

Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций
Кафедра защиты информации

Практическая работа № 2

«DOS и DDOS атаки»

Шифр: 173

Проверила:
Белоусова Е.С.

Выполнила:
ст. гр. 961401
Савченко Е.А.

Минск 2022

Цель: изучить виды DoS и DDoS атак и их отличия, осуществить реализацию атак Ping flood, UDP flood, SYN flood, овладеть навыками настройки защиты от DoS и DDoS атак.

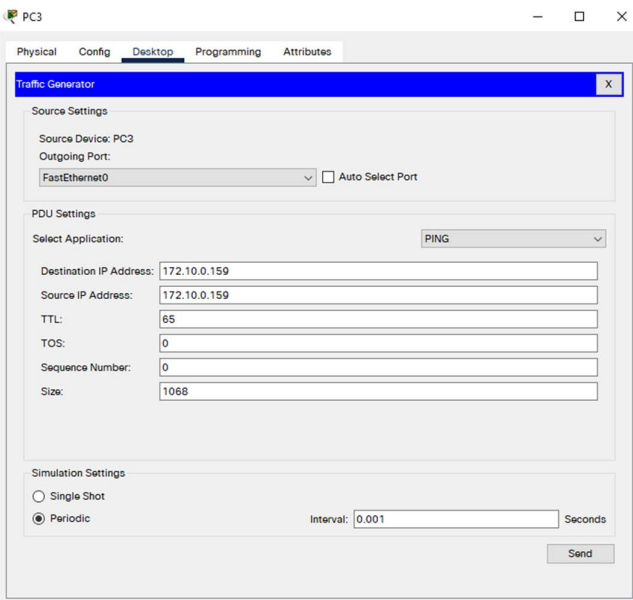
Ход работы:

Таблица 2.1 – Исходные данные для смоделированной сети

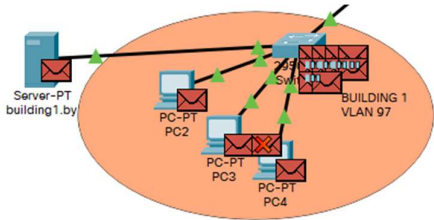
| Третья цифра шифра | Содержимое пакетов при атаке | | | |
|--------------------|-----------------------------------|------|------------------|-----------|
| | Ping flood, UDP flood и SYN flood | | UDP flood | SYN flood |
| | TTL | Size | Destination Port | |
| 0 | 128 | 1064 | DNS | SFTP |
| 1 | 64 | 1066 | TFTP | FINGER |
| 2 | 32 | 1067 | SNMP | FTP |
| 3 | 65 | 1068 | 700 | HTTP |

2. Ping flood

Настраиваю генерацию пакетов ICMP. В качестве адреса источника и назначения указываю широковещательные IP-адреса, с целью скрытия адреса атакующего и вызова ответа на ICMP-пакет, так что каждое устройство получая данный пакет, будет генерировать на него ответ на широковещательный адрес сети. TTL и Size устанавливаю по таблице с исходными данными.



Далее в режиме симуляции наблюдаю лавинное распространение пакетов.



