**Московский государственный технический**

**университет им. Н.Э. Баумана**

Факультет «Информатика и системы управления»

Кафедра ИУ5 «Системы обработки информации и управления»

Курс «Сетевая безопасность»

Отчет по лабораторной работе №1

|  |  |  |
| --- | --- | --- |
| Выполнил: |  | Проверил: |
| студент группы ИУ5-73Б |  | преподаватель каф. ИУ5 |
| Терентьева Софья  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |  | Симонов Михаил Фёдорович  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |

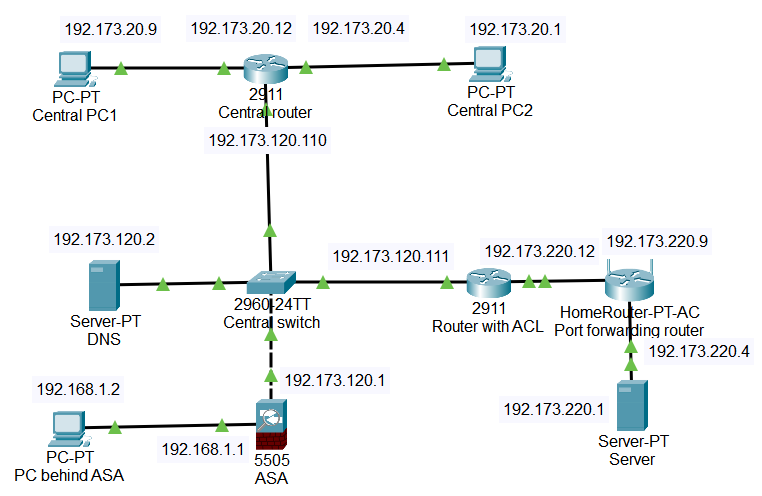
Москва, 2024 г.

Цель работы:

Изучение access control list и возможностей deep packet inspection сетевого оборудования Cisco.

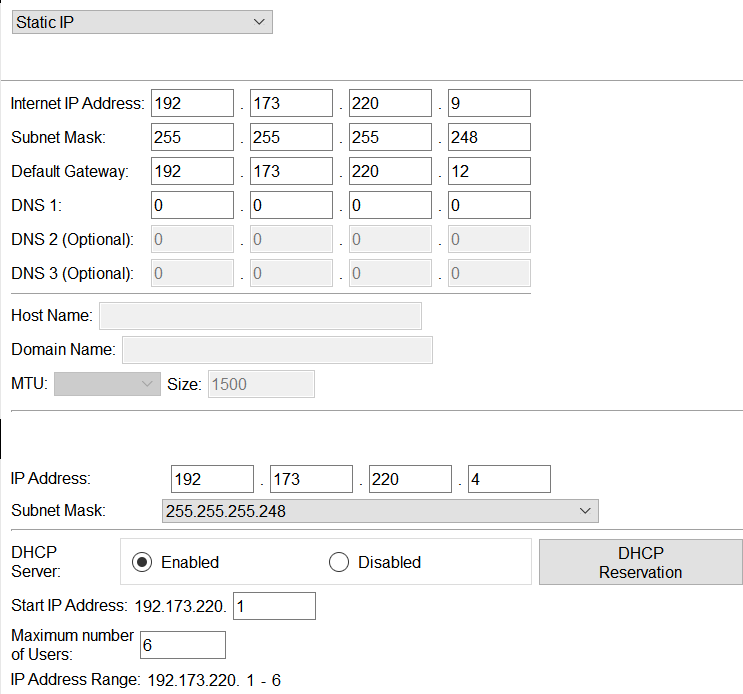
Ход работы:

1. Построить виртуальную сеть с IP-адресами подсетей по варианту:

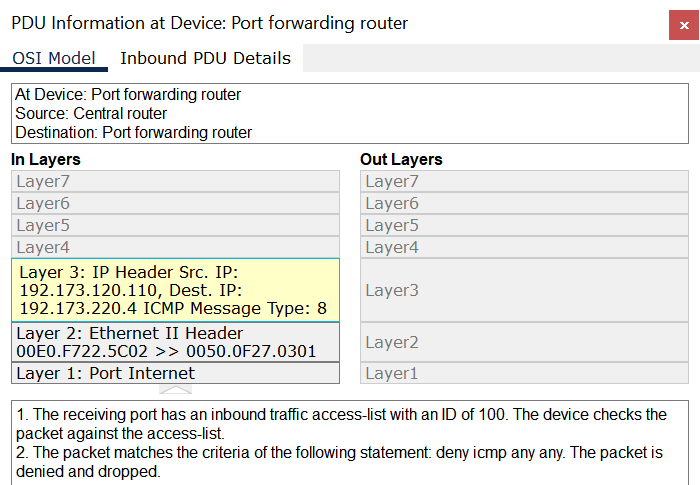


1. Настроить маршрутизацию между Central PC1 и Port forwarding router:

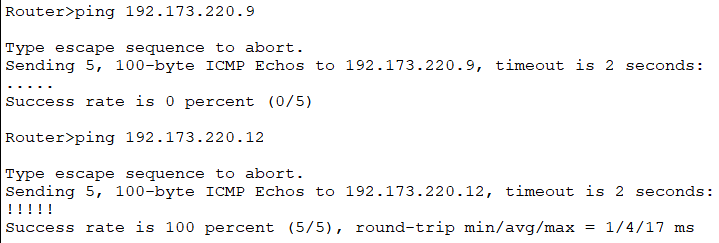
Для настройки маршрутизации пропишем на устройствах IP-адреса, Default gateway и настроим Port forwarding router через GUI:



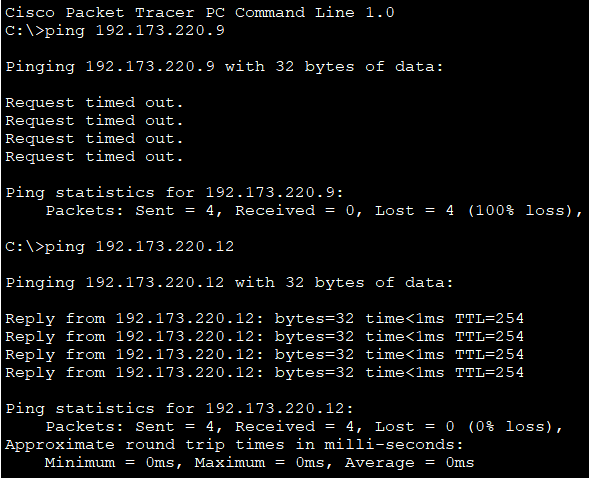
В силу особенностей эмулятора Cisco Packet Tracer у беспроводного роутера есть базовая настройка, которая не изменяется и приводит к ошибке при отправке на него пакетов:

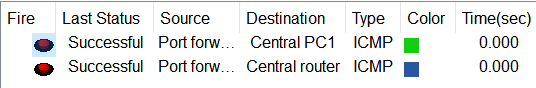


Поэтому для проверки работы соединения следует пинговать не 192.173.220.9, а 192.173.220.12. Проверим связь роутеров:

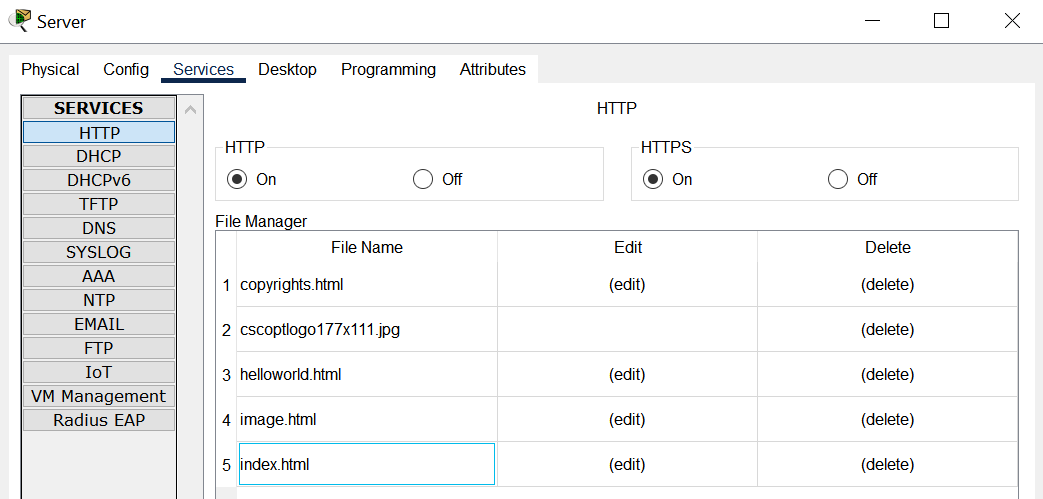


Проверим связь Central PC1 и Port forwarding router:

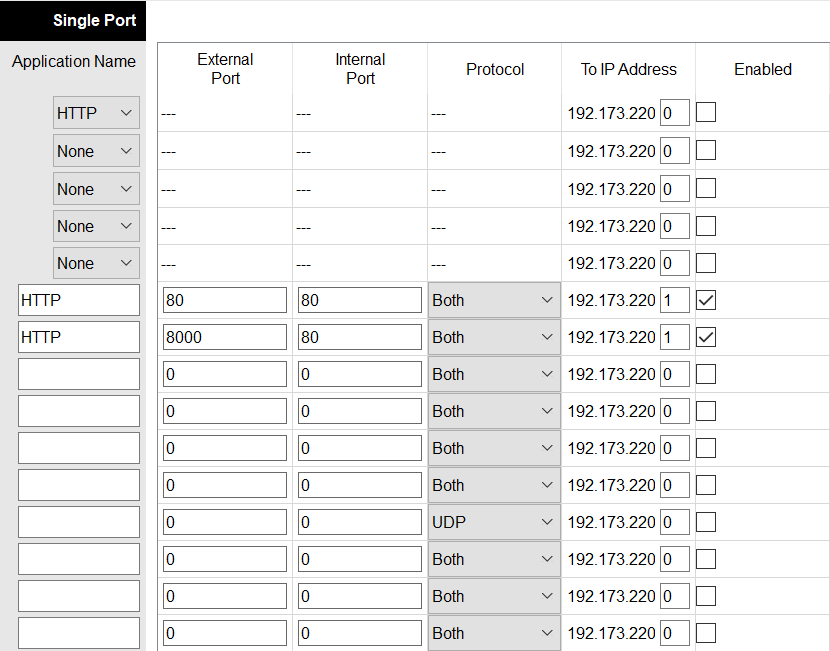




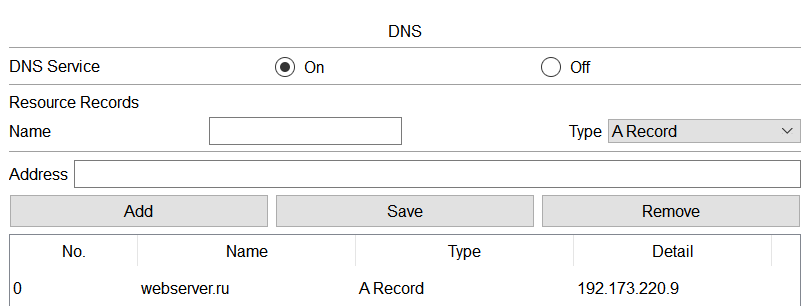
1. Настроить веб-сервер на Server:



1. На Port forwarding router настроить перенаправление портов 80 и 8000 на веб-сервер:

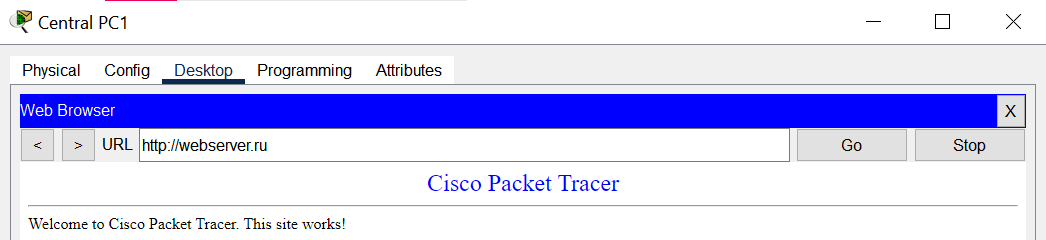


1. Настроить DNS сервер: добавить DNS-запись для доступа к веб-серверу:



IP-адрес Web-сервера также обусловлен особенностью роутера.

