Практическая работа №9

Тема: «Исследование основных функций межсетевого экрана CISCO ASA 5505».

Цель работы: изучить основные функциональные особенности оборудования Cisco ASA 5505, освоить принципы использования оборудования Cisco ASA 5505, а так же освоить принципы конфигурирования оборудования Cisco ASA 5505.

Ход работы:

Для выполнения практической работы необходимо промоделировать сеть, представленную на рисунке 1.

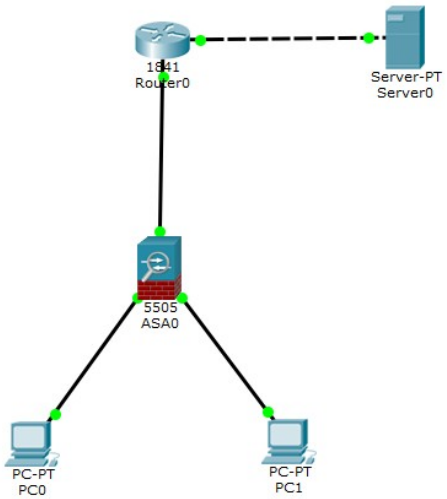

Рис. 1 Исходная сеть

Для входа в управляющую программу сетевого экрана используем HyperTerminal, вводим команду en для входа в привилегированный режим, по умолчанию пароль пустой, поэтому просто нажимаем enter.

```
ciscoasa>en
Password:
ciscoasa#
```

Исходная конфигурация CISCOASA 5505.

```
ciscoasa#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
```

По умолчанию на CISCOASA 5505 работает DHCP-сервер, поэтому подключенные к нему компьютеры автоматически получают IP-адреса.

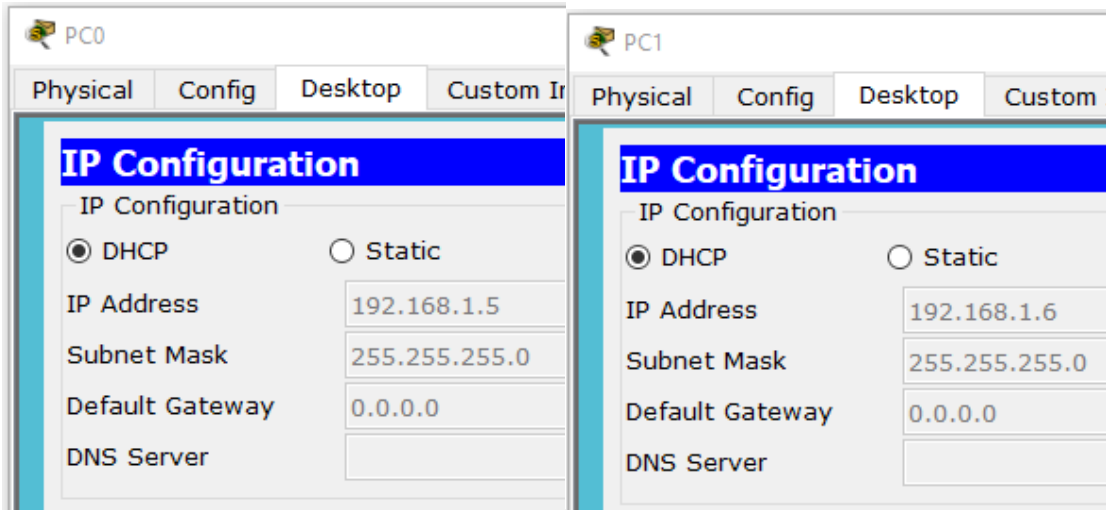

Рис. 2 IP-адреса компьютеров

Для обеспечения безопасного входа на устройство зададим пароль для входа в привилегированный режим и пользовательское имя и пароль.

```
ciscoasa#conf t
ciscoasa(config)#enable password cisco
ciscoasa(config)#username admin password cisco
ciscoasa(config)#
```

Пароли для enable и пользователя сразу зашифрованы.

```
hostname ciscoasa
enable password 4IncP7vTjpaba2aF encrypted

username admin password 4IncP7vTjpaba2aF encrypted
```

С помощью команды show ip address узнаем параметры VLAN (должно быть настроено две VLAN: внутренняя и внешняя сети);

```
ciscoasa(config)#show ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   CONFIG
Vlan2                  outside             unassigned      unassigned      DHCP

Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   CONFIG
Vlan2                  outside             unassigned      unassigned      DHCP
```

