МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

DMZ Design

Отчет по лабораторной работе № 9

по дисциплине «Компьютерные сети»

студента 2 курса группы ПИ-б-о-231(2)  
Аметов Кемран Ленверович

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2024

Ch6: PT Activity 5 – DMZ Design

**Objective**

·         Design and configure a DMZ for the MedGroupNet network.

**Background and Preparation**

The MedGroupNet organization needs to allow the general public to access its two public servers, a DNS server, and a web server with the FQDN www.medgroupnet.com. For security reasons, these two servers are located in a DMZ, which is separate from the internal MedGroupNet network.

The following security policies are to be implemented on the HQ router to protect the MedGroupNet network:

1.     Only HTTP and DNS traffic is allowed from the Internet to the DMZ.

2.     Traffic from the Internet cannot enter the internal MedGroupNet network unless it is in response to traffic initiated by the internal network.

In this lab, you will implement these security policies for the MedGroupNet DMZ.  The NAT function for the internal MedGroupNet network has been configured on the HQ router.  Your tasks include the following:

1.     Configure the IP setting for the servers in the DMZ.

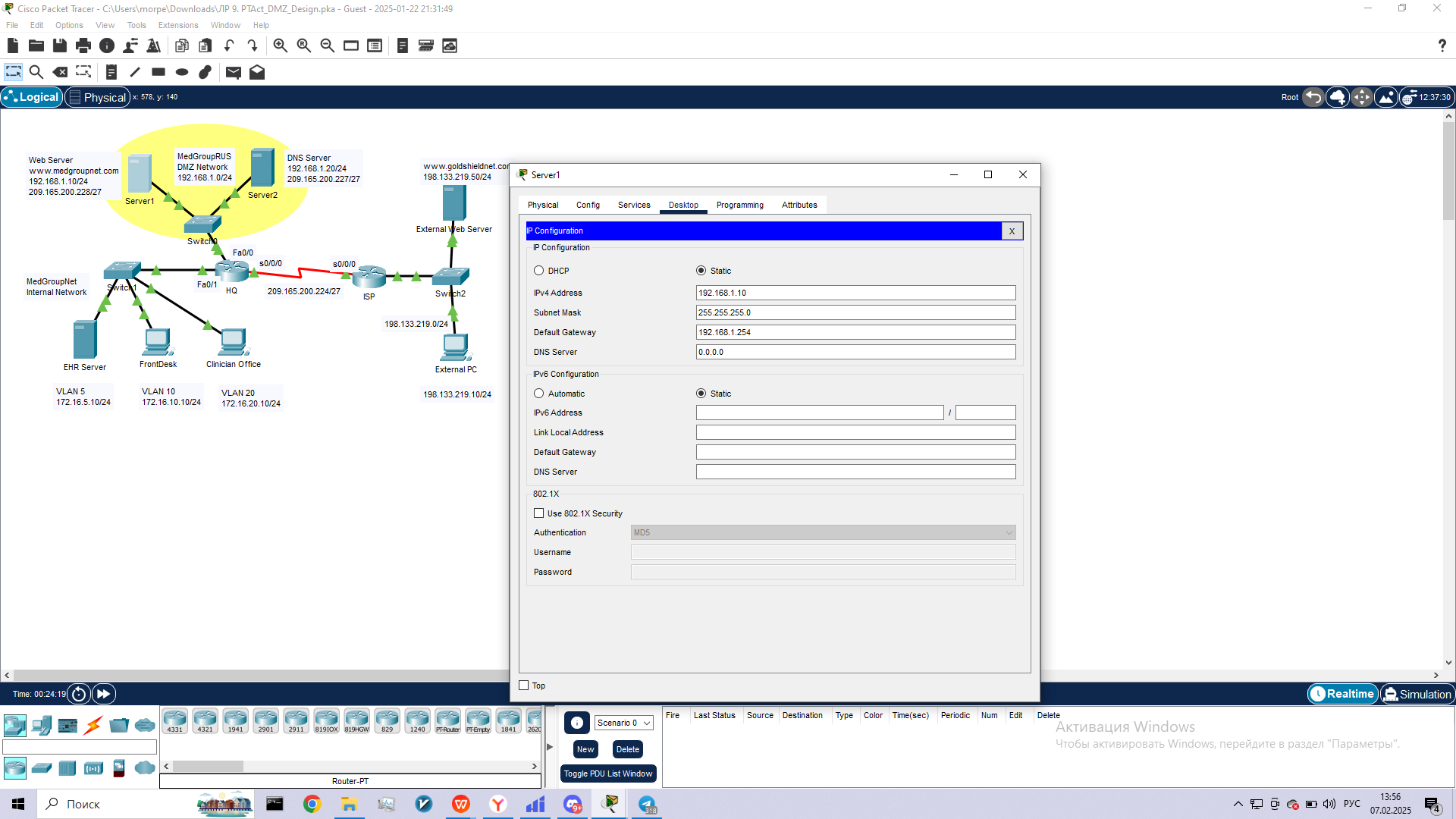
2.     Configure static NAT.

