

Настраиваем SSH на беспроводных точках доступа Cisco

В данной статье пойдёт речь о том, как настроить Secure Shell (SSH) на беспроводных точках доступа (AP – Access Point) Cisco.

Требования

Прежде чем использовать данный документ в рабочей среде, убедитесь в следующем:

- У Вас есть резервная копия конфигураций и имиджа Cisco IOS беспроводных точек доступа
- Вы знаете, как настраивать Cisco Aironet AP
- Вы понимаете, как работает SSH и зачем он нужен. Подробнее о SSH написано по следующей ссылке <http://ru.wikipedia.org/wiki/SSH>

Используемые компоненты

Информация в данном документе базируется на следующем оборудовании и ПО:

- Точки доступа Aironet серии 1200 с Cisco IOS Software Release 12.3(8)JEB
- ПК или ноутбук с SSH клиентом

Примечание: SSH клиент, рассматриваемый в данном документе, используется исключительно для проверки настроек. Вы можете использовать любой другой SSH клиент, если возникнет такая необходимость.

Информация в данном документе была собрана посредством лабораторных работ в тестовой среде. Все устройства были с заводскими установками. Прежде чем использовать данные из этой статьи в рабочей сети убедитесь в том, что Вы осознаёте все действия.

Доступ к интерфейсу командной строки (CLI) точки доступа Cisco Aironet

Вы можете использовать следующие средства для доступа к CLI точек доступа Cisco Aironet AP:

- Консольный порт
- Telnet
- SSH

Если в AP присутствует консольный порт и у Вас есть физический доступ к данному порту, то лучшей использовать именно этот метод доступа, для манипуляций с настройками.

Если у Вас нет возможности использовать консольный порт, то можете воспользоваться протоколами Telnet или SSH для настройки AP.

Как Вы наверное знаете, протокол Telnet использует 23 для соединений. Telnet передаёт и принимает данные открытым текстом. В связи с этим не рекомендуется использовать

данный протокол в WAN (внешних) сетях, потому что есть большая угроза перехвата злоумышленником Ваших данных, будь то конфигурация или пароль. Спецификацию протокола Telnet смотрите по ссылке <http://www.ietf.org/rfc/rfc854.txt>.

SSH – это приложение и протокол, который предоставляет безопасную замену инструментам Berkley r-tools. Протокол SSH предоставляет возможность использовать безопасное соединение с оборудованием второго или третьего сетевого уровня. Существует несколько версий протокола SSH – первая и вторая соответственно. Используемый в данном документе IOS (описан выше) поддерживает обе версии. Если клиентом не задана версия протокола SSH, то по умолчанию будет использоваться SSH второй версии.

Примечание: Функция SSH, используемая в данном релизе Cisco IOS, не поддерживает IP Security (IPSec).

Вы можете настроить SSH как через командную строку так и через WEB интерфейс. В данном документе описаны оба метода.

Конфигурация

Настраиваем SSH при помощи командной строки

Для включения SSH доступа на AP, Вы в первую очередь должны настроить AP в качестве SSH сервера. Ниже описаны инструкции, которые помогут реализовать данный функционал, используя CLI:

1. Настраиваем имя хоста и имя домена для AP.

```
AP#configure terminal

!--- Входим в режим глобальной конфигурации на AP.

AP<config>#hostname Test

!--- В данном примере "Test" это имя нашей AP (host name).

Test<config>#ip domain name abc.com

!--- Данной командой мы настраиваем AP на использование доменного имени "abc.com" .
```

2. Генерируем RSA ключ для нашей AP.

Генерация RSA ключа задействует SSH на AP. Команду необходимо выполнять в режиме глобальной конфигурации:

```
Test<config>#crypto key generate rsa rsa_key_size

!--- Этим мы генерируем RSA ключ и включаем SSH сервер.
```

Примечание: Рекомендуется устанавливать минимальную длину в 1024 для RSA ключа.

