.

См. Раздел поддержки AAA-сервера и Локальной базы данных AAA-серверов Настройки и Локальной базы данных для получения дополнительной информации.

Например, ваше Устройство обеспечения безопасности ASA 7.0 потребностей IP-адрес, от которого устройство безопасности принимает соединения, такие как:

```
hostname(config)#ssh source_IP_address mask source_interface
```

См. раздел Доступа SSH Разрешения AAA-серверов Настройки и Локальной базы данных для получения дополнительной информации.

См. PIX/ASA: Сквозной Прокси для Доступа к сети с помощью TACACS + и Пример Конфигурации сервера RADIUS для получения дополнительной информации о том, как настроить доступ SSH/Telnet к PIX с аутентификацией ACS.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Используйте OIT для просмотра анализа выходных данных команды show.**

Debug SSH

Выполните **команду debug ssh** для включения отладки SSH.

```
pix(config)#debug ssh SSH debugging on
```

Эти выходные данные показывают, что запрос аутентификации от хоста 10.1.1.2 (снаружи к PIX) для "произведения пробу монет" успешен:

```
pix#
Device ssh opened successfully.
   SSH0: SSH client: IP = '10.1.1.2' interface # = 1
   SSH: host key initialised
   SSH0: starting SSH control process
   SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
   SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows
client version string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0:
begin    ser ver key generation
   SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
   SSH2 0: SSH2_MSG_KEXINIT received
   SSH2: kex: client->server aes128-cbc hmac-md5 none
   SSH2: kex: server->client aes128-cbc hmac-md5 none
   SSH2 0: expecting SSH2_MSG_KEXDH_INIT
   SSH2 0: SSH2_MSG_KEXDH_INIT received
   SSH2 0: signature length 143
   SSH2: kex_derive_keys complete
   SSH2 0: newkeys: mode 1
   SSH2 0: SSH2_MSG_NEWKEYS sent
   SSH2 0: waiting for SSH2_MSG_NEWKEYS
   SSH2 0: newkeys: mode 0
   SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix): user authen method is
'no AAA', aaa server group ID = 0
   SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication successful for pix !--- Authentication for the PIX was successful. SSH2
```

```
0: channel open request SSH2 0: pty-req request SSH2 0: requested tty: vt100, height 25, width
80 SSH2 0: shell request SSH2 0: shell message received
```

Если пользователь дает неверное имя пользователя, например, "pix1" вместо "pix", Межсетевой экран PIX отклоняет аутентификацию. Эти выходные данные отладки показывают ошибку проверки подлинности:

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows client version
    string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1960 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix1): user authen method is
'no AAA', aaa server group ID = 0
SSH(pix1): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix1 !--- Authentication for pix1 was not successful due to
the wrong username.
```

Точно так же, если пользователь предоставляет неправильный пароль, этот выход отладки показывает вам ошибку проверки подлинности.

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2'  interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL server version string:
SSH-1.99-Cisco-1.25SSH0: receive      SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for
Windows client version string:SSH-1.99-3.2.0
SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1920 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix): user authen method
```

```
is 'no AAA', aaa server group ID = 0
     SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pixSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix !--- Authentication for PIX was not successful due to the
wrong password.
```

Обзорные активные сеансы SSH

Выполните эту команду для проверки количества Сеансов SSH, которые связаны и состояние соединения с PIX:

```
pix#show ssh session SID Client IP Version Mode Encryption Hmac State Username 0 10.1.1.2 1.99
IN aes128-cbc md5 SessionStarted pix OUT aes128-cbc md5 SessionStarted pix
```

Выберите **Monitoring> Properties> Device Access> Secure Shell Sessions** для просмотра сеансов с ASDM.

Обзорный общедоступный ключ RSA

Выполните эту команду для просмотра общей части RSA, включает устройство безопасности:

```
pix#show crypto key mypubkey rsa Key pair was generated at: 19:36:28 UTC May 19 2006 Key name:
<Default-RSA-Key> Usage: General Purpose Key Modulus Size (bits): 1024 Key Data: 30819f30
0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c172f4 95f66c34 2c2ced37 aa3442d8
12158c93 131480dd 967985ab 1d7b92d9 5290f695 8e9b5b0d d88c0439 6169184c d8fb951c 19023347
d6b3f939 99ac2814 950f4422 69b67328 f64916b1 82e15341 07590da2 390fbefd 38758888 7319196c
de61aef1 165c4bab 03d081d5 ddaf15cc c9ddb204 c2b451e0 f19ce0f3 485b1d69 8b020301 0001
```

Выберите **Configuration> Properties> Certificate> Key Pair** и нажмите **Show Details** для просмотра ключей RSA с ASDM.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Как удалить ключи RSA из PIX

Определенные ситуации, такой как тогда, когда вы обновляете PIX sofware или изменяете версию SSH в PIX, могут потребовать, чтобы вы удалили и воссоздали ключи RSA. Выполните эту команду для удаления Открытых и секретных ключей криптосистемы RSA из PIX:

```
pix(config)#crypto key zeroize rsa
```

Выберите **Configuration> Properties> Certificate> Key Pair** и нажмите **Delete** для удаления ключей RSA с ASDM.

Отказавший SSH - подключение

Сообщение об ошибках на PIX/ASA:

```
%PIX|ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
```

Соответствующее сообщение об ошибках на машине Клиента SSH:

```
Selected cipher type <unknown> not supported by server.
```

Для решения этого вопроса удалите и воссоздайте ключи RSA. Выполните эту команду для удаления Открытых и секретных ключей криптосистемы RSA из ASA:

```
ASA(config)#crypto key zeroize rsa
```

Выполните эту команду для генерации нового ключа:

```
ASA(config)# crypto key generate rsa modulus 1024
```

Неспособный обратиться к ASA с SSH

:

```
ssh_exchange_identification: read: Connection reset by peer
```

Чтобы решить эту проблему, выполните следующие действия:

1. Или повторно загрузите ASA или удалите весь SSH отнесенный config и ключи RSA.
2. Реконфигурируйте команды SSH и восстановите ключи RSA.

Неспособный обратиться к вторичному ASA Использование SSH

Когда ASA находится в режиме аварийного переключения, это не возможно к SSH к резервному ASA через VPN-туннель. Это вызвано тем, что трафик ответа для SSH берет внешний интерфейс резервного ASA.

Дополнительные сведения

- Cisco PIX 500 Series Security Appliances
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- SSH - подключения Настройки - маршрутизаторы Cisco и концентраторы Cisco
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация