В самом начале отчета в лабораторной работе необходимо привести таблицу вашего варианта задания, например:

Таблица 14.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | 22 | | | |
|  | 192.168.257.1/24 | 220.220.10.1/30 | 220.220.20.1/24 | 220.220.30.1/30 |

# DMZ

Теперь в схеме заменим ASA на Router 2811 и попробуем организовать ДМЗ. Поскольку у Router 2811 всего 2 интерфейса, добавим еще один используя слот NM-1FE-TX. Включаем и переходим в консоль.

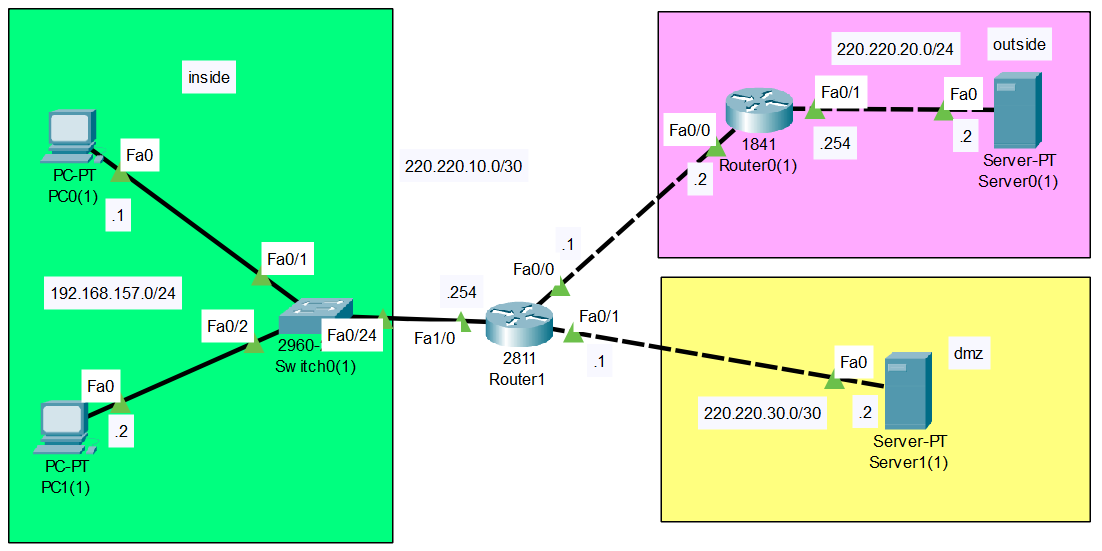


Рис. 1

Настроить адреса на интерфейсах, пометить каждый интерфейс командами: description outside, dmz, inside. На интерфейсе outside ввести команду ip nat outside, и на inside соответственно, на dmz не вводить. Теперь проверим доступность роутера провайдера.

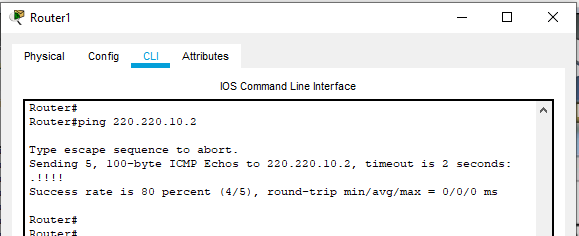


Рис. 2

Проверяем доступность сервера ДМЗ.

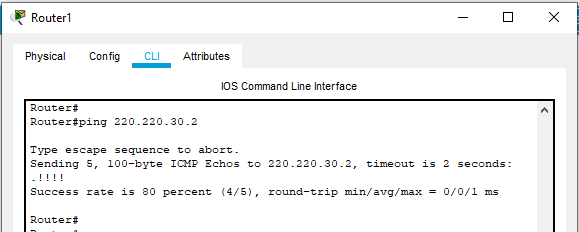


Рис. 3

Как видим сервер доступен. Проверяем доступность внутренней локальной сети.

