SSH версии ASA 9.x и Telnet на внутреннем и внешнем примере конфигурации интерфейсов

Содержание

Введение

Этот документ описывает, как настроить Secure Shell (SSH) на внутренних и внешних интерфейсах Версий Устройства безопасности Cisco серии 9.x и позже. Когда необходимо настроить и контролировать устройство адаптивной защиты Cisco (ASA) удаленно с CLI, использование или Telnet или SSH требуется. Поскольку связи Telnet передаются в открытом тексте, который может включать пароли, SSH настоятельно рекомендован. Трафик SSH зашифрован в туннеле и таким образом помогает защищать пароли и другие чувствительные команды настройки от перехвата.

ASA 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.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Версии 9.1.5 Программного обеспечения межсетевого экрана Cisco ASA.

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:** Версия SSH 2 (SSHv2) поддерживается в Версиях ASA 7.x и позже.

Родственные продукты

Эта конфигурация может также использоваться с Устройством безопасности серии 5500 Cisco ASA с версиями программного обеспечения 9.x и позже.

Условные обозначения

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

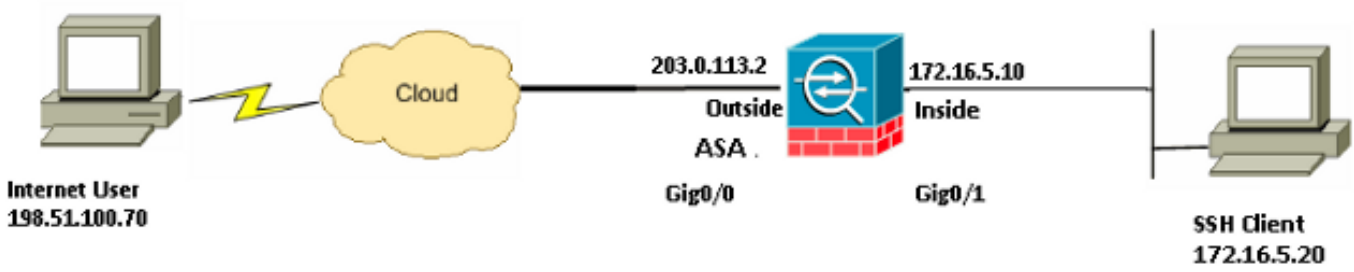
Настройка

Используйте информацию, которая предоставлена в этом разделе для настройки функций, которые описаны в этом документе.

> **Примечание:** Каждое действие настройки, которое описано, предоставляет информацию, которая необходима для использования или CLI 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 этом примере конфигурации ASA, как полагают, является сервером SSH. Трафик от Клиентов SSH (198.51.100.70/32 и 172.16.5.20/24) к серверу SSH зашифрован. Устройство безопасности поддерживает SSH удаленная функциональность оболочки, которая предоставлена 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.

Конфигурации SSH

Эти конфигурации используются в данном документе:

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

Доступ SSH к устройству безопасности

Выполните эти шаги для настройки доступа SSH к устройству безопасности:

1. Сеансы SSH всегда требуют формы проверки подлинности, такой как имя пользователя и пароль. Существует два метода, которые можно использовать для соответствия этому требованию.

   Первый метод, который можно использовать для соответствия этому требованию должен настроить имя пользователя и пароль с использованием Аутентификации, авторизации и учета (AAA):
   ```
   ASA(config)#username username password password
   ASA(config)#aaa authentication {telnet | ssh | http | serial} console
   {LOCAL | server_group [LOCAL]}
   ```
   Примечание: При использовании TACACS + или группа сервера RADIUS для аутентификации можно настроить устройство безопасности так, чтобы это использовало локальную базу данных в качестве метода нейтрализации, если AAA-сервер недоступен. Задайте имя серверной группы, и затем **ЛОКАЛЬНЫЙ** (**ЛОКАЛЬНЫЙ** учитывает регистр). Cisco рекомендует использовать то же имя пользователя и пароль в локальной базе данных и AAA-сервере, потому что приглашение устройства безопасности не дает индикации относительно метода, который используется.Для определения **Локальной резервной копии** для **TACACS +**, используйте эту конфигурацию для аутентификации SSH:
   ```
   ASA(config)#aaa authentication ssh console TACACS+ LOCAL
   ```
   Можно альтернативно

использовать локальную базу данных в качестве основного способа аутентификации без нейтрализации. Чтобы сделать это, войдите **ЛОКАЛЬНЫЙ** один:
`ASA(config)#aaa authentication ssh console LOCAL`**Второй метод**, который можно использовать для соответствия этому требованию должен использовать имя пользователя по умолчанию **ASA** и Пароль Telnet по умолчанию **Cisco**. Можно изменить Пароль Telnet с этой командой:
`ASA(config)#passwd password`**Примечание:** Команда **пароля** может также использоваться в этой ситуации, поскольку обе из команд функционируют так же.