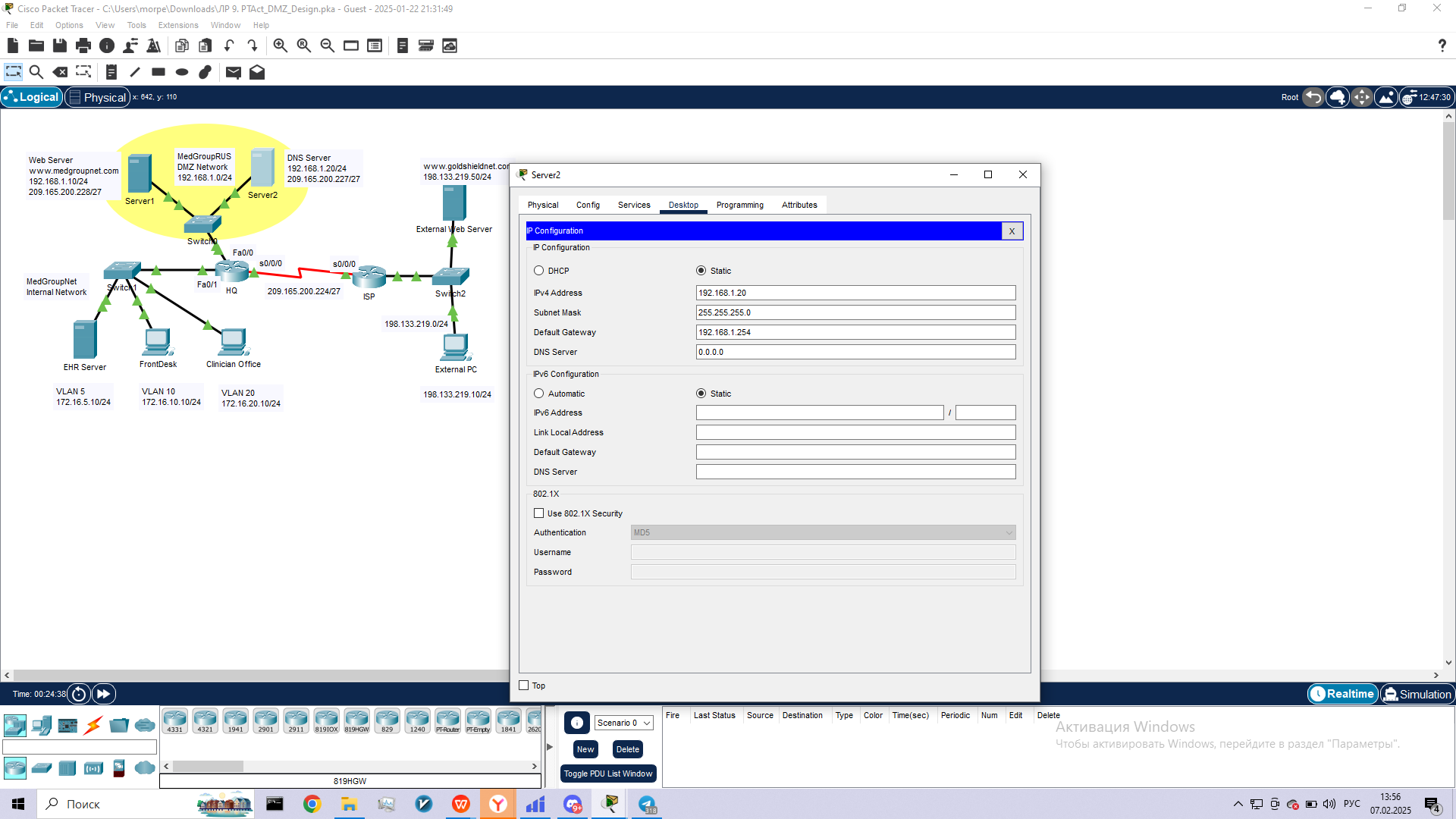
3.     Configure the DNS server in the DMZ for name resolution.

