**Домашнее задание**

|  |  |
| --- | --- |
| Дисциплина | Защита компьютерных сетей и систем |
| Тема | Тема 31. Защита сетевых устройств |
| Форма проверки | **Автоматическая проверка** |
| Имя преподавателя | Антон Носков |
| Время выполнения | 120 минут |
| Цель задания | Закрепить навыки по настройке аутентификации OSPF MD5  Научиться настраивать:   * NTP * маршрутизаторы для записи сообщений в журнал на сервере Syslog * маршрутизатор для защищённого управления с помощью протокола SSH |
| Инструменты для выполнения ДЗ | Компьютер, симулятор сети передачи данных Cisco Packet Tracer 8.1.1, подключённый к интернету |
| Правила приёма работы | * Чтобы выполнить задание, используйте Cisco Packet Tracer * Выполнив задание, нажмите Check Results (Проверить результаты), чтобы просмотреть отзыв и проверить завершённые обязательные компоненты * Файл с выполненным заданием сохраните под своей фамилией и разместите в ЛМС **(ФИО.pka)** |
| Критерии оценки | **Задание считается выполненным, если:**  - Check Results выдаёт положительный отзыв и все обязательные компоненты выполнены  - ссылка на файл с сохранённым заданием размещена в ЛМС  **Задание не выполнено, если:**  - Check Results выдаёт ошибки — нужно проработать ошибки и выполнить Check Results ещё раз  - ссылка на файл с заданием не размещена в ЛМС |
| Дедлайн | *2 недели после вебинара (точную дату см. в ЛМС)* |

**Описание задания**

**Прежде чем выполнять задание:**

1. **Посмотрите запись вебинаров по теме 14 «Мониторинг сетевой инфраструктуры» и теме 31 «Защита сетевых устройств».**
2. **Установите симулятор сети передачи данных Cisco Packet Tracer 8.1.1**

* <https://disk.yandex.ru/d/SdBaqlDc012UYA> — Cisco Packet Tracer 8.1.1 — windows 64;
* <https://disk.yandex.ru/d/dU9AL1YstQzFGg> — Cisco Packet Tracer 8.1.1 — ubuntu 64;
* <https://disk.yandex.ru/d/jwvB6MfZyPZ5sw> — Cisco Packet tracer 8.1.1 — MacOS X.

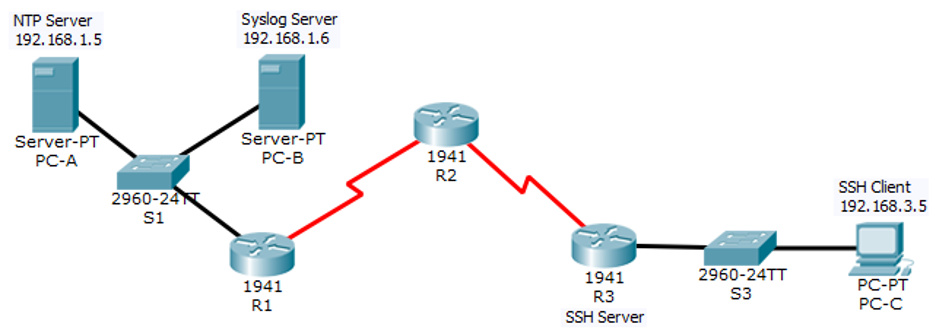
**Инструкция по установке**

Когда Cisco Packet Tracer выдаёт запрос авторизации, выберите Skills for all и авторизуйтесь через учётную запись Google. В ряде сетей может потребоваться VPN при запуске Cisco Packet Tracer.

После установки Cisco Packet Tracer откройте файл **Syslog, NTP, and SSH.pka***(размещён в ЛМС)* и начинайте выполнять задание.

**Исходные данные**

**Топология сети**



**Таблица адресации**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** | **Порт коммутатора** |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | Н/П | S1 F0/5 |
| S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | Н/П | Н/П |
| R2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | Н/П | Н/П |
| S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | Н/П | Н/П |
| R3 | G0/1 | 192.168.3.1 | 255.255.255.0 | Н/П | S3 F0/5 |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 | Н/П | Н/П |
| PC-A | NIC | 192.168.1.5 | 255.255.255.0 | 192.168.1.1 | S1 F0/6 |
| PC-B | NIC | 192.168.1.6 | 255.255.255.0 | 192.168.1.1 | S2 F0/18 |
| PC-C | NIC | 192.168.3.5 | 255.255.255.0 | 192.168.3.1 | S3 F0/18 |

**Исходный сценарий**

В этом задании вы настроите аутентификацию OSPF MD5 для защиты обновлений маршрутизации.