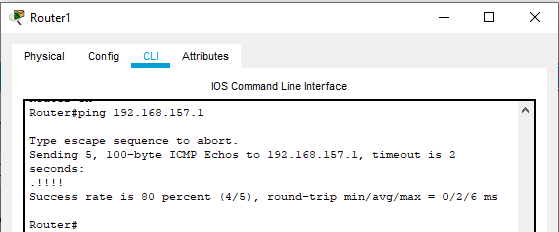


Рис. 4

Внутренняя сеть доступна. Проверяем доступность сервера в интернете.

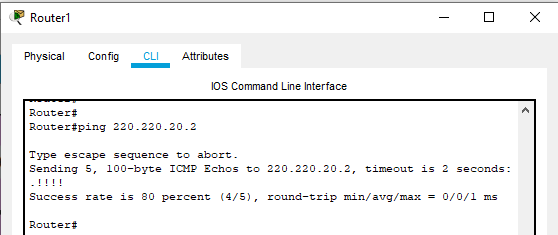


Рис. 5

Сервер интернета так же доступен. Проверяем доступность публичного сервера в интернете из локальной сети. Нужно прописать шлюз по умолчанию на роутере.

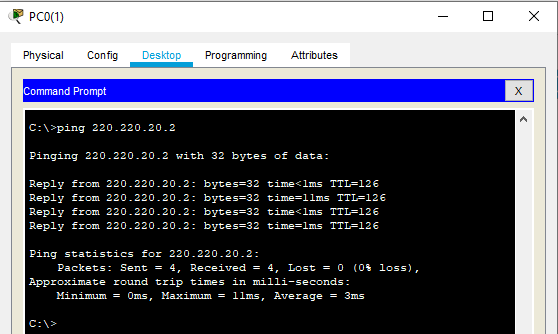


Рис. 6

Проверяем доступность ДМЗ сервера.

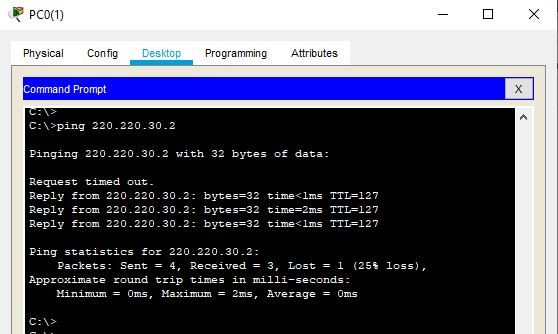


Рис. 7

Доступен. Однако и из интернета локальная сеть доступна, что конечно недопустимо.

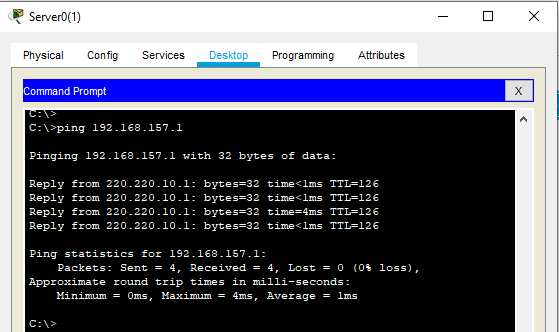


Рис. 8

Необходимо запретить весь входящий трафик в локальную сеть из внешней сети, разрешить на внешнем интерфейсе несколько портов до ДМЗ сервера и запретить трафик из ДМЗ в локальную сеть. А для локальной сети доступ должен быть разрешен всюду. Настроим access-list для внешнего интерфейса на граничном роутере.

1 создаем расширенный access-list с именем FROM-OUTSIDE;

2 разрешаем трафик icmp от любого хоста из интернета до web-сервера в ДМЗ;

3 разрешаем web-трафик от любого хоста из интернета до web-сервера в ДМЗ по 80 порту;

4 все остальное запрещаем;

5 привяжем этот access-list к внешнему интерфейсу в направлении входящего трафика.

