28-1 Конфигурирование ACL - Лабораторное упражнение

В этой лаборатории можно настроить стандартные и расширенные списки управления доступом.

Маршрутизаторы и ПК сконфигурированы с параметрами сетевой адресации, а R2 имеет статический маршрут для внутренних сетей 10.0.1.0/24 и 10.0.2.0/24.

# Лабораторная топология



**Загрузить конфигурации запуска**

Откройте файл «28-1 ACL Configuration .pkt» в Packet Tracer для загрузки лаборатории.

# Пронумерованный стандартный ACL

1. Убедитесь, что все ПК подключены друг к другу, к R1 и R2.
2. Настройте и примените пронумерованный стандартный ACL на R1, который запрещает трафик от всех хостов в подсети 10.0.2.0/24 к R2.

ПК в подсетях 10.0.1.0/24 и 10.0.2.0/24 должны поддерживать связь друг с другом.

Компьютеры в подсети 10.0.1.0/24 должны поддерживать подключение к R2.

1. Проверьте, что трафик защищен в соответствии с требованиями.

Проверьте PC1 и PC2 можете выполнить ping R2. PC3 не удается выполнить ping R2.

PC3 можете ping PC1 и PC2.

# Пронумерованный расширенный ACL

1. Конфигурирование и применение пронумерованного расширенного ACL на R1, который разрешает доступ Telnet от PC1 к R2. Telnet-R2 должен быть запрещен для всех других компьютеров в сети.

Все остальные возможности подключения должны поддерживаться. Не изменяйте существующий ACL.

Доступ к Telnet уже включен на R2. Пароль: «Flackbox»

1. Проверьте, что трафик защищен в соответствии с требованиями. Используйте команду «telnet 10.0.0.2» с ПК для тестирования и пароль «Flackbox». Введите «exit» для выхода из сеанса Telnet.

Убедитесь, что PC1 можете выполнить команду ping и Telnet для R2. PC2 можете выполнить ping R2, но не Telnet.

PC3 не удается выполнить ping или Telnet для R2. Все компьютеры могут проверять связь друг с другом.

1. Сколько пакетов Telnet было разрешено ACL?

# Именованный расширенный ACL

1. Удалите только что сконфигурированный нумерованный расширенный ACL из интерфейса. Не удаляйте ACL.
2. Сконфигурируйте и примените именованный расширенный ACL к R1 следующим образом:

Разрешить Telnet от PC1 к R2. Telnet-R2 должен быть запрещен для всех других компьютеров в сети.

Разрешить ping от PC2 до R2. Проверка связи с R2 должна быть запрещена для всех остальных компьютеров в сети.

Все остальные возможности подключения должны поддерживаться.

1. Проверьте, что трафик защищен в соответствии с требованиями.

Убедитесь, что PC1 не может выполнить ping R2, но может использовать Telnet. PC2 можете выполнить ping R2, но не можете выполнить Telnet для него.

PC3 не удается выполнить ping или Telnet для R2. Все компьютеры могут проверять связь друг с другом.