Рис. 3 Команда show ip address

Установим имя устройства, для повышения безопасности устройства настроем протокол удаленного доступа SSH для этого указываем сеть, из которой будет возможен доступ и интерфейс, с которого будет осуществляться доступ:

```
ciscoasa(config)#hostname ASA5505
ASA5505(config)#ssh 192.168.1.0 255.255.255.0 inside
ASA5505(config)#aaa authentication ssh console Local
ASA5505(config)#
```

Проверим удаленный доступ к CISCO ASA.

```
PC>ssh -l admin 192.168.1.1
Open
Password:



ASA5505>en
Password:
ASA5505#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ASA5505
enable password 4IncP7vTjpaba2aF encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
```

Рис. 4 Получение удаленного доступа к ASA по протоколу SSH

Изменим Security-level и присвоим адрес внешнему интерфейсу, для этого выполним следующие команды:

```
ASA5505(config)#int vlan 1
ASA5505(config-if)#security-level 95
ASA5505(config-if)#exit
ASA5505(config)#int vlan 2
ASA5505(config-if)#security-level 5
ASA5505(config-if)#ip add 210.210.0.2 255.255.255.252
ASA5505(config-if)#no shutdown
ASA5505(config-if)#exit
```

Перейдем к настройке маршрутизатора.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 210.210.0.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip address 210.210.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
Router#
```

Перейдем к настройке Сервера.

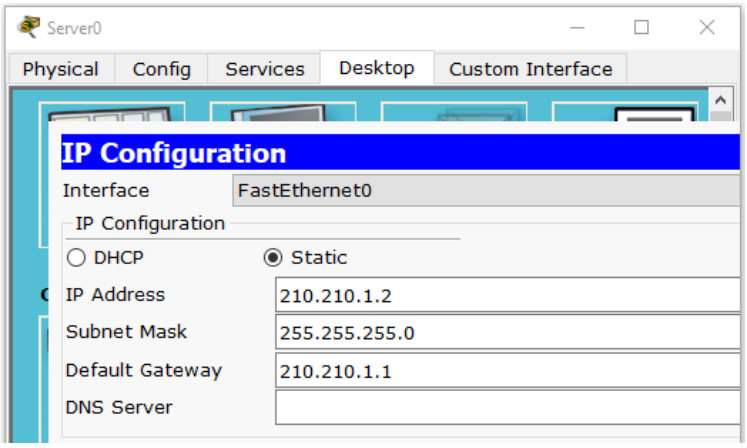

Рис. 5 Настройка Сервера

Пропишем маршрут по умолчанию для роутера во внутреннюю сеть и для ASA во внешнюю.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 192.168.1.0 255.255.255.0 210.210.0.2
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
Router#

ASA5505(config)#route outside 0.0.0.0 0.0.0.0 210.210.0.1
ASA5505(config)#end
ASA5505#
```

Организуем связь между компьютерами, для этого пропишем на маршрутизаторе маршрут в локальную сеть и организуем инспектирование трафика на межсетевом экране, а также инспектирование HTTP-трафика.

```
ASA5505(config)#class-map inspection-default
ASA5505(config-cmap)#match default-inspection-traffic
ASA5505(config-cmap)#exit
ASA5505(config)#policy-map global-policy
ASA5505(config-pmap)#class inspection-default
ASA5505(config-pmap-c)#inspect icmp
ASA5505(config-pmap-c)#exit
ASA5505(config)#service-policy global-policy global
ASA5505(config)#policy-map global-policy
ASA5505(config-pmap)#class inspection-default
ASA5505(config-pmap-c)#inspect http
ASA5505(config-pmap-c)#end
ASA5505#
```

Настроим автоматический NAT на устройстве ASA.

```
ASA5505#conf t
ASA5505(config)#object network FOR-NAT
ASA5505(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA5505(config-network-object)#nat (inside, outside) dynamic interface
ASA5505(config-network-object)#end
ASA5505#wr mem
Building configuration...
Cryptochecksum: 403f0a04 76cb0747 69e071e7 03a939cc

1231  bytes copied in 2.263 secs (543 bytes/sec)
[OK]
ASA5505#
```

Проверим видимость устройств во внутренней сети.

```
PC>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=2ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Рис. 6 Ping PC1 с PC0

```
PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=0ms TTL=127
Reply from 192.168.1.5: bytes=32 time=0ms TTL=127
Reply from 192.168.1.5: bytes=32 time=4ms TTL=127
Reply from 192.168.1.5: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

Рис. 7 Ping PC0 с PC1

Контрольные вопросы

1. Для чего предназначен packet filtering?

2. Для чего предназначен proxy-firewall?

3. Для чего предназначен stateful packet filtering?

4. С помощью, какой команды можно присвоить интерфейсу устройства защиты IP адрес?