Во время атаки доступа из нашей сети во внешнюю получить не удалось

Выполняю ping до атаки

```
Pinging 172.10.0.146 with 32 bytes of data:

Reply from 172.10.0.146: bytes=32 time<1ms TTL=128
Reply from 172.10.0.146: bytes=32 time<1ms TTL=128
Reply from 172.10.0.146: bytes=32 time<1ms TTL=128
Reply from 172.10.0.146: bytes=32 time=1ms TTL=128

Ping statistics for 172.10.0.146:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Выполнения ping после атаки

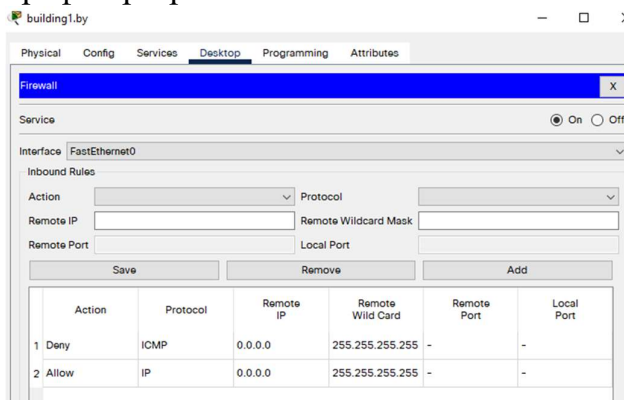
```
Reply from 172.10.0.146: bytes=32 time<1ms TTL=128
Reply from 172.10.0.146: bytes=32 time=1ms TTL=128
Reply from 172.10.0.146: bytes=32 time=10ms TTL=128
Reply from 172.10.0.146: bytes=32 time<1ms TTL=128

Ping statistics for 172.10.0.146:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

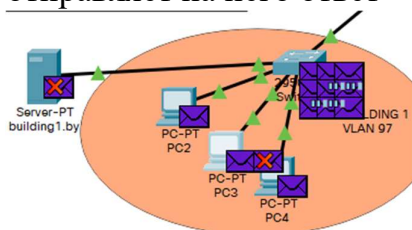
Можно сделать вывод, что время передачи данных после проведения Ping flood увеличилось.

3. Защита от Ping flood

Настраиваю два правила: одно для блокировки ICMP пакетов от всех устройств, второе для разрешения трафика по протоколу IP. Блокировке будут подвергаться любые пакеты ICMP, весь остальной трафик разрешен.