4.     Configure an ACL to implement the two security policies above.

**Step 1: Configure the IP addresses for the servers in the DMZ.**

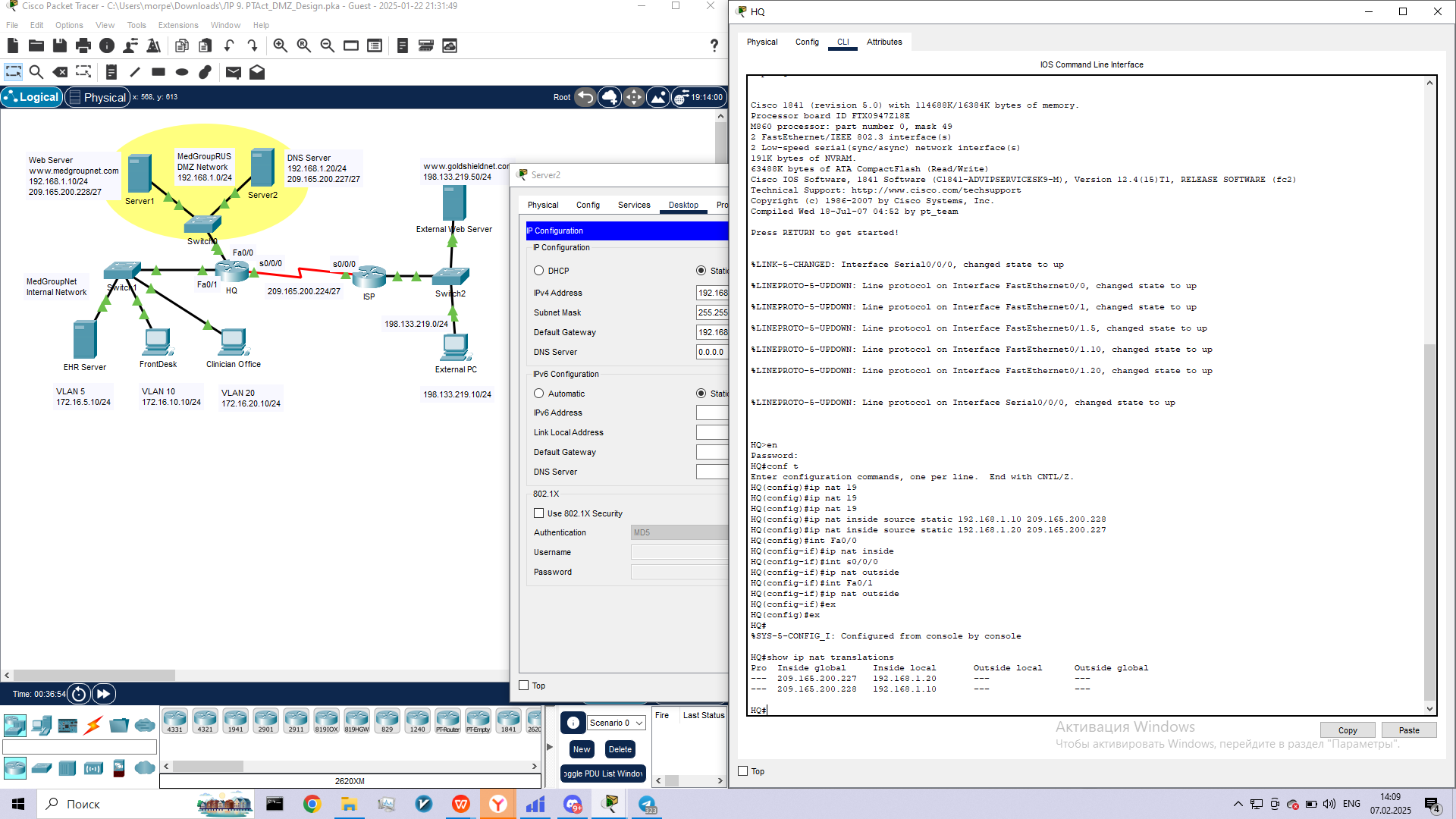
a.     Configure the IP address settings for the web server and DNS server in the DMZ.  What settings should be used for the IP address, subnet mask, and default gateway?

