**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № 4**

на тему «Фильтрация трафика в сети с помощью контроля доступа»

|  |
| --- |
| Выполнил: студент группы ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Решетникова Ирина Витальевна |
| (Фамилия, имя, отчество) |

**Цель:** овладеть основными практическими навыками фильтрации трафика в сети с помощью списков контроля доступа (ACL), в программе Cisco Packer Tracer.

# **Ход работы:**

**Задание 1.** Построить сеть, как показано на рисунке 1. VL2 – сегмент бухгалтерии, VL3 – сегмент пользователей, VL4 – сегмент администрации, VL5 – сегмент сервера 1С.

Для начала построим схему, как указывается в лабораторной работе. Схема представлена на рисунке 1.

Изображение выглядит как текст, диаграмма, снимок экрана, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 1 - схема сети

**Задание 2.** Настроить NAT. Для этого нам необходимо определить интерфейсы, которые будут являться внешними и внутренними для NATa.

Для выполнения задания нужно зайти на Router0 и во вкладке CLI прописать следующие значения, которые представлены на рисунке 2.

Рассмотрим более подробно что делают данные команды.

“Router (config)#int fa0/0” - переходит в режим конфигурации интерфейса FastEthernet0/0.

“Router (config-if)#ip nat outside” – указывает, что текущий интерфейс (fa0/0) является внешним интерфейсом для NAT. Маршрутизатор должен знать, через какой интерфейс пакеты выходят во внешнюю сеть и возвращаются из нее. На этом интерфейсе будет происходить замена внутренних частных IP-адресов на внешний публичный IP-адрес (или пул адресов) при исходящем трафике, и обратная замена при входящем трафике.

“Router(config-if)#exit” – выходит из режима конфигурации интерфейса (fa0/0) обратно в глобальный режим конфигурации (Router(config)#).

“Router(config)#int range fa0/1.2” – переходит в режим конфигурации диапазона интерфейсов. В данном случае диапазон состоит только из одного субинтерфейса FastEthernet0/1.2. fa0/1.2 — это не физический интерфейс, а логический подынтерфейс, созданный на физическом интерфейсе fa0/1. Он обычно используется для маршрутизации трафика определенной VLAN (например, VLAN 2). Здесь настраивается внутренняя сторона NAT.

“Router(config-if-range)#ip nat inside” - указывает, что текущий субинтерфейс (или диапазон субинтерфейсов) fa0/1.2 является внутренним (inside) интерфейсом для NAT. Маршрутизатор должен знать, на каких интерфейсах находятся устройства с частными IP-адресами, которым нужен доступ в Интернет через NAT. Трафик, приходящий *с* этих интерфейсов, будет рассматриваться как "исходящий из локальной сети" и подлежащий трансляции NAT. Трафик, приходящий на эти интерфейсы после трансляции (ответы из интернета), будет подвергаться обратной трансляции.

В итоге имеем, что ip nat outside: Назначен на интерфейс FastEthernet0/0. ip nat inside**:** Назначено на субинтерфейсы: FastEthernet0/1.2, FastEthernet0/1.3, FastEthernet0/1.4.

Мы специально не указали VL5, сеть сервера 1С, чтобы у него, в целях безопасности, не было доступа в интернет.

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 2 – настройка внешних и внутренних интерфейсов на Router0 для NAT

**Задание 3.** Создать Access List для NAT.

Для создания Access-list выполним алгоритм, который представлен на рисунке 3. На этом этапе настраивается сама трансляция адресов (NAT/PAT) с использованием списка доступа (ACL) для определения, какие внутренние адреса будут транслироваться, и указывается внешний интерфейс. Рассмотрим более подробно что выполняет каждая команда и зачем нужна.

“Router(config)#ip access-list standard FOR-NAT” **-** создает стандартный именованный список доступа (ACL) с именем FOR-NAT и переходит в режим его конфигурации (config-std-nacl). Этот ACL будет использоваться для определения внутренних IP-адресов (или сетей), которым разрешено выполнять трансляцию NAT. Имя FOR-NAT выбрано осмысленно (для NAT).

“Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255” **-** Добавляет правило в ACL FOR-NAT. Это правило разрешает (permit) все IP-адреса в сети 192.168.2.0/24. Как работает: 192.168.2.0 — это адрес сети. 0.0.0.255 — это wildcard mask (инвертированная маска подсети). Она означает: "совпадают все адреса, где первые три октета (192.168.2) одинаковы, а последний октет (0–255) может быть любым". То есть это вся сеть 192.168.2.0 с маской 255.255.255.0 (/24).

“Router(config-std-nacl)#permit 192.168.3.0 0.0.0.255” **-** Добавляет второе правило в ACL FOR-NAT, разрешающее всю сеть 192.168.3.0/24.

“Router(config-std-nacl)#permit 192.168.4.0 0.0.0.255” **-** добавляет третье правило в ACL FOR-NAT, разрешающее всю сеть 192.168.4.0/24.

“Router(config-std-nacl)#ip nat inside source list FOR-NAT interface fa0/0 overload” **—** это ключевая команда, активирующая саму трансляцию NAT (PAT).

Изображение выглядит как текст, Шрифт, снимок экрана, документ

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 3 – создание access-list для NAT

**Задание 4.** Проверить настройку Access List, используя команду ping c любого настроенного устройства.

Теперь попробуем с ПК бухгалтерии выполнить ping на наш сервер с адресом 210.210.1.2. По рисунку 4 видно, что не весь трафик проходит, но доступ к серверу есть.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4 – пинг с ПК бухгалтера

**Задание 5.** Проверить настройку Access List, используя команду ping c любого ненастроенного устройства.

Попробуем теперь выполнить пинг с сервера “1C” на сервер с IP 210.210.1.2. Результат представлен на рисунке 5.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 5 – пинг с сервера 1C

**Задание 6.** Настроить безопасность локальной сети, защитив от возможных атак из сети интернет. Для выполнения задания использовать Access List.

Для выполнения данного задания создадим access list c названием “FROM-OUTSIDE” и пропишем правила, которые представлены на рисунке 6.

Здесь команды создают и применяют расширенный именованный ACL, который блокирует весь входящий трафик извне во внутренние сети. Разберем подробно.

“Router(config)#ip access-list extended FROM-OUTSIDE” – создает расширенный ACL c именем “FROM-OUTSIDE”. Расширенный трафик позволяет фильтровать трафик на основе IP-адресов источника / назначения. Протоколов (IP, TCP, UDP, ICMP и т.п.). Порт назначения (для TCP/UDP).

Теперь рассмотрим все команды, где есть deny. Каждое правило deny запрещает весь IP трафик (any) на ip: 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24, 192.168.5.0/24.

“Router(config)#int fa0/0; Router(config-if)#ip access-group FROM-OUTSIDE in” – применяет ACL FROM-OUTSIDE к интерфейсу fa0/0 (внешний интерфейс) на входящий трафик (in). Фильтрация применяется к пакетам, поступающим из интернета на маршрутизатор. Трафик, направленный во внутренние сети (192.168.2.0/24, 192.168.3.0/24 и т.д.), будет отброшен.

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 6 – настройка access list для безопасности локальной сети

**Задание 7.** Проверить пинг с Router1 в локальную сеть командой. Должно быть видно, что ни один пакет не прошел.

Теперь проверим, что информация с Router1 не проходит в локальную сеть командой ping. В результате получается такой вот вывод, который представлен на рисунке 7.

Изображение выглядит как текст, чек, Шрифт, алгебра

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 7 – проверка, что доступ с Router1 не проходит в локальную сеть

**Задание 8.** Восстановить доступ к интернету.

Для восстановления доступа к интернету, необходимо написать разрешающее правило, которое допустит исходящий трафик на внешний интерфейс для Router0. Команды представлены на рисунке 8. Рассмотрим более подробно команды, которые используются.

Данные команды добавляют разрешающее правило в существующий ACL FROM-OUTSIDE, чтобы разрешить доступ к интернету для устройств.

“en” - сокращение от enable. Переключает в привилегированный режим. Данная команда нужна для внесения изменений в конфигурацию нужны права администратора.

“conf t” - сокращение от configure terminal. Переходит в режим глобальной конфигурации. Она нужна, чтобы начать редактирование конфигурации устройства.