NTP Server является главным NTP-сервером в этом задании. Вы настроите аутентификацию на NTP-сервере и маршрутизаторах. Вы настроите маршрутизаторы так, чтобы разрешить NTP-серверу синхронизировать программные часы с сервером времени. Вы также настроите маршрутизаторы для периодического обновления аппаратных часов с учётом времени, полученного с NTP-сервера.

Сервер Syslog будет обеспечивать ведение журнала сообщений в этом задании. Вы настроите маршрутизаторы для определения удалённого хоста (сервера Syslog), который будет получать регистрируемые сообщения.

Вам потребуется настроить сервис временных меток для ведения журналов на маршрутизаторах. Очень важно, чтобы в сообщениях Syslog отображались правильные дата и время, когда Syslog используется для мониторинга сети.

Вы настроите маршрутизатор R3 для защищённого управления с помощью протокола SSH вместо Telnet. Серверы были предварительно настроены на использование сервисов NTP и Syslog соответственно. NTP не будет требовать аутентификацию. На маршрутизаторах были предварительно настроены следующие пароли:

· пароль привилегированного доступа: **ciscoenpa55;**

· пароль для линий VTY: **ciscovtypa55.**

**Примечание**. MD5 — самый стойкий алгоритм шифрования, поддерживаемый в версии Packet Tracer. Хотя MD5 имеет известные уязвимости, следует использовать алгоритм шифрования, отвечающий требованиям вашей организации по безопасности. В этом задании требования по безопасности предписывают использовать MD5.

**Часть 1. Настройте аутентификацию OSPF MD5**

**Шаг 1.** Проверьте связь. Все устройства должны успешно отправлять эхо-запросы по всем прочим IP-адресам.

**Шаг 2.** Настройте аутентификацию OSPF MD5 для всех маршрутизаторов в зоне 0.

R1(config)# **router ospf 1**

R1(config-router)# **area 0 authentication message-digest**

**Шаг 3.** Настройте ключ MD5 для всех маршрутизаторов в зоне 0.

Настройте ключ MD5 на последовательных интерфейсах маршрутизаторов **R1, R2** и **R3.** Используйте пароль **MD5pa55** для ключа **1**.

R1(config)# **interface s0/0/0**

R1(config-if)# **ip** **ospf message-digest-key 1 md5 MD5pa55**

**Шаг 4.** Проверьте конфигурации.

a. Проверьте конфигурации аутентификации MD5 с помощью команд **show ip ospf interface**.

b. Проверьте сквозную связь.

**Часть 2. Настройте NTP**

**Шаг 1.** Включите аутентификацию NTP на компьютере PC-A.

a. На компьютере **PC-A** выберите **NTP** на вкладке Services, чтобы проверить, включена ли служба NTP.

b. Чтобы настроить аутентификацию NTP, нажмите **Enable** (Включить) в разделе Authentication. Используйте ключ **1** и пароль **NTPpa55** для аутентификации.

**Шаг 2.** Настройте маршрутизаторы R1, R2 и R3 как клиентов NTP.

Проверьте конфигурацию клиентов с помощью команды **show ntp status**.

**Шаг 3.** Настройте маршрутизаторы на обновление аппаратных часов.

Настройте маршрутизаторы R1, R2 и R3 на периодическое обновление аппаратных часов с учётом времени, полученного с NTP-сервера.

Выйдите из режима глобальной настройки и убедитесь, что аппаратные часы были обновлены, с помощью команды **show clock**.

**Шаг 4.** Настройте аутентификацию NTP на маршрутизаторах.

Настройте аутентификацию NTP на маршрутизаторах **R1**, **R2** и **R3**, используя ключ **1** и пароль **NTPpa55**.

R1(config)# **ntp authenticate**

R1(config)# **ntp trusted-key 1**

R1(config)# ntp authentication-key 1 md5 NTPpa55

**Шаг 5.** Настройте маршрутизаторы на создание временных меток для сообщений журналов.

Настройте сервис временных меток для ведения журналов на маршрутизаторах.

**Часть 3. Настройте маршрутизаторы на регистрацию сообщений на сервере Syslog**

**Шаг 1.** Настройте маршрутизаторы для определения удалённого хоста (сервера Syslog), который будет получать регистрируемые сообщения.

Консоль маршрутизатора отобразит сообщение о том, что ведение журнала началось.

**Шаг 2.** Проверьте конфигурацию ведения журналов.

С помощью команды **show logging** убедитесь, что ведение журналов активировано.