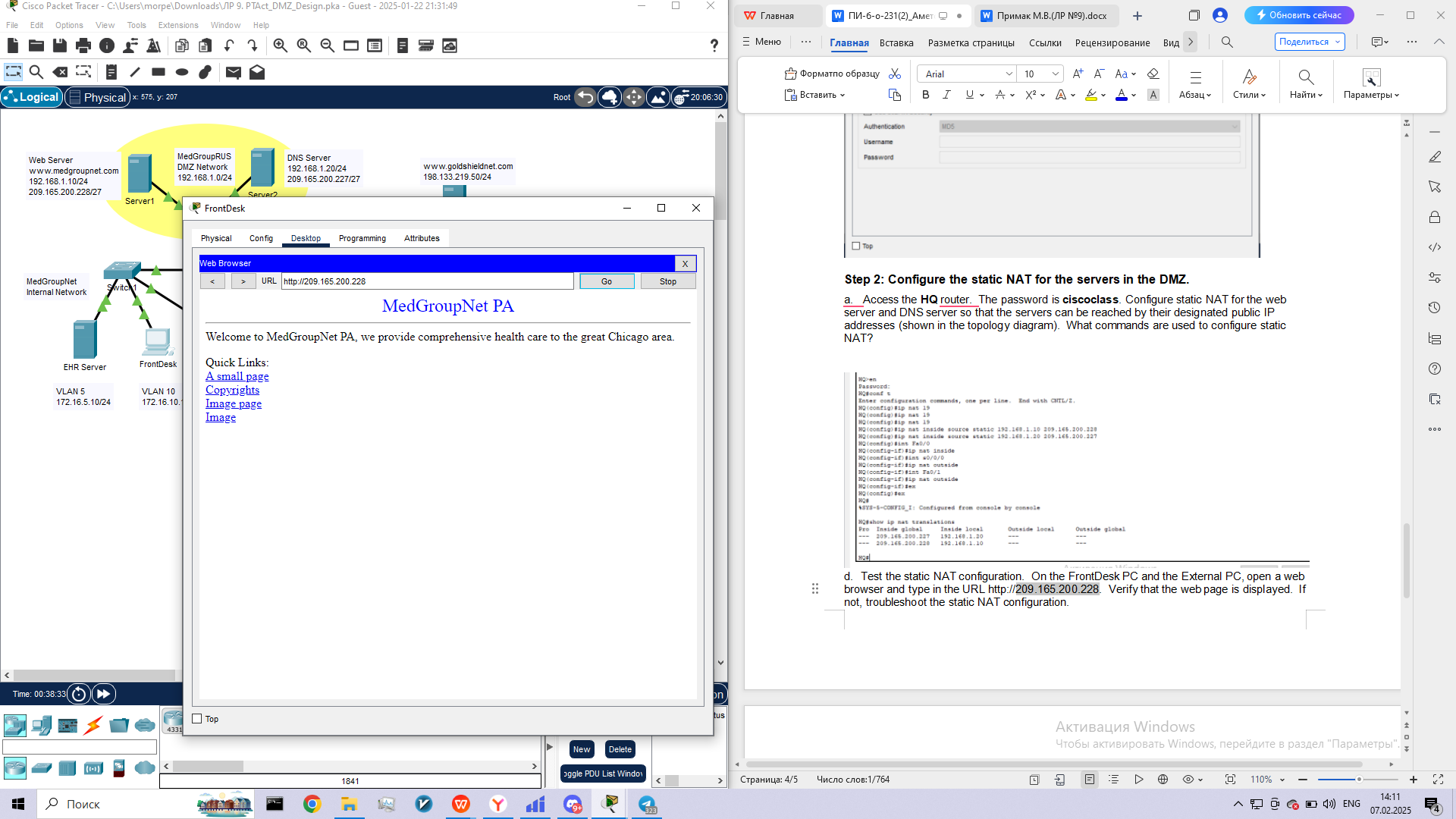


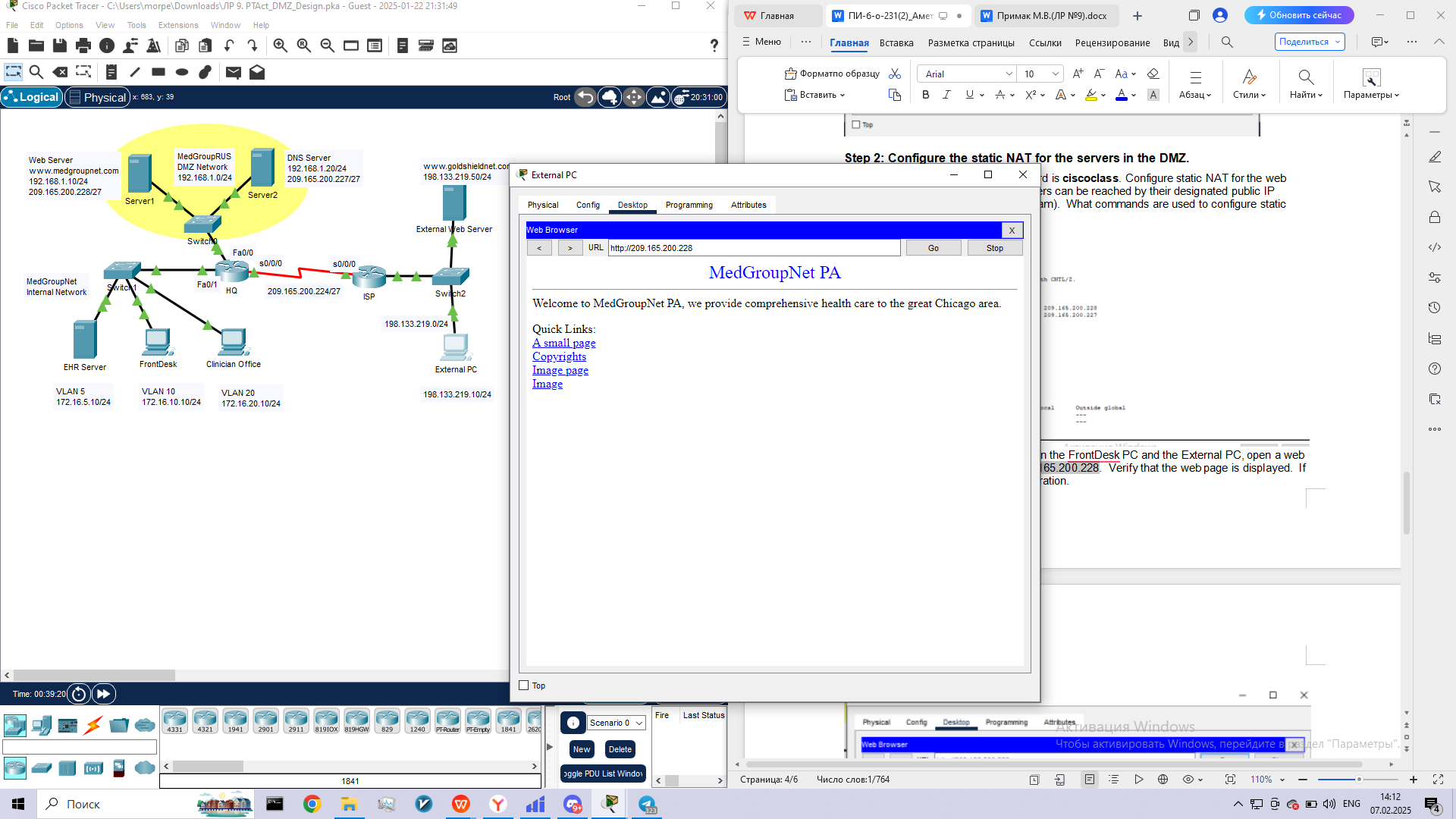


**Step 2: Configure the static NAT for the servers in the DMZ.**

a.     Access the **HQ**router.  The password is **ciscoclass**. Configure static NAT for the web server and DNS server so that the servers can be reached by their designated public IP addresses (shown in the topology diagram).  What commands are used to configure static NAT?