2. Генерируйте Открытые и секретные ключи криптосистемы RSA для Межсетевого экрана ASA, который требуется для SSH:
`ASA(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 2048 рекомендуется. Команда, которая используется для генерации Открытых и секретных ключей криптосистемы RSA является другой для версий программного обеспечения ASA ранее, чем Версия 7. x. В более ранних версиях должно быть установлено доменное имя, прежде чем можно будет создать ключи. В многоконтекстном режиме необходимо генерировать ключи RSA для каждого контекста.
3. Задайте хосты, которым позволяют соединиться с устройством безопасности. Эта команда задает адрес источника, маску подсети и интерфейс хоста (хостов), которому позволяют соединиться 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:
```
ASA(config)#ssh 172.16.5.20 255.255.255.255 inside
ASA(config)#ssh 198.51.10.70 255.255.255.255 outside
```
4. Этот шаг не является обязательным. По умолчанию устройство безопасности позволяет и Версию SSH 1 и Версию 2. Введите эту команду для ограничения соединений с определенной версией:
`ASA(config)# ssh version <version_number>`**Примечание: version_number** может быть или **1** или **2**.
5. Этот шаг не является обязательным. По умолчанию Сеансы SSH закрыты после пяти минут бездействия. Этот таймаут может быть настроен для длительности между 1 и 60 минутами:
`ASA(config)#ssh timeout minutes`

Конфигурация ASA

Используйте эту информацию для настройки ASA:

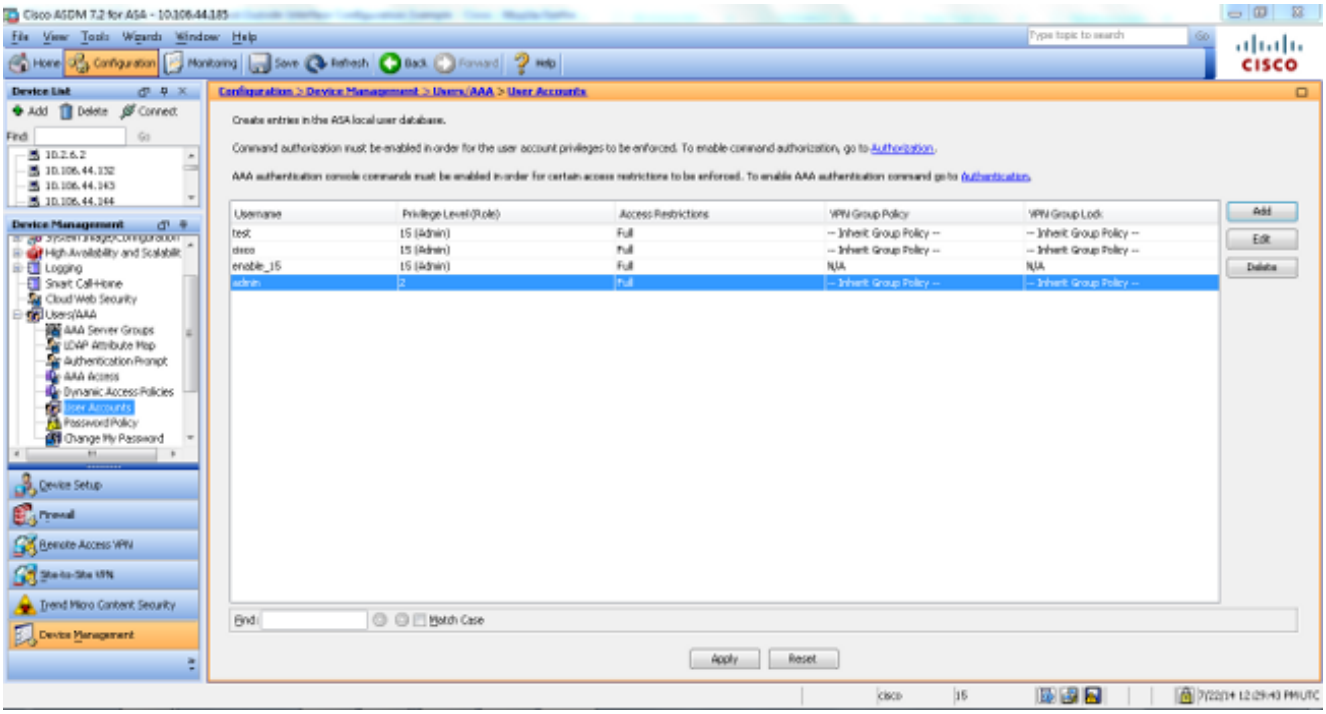
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.255.0
!
interface GigabitEthernet0/1
```

