**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

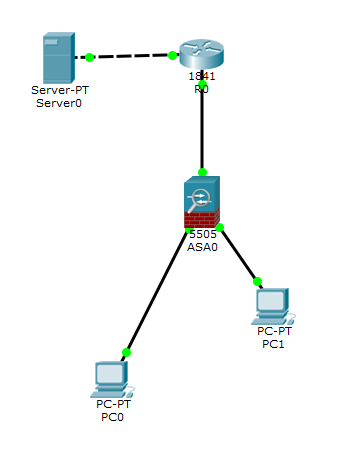
оборудования Cisco ASA 5505, а так же освоить принципы

конфигурирования оборудования Cisco ASA 5505.

Ход работы:

Для выполнения практической работы необходимо промоделировать

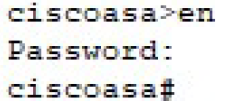
сеть.



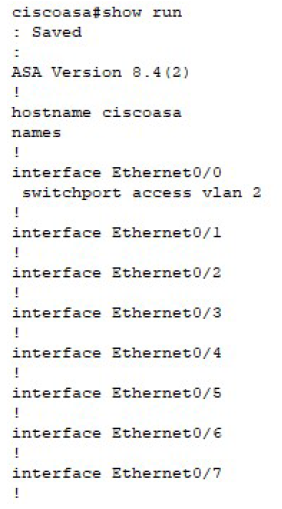
Для входа в управляющую программу сетевого экрана используем

HyperTerminal, вводим команду en для входа в привилегированный режим,

по умолчанию пароль пустой, поэтому просто нажимаем Enter.

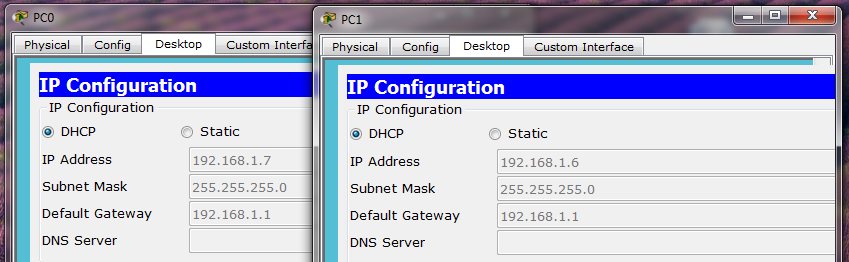


Исходная конфигурация CISCOASA 5505.



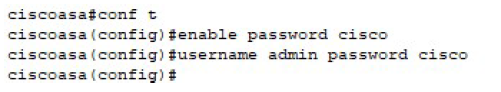
По умолчанию на CISCOASA 5505 работает DHCP-сервер, поэтому

подключенные к нему компьютеры автоматически получают IP-адреса.

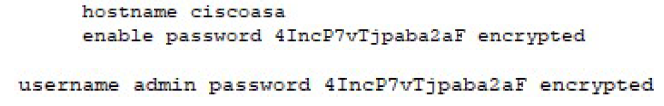


Для обеспечения безопасного входа на устройство зададим пароль для

входа в привилегированный режим и пользовательское имя и пароль.

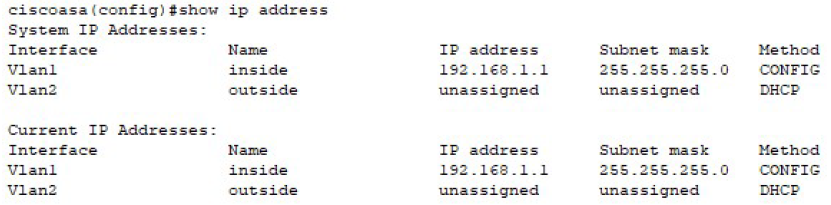


Пароли для enable и пользователя сразу зашифрованы.



С помощью команды show ip address узнаем параметры VLAN (должно

быть настроено две VLAN: внутренняя и внешняя сети)

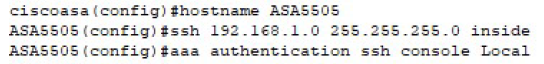


Установим имя устройства, для повышения безопасности устройства

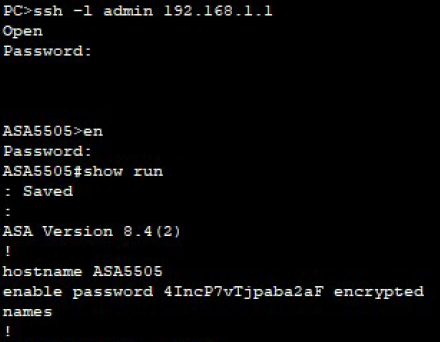
настроем протокол удаленного доступа SSH для этого указываем сеть, из

которой будет возможен доступ (внутренняя сеть) и интерфейс, с которого

будет осуществляться доступ



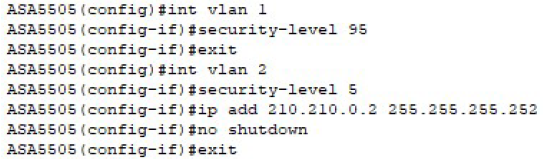
Проверим удаленный доступ к CISCO ASA.