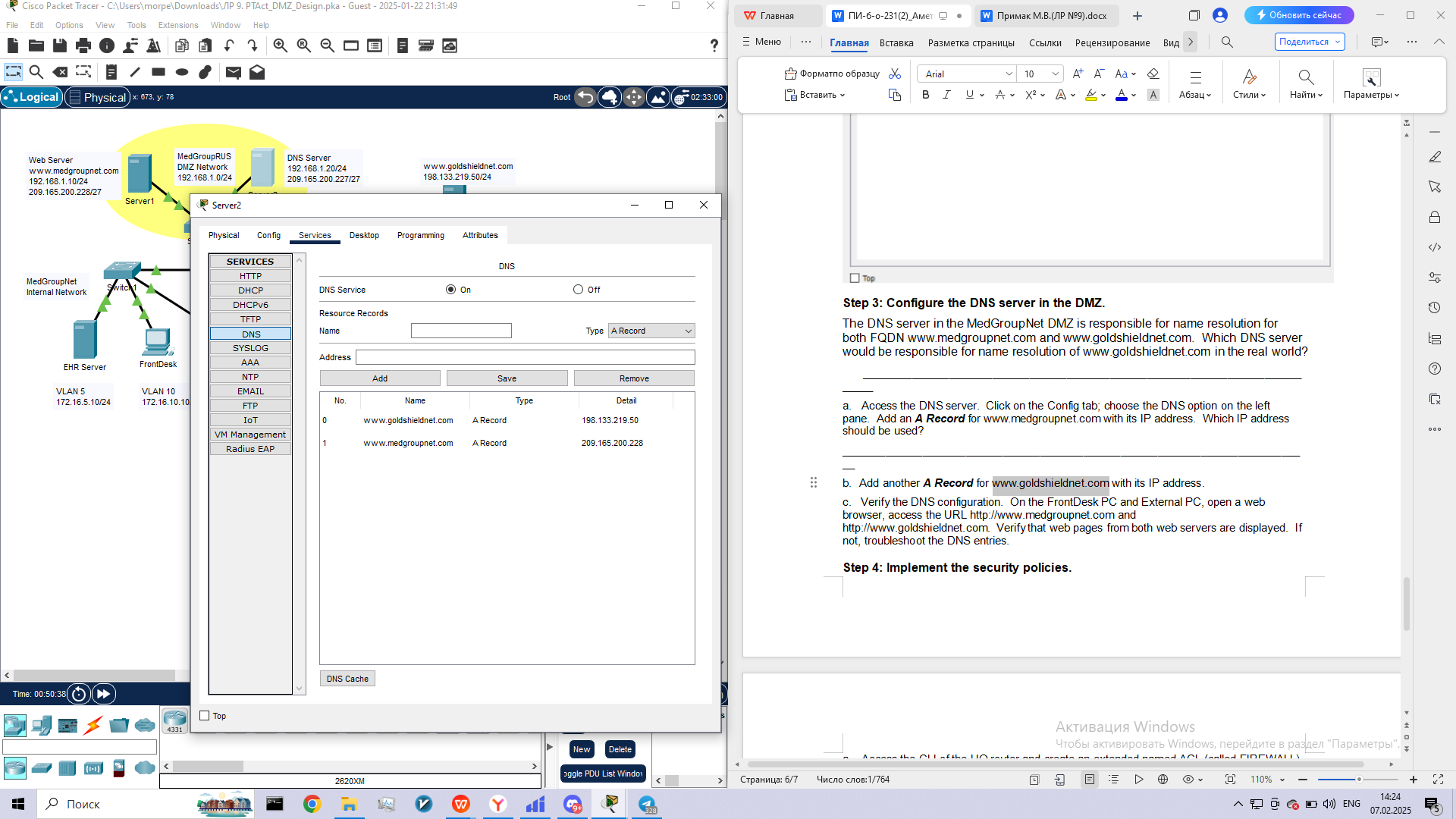
d.    Test the static NAT configuration.  On the FrontDesk PC and the External PC, open a web browser and type in the URL http://209.165.200.228.  Verify that the web page is displayed.  If not, troubleshoot the static NAT configuration.