```
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.0

!--- AAA for the SSH configuration

username ciscouser password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL

http server enable
http 172.16.5.0 255.255.255.0 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 172.16.5.20 255.255.255.255 inside
ssh 198.51.100.70 255.255.255.255 outside

!--- Allows the users on the host 172.16.5.20 on inside
!--- Allows SSH access to the user on internet 198.51.100.70 on outside
!--- to access the security appliance
!--- on the inside interface.

ssh 172.16.5.20 255.255.255.255 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
```

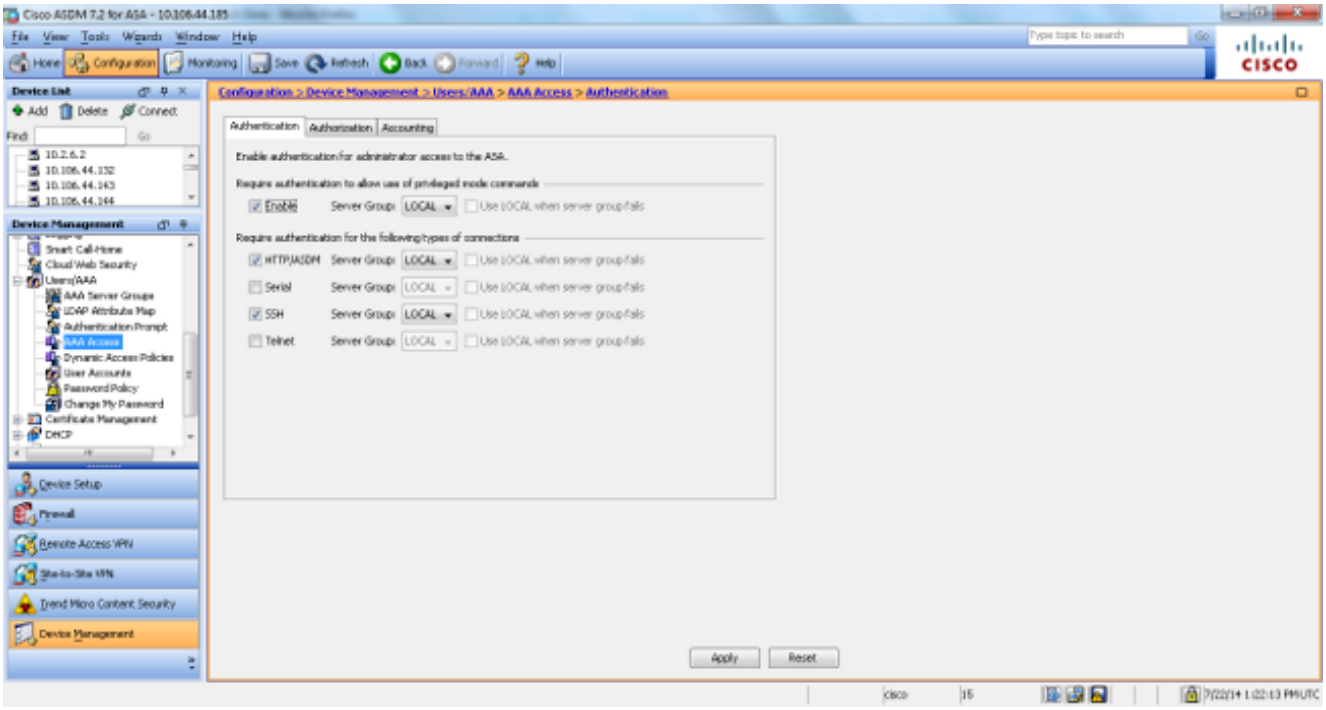
Конфигурация версии 7.2.1 ASDM

Выполните эти шаги для настройки Версии 7.2.1 ASDM:

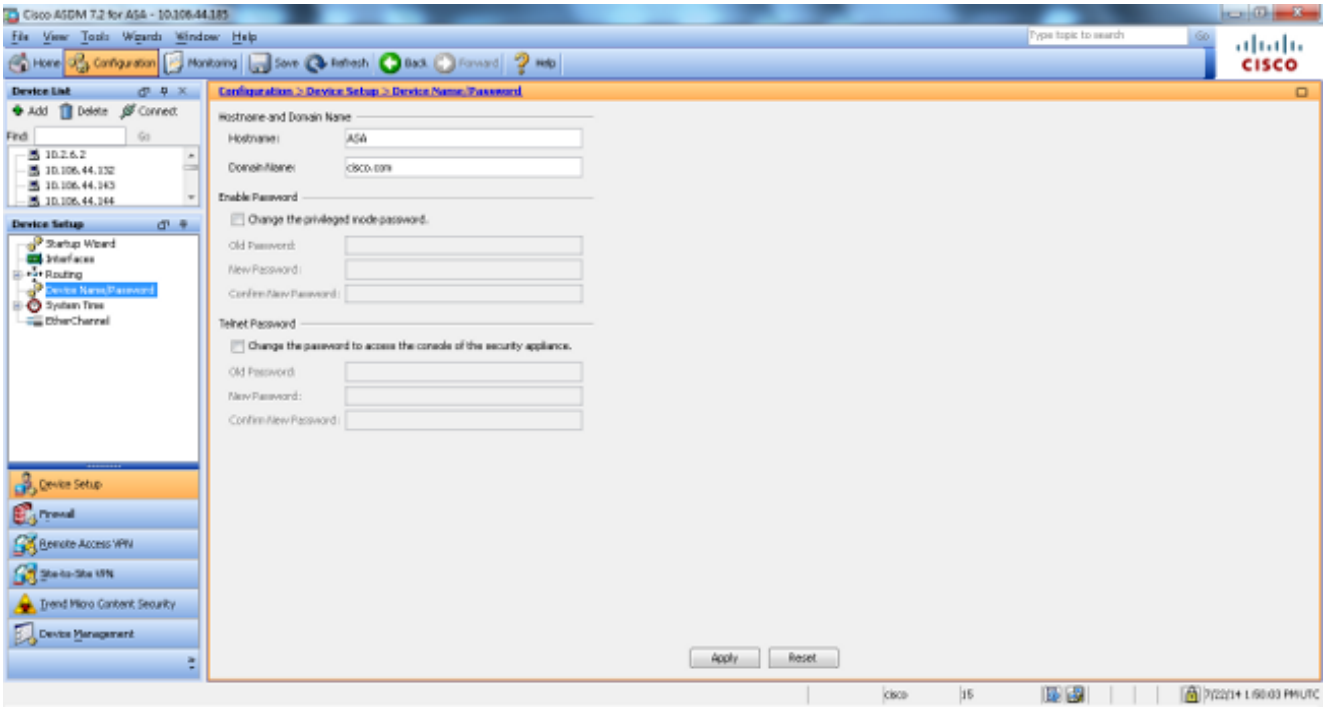
1. Перейдите к **Конфигурации>> Users Управления устройствами / AAA> Учетные записи пользователя** для добавления пользователя с ASDM.



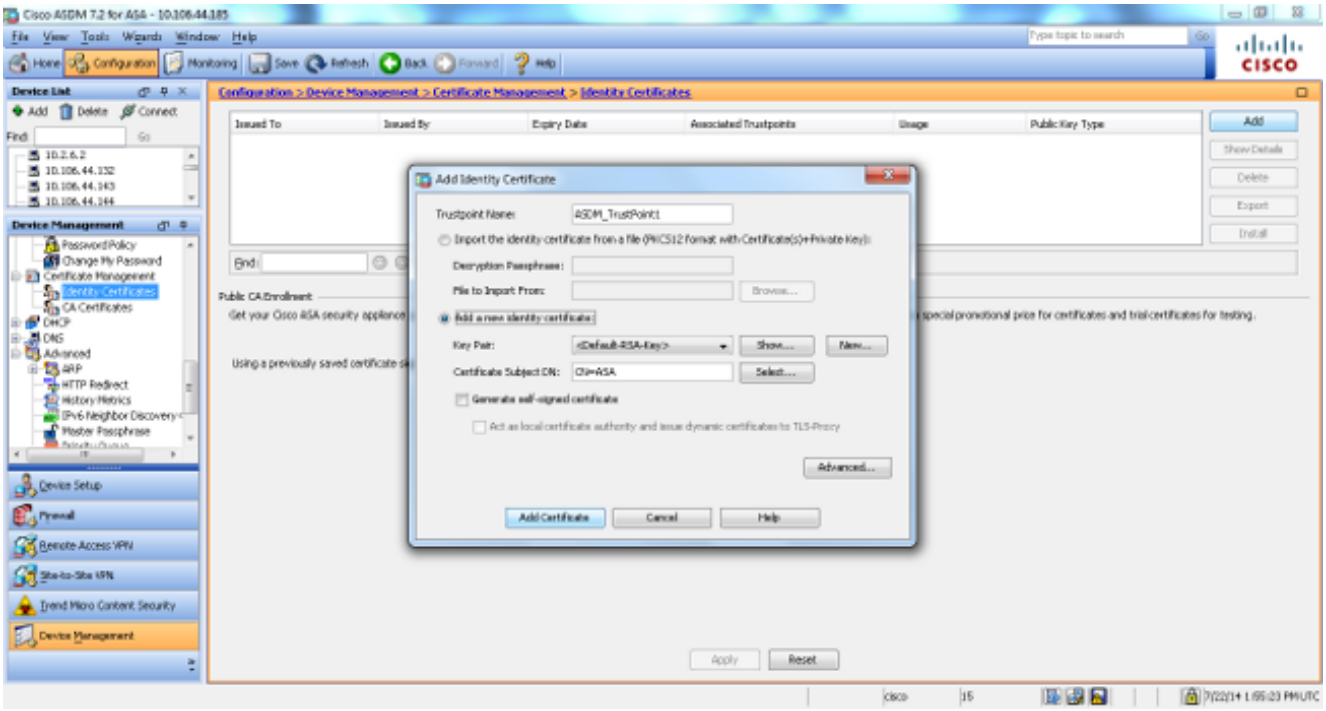
2. Перейдите к **Конфигурации>> Users Управления устройствами / AAA> Доступ AAA> Аутентификация** для устанавливания аутентификации AAA (проверка подлинности, авторизация и учет) для SSH с ASDM.