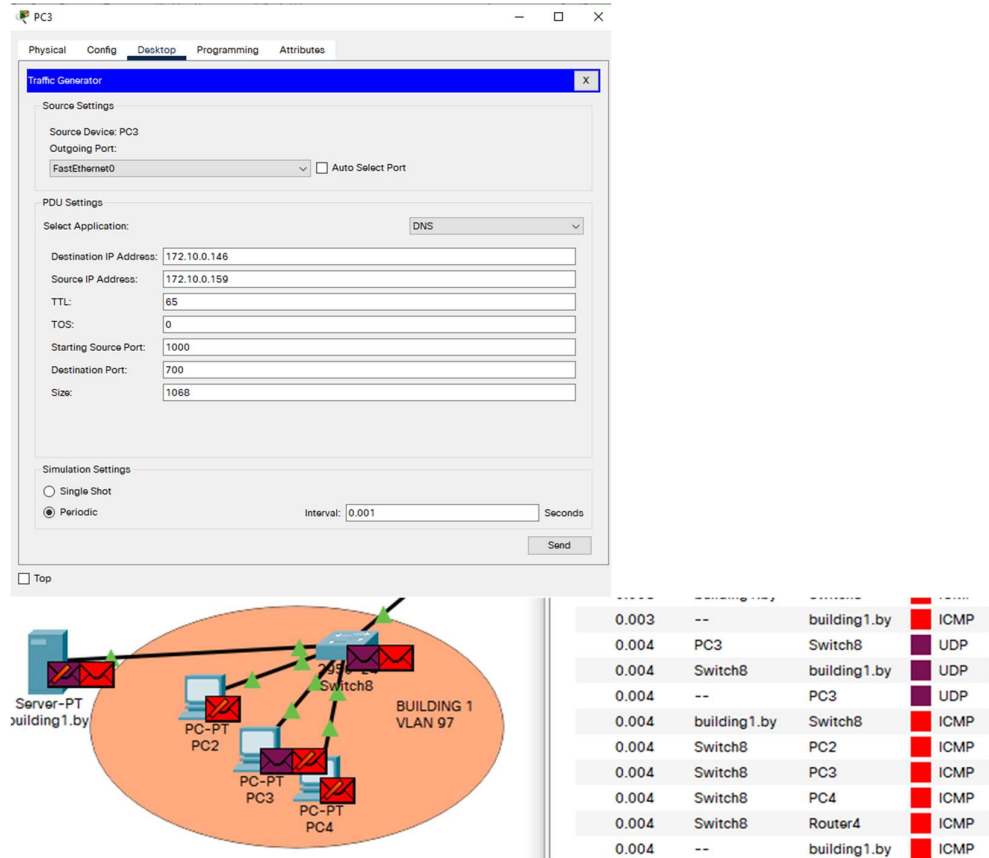


На рисунке видно, что сервер блокирует пакет ICMP и не отправляет на него ответ



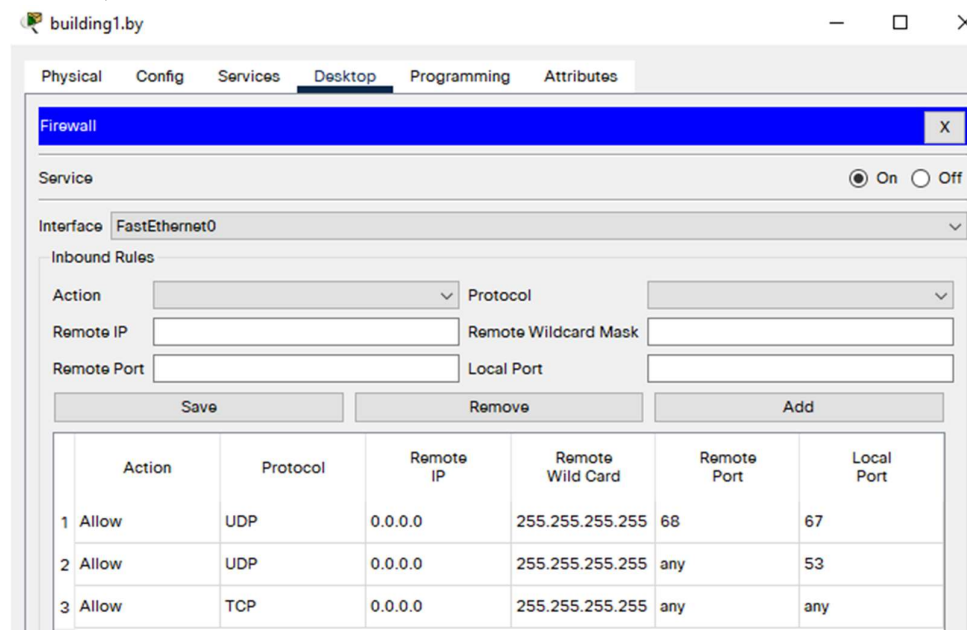
4. UDP flood атака

Настройка генерации трафика пакетов DNS, так как он использует UDP запросы. В качестве IP-адреса назначения использую адрес сервера, источник – широковещательный адрес для того, чтобы ответы сервера рассылались всем устройствам в сети и перегружали ее.



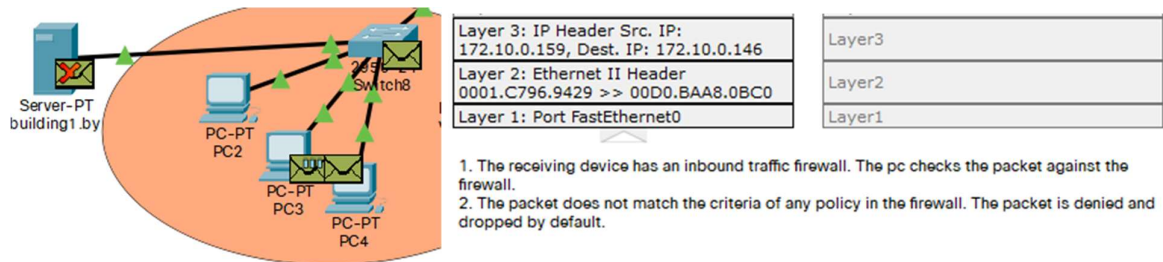
| Seq | Source | Destination | Protocol |
|-------|--------------|--------------|----------|
| 0.003 | -- | building1.by | ICMP |
| 0.004 | PC3 | Switch8 | UDP |
| 0.004 | Switch8 | building1.by | UDP |
| 0.004 | -- | PC3 | UDP |
| 0.004 | building1.by | Switch8 | ICMP |
| 0.004 | Switch8 | PC2 | ICMP |
| 0.004 | Switch8 | PC3 | ICMP |
| 0.004 | Switch8 | PC4 | ICMP |
| 0.004 | Switch8 | Router4 | ICMP |
| 0.004 | -- | building1.by | ICMP |