1. Проверить доступ к веб-серверу с Central PC1 по доменному имени:



1. Настроить расширенный ACL на роутере Router with ACL для запрета доступа с Central PC1 к веб-серверу на стандартном порте:

Настраивать ACL будем на интерфейсе Gig0/0 (для входящего трафика), чтобы уменьшить нагрузку на роутер.

*Router(config)#access-list 100 deny tcp 192.173.20.9 0.0.0.7 host 192.173.220.9 eq 80*

*Router(config)#access-list 100 permit tcp any any*

*Router(config)#access-list 100 permit ip any any*

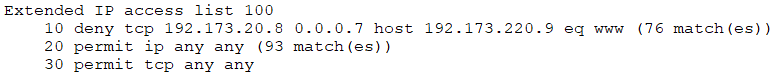
*Router(config)#interface GigabitEthernet0/0*

*Router(config-if)#ip access-group 100 in*

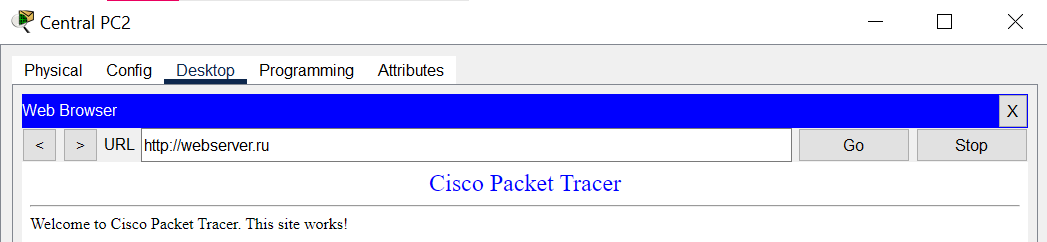
*Router(config-if)#exit*

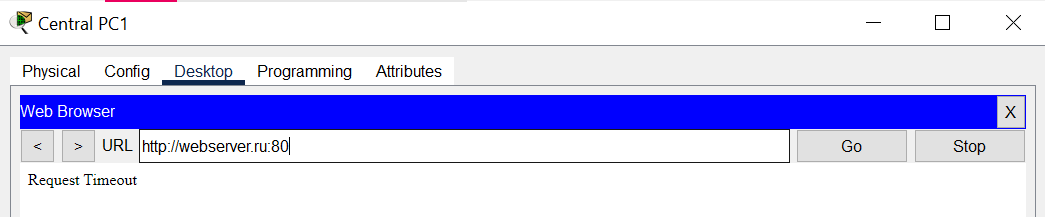
*Router(config)#exit*

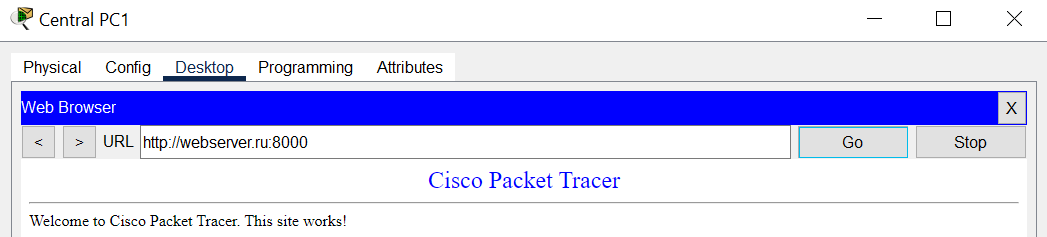
*Router#show access-lists*



1. Продемонстрировать доступ к веб-серверу по доменному имени с Central PC2, отсутствие доступа с Central PC1 на стандартном порте и наличие на нестандартном:







1. Настроить NAT и DPI на ASA 5505, разрешить исходящий ICMP и DNS трафик:

В силу особенностей эмулятора Cisco Packet Tracer пришлось дать расположенному во внутренней подсети компьютеру IP-адрес 192.168.1.2, так как адрес внутреннего интерфейса по умолчанию 192.168.1.1. Вероятно, это связано с политикой белых и серых IP-адресов.

