Packet Tracer. Настройка зонального межсетевого экрана (ZPF)

Топология

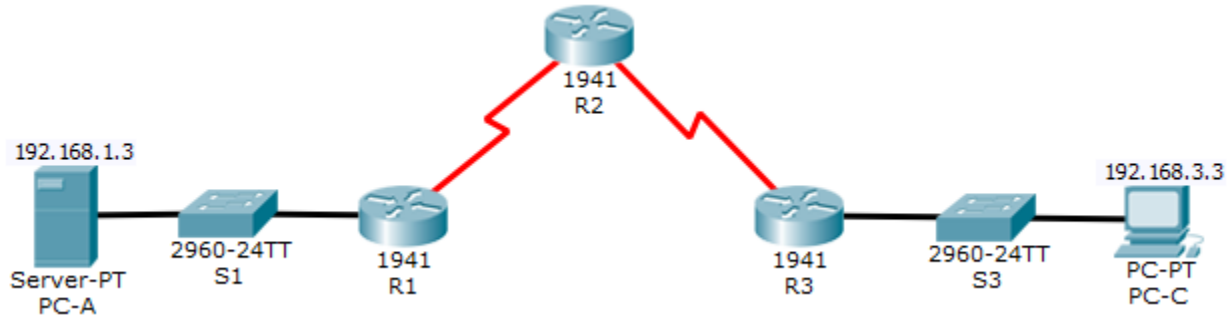

Таблица адресации

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	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Задачи

- Проверка связи между устройствами перед настройкой межсетевого экрана.
- Настройка зонального межсетевого экрана (ZPF) на маршрутизаторе R3.
- Проверка работоспособности межсетевого экрана ZPF с помощью эхо-запросов, SSH-подключения и веб-браузера.

Исходные данные/сценарий

ZPF – новейшее достижение в технологиях межсетевых экранов Cisco. В этом задании вы настроите простой межсетевой экран ZPF на граничном маршрутизаторе R3, разрешающий внутренним хостам доступ к внешним ресурсам и блокирующий доступ внешних хостов к внутренним ресурсам. Затем вы проверите работоспособность межсетевого экрана с внутренних и внешних хостов.

На маршрутизаторах были предварительно настроены следующие параметры.

- Пароль консоли: **ciscoconpa55**
- Пароль для линий VTY: **ciscovtypa55**
- Пароль привилегированного доступа: **ciscoenpa55**
- Имена и IP-адреса хостов
- Имя локального пользователя и пароль: **Admin/Adminpa55**
- Статическая маршрутизация

Часть 1: Проверка базовой связи по сети

Проверьте связь по сети перед настройкой зонального межсетевого экрана.

Шаг 1: Из командной строки компьютера PC-A отправьте эхо-запрос компьютеру PC-C по адресу 192.168.3.3.

Шаг 2: Получите доступ к маршрутизатору R2 по протоколу SSH.

a. Из командной строки компьютера **PC-C** установите SSH-подключение к интерфейсу S0/0/1 на маршрутизаторе **R2** по адресу **10.2.2.2.** Используйте имя пользователя **Admin** и пароль **Adminpa55** для входа.

```
PC> ssh -l Admin 10.2.2.2
```

b. Выйдите из SSH-сеанса.

Шаг 3: В браузере компьютера PC-C перейдите по адресу сервера PC-A.

a. Перейдите на вкладку **Desktop** (Рабочий стол) и выберите приложение **Web Browser** (Браузер). Введите IP-адрес компьютера **PC-A (192.168.1.3)** в формате URL. Должна появиться приветственная страница Packet Tracer с веб-сервера.

b. Закройте окно браузера на компьютере **PC-C**.

Часть 2: Создайте зоны межсетевого экрана на маршрутизаторе R3

Примечание. Для всех задач по конфигурированию необходимо указывать точные наименования.

Шаг 1: Активируйте пакет Security Technology.

a. На маршрутизаторе **R3** выполните команду **show version** для просмотра сведений о лицензии Technology Package.

b. Если пакет Security Technology не активирован, сделайте это с помощью следующей команды.

```
R3(config)# license boot module c1900 technology-package securityk9
```

c. Примите условия лицензионного соглашения с конечным пользователем.

d. Сохраните текущую конфигурацию и перезагрузите маршрутизатор, чтобы активировать лицензию Technology Package.

e. Убедитесь, что пакет Security Technology активирован, с помощью команды **show version.**

Шаг 2: Создайте внутреннюю зону.

С помощью команды **zone security** создайте зону с именем **IN-ZONE**.

```
R3(config)# zone security IN-ZONE
R3(config-sec-zone) exit
```

Шаг 3: Создайте внешнюю зону.

С помощью команды **zone security** создайте зону с именем **OUT-ZONE**.

```
R3(config-sec-zone)# zone security OUT-ZONE
R3(config-sec-zone)# exit
```


Часть 3: Идентификация трафика с помощью карты классов

Шаг 1: Создайте список контроля доступа (ACL), определяющий внутренний трафик.

С помощью команды **access-list** создайте расширенный список ACL **101**, чтобы разрешить передачу всего IP-трафика из сети источника **192.168.3.0/24.**

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any
```

Шаг 2: Создайте карту классов со ссылкой на внутренний трафик ACL.

Используя команду **class-map type inspect** с параметром **match-all**, создайте карту классов с именем **IN-NET-CLASS-MAP**. Используя команду **match access-group**, задайте сопоставление со списком ACL **101**.