5. Защита от UDP flood



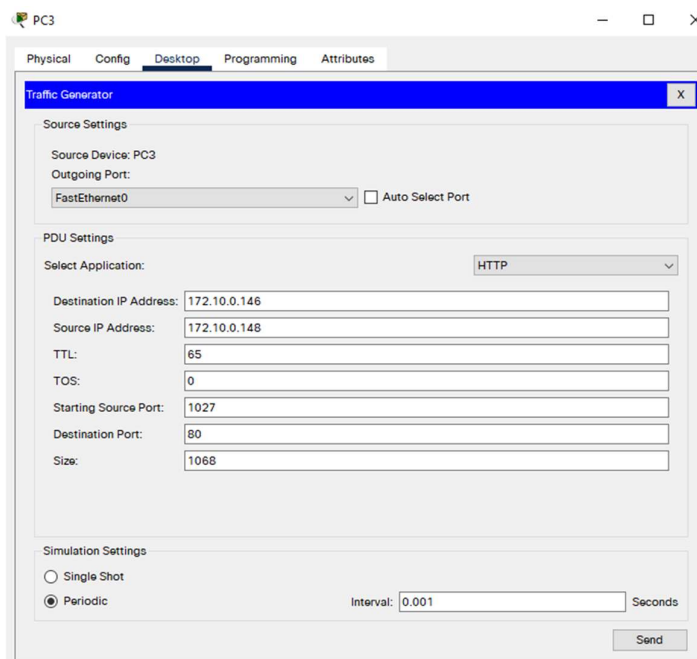
| Action | Protocol | Remote IP | Remote Wild Card | Remote Port | Local Port |
|---------|----------|-----------|------------------|-------------|------------|
| 1 Allow | UDP | 0.0.0.0 | 255.255.255.255 | 68 | 67 |
| 2 Allow | UDP | 0.0.0.0 | 255.255.255.255 | any | 53 |
| 3 Allow | TCP | 0.0.0.0 | 255.255.255.255 | any | any |

Осуществлена настройка firewall для сервера. Пакеты неудовлетворяющие параметрам firewall отклоняются

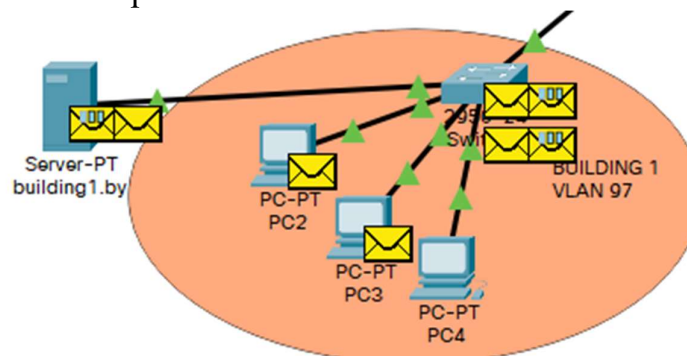


6. SYN flood

В качестве адреса назначения – сервер. В качестве источника – адрес любого оконечного устройства в сети для того, чтобы ответы сервера отправлялись устройству, что обозначает открытие сессии для данного устройства и ожидание сервером пакета TCP с флагом подтверждения от устройства.