**Шаг 3.** Изучите журналы сервера Syslog Server.

На вкладке **Services** диалогового окна **Syslog Server** необходимо нажать кнопку служб **Syslog**. Следите за регистрацией сообщений, получаемых от маршрутизаторов.

**Примечание.** Сообщения журналов могут генерироваться на сервере путём выполнения команд на маршрутиза­торах. Например, при входе в режим глобальной настройки и при выходе из него генерируется информационное сообщение о конфигурации. Возможно, вам потребуется выбрать другой сервис и снова нажать кнопку **Syslog**, чтобы обновить отображаемое сообщение.

**Часть 4. Настройте маршрутизатор R3 для поддержки подключений SSH**

**Шаг 1.** Настройте доменное имя.

Настройте доменное имя **ccnasecurity.com** на маршрутизаторе **R3**.

**Шаг 2.** Настройте пользователей для входа на SSH-сервер на маршрутизаторе R3.

Создайте идентификатор пользователя **SSHadmin** с наивысшим уровнем привилегий и секретным паролем **ciscosshpa55**.

R3(config)# **username SSHadmin privilege 15 secret ciscosshpa55**

**Шаг 3.** Настройте входящие линии vty на маршрутизаторе R3.

Используйте локальные учётные записи пользователей на обязательный вход в систему и проверку достоверности. Настройте разрешение только подключений SSH.

**Шаг 4.** Удалите существующие пары ключей на маршрутизаторе R3.

На маршрутизаторе следует удалить любые имеющиеся пары ключей RSA.

**Примечание.** Если ключи отсутствуют, вы можете получить следующее сообщение: % No Signature RSA Keys found in configuration.

**Шаг 5.** Сгенерируйте пару ключей RSA-шифрования для маршрутизатора R3.

Маршрутизатор использует пару ключей RSA для аутентификации и шифрования передаваемых SSH-данных. Настройте ключи RSA с модулем **1024**. Значение по умолчанию — 512, диапазон — от 360 до 2 048.

R3(config)# **crypto key generate rsa**

The name for the keys will be: R3.ccnasecurity.com.

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: **1024**

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

**Примечание.** Команда для генерирования ключа шифрования RSA для маршрутизатора R3 в Packet Tracer отличается от команд, используемых в лабораторной работе.

**Шаг 6.** Проверьте конфигурацию SSH.

Используйте команду **show ip ssh** для просмотра текущих настроек. Убедитесь, что для времени ожидания аутентификации и количества повторных попыток установлены значения по умолчанию — 120 и 3.

**Шаг 7.** Настройте время ожидания SSH и параметры аутентификации.

Значения времени ожидания и параметров аутентификации SSH по умолчанию можно изменить на более ограничительные. Задайте время ожидания **90** секунд, количество попыток аутентификации **2** иверсию **2**.

Используйте команду **show ip ssh** для подтверждения изменения значений.

**Шаг 8.** Попытайтесь подключиться к маршрутизатору R3 по Telnet с компьютера PC-C.

Откройте рабочий стол (Desktop) на компьютере **PC-C**. Выберите значок Command Prompt. На компьютере **PC-C** введите команду для подключения к маршрутизатору **R3** по протоколу Telnet.

PC> **telnet 192.168.3.1**

Эта попытка подключения должна закончиться неудачно, так как на маршрутизаторе R3 настроено разрешение только подключений SSH по линиям виртуального терминала.

**Шаг 9.** Подключитесь к маршрутизатору R3 с помощью SSH на компьютере PC-C.

Откройте рабочий стол (Desktop) на компьютере **PC-C**. Выберите значок Command Prompt. На компьютере **PC-C** введите команду для подключения к маршрутизатору R3 по протоколу SSH. При появлении запроса пароля введите пароль, настроенный для администратора (**ciscosshpa55**).

PC> **ssh –l SSHadmin 192.168.3.1**

**Шаг 10.** Подключитесь к маршрутизатору R3 с помощью SSH на маршрутизаторе R2.

Чтобы выявлять и устранять неполадки маршрутизатора **R3** и обслуживать его, администратор на стороне ISP должен использовать SSH для доступа к интерфейсу командной строки маршрутизатора. Через интерфейс командной строки маршрутизатора **R2** введите команду для подключения к маршрутизатору **R3** по протоколу SSH версии **2** с учётной записью пользователя **SSHadmin**. При появлении запроса пароля введите пароль, настроенный для администратора (**ciscosshpa55**).

R2# **ssh –v 2 –l SSHadmin 10.2.2.1**

**Проверка результатов**

Вы полностью выполнили задание. Нажмите **Check Results (проверить результаты)** для просмотра отзыва и проверки завершённых обязательных компонентов.