Конфигурация Syslog, NTP, SSH и Telnet на маршрутизаторах Cisco

Топология

Адресная таблица

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	Fa0/1 S0/0/0 (DCE)	192.168.*X*+1.1 10.1.*X*+1.1	255.255.255.0 255.255.255.252	N/A N/A	S1 Fa0/5 N/A
R2	S0/0/0 S0/0/1 (DCE)	10.1.*X*+1.2 10.2.*X*+2.2	255.255.255.252 255.255.255.252	N/A N/A	N/A N/A
R3	Fa0/1 S0/0/1	192.168.*X*+3.1 10.2.*X*+2.1	255.255.255.0 255.255.255.252	N/A N/A	S3 Fa0/5 N/A
PC-A	NIC	192.168.*X*+1.5	255.255.255.0	192.168.*X*+1.1	S1 Fa0/6
PC-B	NIC	192.168.*X*+1.6	255.255.255.0	192.168.*X*+1.1	S2 Fa0/18
PC-C	NIC	192.168.*X*+3.5	255.255.255.0	192.168.*X*+3.1	S3 Fa0/18

Задание

- сконфигурировать маршрутизаторы как NTP клиенты
- сконфигурировать маршрутизаторы для обновления аппаратных часов от NTP сервера
- сконфигурировать маршрутизаторы для отправки log сообщений на syslog сервер.
- сконфигурировать маршрутизаторы для выдачи отметки времени на log сообщениях.
- создать локальных пользователей.

- сконфигурите VTY lines устройств для доступа только по протоколу SSH.
- сконфигурите RSA key pair (пару ключей) для SSH сервера
- проверить SSH подключения из PC клиента и клиента маршрутизатора.

Сценарий выполнения

На сетевой топологии имеется 3 маршрутизатора. Вы должны сконфигурите NTP и Syslog клиентов на всех маршрутизаторах Вы должны настроить SSH сервер на R3.

Network Time Protocol (NTP) позволяет всем маршрутизаторам сети синхронизировать установку единого времени и даты от NTP сервера. Единые отметки даты и времени позволяют легко проанализировать сообщения пересылаемые на Syslog сервер. Это поможет при устранении неполадок в сети, при возникновении сетевых атак. При создании NTP сервера в сети возможна синхронизация от внутренних часов (private master clock) или от публичного NTP сервера Internet.

Здесь используется NTP сервер как master сервер. Необходимо сконфигурите все маршрутизаторы как NTP клиенты для синхронизации времени с NTP сервером. Также необходимо настроить все маршрутизаторы для периодического обновления аппаратных часов от сервера NTP. В противном случае аппаратные часы, как правило, могут опережать или отставать от программных часов, что может привести к их рас синхронизации.

Syslog Server обеспечивает регистрацию событий (log сообщений) сети, что позволяет отобразить все события сети, от всех устройств, на удаленном хосте (Syslog server) .

Необходимо настроить сервис отметок даты и времени на всех маршрутизаторах. Отображение даты и времени в Syslog сообщениях необходимо для мониторинга сети. Отсутствие в Syslog сообщениях даты и времени не позволяет определить какое событие вызвало данное сообщение.

R2 является ISP и подключен к двум удаленным сетям: R1 и R3. Администратор R3 настраивает маршрутизатор и устраняет неисправности, но поскольку R3 является транзитным маршрутизатором, провайдеру R2 необходим доступ к R3 для поиска и устранения неисправностей или обновлений. Для доступа в безопасном режиме к R3 от ISP используется протокол SSH.

Для безопасного доступа к управлению маршрутизатором через CLI настройте доступ по протоколу SSH вместо TELNET. SSH это сетевой протокол, который в режиме эмуляции терминала

устанавливает защищенное соединение с сетевыми устройствами. SSH шифрует всю информацию и обеспечивает аутентификацию при удаленном соединении. SSH заменяет открытый протокол Telnet.

Сконфигурите NTP и SYSLOG сервера без аутентификации соответственно. NTP сервис не будет требовать аутентификации. Маршрутизаторы сконфигурированы с параметрами:

- Вход в привилегированный режим Enable password: **ciscoenpa55**
- Вход в терминальный режим vty lines пароль: **ciscovtypa55**
- Настройте статическую маршрутизацию.

Часть 1: Конфигурирование маршрутизаторов как NTP Clients

Шаг 1: Тест соединений.

- Ping из **PC-C** к **R3**.
- Ping из **R2** к **R3**.
- Telnet из **PC-C**к **R3**. Выход из Telnet сессии
- Telnet из **R2** к **R3**. Выход из Telnet сессии.

Шаг 2: Конфигурирование R1, R2, и R3 как NTP clients.

```
R1(config)# ntp server 192.168.X+1.5
R2(config)# ntp server 192.168.X+1.5
R3(config)# ntp server 192.168.X+1.5
```

проверьте конфигурацию NTP клиента командой **show ntp status**.

Шаг 3: Сконфигурите маршрутизаторы для обновления аппаратных часов.

Сконфигурите **R1**, **R2**, **и R3** для периодического обновления аппаратных часов от сервера NTP.

```
R1(config)# ntp update-calendar
R2(config)# ntp update-calendar
R3(config)# ntp update-calendar
```

Проверьте обновление аппаратных часов командой **show clock**.