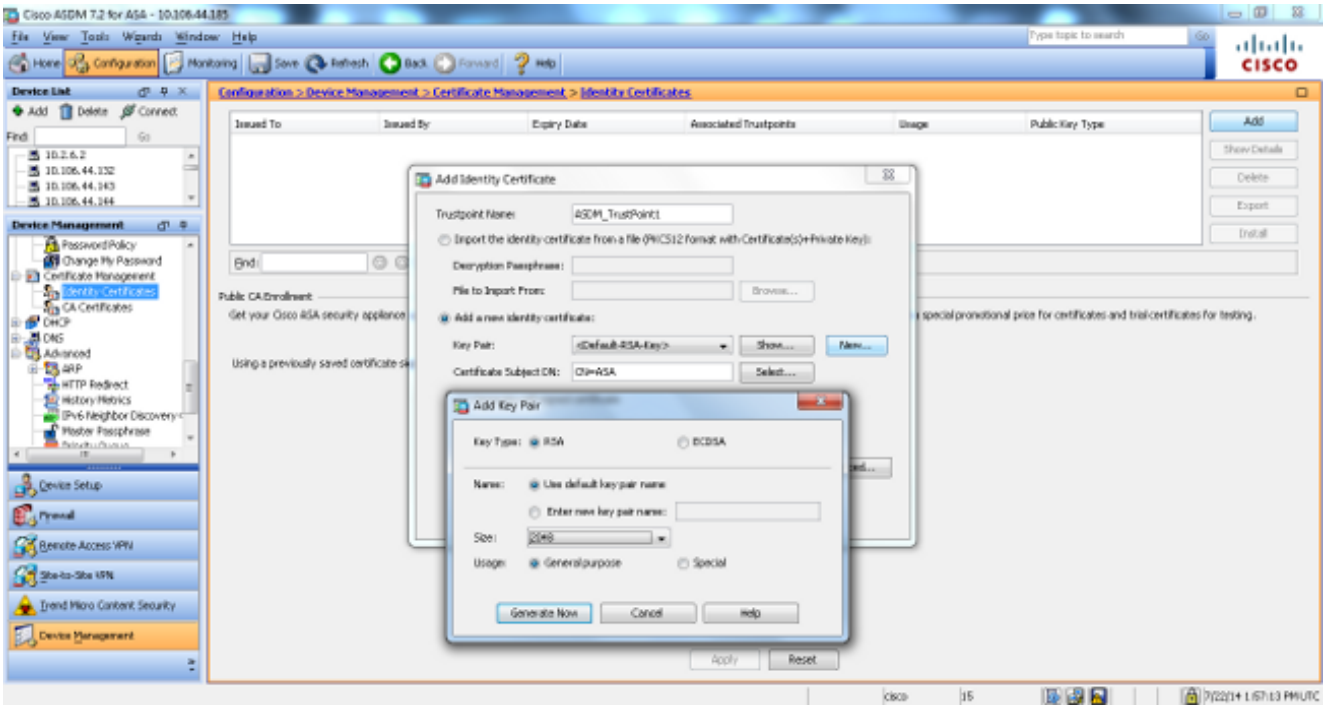
3. Перейдите к **Конфигурации> Настройка устройства> Имя устройства / Пароль** для изменения Пароля Telnet с ASDM.



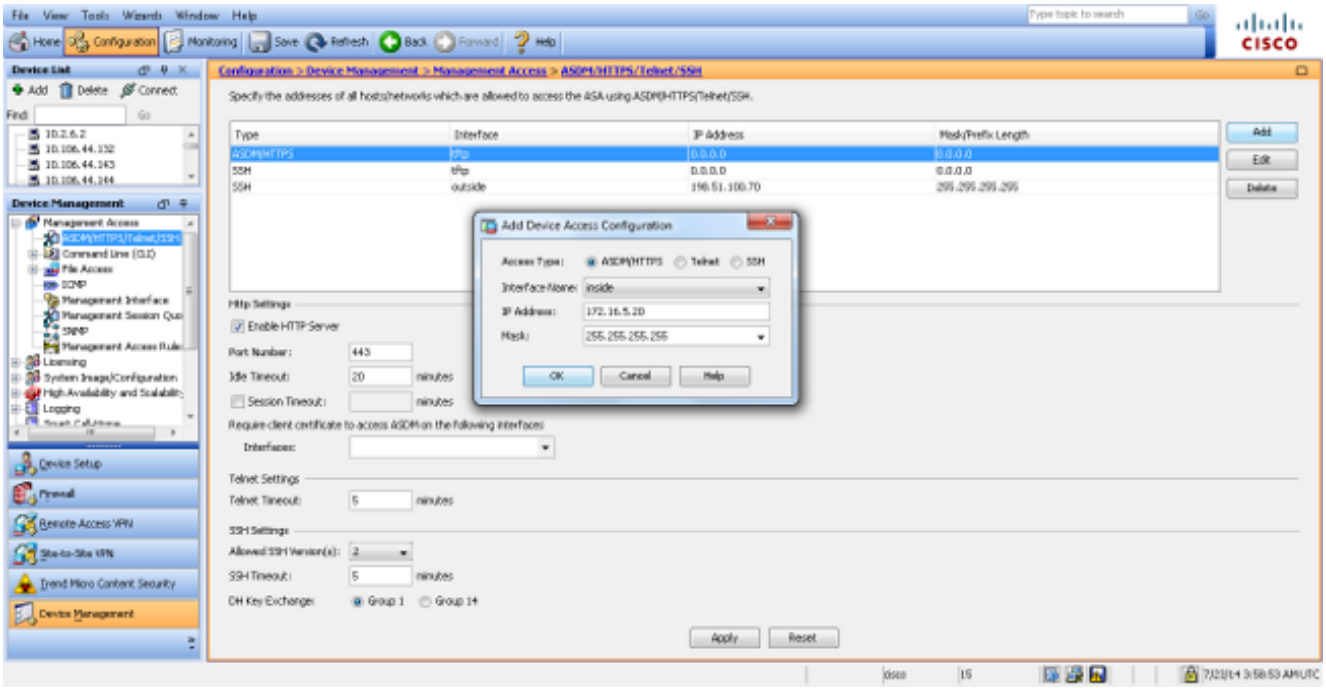
4. Перейдите к **Конфигурации>> Certificate Management Управления устройствами> Сертификаты идентификации**, **нажмите Add** и используйте параметры по умолчанию, которые доступны для генерации тех же ключей RSA с ASDM.



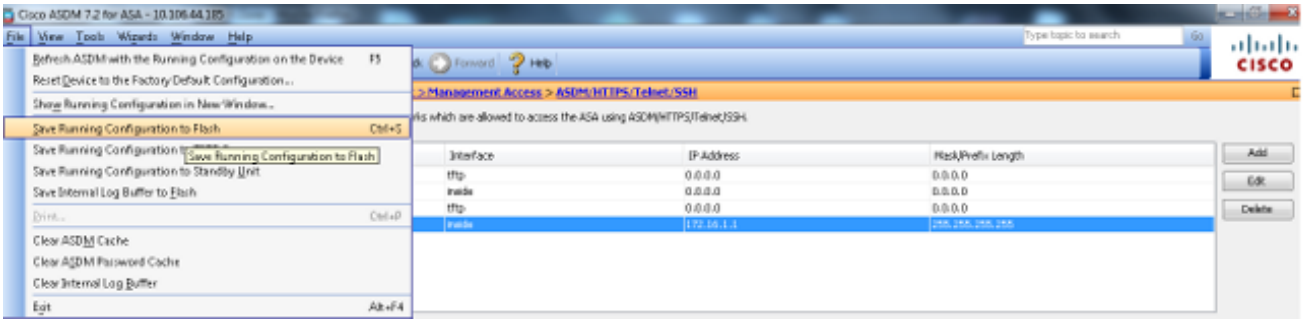
5. Нажмите **Add новая** кнопка с зависимой фиксацией **Сертификата идентификации** и нажмите **New** для добавления пары ключа по умолчанию, если вы не существуете. Однажды завершенный, нажмите **Generate Now**.



6. Перейдите к **Конфигурации> Управление устройствами> Управляющий доступ> Командная строка (CLI)> Secure Shell (SSH)** для использования ASDM так, чтобы можно было задать хосты, которым позволяют соединиться с SSH и для определения версии и параметров таймаута.



7. Нажмите **Save** от всплывающего 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, введите **команду telnet** в режим 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 no**.

