Packet Tracer. Настройка операций Syslog, NTP и SSH на маршрутизаторах Cisco

Топология

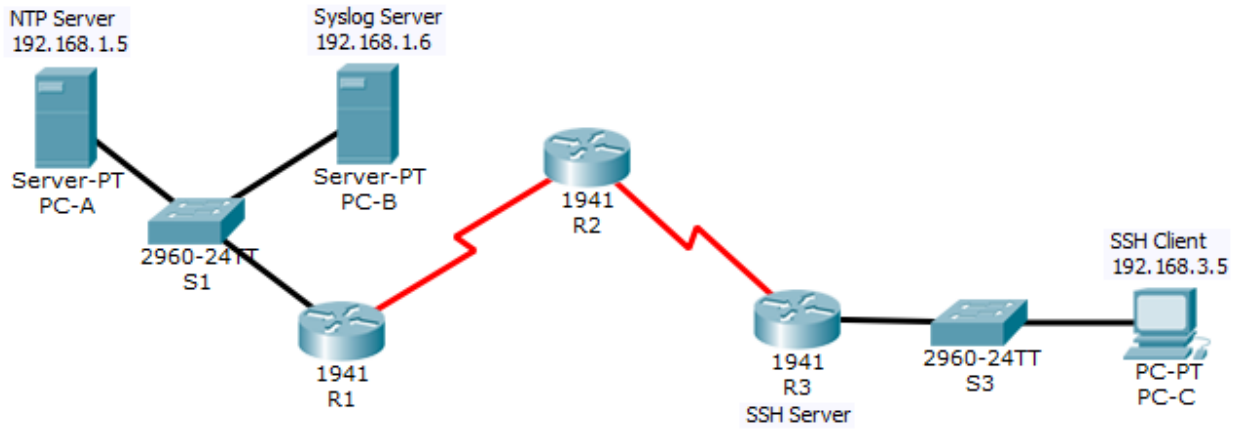

Таблица адресации

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

Задачи

- Настройте аутентификацию OSPF MD5.
- Настройте NTP.
- Настройте маршрутизаторы для записи сообщений в журнал на сервере Syslog.
- Настройте маршрутизатор R3 для поддержки подключений SSH.

Исходные данные/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 учетом времени, полученного с NTP-сервера.

Сервер Syslog будет обеспечивать ведение журнала сообщений в данном задании. Вы настроите маршрутизаторы для определения удаленного 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 защищенного 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. Примечание. MD5 – самый стойкий алгоритм шифрования, поддерживаемый в версии Packet Tracer, которая использовалась для разработки этого задания (6.2). 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.

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 учетом 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 удаленного 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 путем 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 учетные 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 2048.

```
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** и версию **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 учетной записью пользователя **SSHadmin**. При появлении запроса пароля введите пароль, настроенный для администратора (**ciscosshpa55**).

```
R2# ssh –v 2 –l SSHadmin 10.2.2.1
```

Шаг 11: Проверьте результаты.

Вы полностью выполнили задание. Нажмите **Check Results** (Проверить результаты) для просмотра обратной связи и проверки завершенных обязательных компонентов.