3. Настраиваем пользовательскую аутентификацию на AP.

На беспроводной точке доступа Cisco у Вас есть возможность настроить как локальную, так и внешнюю аутентификацию, авторизацию и аккаунтинг (мы говорим об AAA сервере). В данном примере мы рассмотрим создание локальных пользователей:

```
Test<config>#aaa new-model

!--- Задействуем AAA аутентификацию.

Test<config>#aaa authentication login default local none

!--- Используем локальную базу данных, для аутентификации
пользователей.

Test<config>#username Test password Test123

!--- Создаём пользователя с именем "Test" и паролем "Tetst123".

Test<config>#username ABC password xyz123

!--- Создаём ещё одного пользователя с именем "ABC" и паролем "
xyz123".
```

Данными командами мы задействовали пользовательскую аутентификацию на нашей AP для использования ей (AP) локальной базы пользователей.

4. Настраиваем параметры SSH.

```
Test<config>#ip ssh {[timeout seconds] | [authentication-retries
integer]}

!--- Данная команда может использоваться для более тонкой
настройки SSH на AP.
```

Примечание: Вы можете выставить тайм аут в секундах, который не может превышать значения 120 (больше 120 секунд сделать нельзя). По умолчанию тайм аут равен 120 секундам. Данное значение применяется к фазе инициализации (клиент подключается к серверу) SSH. Вы так же можете задать количество неудачных попыток аутентификации, но это количество не может превышать пяти. По умолчанию разрешено три неудачных попытки входа.

Настраиваем SSH на беспроводной точке доступа Cisco, используя Web интерфейс

Следуйте следующим шагам, чтобы настроить SSH через WEB интерфейс:

1. Выполните вход на AP, используя браузер.

После входа появится примерно следующее:

The screenshot shows the Cisco Aironet 1200 Series Access Point configuration page. The left sidebar contains a menu with options: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area displays the following information:

- Hostname: ap
- ap uptime is 2 minutes
- Home: Summary Status
- Association: Clients_0, Repeaters_0
- Network Identity: IP Address 10.0.0.2, MAC Address 000e.d77c.343e
- Network Interfaces: A table with columns Interface, MAC Address, and Transmission Rate.
- Event Log: A table with columns Time, Severity, and Description.

Interface	MAC Address	Transmission Rate
FastEthernet	000e.d77c.343e	100Mb/s
Radio0-802.11B	000d.eded.708a	11.0Mb/s
Radio1-802.11A	000e.8405.0d4d	54.0Mb/s

Time	Severity	Description
Mar 1 00:01:46.786	Notification	Configured from console by console
Mar 1 00:00:26.801	Notification	Line protocol on interface BV11, changed state to up
Mar 1 00:00:26.769	Notification	Line protocol on interface Dot11Radio0, changed state to down
Mar 1 00:00:26.765	Notification	Line protocol on interface Dot11Radio1, changed state to down
Mar 1 00:00:25.898	Notification	SNMP agent on host ap is undergoing a cold start
Mar 1 00:00:25.898	Notification	System restarted --
Mar 1 00:00:25.819	Warning	Unexpected end of configuration file.

2. Нажмите **Services** в левом меню.

The screenshot shows the Cisco Aironet 1200 Series Access Point configuration page with the Services menu item highlighted in the left sidebar. The main content area displays the Services Summary table:

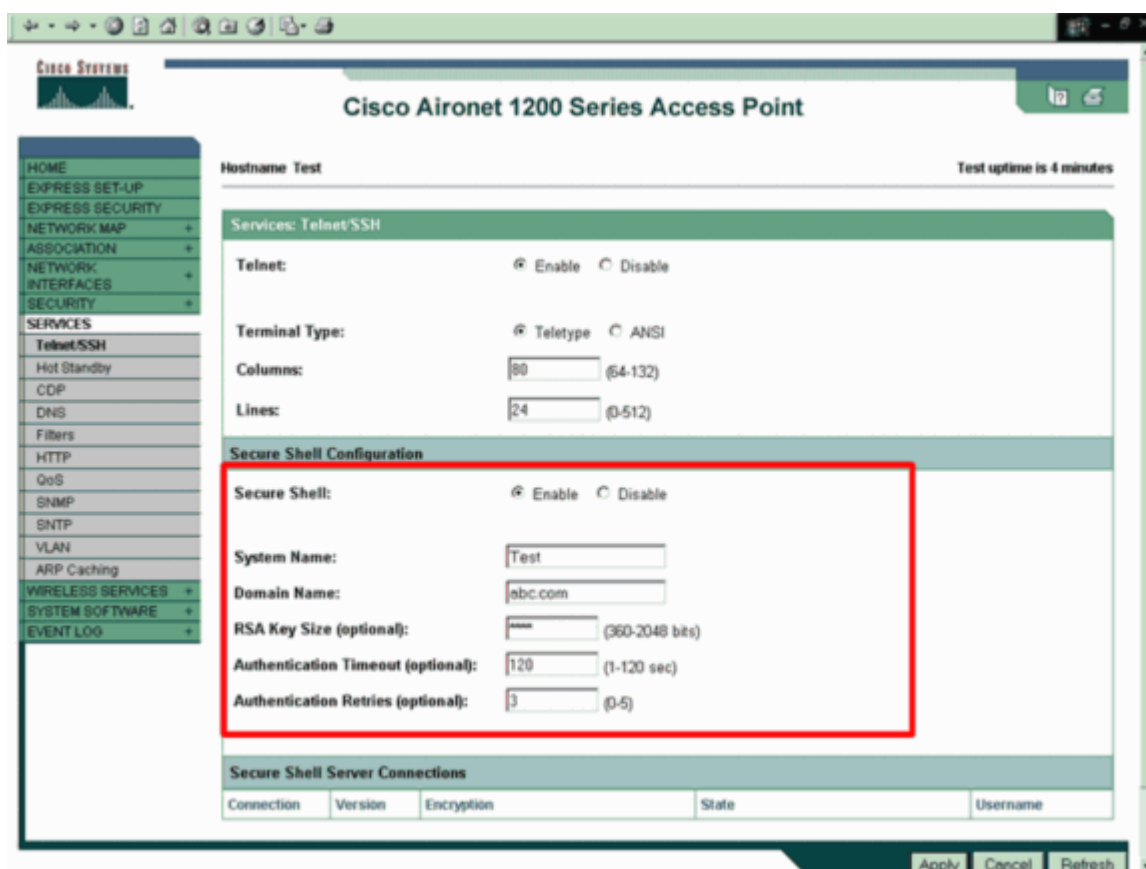
Services Summary	
TeletypeSSH: Enabled/Disabled	Hot Standby: Disabled
CDP: Enabled	DNS: Disabled
Filters: Disabled	HTTP: Enabled
QoS: Disabled	SNMP: Disabled
SNTP: Disabled	VLAN: Disabled
ARP Caching: Disabled	

3. Нажмите на ссылку **Telnet/SSH** для настройки параметров Telnet/SSH.

Закладка **Services**: Отображает настройки для Telnet/SSH. Прокрутите экран вниз до **Secure Shell Configuration**. Нажмите **Enable** beside Secure Shell и введите свои параметры, пример которых представлен ниже:

Пример параметров:

- System Name: Test
- Domain Name: abc.com
- RSA Key Size: 1024
- Authentication Timeout: 120
- Authentication Retries: 3



4. Нажмите **Apply** для сохранения сделанных изменений.

Проверка

В данной секции описаны методы, при помощи которых можно проверить настройки SSH.