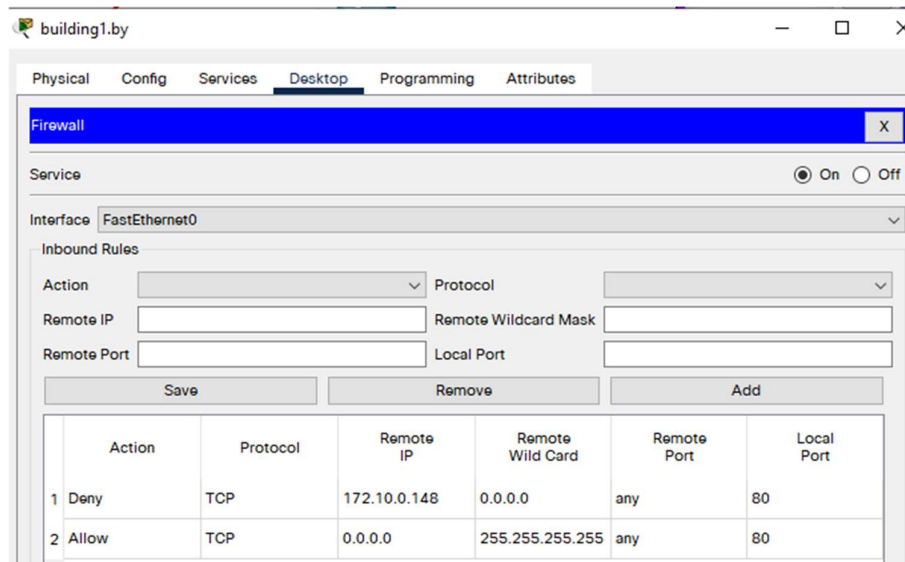


Лавинная рассылка TCP пакетов в сети

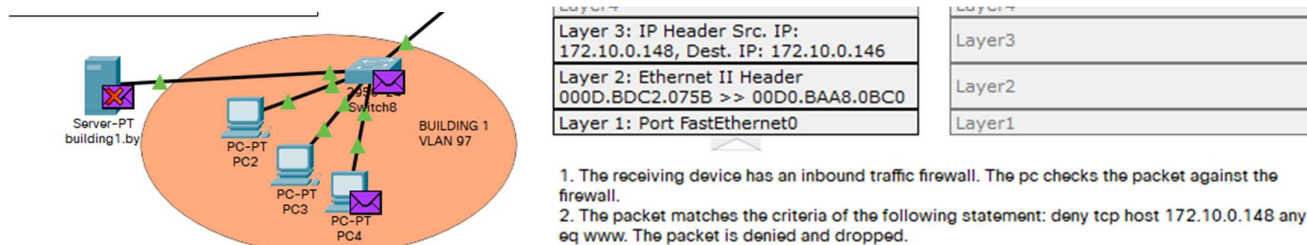


7. Защита от SYN flood

Конфигурация критериев firewall, после обнаружения SYN flood атаки. В результате все пакеты от устройства с ip-адресом 172.10.0.148 будут заблокированы.



Результат проверки блокировки пакетов



Вывод: конечная цель DDoS и DoS-атак – повлиять на доступность ресурсов, обеспечить отказ в обслуживании. Я рассмотрела атаки с истощением ресурсов (Ping flood, UDP flood), атаку на уровне протоколов (SYN flood). При ping flood на сервер отправляются пакеты эхо-запросов ICMP. После отправки такого запроса сервер сразу же отвечает на него, следовательно, при большом кол-ве запросов злоумышленник истощает пропускную способность во входящем и исходящем направлении. UDP flood проводится на случайно выбираемые порты с помощью UDP пакетов, сервер проверяет порты на наличие соответствующих приложений. Если приложение найти не удастся, система отправляет на каждый запрос пакет с информацией о том, что получатель недоступен, следовательно, трафик может превысить ресурсы среды. SYN flood – атака, при которой злоумышленник отправляет внешне нормальные запросы на сервер, который отвечает SYN-ACK. Обычно клиент отвечает ACK, и устанавливает сетевое соединение. Но при атаке злоумышленник не отправляет последний ACK (незавершенные запросы), что создает большую нагрузку на сеть.

