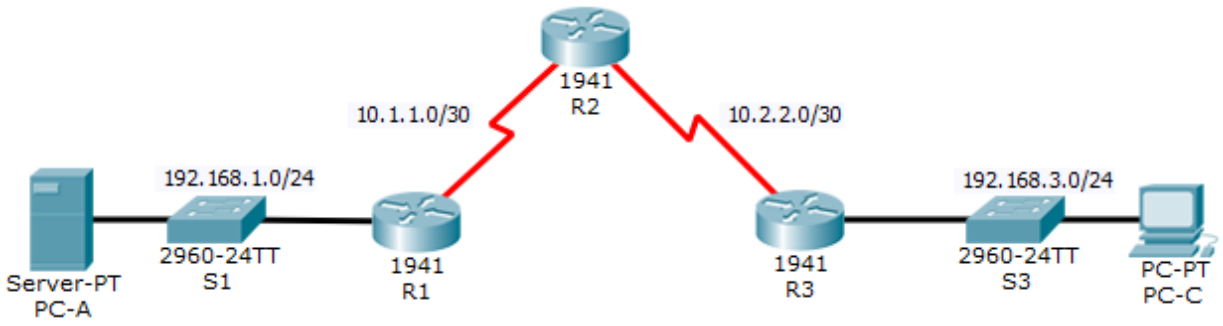
# Packet Tracer. Настройка списков ACL для IP-адресов с целью нейтрализации атак

## 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 |
| | Lo0 | 192.168.2.1 | 255.255.255.0 | 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.
- Использование списков ACL для настройки удаленного доступа к маршрутизаторам доступно только со станции управления PC-C.
- Настройка списков ACL на маршрутизаторах R1 и R3 для нейтрализации атак.
- Проверка работоспособности функции ACL.

## Исходные данные/сценарий

Доступ к маршрутизаторам R1, R2 и R3 должен быть разрешен только со станции управления PC-C. PC-C также используется для проверки связи с PC-A – сервером, предоставляющим сервисы DNS, SMTP, FTP и HTTPS.

Стандартный порядок действий – применить списки ACL на граничных маршрутизаторах для нейтрализации обычных угроз на основе IP-адресов источника и назначения. В этом задании вы с данной целью создадите списки ACL на граничных маршрутизаторах R1 и R3. Затем вы проверите работоспособность списков ACL с внутренних и внешних хостов.

На маршрутизаторах были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: **ciscoenpa55**
- Пароль для консоли: **ciscoconpa55**
- Имя пользователя и пароль SSH: **SSHadmin/ciscosshpa55**
- IP-адресация
- Статическая маршрутизация

## Часть 1: Проверьте базовую связь по сети

Проверьте связь по сети перед настройкой списков ACL для IP.

### Шаг 1: С компьютера PC-A проверьте связь с компьютером PC-C и маршрутизатором R2.

a. Отправьте эхо-запрос на компьютер **PC-C** (192.168.3.3) из командной строки.

b. Из командной строки установите SSH-сеанс связи с интерфейсом Lo0 маршрутизатора R2 (192.168.2.1), используя имя пользователя **SSHadmin** и пароль **ciscosshpa55**. По окончании выйдите из сеанса SSH.

```
SERVER> ssh -l SSHadmin 192.168.2.1
```

### Шаг 2: С компьютера PC-C проверьте связь с компьютером PC-A и маршрутизатором R2.

a. Отправьте эхо-запрос на компьютер **PC-A** (192.168.1.3) из командной строки.

b. Из командной строки установите SSH-сеанс связи с интерфейсом Lo0 маршрутизатора R2 (192.168.2.1), используя имя пользователя **SSHadmin** и пароль **ciscosshpa55**. По окончании закройте сеанс SSH.

c. Откройте в браузере веб-страницу сервера **PC-A** (192.168.1.3). По окончании закройте окно браузера.

## Часть 2: Защитите доступ к маршрутизаторам

### Шаг 1: Настройте ACL 10 для полной блокировки удаленного доступа к маршрутизаторам со всех систем, кроме PC-C.

Используйте команду **access-list** для создания нумерованного списка ACL для IP на маршрутизаторах **R1**, **R2** и**R3**.

### Шаг 2: Примените список ACL 10 к входному трафику на линиях VTY.

С помощью команды **access-class** примените список контроля доступа к входному трафику на линиях VTY.

