

Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Защита информации в информационных системах

ОТЧЕТ
по лабораторной работе № 3
на тему
«Конфигурирование списков доступа для реализации методов разграничения
доступа к ресурсом информационной системы»

Студент:

Преподаватель:

МИНСК 2024

1 ЦЕЛЬ РАБОТЫ

Получить навыки по конфигурированию списков доступа для реализации методов разграничения доступа к ресурсам информационной системы.

2 ИСХОДНЫЕ ДАННЫЕ К РАБОТЕ

В данной лабораторной работе необходимо:

- Сконфигурировать в среде моделирования сеть;
- Сконфигурировать списки доступа согласно заданию

3 ВЫПОЛНЕНИЕ РАБОТЫ

Создание пользователя:

```
username superadmin privilege 15 secret 5 superadmin
```

Создание списка доступа со следующими параметрами:

- 1) Разрешение удалённого доступа по протоколу SSH;
- 2) Отклонение всего трафика, кроме ICMP;
- 3) Блокировка HTTP- и HTTPS-доступа.

Данный список изображён на рисунке 3.1.

```
access-list 100 permit tcp 0.0.0.0 255.252.0.0 any eq 22
access-list 100 deny tcp 0.0.0.0 255.252.0.0 any eq www
access-list 100 deny tcp 0.0.0.0 255.252.0.0 any eq 443
access-list 100 deny ip any any
```

Рисунок 3.1 – Создание списка доступа

Создание списка доступа с именем BLOCK_ICMP со следующими параметрами:

- 1) Блокировка всего трафика ICMP;
- 2) Разрешение передачи трафика IPv6.

Данный список изображён на рисунке 3.2.

```
ipv6 access-list BLOCK_ICMP
deny icmp any any
permit ipv6 any any
```

Рисунок 3.2 – Создание списка доступа с именем BLOCK_ICMP

Для создания списка доступа по времени необходимо:

- 1) Создать временной диапазон:

```
time-range Time_list
Periodic Monday 08:00 to 13:00
```

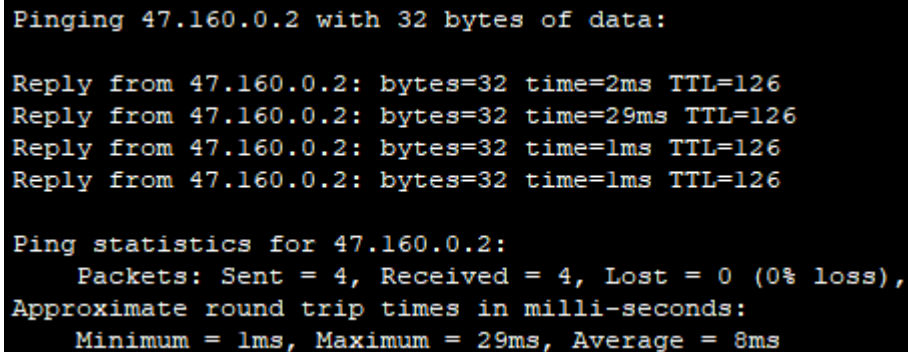
- 2) Разрешить списку доступа использовать данный временной диапазон:

```
access-list 100 permit ip 47.160.0.1 255.252.0.0 any time-range  
Time_list
```

3) Применить к интерфейсу:

```
interface FastEthernet 0/0  
ip access-group 100 in
```

Проверка:



```
Pinging 47.160.0.2 with 32 bytes of data:  
  
Reply from 47.160.0.2: bytes=32 time=2ms TTL=126  
Reply from 47.160.0.2: bytes=32 time=29ms TTL=126  
Reply from 47.160.0.2: bytes=32 time=1ms TTL=126  
Reply from 47.160.0.2: bytes=32 time=1ms TTL=126  
  
Ping statistics for 47.160.0.2:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 29ms, Average = 8ms
```

4 КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Дайте определение списка доступа?

ACL (Access Control List) — это набор текстовых выражений, которые что-то разрешают, либо что-то запрещают.

2) Какие функции могут выполнять списки доступа?

Контроль трафика, фильтрация по критериям, разграничение доступа, управление сетевыми политиками, заглядывать внутрь IP-пакета, просматривать тип пакета, TCP и UDP порты.

3) Основные виды списков доступа? Их порядковая нумерация.

Стандартные списки доступа(1-99), расширенные списки доступа(100-199).

4) Какой командой создается список доступа?

```
Ip access-list [номер] [permit|deny] [source]
```

5) Какой командой можно повесить список доступа на интерфейс? От чего зависит выбор конкретного интерфейса?

```
interface [тип интерфейса] [номер интерфейса]  
ip access-group [номер списка доступа] [in|out]
```

6) На какой интерфейс целесообразно размещать стандартные списки доступа?

На интерфейс, который находится ближе к получателю трафика. Это связано с тем, что стандартные ACL фильтруют пакеты только по IP-адресу

источника, и их размещение ближе к получателю позволяет более эффективно управлять трафиком, который уже достиг целевой сети.

7) На какой интерфейс целесообразно размещать расширенные списки доступа?

На интерфейс, который находится ближе к источнику трафика. Это позволяет более эффективно фильтровать пакеты, так как расширенные ACL могут учитывать не только IP-адреса источника, но и адреса назначения, протоколы и номера портов.

8) По каким критериям происходит фильтрация трафика в стандартном ACL?

По ip-адресу источника и по действиям(permit/deny).

9) По каким критериям можно фильтровать трафик в расширенных списках доступа?

По ip-адресам источника, назначения, по протоколу, номерам портов и типу трафика.

10) Каково назначение динамического списка доступа?

Автоматизация управления доступом, улучшение безопасности и гибкость.

11) Опишите принцип действия рефлексивного списка доступа?

Рефлексивные ACL работают таким образом: блокируется полностью доступ (deny any) но формируется ещё один специальный ACL, который может читать параметры пользовательских сессий, которые сгенерированы из локальной сети и для них открывать проход в deny any, в результате получается что из Интернета не смогут установить соединение. А на сессии из локальной сети будут приходить ответы.

12) Что позволяет список ограничения по времени? Как его задать?

Список ограничения по времени позволяет контролировать доступ пользователей к определённым ресурсам или устройствам в зависимости от времени суток. Для его создания необходимо создать временной диапазон, применить его к списку доступа и список доступа применить к интерфейсу.

13) Какая особенность представления маски сети? Как она вычисляется?

Особенность представления маски сети заключается в том, что она представляет собой последовательность битов, где сначала идут единицы, а затем нули. Это позволяет четко определить, какая часть IP-адреса относится

к сети, а какая — к хосту. Вычисление происходит так: определить количество хостов, определить количество битов для сети и сформировать маску.

5 ВЫВОД

Получил навыки по конфигурированию списков доступа для реализации методов разграничения доступа к ресурсам информационной системы.