```
R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)# match access-group 101
R3(config-cmap)# exit
```

Часть 4: Определение политик межсетевого экрана

Шаг 1: Создайте карту политик, определяющую действия с соответствующим трафиком.

Введите команду **policy-map type inspect** и создайте карту политик с именем **IN-2-OUT-PMAP**.

```
R3(config)# policy-map type inspect IN-2-OUT-PMAP
```

Шаг 2: Укажите тип класса inspect и эталонную карту классов IN-NET-CLASS-MAP.

```
R3(config-pmap)# class type inspect IN-NET-CLASS-MAP
```

Шаг 3: Укажите действие инспектирования для данной карты политик.

Команда **inspect** инициирует контроль доступа к учетом контекста (другие параметры – pass и drop).

```
R3(config-pmap-c)# inspect

%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will
be inspected.
```

Дважды введите команду **exit**, чтобы выйти из режима **config-pmap-c** и вернуться в режим **config**.

```
R3(config-pmap-c)# exit
R3(config-pmap)# exit
```

Часть 5: Применение политик межсетевого экрана

Шаг 1: Создайте пару зон.

С помощью команды **zone-pair security** создайте пару зон с именем **IN-2-OUT-ZPAIR**. Укажите зоны источника и назначения, созданные в задаче 1.

```
R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
```

Шаг 2: Настройте карту политик для обработки трафика между двумя зонами.

Добавьте карту политик и связанные с ней действия к паре зон с помощью команды **service-policy type inspect** и укажите ранее созданную карту политик **IN-2-OUT-PMAP**.

```
R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)# exit
R3(config)#
```


Шаг 3: Назначьте интерфейсы соответствующим зонам безопасности.

С помощью команды **zone-member security** в режиме интерфейсной настройки назначьте интерфейс G0/1 зоне **IN-ZONE**, а интерфейс S0/0/1 – зоне **OUT-ZONE**.

```
R3(config)# interface g0/1
R3(config-if)# zone-member security IN-ZONE
R3(config-if)# exit
R3(config)# interface s0/0/1
R3(config-if)# zone-member security OUT-ZONE
R3(config-if)# exit
```

Шаг 4: Скопируйте текущую конфигурацию в конфигурацию запуска.

Часть 6: Проверка работы межсетевого экрана в направлении от зоны IN-ZONE к OUT-ZONE

Убедитесь, что после настройки ZPF внутренние хосты могут по-прежнему получать доступ к внешним ресурсам.

Шаг 1: Отправьте эхо-запрос с внутреннего компьютера PC-C на внешний сервер PC-A.

Из командной строки компьютера **PC-C** отправьте эхо-запрос серверу **PC-A** по адресу 192.168.1.3. Эхо-запрос должен завершиться успешно.

Шаг 2: С внутреннего компьютера PC-C установите SSH-подключение к интерфейсу S0/0/1 маршрутизатора R2.

a. Из командной строки компьютера **PC-C** установите SSH-подключение к маршрутизатору **R2** по адресу 10.2.2.2. Для доступа к маршрутизатору R2 используйте имя пользователя **Admin** и пароль **Adminpa55**. SSH-сеанс должен быть установлен успешно.

b. В активном SSH-сеансе введите команду **show policy-map inspect zone-pair sessions** на маршрутизаторе **R3** для просмотра установленных сеансов.

Назовите IP-адрес и номер порта источника.

_____

Назовите IP-адрес и номер порта назначения.

_____

Шаг 3: С компьютера PC-C выйдите из SSH-сеанса на маршрутизаторе R2 и закройте окно командной строки.

Шаг 4: Откройте в браузере внутреннего компьютера PC-C страницу сервера PC-A.

Введите IP-адрес сервера **192.168.1.3** в адресную строку браузера и нажмите **Go**. Сеанс HTTP должен быть установлен успешно. Введите в активном HTTP-сеансе команду **show policy-map inspect zone-pair sessions** на маршрутизаторе **R3** для просмотра установленных сеансов.

Примечание. Если время ожидания HTTP-сеанса истечет, прежде чем будет выполнена команда на маршрутизаторе **R3**, нажмите кнопку **Go** (Перейти) на компьютере **PC-C**, чтобы установить сеанс между **PC-C** и **PC-A**.

Назовите IP-адрес и номер порта источника.

_____

Назовите IP-адрес и номер порта назначения.

_____

Шаг 5: Закройте окно браузера на компьютере PC-C.

Часть 7: Проверка работы межсетевого экрана в направлении от зоны OUT-ZONE к зоне IN-ZONE

Убедитесь, что после настройки ZPF внешние хосты НЕ могут получать доступ к внутренним ресурсам.

Шаг 1: Из командной строки сервера PC-A отправьте эхо-запрос компьютеру PC-C.

Из командной строки компьютера **PC-A** отправьте эхо-запрос компьютеру **PC-C** по адресу 192.168.3.3. Эхо-запрос должен завершиться неудачно.

Шаг 2: Отправьте эхо-запрос компьютеру PC-C с маршрутизатора R2.

С маршрутизатора **R2** отправьте эхо-запрос компьютеру **PC-C** по адресу 192.168.3.3. Эхо-запрос должен завершиться неудачно.

Шаг 3: Проверьте результаты.

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