### Шаг 3: Проверьте монопольный доступ со станции управления PC-C.

a. Установите сеанс соединения SSH с 192.168.2.1 с компьютера **PC-C** (попытка подключения должна быть успешной).

b. Установите SSH-сеанс связи с узлом 192.168.2.1 с компьютера **PC-A** (попытка подключения должна завершиться неудачно).

## Часть 3: Создайте нумерованный список ACL 120 для IP на маршрутизаторе R1

Создайте нумерованный список ACL 120 для IP по следующим правилам.

- Разрешать всем внешним хостам доступ к сервисам DNS, SMTP и FTP на сервере **PC-A.**
- Запрещать всем внешним хостам доступ к сервисам HTTPS на **PC-A.**
- Разрешать **PC-C** доступ к маршрутизатору **R1** через SSH.

**Примечание.** При нажатии Check Results (проверить результаты) не будет отображаться правильная конфигурация ACL 120, пока вы не измените ее в части 4.

### Шаг 1: Убедитесь, что компьютер PC-C может получать доступ к PC-A по протоколу HTTPS с помощью браузера.

Отключите HTTP и включите HTTPS на сервере **PC-A**.

### Шаг 2: Настройте список ACL 120 для разрешения и отклонения указанного трафика.

С помощью команды **access-list** создайте нумерованный список ACL для IP.

### Шаг 3: Примените список ACL к интерфейсу S0/0/0.

С помощью команды **ip access-group** примените список контроля доступа к входящему трафику на последовательном интерфейсе 0/0/0.

### Шаг 4: Убедитесь, что компьютер PC-C не может получить доступ к PC-A по протоколу HTTPS с помощью браузера.

## Часть 4: Измените существующий список ACL на маршрутизаторе R1

Разрешите ответы на эхо-запросы ICMP и сообщения о недоступном пункте назначения из внешней сети (по отношению к **R1**). Запретите все другие входящие пакеты ICMP.

### Шаг 1: Убедитесь, что компьютер PC-A не может успешно отправлять эхо-запросы на интерфейс loopback на маршрутизаторе R2.

### Шаг 2: Внесите необходимые изменения в список ACL 120 для разрешения и отклонения указанного трафика.

Используйте команду **access-list** для создания нумерованного списка ACL для IP.

### Шаг 3: Убедитесь, что компьютер PC-A может успешно отправлять эхо-запросы интерфейсу loopback на маршрутизаторе R2.

## Часть 5: Создайте нумерованный список ACL 110 для IP на маршрутизаторе R3

Запретите все исходящие пакеты, в которых адрес источника находится за пределами диапазона внутренних IP-адресов на маршрутизаторе **R3**.

### Шаг 1: Настройте список ACL 110 для разрешения только трафика из внутренней сети.

Используйте команду **access-list** для создания нумерованного списка ACL для IP.

### Шаг 2: Примените список ACL к интерфейсу G0/1.

Используйте команду **ip access-group,** чтобы применить список контроля доступа к входящему трафику на интерфейсе G0/1.

## Часть 6: Создайте нумерованный список ACL 100 для IP на маршрутизаторе R3

На маршрутизаторе **R3** заблокируйте все пакеты, содержащие IP-адрес источника из следующего пула адресов: любые частные адреса RFC 1918, 127.0.0.0/8 и любые групповые IP-адреса. Поскольку **PC-C** используется для удаленного администрирования, необходимо разрешить трафик SSH сети 10.0.0.0/8 для возврата на хост **PC-C**.

### Шаг 1: Настройте список ACL 100 для блокировки всего указанного трафика из внешней сети.

Следует также заблокировать трафик из вашего собственного пространства внутренних адресов, если это не адрес RFC 1918. В этом задании ваше пространство внутренних адресов входит в пространство частных адресов, определенное в документе RFC 1918.

С помощью команды **access-list** создайте нумерованный список ACL для IP.

### Шаг 2: Примените список ACL к интерфейсу Serial 0/0/1.

С помощью команды **ip access-group** примените список контроля доступа к входящему трафику на последовательном интерфейсе 0/0/1.

### Шаг 3: Убедитесь, что указанный трафик, поступающий на последовательный интерфейс 0/0/1, обрабатывается правильно.

a. Отправьте эхо-запрос на сервер PC-A из командной строки компьютера PC-C. ACL блокирует ответы на эхо-запросы ICMP, поскольку их источником является адресное пространство 192.168.0.0/16.

b. Установите сеанс соединения SSH с 192.168.2.1 с компьютера **PC-C** (попытка подключения должна быть успешной).

### Шаг 4: Проверьте результаты.

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