Шаг 4: Сконфигурите маршрутизаторы для создания отметки timestamp в log сообщениях

Сконфигурите timestamp service регистрации на маршрутизаторах.

```
R1(config)# service timestamps log datetime msec
R2(config)# service timestamps log datetime msec
R3(config)# service timestamps log datetime msec
```

Часть 2: Настройте R1-R3 для передачи Log сообщений на Syslog Server

Шаг 1: Настройте маршрутизаторы для идентификации удаленного хоста (Syslog Server), на который будут отправляться Log сообщения.

```
R1(config)# logging host 192.168.X+1.6
R2(config)# logging host 192.168.X+1.6
R3(config)# logging host 192.168.X+1.6
```

Консоль маршрутизатора отобразит сообщение, что регистрация происходит.

Шаг 2: Проверьте конфигурацию регистрации командой show logging.

Шаг 3: Проверьте отправку log сообщений на Syslog Server.

На вкладке **Services** сервера нажмите кнопку **Syslog**. Наблюдайте Log сообщения полученные от маршрутизаторов.

Примечание: Log сообщения могут быть сгенерированы при выполнении различных команд на маршрутизаторе. Пример, выход (вход) в режим глобальной конфигурации маршрутизатора.

Часть 3: Настройка R3 для поддержки SSH соединения

Шаг 1: Сконфигурите domain name.

Сконфигурите domain name "**ccnasecurity.com"** на **R3**.

```
R3(config)# ip domain-name ccnasecurity.com
```

Шаг 2: Создайте пользователя для регистрации на SSH server маршрутизатора R3.

Создайте пользователя с ID **SSHadmin** с самым высоким уровнем привилегий и secret password "**ciscosshpa55**" (пароль зашифрован).

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

Шаг 3: Настройте вход на терминал VTY lines на R3.

Используйте локальные учетные данные созданные раннее. Доступ только по протоколу SSH.

```
R3 (config)# line vty 0 4
R3 (config-line)# login local
R3(config-line)# transport input ssh
```

Шаг 4: Удалите существующие ключи (key pairs) на R3.

Любой существующий RSA key pairs на маршрутизаторе должен быть удален.

```
R3(config)# crypto key zeroize rsa
```

Примечание: Если ни одного ключа не существует, то будет сообщение:

% No Signature RSA Keys found in configuration.

Шаг 5: Генерация RSA encryption key pair на R3.

Маршрутизатор использует RSA key pair для аутентификации и зашифрованной передачи данных SSH. Создайте RSA keys длиной **1024**, по умолчанию ширина ключа 512, ,дипазон 360 - 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: Эта команда генерит RSA encryption key pairs на **R3** в среде Packet Tracer.

Шаг 6: Проверка SSH конфигурации

Используя команду **show ip ssh** просмотрите текущую конфигурацию. Убедитесь, что timeout аутентификации и повторные запросы находятся в интервале 3-120 сек. по умолчанию.

Шаг 7: Конфигурирование SSH timeouts и authentication параметров.

По умолчанию SSH timeouts и authentication parameters могут быть изменены. Установите timeout регистрации через **90** секунд, количество попыток аутентификации **2**, версию 2.

```
R3(config)# ip ssh time-out 90
R3(config)# ip ssh authentication-retries 2
R3(config)# ip ssh version 2
```

введите команду **show ip ssh** для проверки внесенных изменений.

Шаг 8: Попытка соединения с R3 через Telnet с PC-C.

Откройте the Desktop of **PC-C**. Выберите Command Prompt icon. Из **PC-C**, введите команду для соединения по telnet с маршрутизатором R3.

```
PC> telnet 192.168.X+3.1
```

Соединения не должно быть т.к. маршрутизатор **R3** сконфигурирован для доступа к vty terminal

Шаг 9: Соединение с R3 с использованием SSH с PC-C.

Откройте вкладку Desktop на **PC-C**. Выберите Command Prompt icon. На **PC-C**, введите команду для соединения с R3 по SSH. Когда увидите приглашение, введите пароль, созданный раннее (пароль администратора **ciscosshpa55)**.

```
PC> ssh –l SSHadmin 192.168.X+3.1
```

Шаг 10: Соединение с R3 используя SSH на R2.

Для устранения неисправностей и поддержания R3, администратор интернет-провайдера должен использовать SSH для доступа к маршрутизатору через CLI. Из CLI из R2, введите команду для подключения к R3 через SSH версии 2 с использованием учетной записи пользователя SSHadmin. При запросе пароля введите пароль, настроенный для администратора: **ciscosshpa55**.

```
R2# ssh –v 2 –l SSHadmin 10.2.X+2.1
```

Шаг 11: Проверка результатов

!!!Scripts for R1 and R2!!!!

```
service timestamps log datetime
msec logging 192.168.1.6

ntp server
192.168.1.5 ntp
update-calendar
```

!!!Scripts for R3!!!!

```
service timestamps log datetime
msec logging 192.168.1.6

ntp server
192.168.1.5 ntp
update-calendar
ip domain-name ccnasecurity.com
username SSHadmin privilege 15 secret ciscosshpa55
 line vty 0 4
 login local

 transport input ssh
crypto key zeroize
rsa crypto key
generate rsa 1024
ip ssh time-out 90

ip ssh authentication-
retries 2 ip ssh version 2
```