

## Практическая работа №9

**Тема:** исследование основных функций межсетевого экрана CISCOASA 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.

**Используемые средства и оборудование:** IBM/PC совместимый компьютер с пакетом Cisco Packet Tracer; лабораторный стенд Cisco.

этапы выполнения работы.

### Практическая часть:

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

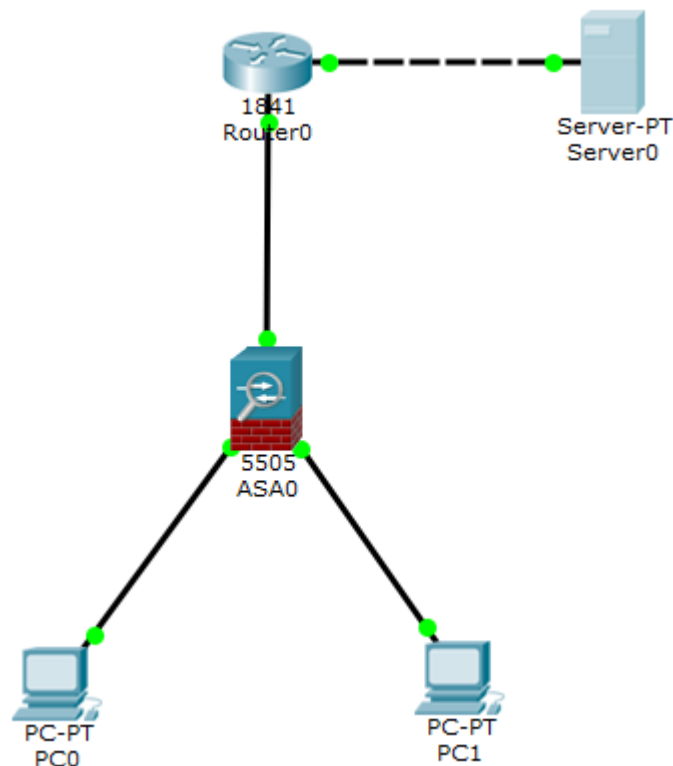


Рисунок 1 – Исходная сеть

					<i>ИКСиС.09.03.02.070000.ПР</i>					
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дат</i>	Практическая работа №4 «начальная конфигурация маршрутизатора CISCO.»			<i>Лит.</i>	<i>Лист</i>	<i>Листов</i>
<i>Разраб.</i>	<i>Клейменкин Д.</i>									
<i>Провер.</i>	<i>Береза А.Н.</i>								2	
<i>Реценз</i>								<i>ИСОиП (филиал) ДГТУ в г.Шахты ИСТ-Тб21</i>		
<i>Н. Контр.</i>										
<i>Утверд.</i>										

Войдём в управляющую программу сетевого экрана через HyperTerminal и затем в режим конфигурации, по умолчанию пароль пустой поэтому просто нажимаем enter.

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

Что предустановлено на 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
!
<--- More --->
```

CISCOASA 5505 раздает IP-адреса подключенным компьютерам

IP Configuration	
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IP Address	192.168.1.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	

IP Configuration	
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IP Address	192.168.1.6
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	

Рисунок 2 – IP-адреса компьютеров

Для того, чтобы выписать индивидуальное имя устройства перейдем в режим конфигурации и зададим имя и настроим параметры безопасности:

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

configure mode commands/options:
  encrypted Indicates the <password> entered is encrypted
  <cr>
ciscoasa(config)#username admin password cisco |
```

Пароль на enable и на пользователе сразу зашифрован

```
hostname ciscoasa
enable password 4IncP7vTjpaba2aF encrypted

username admin password 4IncP7vTjpaba2aF encrypted
```

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

```
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

ciscoasa(config)#
```

Рисунок 3 – Команда show ip address

Настроим параметры безопасности на Cisco ASA5505.

```
ASA5505(config)#enable password cisco
ASA5505(config)#username admin password cisco
```

С помощью команды show run проверим измененные параметры:

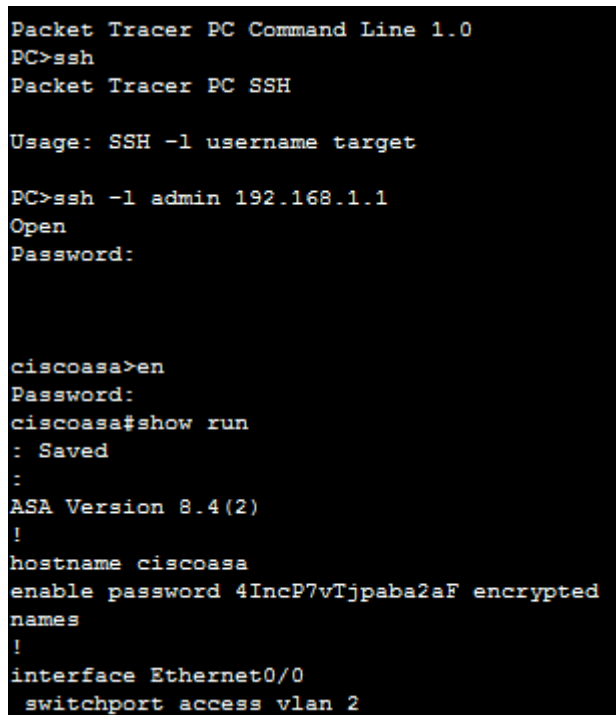
```
ASA Version 8.4(2)
!
hostname ASA5505
enable password 4IncP7vTjpaba2aF encrypted
names
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
  nameif inside
```

Рисунок 4 – Параметры безопасности

Для повышения безопасности устройства настроим протокол удаленного доступа SSH для этого указываем сеть, из которой будет возможен доступ (внутренняя сеть) и интерфейс, с которого будет осуществляться доступ:

```
ciscoasa(config)#ssh ?

configure mode commands/options:
  WORD                               The IP address of the host and/or network authorized to
                                   login to the system
  X:X:X:X::X/<0-128>                 IPv6 address/prefix authorized to login to the system
  timeout                            Configure ssh idle timeout
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)#aaa authentication ssh console Local
```



```
Packet Tracer PC Command Line 1.0
PC>ssh
Packet Tracer PC SSH

Usage: SSH -l username target

PC>ssh -l admin 192.168.1.1
Open
Password:

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

Рисунок 5 – Получение удаленного доступа к по протоколу SSH

Изменим Security-level и до настроим внешний интерфейс выполним следующие команды:

```
ciscoasa(config)#int vlan
% Incomplete command.
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#security-level 95
ciscoasa(config-if)#end
ciscoasa#int vlan 2
^
% Invalid input detected at '^' marker.

ciscoasa#conf t
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip add 210.210.0.2 255.255.255.252
ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#exit
ciscoasa(config)#
```

## 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 210.210.0.0 255.255.255.252
Bad mask /30 for address 210.210.0.0
Router(config-if)#ip address 210.210.0.1 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

Router(config-if)#
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up

Router(config-if)#ip address 210.210.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#wr mem
^
% Invalid input detected at '^' marker.

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

## Перейдем к настройке Сервера

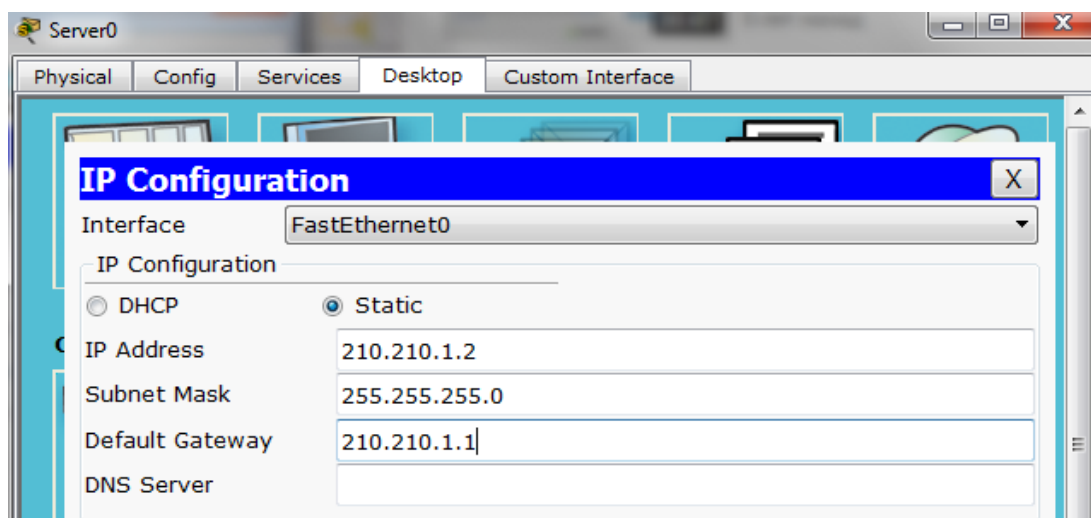


Рисунок 6 – настройка Сервера

Изм.	Лист	№ докум.	Подпись	Дата

ИКСиС.09.03.02.070000.ИП

Лист

6

Пропишем маршрут по умолчанию