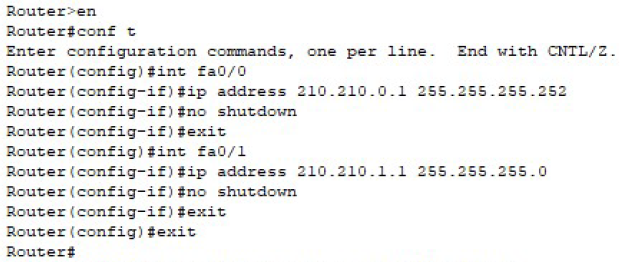
Получение удаленного доступа к ASA по протоколу SSH

Изменим Security-level и присвоим адрес внешнему интерфейсу, для

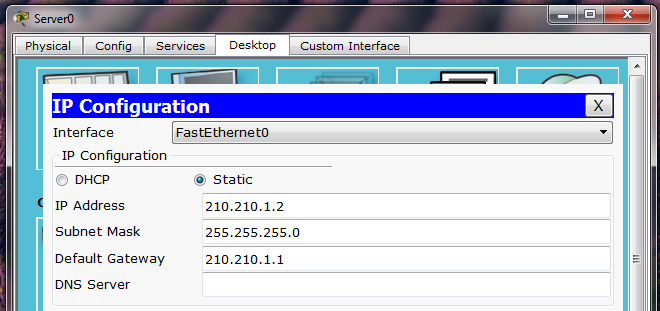
этого выполним следующие команды:



Перейдем к настройке маршрутизатора.



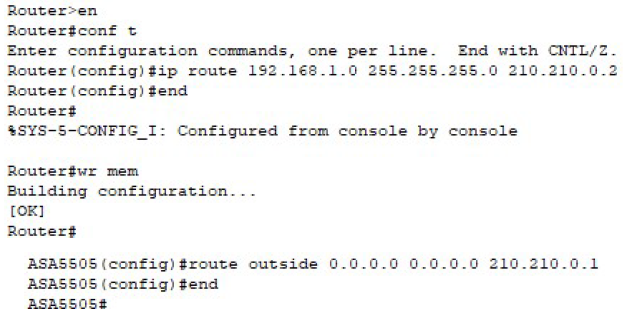
Перейдем к настройке Сервера.



Настройка Сервера

Пропишем маршрут по умолчанию для роутера во внутреннюю сеть и

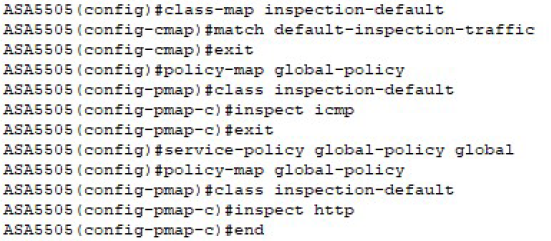
для ASA во внешнюю.



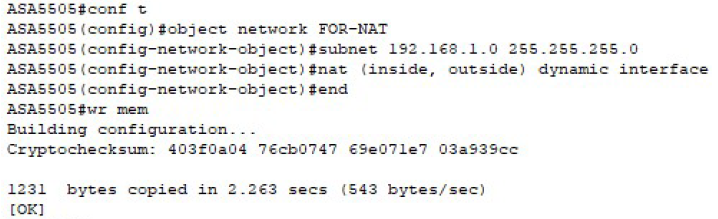
Организуем связь между компьютерами, для этого пропишем на

маршрутизаторе маршрут в локальную сеть и организуем инспектирование

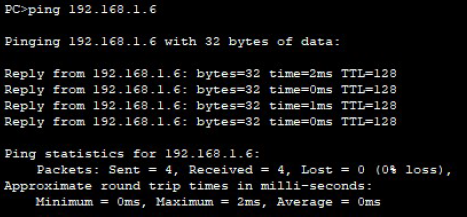
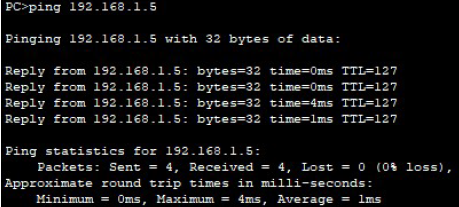
трафика на межсетевом экране, а также инспектирование HTTP-трафика.



Настроим автоматический NAT на устройстве ASA.



Проверим видимость устройств во внутренней сети.



**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?