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

Таблица 12.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | 22 | | | |
| Сеть 1 | 192.168.157.1/24 | 220.220.10.1/30 | 220.220.20.1/24 |  |

# DMZ

Необходимо собрать следующую схему, на каждом устройстве настроить указанные на схеме адреса.

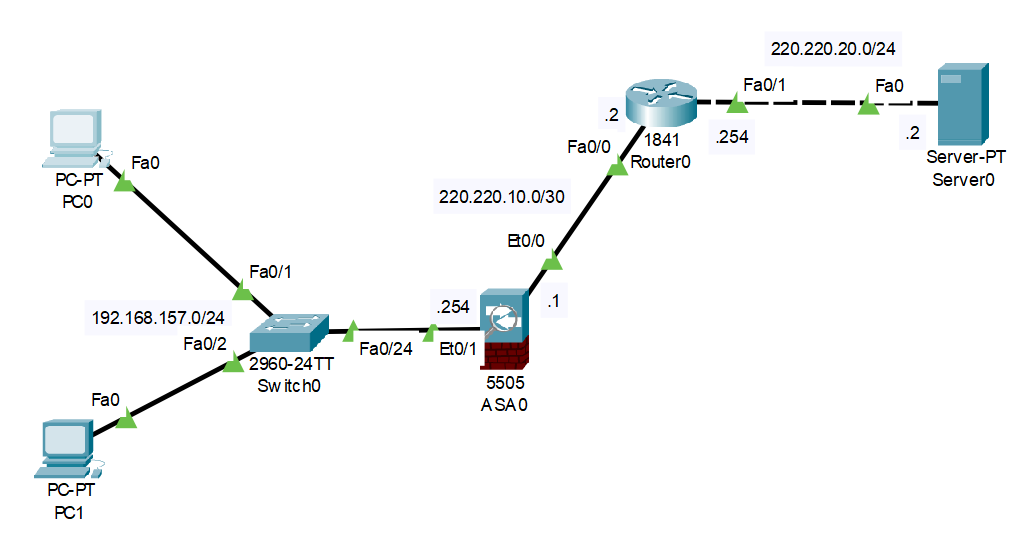


Рис. 1

На cisco ASA на интерфейсе inside изменить адрес, на интерфейсе outside настроить новый адрес. Настроить NAT для выхода из внутренней сети к провайдеру и инспектирование трафика icmp, http.

На маршрутизаторе прописать адреса на обоих интерфейсах и роутинг во внутреннюю сеть.

Теперь мы хотим добавить DMZ-сегмент, в который мы хотим публичный сервер (путь это будет web-сервер). На межсетевом экране cisco ASA DMZ организуется с помощью security-level. Мы уже имеем на inside сети security-level = 100, а на outside сети security-level = 0. Выбор security-level для DMZ осуществляется в диапазоне строго больше нуля и строго меньше 100. Выберем 50. При этом:

1 трафик из inside сети в outside сеть будет разрешен по умолчанию;

2 из outside сети в inside сеть будет запрещен;

3 также трафик из inside сети в DMZ сеть будет разрешен по умолчанию;

4 из DMZ сети в inside сеть будет запрещен;

5 из DMZ сети в outside сеть будет разрешен по умолчанию;

6 outside сети в DMZ сеть будет запрещен.