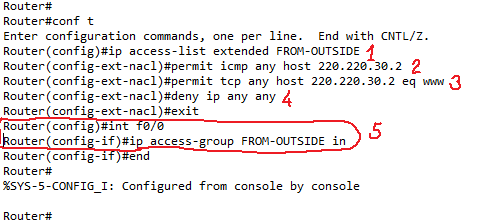


Рис. 9

Проверяем доступ из интернета до сервера в ДМЗ

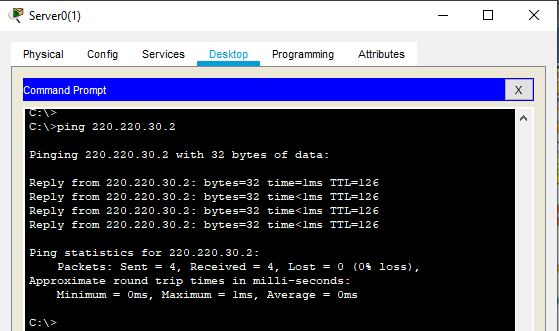


Рис. 10

Доступен. Web-доступ до сервера тоже есть.

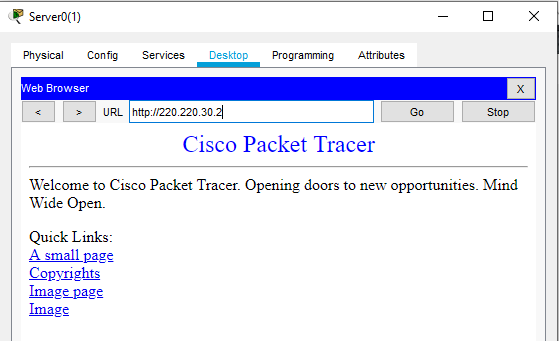


Рис. 11

Но при этом из локальной сети пропал доступ в интернет.

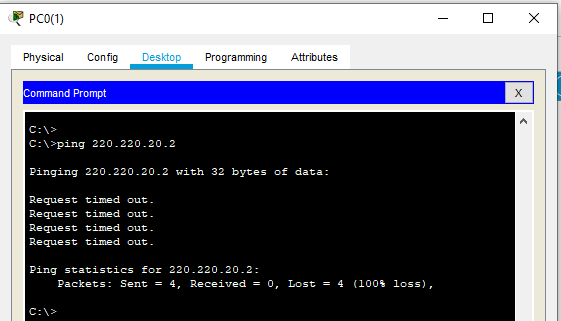


Рис. 12

Это связано с access-list, который повесили на внешний интерфейс пропускающий трафик только до публичного сервера в ДМЗ. Для устранения этого недостатка используем технологию инспектирования трафика.

1 определяем какой именно трафик будет разрешен локальному пользователю, который нужно инспектировать трафик будет направлен из внутренней сети во внешнюю;

2 инспектируем его на входе из внутренней сети

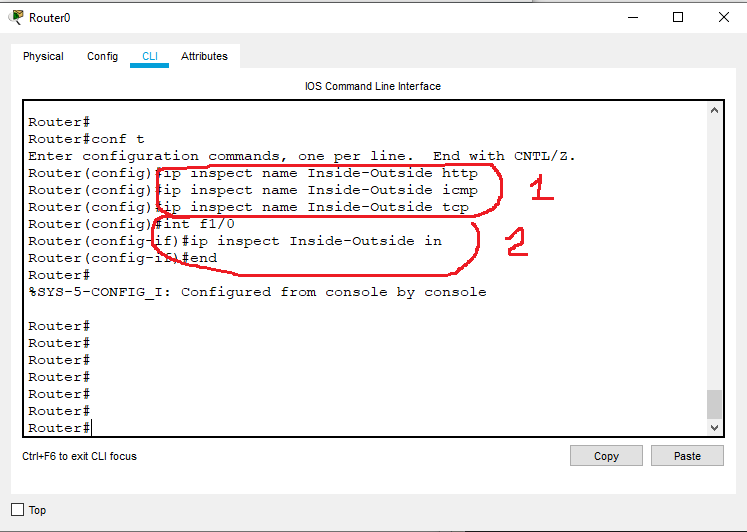


Рис. 13

Как только трафик попадает на роутер он инспектируется в соответствии с настроенными правилами, т.е. добавляется во временную таблицу маршрутизатора запоминает сессию, выпускает трафик во вне и как только придет обратный трафик маршрутизатор определит, что этот трафик был инициирован из внутренней сети и его необходимо пропустить. При этом трафик, инициированный из вне не будет пропущен.