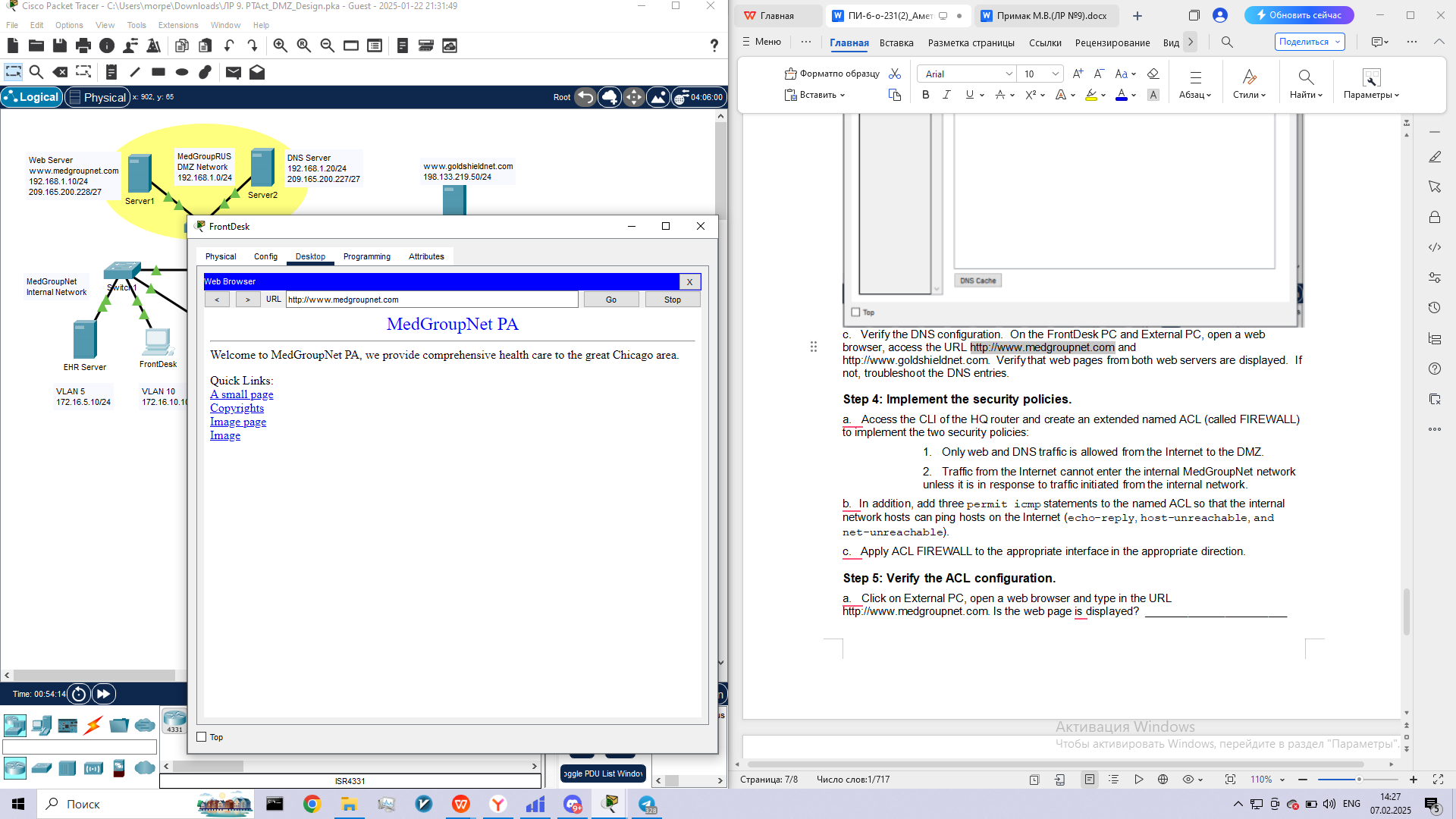


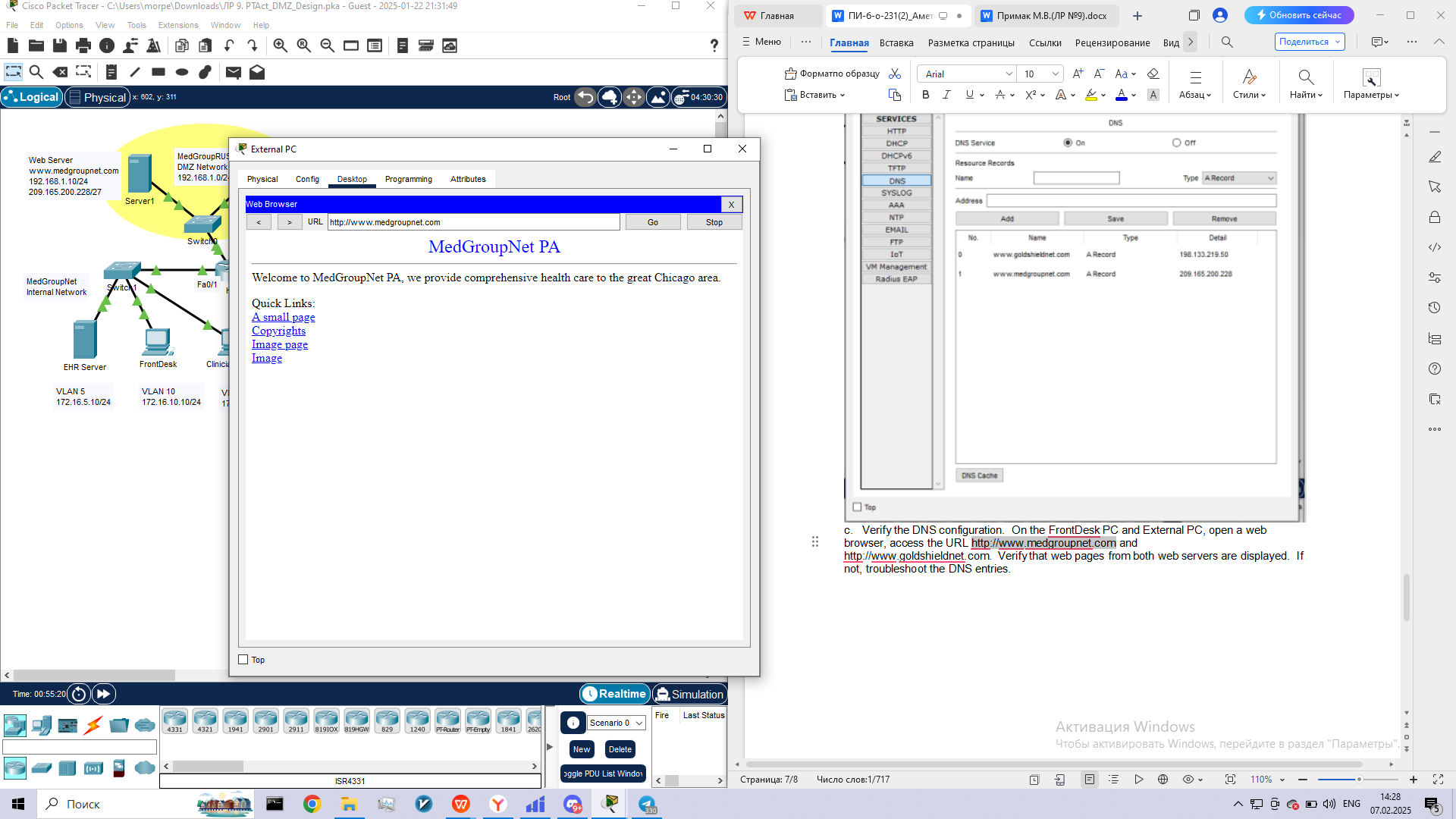