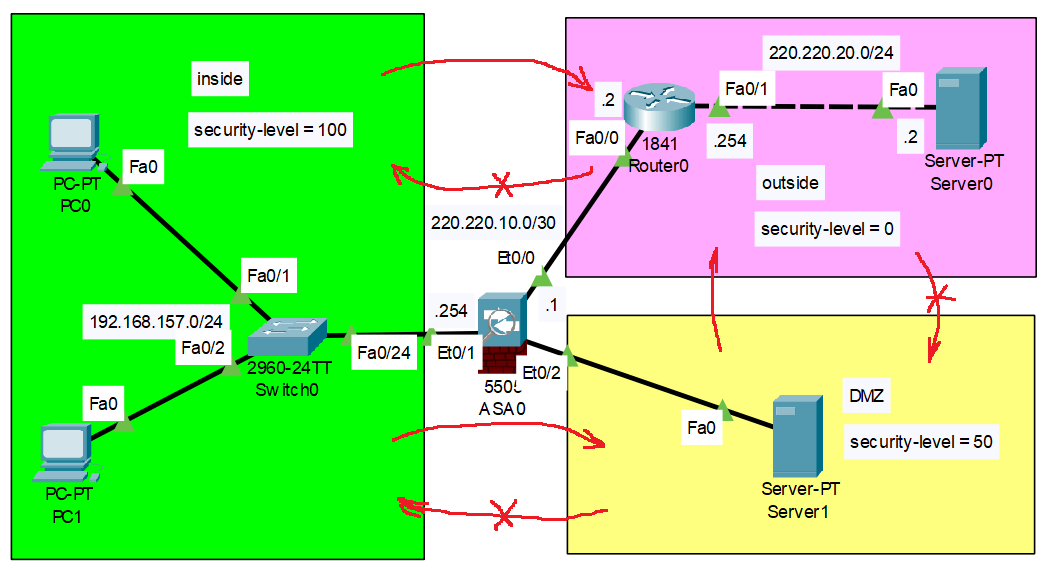


Рис. 2

На маршрутизаторе провайдера прописать маршрут в сеть ДМЗ через внешний интерфейс cisco ASA, чтобы остальные могли находить ДМЗ.

Ip route 220.220.3.0 255.255.255.252 220.220.10.1

На самой cisco ASA создаем еще один сегмент, но если посмотреть версию cisco ASA, то мы увидим

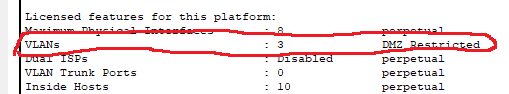


Рис. 3

Мы видим, что доступно всего 3 вилана, при этом ДМЗ ограниченный. Попробуем создать сегмент. Создаем на интерфейсе eth0/2 вилан с номером 3 и присваиваем ему имя DMZ.

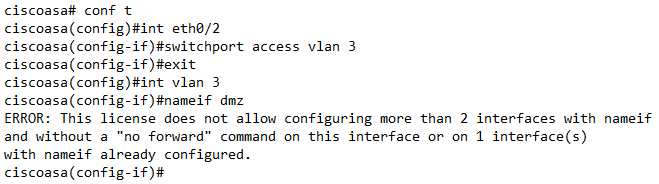


Рис. 4

Получаем ошибку, которая говорит о том, что лицензия не позволяет использовать более двух интерфейсов, не употребляя функции no forward. Это значит, что необходимо указать на ASA один интерфейс, на который не будет передаваться трафик. Это неудобно, но Packet Tracer по-другому нельзя.

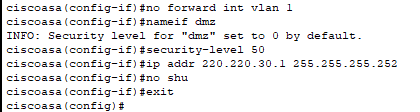


Рис. 5

И тут же с ASA мы увидели сервер ДМЗ.