“ip access-list extended FROM-OUTSIDE” - Переходит в режим редактирования, существующего расширенного ACL с именем FROM-OUTSIDE. Здесь мы добавляем новое правило к ACL, созданному ранее для фильтрации входящего трафика.

“permit ip any host 210.210.0.2” – разрешить для любого трафика с любого источника доносить информацию на 210.210.0.2.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 8 – настройка Router0 для доступа в интернет

**Задание 9**. Выполнить проверку, что интернет на устройствах появился.

Теперь попробуем с бухгалтерского устройства выполнить запрос на 210.210.1.2. Результат представлен на рисунке 9.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 9 – удачный пинг с бухгалтерского ПК на 210.210.1.2

**Задание 10.** Настроить Router0 на доступ по telnet.

Произведем теперь настройку Router0. Для выполнения данного задания нужно выполнить команды, которые представлены на рисунке 10.

Telnet — это протокол удалённого управления сетевыми устройствами (маршрутизаторами, коммутаторами и т. д.) через сеть. В данном случае он используется для: удалённого подключения к Router0 с других устройств в сети, конфигурирования маршрутизатора без физического доступа к консоли, мониторинга состояния устройства, диагностики сетевых проблем.

“username admin privilege 15 password cisco” **–** создает учетную запись пользователя. admin – имя пользователя, privilege 15 – максимальный уровень привилегий (полный доступ), password cisco – пароль для аутентификации.

“enable password cisco” – устанавливает пароль для входа в привилегированный режим (режим enable).

“line vty 0 4” – переходит в режим конфигурации виртуальных терминалов (VTY), здесь настраивается 5 одновременных сессий.

“login local” – включает аутентификацию по локальной базе пользователей.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 10 – настройка роутера по telnet

**Задание 11.** Проверить доступ к telnet c публичного сервера. Воспользоваться access list для ограничения доступа по telnet из внешней сети.

Попробуем в начале выполнить запрос с сервера 210.210.1.2, в результате на рисунке 11 видно, что подключение по telnet происходит удачно, но такое поведение нам не подходит и мы должны ограничить доступ из внешней сети.

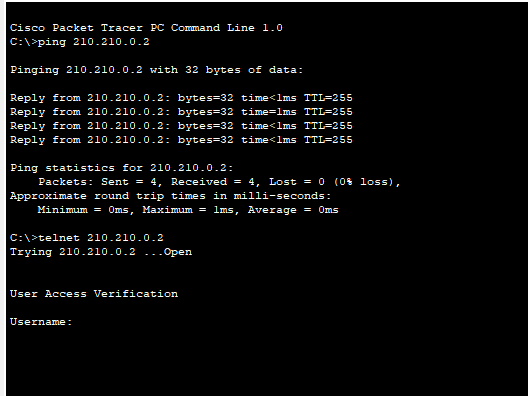


Рисунок 11 – подключение по telnet к удаленному серверу

Теперь попробуем настроить access list, чтобы запроса извне не проходили в нашу сеть. Для выполнения действий использовались команды, которые представлены на рисунке 12. Описание команд представлено ниже.

“Router>en” - сокращение от enable - переход в привилегированный режим.

“Router#conf t” - сокращение от configure terminal - вход в режим глобальной конфигурации.

“no ip access-list extended FROM-OUTSIDE” - удаляет существующий ACL "FROM-OUTSIDE". Данная команда "обнуляет" текущую конфигурацию ACL, но не снимает с интерфейса (если ACL был применён ранее, он остаётся привязанным, но пустым).

“ip access-list extended FROM-OUTSIDE” - создаёт новый одноимённый ACL и переходит в режим его настройки.

“deny tcp any host 210.210.0.2 eq telnet” **-** блокирует Telnet-доступ к маршрутизатору извне. Deny – запретить, tcp – протокол TCP, any – c любого источника, host 210.210.0.2 – на IP-адрес маршрутизатора, eq Telnet – для Telnet.

“permit ip any host 210.210.0.2” – разрешает остальной трафик на маршрутизатор.