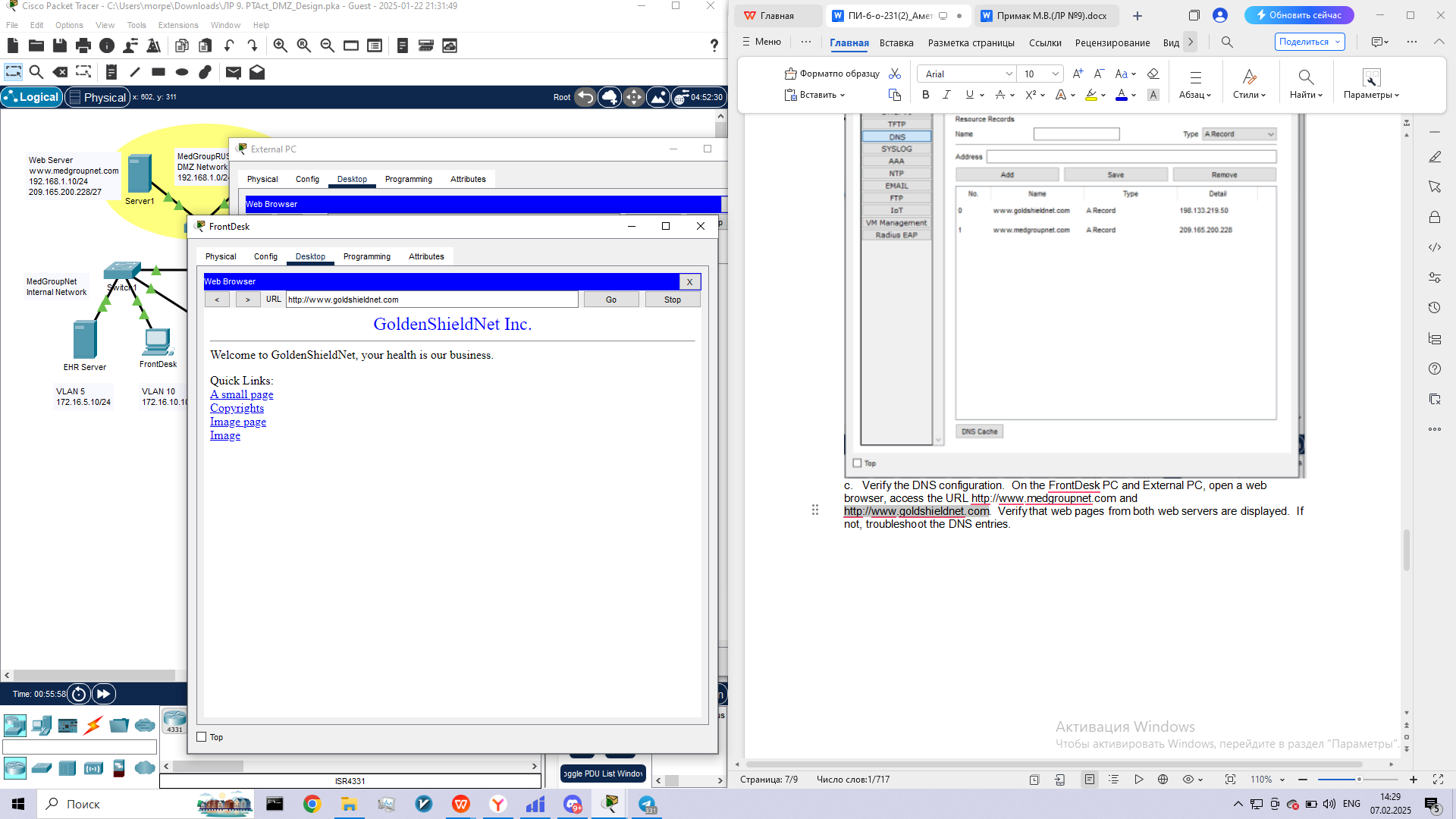
**Step 3: Configure the DNS server in the DMZ.**