```
ciscoasa(config)#route ?

configure mode commands/options:
  inside      Name of interface Vlan1
  outside     Name of interface Vlan2
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 210.210.0.1
ciscoasa(config)#end
```

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

```
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]

ciscoasa#class-map inspection_default
^
% Invalid input detected at '^' marker.

ciscoasa#conf t
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
^
% Invalid input detected at '^' marker.

ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
^
% Invalid input detected at '^' marker.

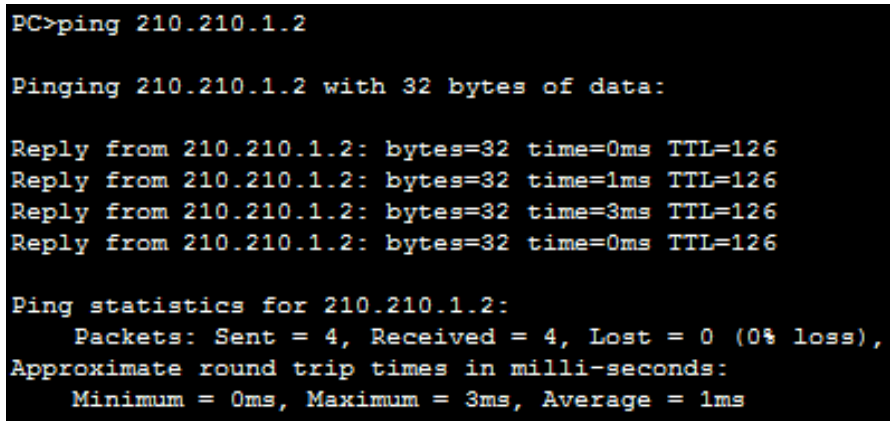
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#service-policy global_policy global
ciscoasa(config)#
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect http
ciscoasa(config-pmap-c)#end
ciscoasa#
```

## Создадим Object network FOR-NAT

```
ciscoasa(config)#object network FOR-NAT
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
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 6be57482 051d0cbb 22d16148 18cd73f0

1232 bytes copied in 2.314 secs (532 bytes/sec)
[OK]
ciscoasa#
```

## Проверим пинг



```
PC>ping 210.210.1.2

Pinging 210.210.1.2 with 32 bytes of data:

Reply from 210.210.1.2: bytes=32 time=0ms TTL=126
Reply from 210.210.1.2: bytes=32 time=1ms TTL=126
Reply from 210.210.1.2: bytes=32 time=3ms TTL=126
Reply from 210.210.1.2: bytes=32 time=0ms TTL=126

Ping statistics for 210.210.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Рисунок 7 – пинг на PC0

## Контрольные вопросы

1. Для чего предназначен packet filtering?
2. Для чего предназначен проху-firewall?
3. Для чего предназначен stateful packet filtering?
4. С помощью, какой команды можно присвоить интерфейсу устройства защиты IP адрес?