Настройка NAT на ASA 5505:

*ciscoasa(config)#interface vlan 2*

*ciscoasa(config-if)#nameif outside*

*ciscoasa(config-if)#ip address 192.173.120.1 255.255.255.0*

*ciscoasa(config-if)#security-level 0*

*ciscoasa(config-if)#interface vlan 1*

*ciscoasa(config-if)#nameif inside*

*ciscoasa(config-if)#security-level 100*

*ciscoasa(config-if)#dhcpd dns 192.173.120.2*

*ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 192.173.120.111*

*ciscoasa(config)#object network inside-net*

*ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0*

*ciscoasa(config-network-object)#nat (inside,outside) dynamic interface*

*ciscoasa(config-network-object)#end*

Настройка DPI на ASA 5505:

*ciscoasa(config)#class-map inspection\_default*

*ciscoasa(config-cmap)#match default-inspection-traffic*

*ciscoasa(config-cmap)#exit*

*ciscoasa(config)#policy-map global\_policy*

*ciscoasa(config-pmap)#class inspection\_default*

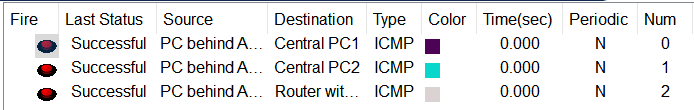
*ciscoasa(config-pmap-c)#inspect icmp*

*ciscoasa(config-pmap-c)#inspect dns*

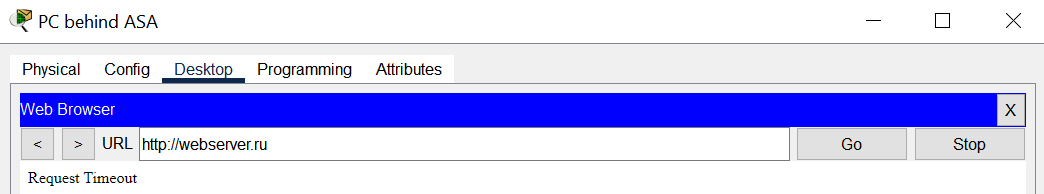
*ciscoasa(config-pmap-c)#exit*

*ciscoasa(config)#service-policy global\_policy global*

1. С PC behind ASA продемонстрировать работу ICMP и отсутствие доступа к веб-серверу:



Видно, что ICMP-трафик успешно проходит в любые сегменты сети.

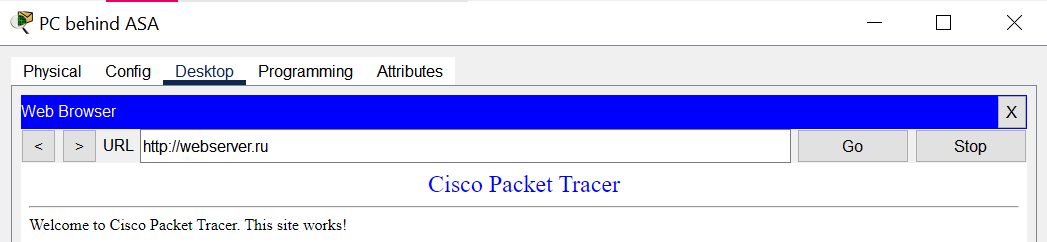


1. Разрешить HTTP-трафик в DPI на ASA 5505, продемонстрировать наличие доступа к веб-серверу с PC behind ASA:

Добавим в конфигурацию выше строчку:

*ciscoasa(config-pmap-c)#inspect http*

Проверим изменения:



Результаты выполнения работы:

В процессе выполнения лабораторной работы я освежила знания о технологии ACL, познакомилась с межсетевым экраном ASA 5505 и технологиями фильтрации трафика с его помощью и научилась применять их на практике.