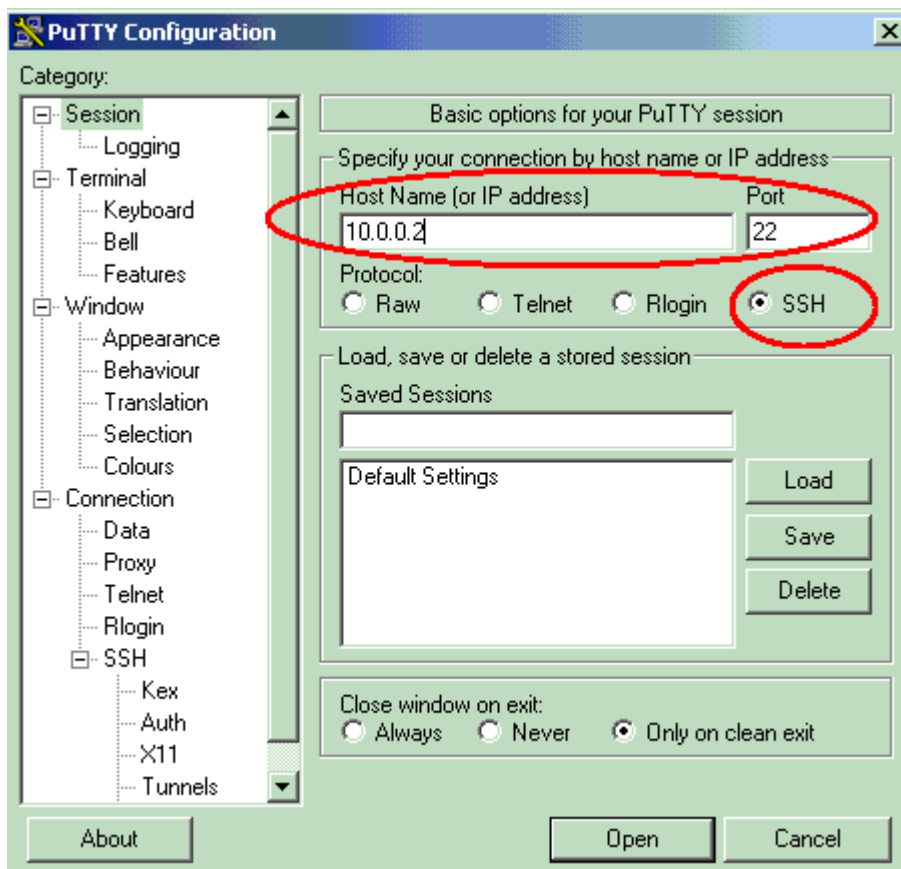
- **show ip ssh**— отображает включен ли SSH на AP, какой он (SSH) версии и прочее. Рассмотрим пример:

```
Test#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

- **show ssh**— позволяет просматривать статус соединений SSH сервера.

```
Test#show ssh
Connection Version Mode Encryption Hmac      State      Username
0      2.0  IN aes256-cbc hmac-sha1  Session started  ABC
0      2.0  OUT aes256-cbc hmac-sha1  Session started  ABC
```

Теперь давайте попробуем подключиться к беспроводной точке доступа Cisco, используя ПК/ноутбук и SSH клиент. В данной примере у точки доступа ip адрес 10.0.0.2:





Решение проблем

Убедитесь в том, что Вы верно ввели команду для генерации RSA ключа. В большинстве случаев проблема с доступом по SSH заключается именно в этом.

Отключение SSH

Для того, чтобы отключить SSH на AP Вам необходимо удалить пару RSA ключей с устройства беспроводного доступа. Для этого используйте команду **crypto key zeroize rsa**. После удаления пары RSA ключей сервер SSH будет автоматически отключен на беспроводной точке доступа Cisco. Рассмотрим пример:

```
Test(config)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
```

Более подробно о настройке сервера SSH на беспроводных точках доступа Cisco [написано в официальной документации](#).

Если у Вас появились вопросы, можете задать их в форуме.