```
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 задавать хосты, которые могут обратиться к консоли устройства безопасности через Telnet.

> **Примечание:** Можно включить Telnet к устройству безопасности на всех интерфейсах. Однако устройство безопасности требует, чтобы весь трафик Telnet к внешнему интерфейсу был защищен IPsec. Для включения сеанса Telnet к внешнему интерфейсу настройте IPsec на внешнем интерфейсе так, чтобы это включало IP - трафик, который генерируется устройством безопасности, и включите Telnet на внешнем интерфейсе.

> **Примечание:**. в целом, если какой-либо интерфейс Telnet тому интерфейсу, который имеет уровень безопасности нуля или ниже, чем какой-либо другой интерфейс, ASA не позволяет

> **Примечание:** Cisco не рекомендует доступ к устройству безопасности через сеанс Telnet. Информация об учетных данных для аутентификации, такая как пароль, передается как открытый текст. Cisco рекомендует использовать SSH для большего количества связи защищенных данных.

Введите команду **пароля** для установки пароля для доступа Telnet к консоли. **Пароль по умолчанию – cisco**. Войдите**, кто** дает команду для просмотра IP-адресов, которые в настоящее время обращаются к консоли устройства безопасности. Введите команду **уничтожения** для завершения активного сеанса консоли Telnet.

Примеры сценария telnet

Для включения сеанса Telnet к внутреннему интерфейсу рассмотрите примеры, которые

предоставлены в этом разделе.