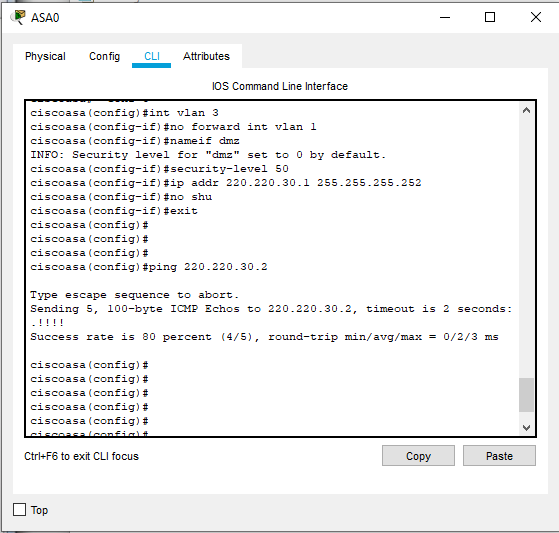


Рис. 6

Вот схема сети с адресами

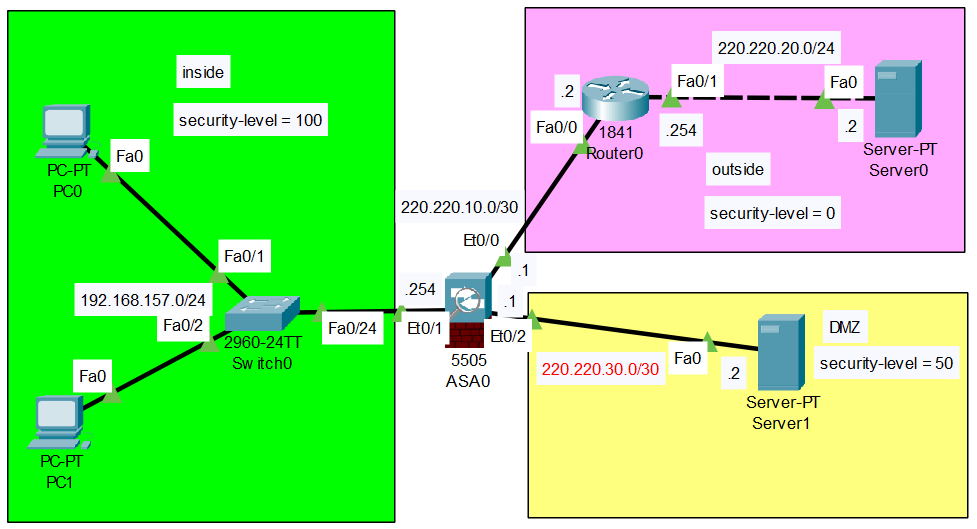


Рис. 7

Однако ping с публичного сервера до сервера ДМЗ не проходит потому, что security-level на outside составляет 0, а security-level на DMZ составляет 50. По умолчанию этот трафик запрещен.

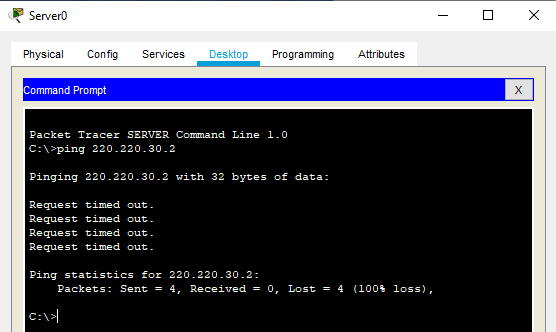


Рис. 8

Следовательно, мы должны прописать access-list чтобы разрешить трафик определенного типа, до DMZ. Создаем access-group, название которой должно совпадать с названием access-list и вешаем на внешний интерфейс на входящий трафик.

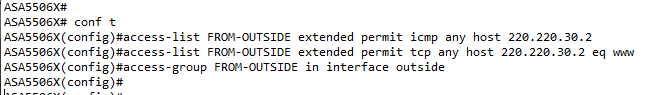


Рис. 9

Как видим ping с сервера в интернете до сервера в ДМЗ пошел.

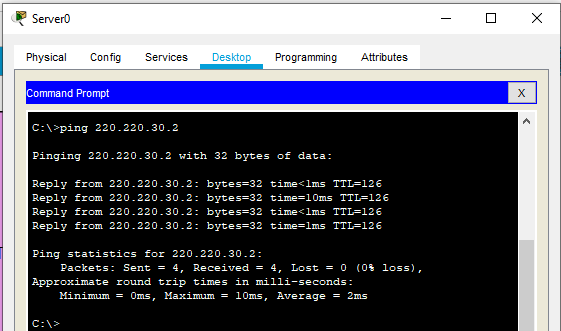


Рис. 10

Проверяем доступность Web-сервера

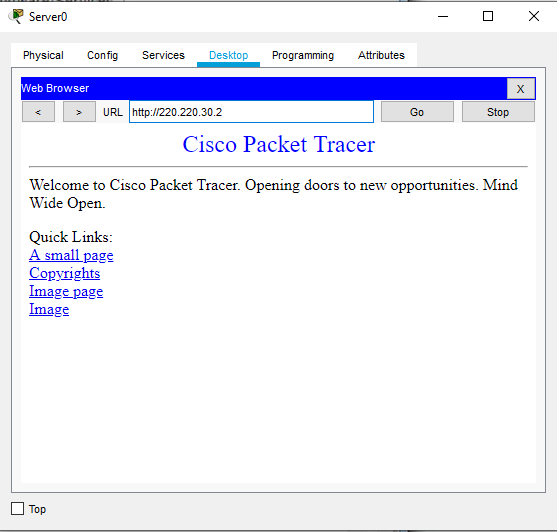


Рис. 11

Теперь проверяем доступ из локальной сети

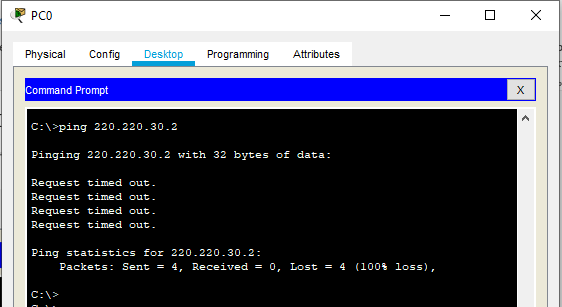


Рис. 12

Не проходит. Это потому, что не позволяет лицензия.