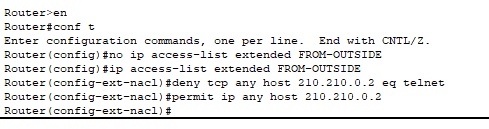


Рисунок 12 – настройка access list для Router0

Проверим теперь, что у нас с сервера 210.210.1.2 не проходят запросы по telnet. Результат представлен на рисунке 13.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 13 – отсутствие доступа по telnet c интернета в локальную сеть

**Задание 12.** Настроить Router0 так, чтобы только сегмент из сети “Бухгалтерия” имел доступ к серверу 1С. Для выполнения использовать access list.

Теперь рассмотрим стандартные Access List. У нас имеется сервер 1С, очевидно, что к нему должен иметь доступ только сегмент сети «Бухгалтерия», а остальные не должны. Для этого на Router0 пропишем следующие команды, которые представлены на рисунке 14. А ниже распишем что представляет из себя каждая команда.

“ip access-list standard PROTECT-1C” - Создаёт именованный стандартный ACL с именем PROTECT-1C.

“permit 192.168.3.0 0.0.0.255” - Разрешает доступ только для сети "Бухгалтерия" (предположим, это сеть 192.168.3.0/24).

“deny any” - Блокирует все остальные подсети (неявное правило deny any есть по умолчанию, но явное указание делает конфигурацию понятнее).

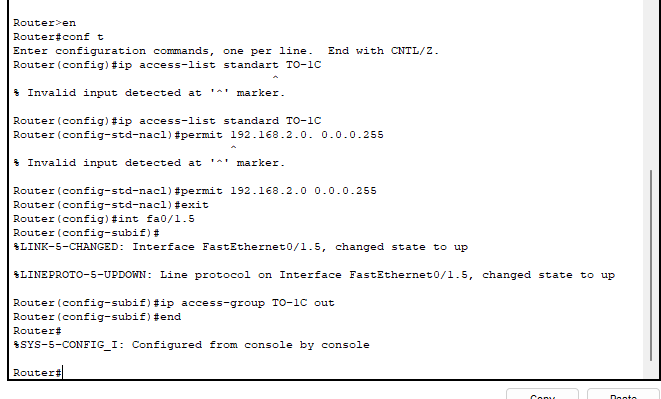


Рисунок 14 – настройка access list, чтобы бухгалтер имел только доступ к серверу 1С

**Задание 13.** Выполнить проверку с компьютера бухгалтерии командой ping.

Теперь выполним “ping” с ПК бухгалтера и убедимся, что все работает. Результат представлен на рисунке 15.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 15 – пинг с ПК бухгалтера на сервер 1С

**Задание 14.** Выполнить ping c любого иного ПК.

Теперь выполним “ping” с иного ПК. В нашем случае будет использоваться ПК 192.168.3.2 для запроса к серверу 1С. Результат представлен на рисунке 16.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 16 – пинг с ПК 192.168.3.2 на сервер 1С

**Вывод:** в данной лабораторной работе, мы познакомились с Access List и настроили контроль доступа трафика в нашей сети.

# **Контрольные вопросы**

1. **Сформируйте определение ACL.**

ACL (Access Control List) — это упорядоченный набор правил, используемый сетевыми устройствами (маршрутизаторами, коммутаторами) для: фильтрации трафика (разрешить/запретить передачу пакетов), контроля доступа к сетевым ресурсам, идентификации трафика для других функций (NAT, QoS, VPN)

Его ключевые свойства: работает на уровнях L3 (IP) и L4 (TCP/UDP) модели OSI, обрабатывает правила сверху вниз (первое совпадение определяет действие), В конце списка всегда присутствует неявное правило deny any (запрет всего трафика)

1. **Что такое NAT?**

NAT (Network Address Translation) — это технология преобразования IP-адресов в заголовках сетевых пакетов. Решает две ключевые задачи:

1. Сохранение IPv4-адресов**:**
   * Позволяет множеству устройств в частной сети (192.168.x.x, 10.x.x.x) использовать один публичный IP-адрес для выхода в Интернет.
   * Реализуется через PAT (Port Address Translation).
2. Безопасность**:**
   * Скрывает внутреннюю структуру сети от внешних узлов.
3. **По каким параметрам ACL может фильтровать трафик?**

ACL бывает двух видов: расширенный и обычный.

Для стандартного ACL можно фильтровать траффик только по источнику (IP).

Для расширенного можно фильтровать по протоколу, по IP источника, по IP назначения, по портам, по флагам.