Пример 1

Данный пример позволяет только **хосту 172.16.5.20** получать доступ к консоли устройства безопасности через Telnet:

```
ASA(config)#telnet 172.16.5.20 255.255.255.255 inside
```

Пример 2

Данный пример позволяет только сети **172.16.5.0/24** получать доступ к консоли устройства безопасности через Telnet:

```
ASA(config)#telnet 172.16.5.0 255.255.255.0 inside
```

Пример 3

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

```
ASA(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 устройства безопасности и консольного доступа Telnet 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
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

> **Примечание:** Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Используйте OIT для**

просмотра анализа выходных данных команды show.

Debug SSH

Введите **команду debug ssh** для включения отладки SSH:

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

Эти выходные данные показывают попытку SSH от внутреннего IP-адреса (172.16.5.20) к внутреннему интерфейсу ASA. Эти отладки изображают успешное подключение и аутентификацию:

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
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 received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication successful for cisco

!--- Authentication for the ASA 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 неверное имя пользователя введено, такие как **cisco1** вместо **Cisco**, Межсетевой экран ASA отклоняет аутентификацию. Эти выходные данные отладки показывают ошибку проверки подлинности:

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
```

```
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
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 received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA1 was not successful due to the wrong username.
```

Точно так же, если неверный пароль предоставлен, опознавательные сбои. Эти выходные данные отладки показывают ошибку проверки подлинности:

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
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 received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA was not successful due to the wrong password.
```

Обзорные активные сеансы SSH

Введите эту команду для проверки количества Сеансов SSH, которые связаны (и состояние

соединения) к ASA:

```
ASA(config)# show ssh sessions

SID Client IP   Version Mode Encryption Hmac State          Username
0  172.16.5.20 2.0    IN  aes256-cbc sha1 SessionStarted cisco
                         OUT aes256-cbc sha1 SessionStarted cisco
```

Перейдите к **Мониторингу> Свойства> Доступ к устройству> Сеансы Secure Shell** для просмотра сеансов с ASDM.

Введите **команду show asp table socket**, чтобы проверить, что установлен сеанс TCP:

```
ASA(config)# show asp table socket

Protocol Socket State Local Address Foreign Address

SSL 02444758 LISTEN 203.0.113.2:443 0.0.0.0:*
TCP 02448708 LISTEN 203.0.113.2:22 0.0.0.0:*
SSL 02c75298 LISTEN 172.16.5.10:443 0.0.0.0:*
TCP 02c77c88 LISTEN 172.16.5.10:22 0.0.0.0:*
TCP 02d032d8 ESTAB 172.16.5.10:22 172.16.5.20:52234
```

Обзорные общедоступные ключи RSA

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

```
ASA(config)#show crypto key mypubkey rsa
Key pair was generated at: 23:23:59 UTC Jul 22 2014
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Key:

 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
 00aa82d1 f61df1a4 7cd1ae05 c92322c1 1ce490e3 c9db00fd d75afe77 1ea0b2c2
 3325576f a7dc5ffe a6166bf5 7f0f2551 25b8cb23 a8908b49 81c42618 c98e3aea
 ce6f9e42 367974d1 5c2ea6b1 e7aac40b 44a6c0a5 23c4d845 a57d4c04 6de49dbb
 2c6f074e 25e3b19e 7c5da809 ac7d775c 0c01bb9d 211b7078 741094b4 94056e75
 72d5e938 c59baaec 12285005 ee6abf81 90822610 cf7ee4c1 ae8093d9 6943bde3
 16d8748c d86b5f66 1a6ccf33 9cde0432 b3cabab5 938b1874 c3d7c13e 43a95a8f
 ed36db2e f9ca5d2c 0c65858e 3e513723 2d362b47 7984d845 faf22579 654113d1
 24d59f27 55d2ddf3 20af3b65 62f039cb a3aafc31 d92a3d9b 14966eb3 cb6ca249
 55020301 0001
```

Перейдите к **Конфигурации> Свойства> Сертификат> Пара ключей** и нажмите **Show Details** для просмотра ключей RSA с ASDM.

Устранение неполадок

Этот раздел предоставляет сведения, который можно использовать для устранения проблем конфигурации.

Удалите ключи RSA из ASA

В определенных ситуациях, такой как тогда, когда вы обновляете программное обеспечение

ASA или изменяете версию SSH в ASA, вы могли бы быть обязаны удалять и воссоздавать ключи RSA. Введите эту команду для удаления Открытых и секретных ключей криптосистемы RSA из ASA:

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

Перейдите к **Конфигурации> Свойства> Сертификат> Пара ключей** и нажмите **Delete** для удаления ключей RSA с ASDM.

Отказавший SSH - подключение

Вы получаете это сообщение об ошибках на ASA:

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

Это - сообщение об ошибках, которое появляется на машине Клиента SSH:

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

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

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

Введите эту команду для генерации нового ключа:

```
ASA(config)# crypto key generate rsa modulus 2048
```