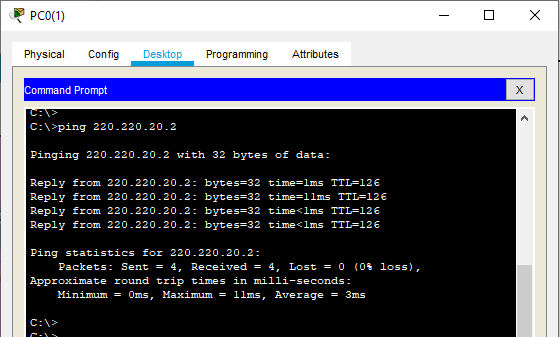


Рис. 14

Как видим теперь доступ в интернет из локальной сети разрешен.

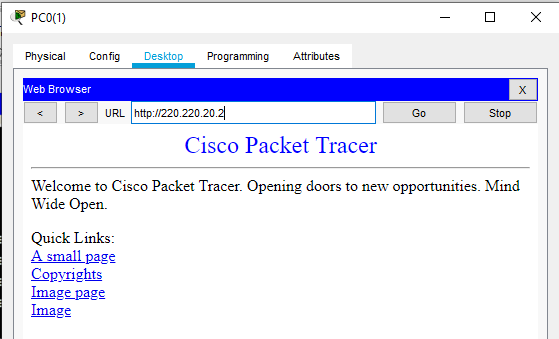
****

Рис. 15

Web-доступ так же разрешен. Проверим доступ в локальную сеть из интернета.

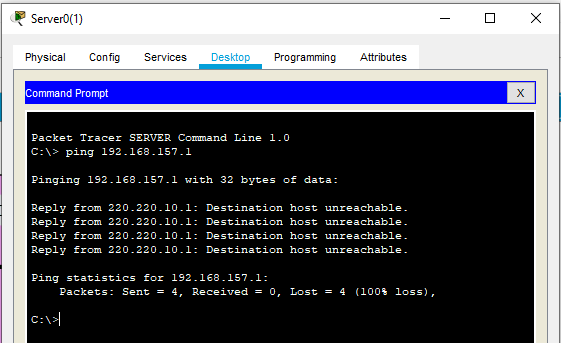


Рис. 16

Доступ запрещен.

Аналогично необходимо запретить трафик во внутреннюю сеть из ДМЗ. Запретить трафик во внутреннюю сеть.

1 создаем access-list с именем FROM-DMZ

2 запрещаем трафик от хоста 220.220.30.2 до локальной сети 192.168.157.0 с маской 0.0.0.255

3 сервер должен отвечать на запросы внешних источников.

Поскольку правила обрабатываются в порядке записи, то в случае появления запроса из ДМЗ в локальную сеть сработает первое правило. Если сгенерируется трафик, который не подпадает под первое правило, то вторым правилом трафик будет разрешен, т.е. ответы будут уходить в интернет.

4 привяжем этот access-list к интерфейсу f0/1 на вход.

