Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Условные обозначения](#)
[Настройка](#)
[Настройте PuTTYgen](#)
[Проверка](#)
[Аутентификация RSA](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)

Введение

Этот документ объясняет, как использовать Ключевой генератор для PuTTY (PuTTYgen) для генерации авторизовавших ключей Secure Shell (SSH) и аутентификации RSA для использования на Cisco Secure Intrusion Detection System (IDS). Основная проблема при установлении авторизовавших ключей SSH - то, что только более старый формат ключа RSA1 приемлем. Это означает, что необходимо сказать ключевому генератору создавать ключ RSA1, и необходимо ограничить Клиента SSH для использования протокола SSH1.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Последний putty - 7 февраля 2004
- Cisco Secure IDS

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.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании

условных обозначений, используемых в технической документации Cisco.

Настройка

В данном разделе содержится информация о настройке функций, описанных в этом документе.

Примечание: Для поиска дополнительных сведений о командах в данном документе используйте Средство поиска команд (только для зарегистрированных клиентов).

Настройте PuTTYgen

Выполните эти шаги для настройки PuTTYgen.

1. PuTTYgen запуска.
2. Нажмите тип ключа **SSH1** и определите номер битов в генерируемом ключе к **2048** в группе Параметров у основания диалогового окна.
3. Нажмите **Generate** и следуйте инструкциям.Основная информация отображена в верхнем разделе диалогового окна.
4. Очистите окно редактирования Key Comment.
5. Выберите весь текст в Открытом ключе для вставки в authorized_keys файл и нажмите **Ctrl-C**.
6. Введите пароль в Ключевом пароле и Подтвердите окна редактирования пароля.
7. Нажмите **секретный ключ Save**.
8. Сохраните файл закрытого ключа PuTTY в каталог private к вашему входу в систему Windows (в Документах и Параметрах настройки / (идентификатор пользователя) / Мое поддерево Документов в Windows 2000/XP).
9. Запуск PuTTY.
10. Создайте новый Сеанс PuTTY, как замечено здесь:**Сеанс:IP-адрес:** IP-адрес Детектора обнаружения несанкционированного доступа (IDS Sensor)**Протокол:** SSH**Порт:** 22**Соединение:Имя пользователя автовхода в систему:** Cisco (может также быть вход в систему, который вы используете на Датчике),**Соединение/SSH:Предпочтительная версия SSH:** 1 только**Соединение/SSH/Аутентификация:Файл закрытого ключа для аутентификации:** Перейдите к файлу.PPK, хранившему в шаге 8.**Сеанс:** (назад к вершине)**Сохраненные сеансы:** (введите имя датчика, нажмите **Save**),
11. Нажмите **Open** и используйте проверку подлинности с помощью пароля для соединения с CLI Датчика, так как открытый ключ еще не находится на Датчике.
12. Введите команду CLI **configure terminal** и нажмите **Enter**.
13. Введите **санкционированный ключ ssh mykey** команда CLI, но не нажимайте Enter в это время. Удостоверьтесь и введите пространство в конце.
14. Щелкните правой кнопкой мыши в окне терминала PuTTY.Содержимое буфера обмена, скопированное в шаге 5, введено в CLI.
15. **!--- Нажмите клавишу Enter.**
16. Введите **команду выхода** и нажмите **Enter**.
17. Подтвердите, что санкционированный ключ введен должным образом. Введите **команду show ssh authorized-keys mykey** и нажмите **Enter**.
18. Введите **команду выхода**, чтобы оставить CLI IDS и нажать **Enter**.

Проверка

Аутентификация RSA

Выполните следующие действия.

1. Запуск PuTTY.
2. Найдите Сохраненный Сеанс, созданный в шаге 10 и двойном нажатии на нем. Окно терминала PuTTY открывается, и этот текст появляется:
3. Введите пароль с закрытым ключом, который вы создали в шаге 6, и нажмите **Enter**.В вас автоматически входят.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Страницы технической поддержки обнаружения несанкционированного доступа в сеть
- Cisco Systems – техническая поддержка и документация