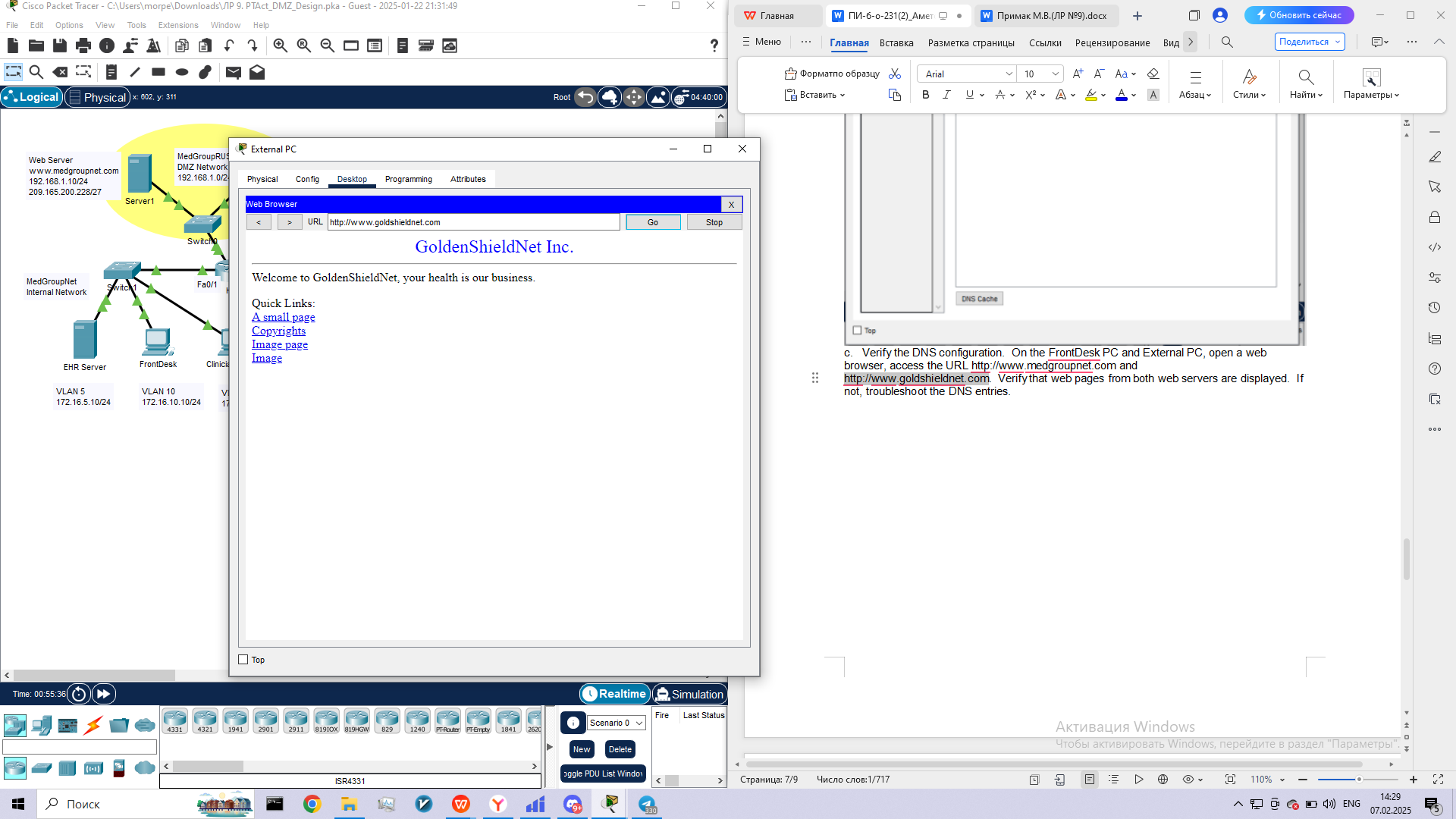
The DNS server in the MedGroupNet DMZ is responsible for name resolution for both FQDN www.medgroupnet.com and www.goldshieldnet.com.  Which DNS server would be responsible for name resolution of www.goldshieldnet.com in the real world?

c.     Verify the DNS configuration.  On the FrontDesk PC and External PC, open a web browser, access the URL http://www.medgroupnet.com and http://www.goldshieldnet.com.  Verify that web pages from both web servers are displayed.  If not, troubleshoot the DNS entries.









**Step 4: Implement the security policies.**

a.     Access the CLI of the HQ router and create an extended named ACL (called FIREWALL) to implement the two security policies:

1.     Only web and DNS traffic is allowed from the Internet to the DMZ.

2.     Traffic from the Internet cannot enter the internal MedGroupNet network unless it is in response to traffic initiated from the internal network.

b.    In addition, add three permit icmp statements to the named ACL so that the internal network hosts can ping hosts on the Internet (echo-reply, host-unreachable, and net-unreachable).

c.     Apply ACL FIREWALL to the appropriate interface in the appropriate direction.

**Step 5: Verify the ACL configuration.**

a.     Click on External PC, open a web browser and type in the URL http://www.medgroupnet.com. Is the web page is displayed?  ­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b.    From External PC, ping either the web server or DNS server in the MedGroupNet DMZ.  Was the ping successful?

c.     Click on the FrontDesk PC, and ping External PC with its IP address. Was the ping successful? \_\_\_\_\_\_\_\_\_\_\_

d.    From the FrontDesk or Clinician Office PC, ping the GoldShieldNetweb server with its FQDN.  Was the ping successful? \_\_\_\_\_\_\_\_\_\_

e.     On the FrontDesk or Clinician OfficePC, open a web browser and type in the URLs http://www.medgroupnet.comand http://www.goldshieldnet.com.  Are the web pages from both web servers displayed? \_\_\_\_\_\_\_

f.     Click the HQ router and issue the **show ip nat translations** command. What is displayed?

**Reflection**

What can be done to further protect the DMZ from attacks from the internal network?