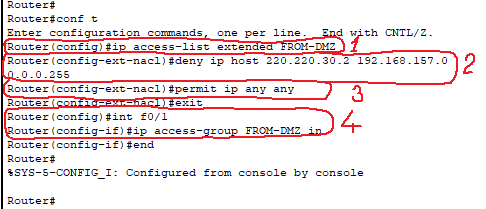


Рис. 17

Проверим доступность сервера ДМЗ из локальной сети

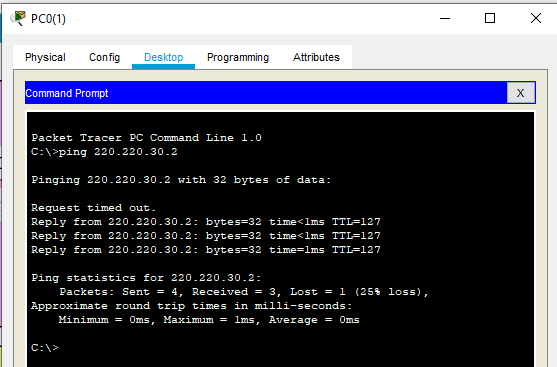


Рис. 18

Сервер ДМЗ доступен. Проверим по web-интерфейсу.

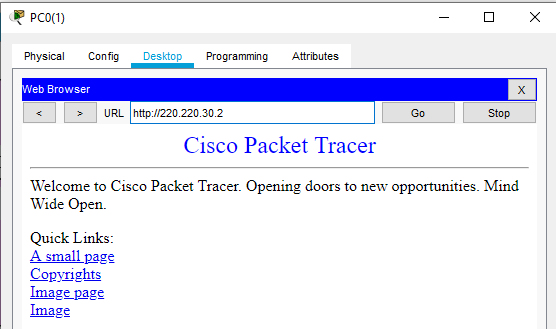


Рис. 19

Доступен. А теперь с ДМЗ посмотрим доступ в локальную сеть.

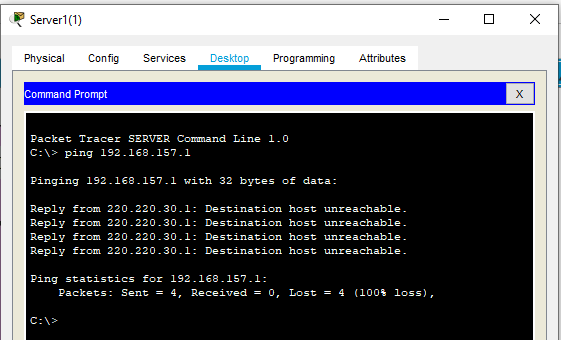


Рис. 20

Доступ запрещен. Мы это запрещали специально. Проверяем доступность ДМЗ сервера из интернета.

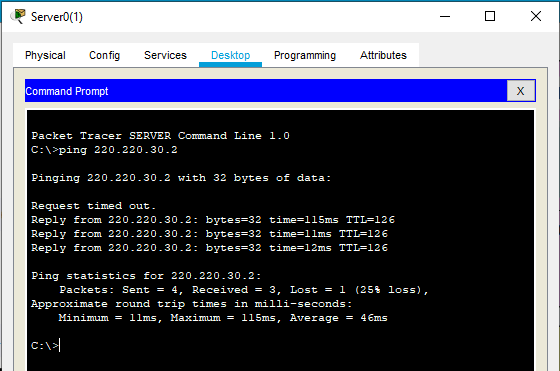


Рис. 21

Доступен. А теперь проверим доступность по web-интерфейсу.

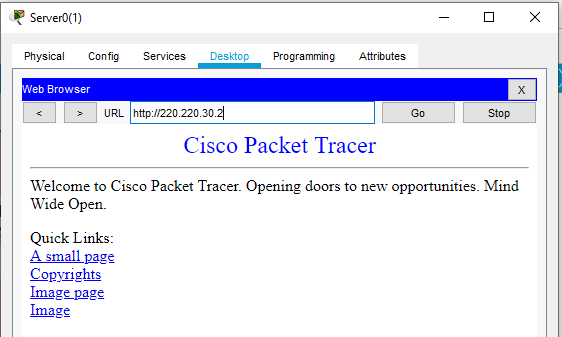


Рис. 22

На этом настройка закончена. Хочу обратить внимание на то, что все сервера, которым предоставляется доступ из интернета, выносить в отдельный сегмент, разрешать к ним доступ из интернета и запрещать доступ из этого сегмента в локальную сеть чтобы обезопасить пользователей от злоумышленников, взломавших публичные серверы.