Лабораторная работа №8. Доступ к сетевым устройствам по протоколу SSH и обеспечение безопасности сетевых устройств

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1_ФАМИЛИЯ	G0/1	192.168.1. X	255.255.255.0	—
S1	VLAN 1	192.168.1. X+10	255.255.255.0	192.168.1. X
PC-A	NIC	192.168.1. X+20	255.255.255.0	192.168.1. X

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка маршрутизатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

Часть 3. Настройка коммутатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

Часть 4. Настройка протокола SSH через интерфейс командной строки (CLI) коммутатора

Часть 5. Защита лабораторной работы (ответ контрольные вопросы и вопросы преподавателя)

Необходимые ресурсы

- 1 маршрутизатор Cisco
- 1 коммутатор Cisco
- 1 ПК (Windows 7 или 8 с программой эмуляции терминала Tera Term или Putty)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров устройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе. Вместо X в последнем октете IP-адресов запишите собственные значения (X – номер студента в журнале). Они вам понадобятся при настройке узлов.

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.

b. Войдите в режим глобальной конфигурации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

d. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.

f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.

g. Зашифруйте открытые пароли.

h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

i. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.

j. Сделайте так, чтобы маршрутизатор блокировал попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введен неверный пароль.

k. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Установите более надежные пароли.

Примечание. Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли cisco и class.

a. Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями. Установите следующий пароль: **Enablep@55**.

b. Установите минимальную длину 10 символов для всех паролей.

Шаг 5: Настройте компьютер PC-A.

c. Настройте для PC-A IP-адрес и маску подсети.

d. Настройте для PC-A шлюз по умолчанию.

Шаг 6: Проверьте подключение к сети.

Пошлите с PC-A эхо-запрос на маршрутизатор R1_ФАМИЛИЯ. Убедитесь, что эхо-запрос выполнен успешно.

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.

a. Задайте имя устройства.

b. Задайте домен для устройства.

Шаг 2: Создайте ключ шифрования с указанием его длины.

a. Установите ключ шифрования с длиной 1024 бит.

Шаг 3: Создайте имя пользователя в локальной базе учетных записей.

a. Создайте имя пользователя и пароль для него с максимальными привилегиями. Используйте имя пользователя **SSHadmin** и пароль **Admin1p@55**.

Примечание. Уровень привилегий 15 дает пользователю права администратора.

Шаг 4: Активируйте протокол SSH на линиях VTY.

a. Активируйте протокол SSH на входящих линиях VTY.

b. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

Подсказка: данная команда начинается со слова **login**.

Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 6: Установите соединение с маршрутизатором по протоколу SSH.

a. Запустите Tera Term с PC-A.

b. Установите SSH-подключение к R1_ФАМИЛИЯ. Используйте имя пользователя **admin** и пароль **adminpass**. У вас должно получиться установить SSH-подключение к R1_ФАМИЛИЯ.

Шаг 7: Убедитесь, что все меры безопасности внедрены правильно.

a. Подключитесь к маршрутизатору R1_ФАМИЛИЯ по протоколу Telnet. Разрешает ли R1_ФАМИЛИЯ подключение по протоколу Telnet? Дайте пояснение.

b. Подключитесь к маршрутизатору R1_ФАМИЛИЯ по протоколу SSH. Разрешает ли R1_ФАМИЛИЯ подключение по протоколу SSH?

c. Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток.

Что произошло после ввода неправильных данных для входа в систему во второй раз?

d. Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведенном ниже примере команда **show login** была введена в течение 30-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме Quiet.

e. По истечении 30 секунд повторите попытку подключения к R1_ФАМИЛИЯ по протоколу SSH и войдите в систему, используя имя **SSHadmin** и пароль **Admin1p@55**.

Что отобразилось после успешного входа в систему?

f. Войдите в привилегированный режим EXEC и введите в качестве пароля **Enablep@55**.

Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 120 секунд? Дайте пояснение.

Часть 3: Настройка коммутатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

Шаг 1: Настройте основные параметры коммутатора.

a. Подключитесь к коммутатору с помощью консольного подключения и активируйте привилегированный режим EXEC.

b. Войдите в режим конфигурации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

d. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.

f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.

g. Зашифруйте открытые пароли.

e. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

f. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.

h. Сделайте так, чтобы маршрутизатор блокировал попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введен неверный пароль.

g. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 2: Настройте коммутатор для соединения по протоколу SSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

a. Настройте имя устройства, как указано в таблице адресации.

b. Задайте домен для устройства.

c. Создайте ключ шифрования с указанием его длины.

d. Создайте имя пользователя в локальной базе учетных записей.

e. Активируйте протоколы Telnet и SSH на линиях VTY.

f. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

Шаг 3: Установите более надежные пароли.

a. Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями. Установите следующий пароль: **Enablep@55**.

b. Установите минимальную длину 10 символов для всех паролей.

Шаг 4: Убедитесь, что все неиспользуемые порты отключены.

По умолчанию порты коммутатора включены. Отключите на коммутаторе все неиспользуемые порты.

a. Проверьте состояние портов коммутатора.

Шаг 5: Установите соединение с коммутатором по протоколу SSH.

С компьютера PC-A установите подключение по протоколу SSH к интерфейсу SVI коммутатора S1.

Удалось ли вам установить SSH-соединение с коммутатором?

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

a. Убедитесь, что протокол Telnet на коммутаторе отключен.

b. Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

c. По истечении 30 секунд повторите попытку подключения к R1_ФАМИЛИЯ по протоколу SSH и войдите в систему, используя имя пользователя **SSHadmin** и пароль **Admin1p@55**.

   Появился ли баннер после успешного входа в систему?

d. Войдите в привилегированный режим EXEC, используя **Enablep@55** в качестве пароля.

Часть 4: Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора

Клиент SSH встроен в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 4 вам предстоит установить соединение с маршрутизатором по протоколу SSH, используя интерфейс командной строки коммутатора.

Шаг 1: Посмотрите доступные параметры для клиента SSH в Cisco IOS.

Используйте вопросительный знак (**?**), чтобы отобразить варианты параметров для команды **ssh**. Какие параметры вы видите?

Шаг 2: Установите с коммутатора S1 соединение с маршрутизатором R1_ФАМИЛИЯ по протоколу SSH.

a. Чтобы подключиться к маршрутизатору R1_ФАМИЛИЯ по протоколу SSH, введите команду **ssh –l admin 192.168.1. X**. Это позволит вам войти в систему под именем **admin**. При появлении приглашения введите в качестве пароля **adminpass**.

b. Чтобы вернуться к коммутатору S1, не закрывая сеанс SSH с маршрутизатором R1_ФАМИЛИЯ, нажмите комбинацию клавиш **Ctrl**+**Shift**+**6**. Отпустите клавиши **Ctrl**+**Shift**+**6** и нажмите **x**. Отображается приглашение привилегированного режима EXEC коммутатора.

c. Чтобы вернуться к сеансу SSH на R1_ФАМИЛИЯ, нажмите клавишу Enter в пустой строке интерфейса командной строки. Чтобы увидеть окно командной строки маршрутизатора, нажмите клавишу Enter еще раз.

d. Завершите сеанс SSH на маршрутизаторе R1_ФАМИЛИЯ.

Часть 5: Защита лабораторной работы (ответ контрольные вопросы и вопросы преподавателя)

1. Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?
2. Какие версии протокола SSH поддерживаются при использовании интерфейса командной строки?

