Lab 5 - Configure Static NAT and Dynamic NAT

Objectives

Part 1: Test Access without NAT

Part 2: Configure Static NAT

Part 3: Test Access with NAT

Part 4: Configure Dynamic NAT

Part 5: Verify NAT Implementation

Scenario

In IPv4 configured networks, clients and servers use private addressing. Before packets with private addressing can cross the internet, they need to be translated to public addressing. Servers that are accessed from outside the organisation are usually assigned both a public and a private static IP address. In this activity, you will configure static NAT so that outside devices can access an inside server at its public address. You will then configure dynamic NAT to create a pool of public addresses to be shared amongst multiple private hosts.

Instructions

Part 1: Test Access without Static NAT

Step 1: Attempt to connect to Server1 using Simulation Mode.

a. Switch to Simulation mode.

b. From **PC1**, attempt to ping **Server1** at 172.16.16.1. Continue to click the **Capture Forward** button.

QUESTION 1 What happens to the ICMP packets?

Before proceeding, go to the "Lab 5 - Configure Static NAT and Dynamic NAT - QUESTIONS" quiz on the Moodle page and enter your answer for question 1. Leave the quiz open while you complete the rest of the lab sheet.

c. Exit **Simulation** mode.

d. From **PC1**, ping the **R1** S0/0/0 interface (210.165.201.2). The ping should succeed.

Step 2: View R1 routing table and running-config.

a. View the running configuration of **R1**. Note that there are no commands referring to NAT. An easy way to confirm this is to issue the following command:

```
R1# show run | include nat
```

b. Verify that the routing table does not contain entries referring to the IP network addresses for **PC1** and **L1**.

QUESTION 2 What command did you use to view the routing table?

Before proceeding, return to the quiz on the Moodle page and enter your answer for question 2. Leave the quiz open while you complete the rest of the lab sheet.

    c.   Verify that NAT is not being used by **R1**.

```
R1# show ip nat translations
```

Part 2: Configure Static NAT

Step 1: Configure static NAT statements.

Refer to the Topology. Create a static NAT translation to map the **Server1** inside address to its outside address.

```
R1(config)# ip nat inside source static 172.16.16.1 64.100.50.1
```

Step 2: Configure NAT interfaces.

    a.   Configure the **G0/0** interface as an inside NAT interface.

```
R1(config)# interface g0/0
R1(config-if)# ip nat inside
```

    b.   Configure the **S0/0/0** public interface as an outside interface.

Part 3: Test Access with Static NAT

Step 1: Verify connectivity to the Server1 web page.

    a.   Open the command prompt on **PC1** or **L1**, attempt to ping the public address for **Server1**.

    b.   Verify that both **PC1** and **L1** can now access the **Server1** web page.

QUESTION 3 Which, if any, of the connection attempts to Server1 were successful?

Before proceeding, return to the quiz on the Moodle page and enter your answer for question 3. Leave the quiz open while you complete the rest of the lab sheet.

Step 2: View NAT translations.

Use the following commands to verify the static NAT configuration on **R1**:

```
show running-config
show ip nat translations
show ip nat statistics
```

Part 4: Configure Dynamic NAT

Step 1: Configure traffic that will be permitted.

On **R2**, configure one statement for ACL 20 to permit any address belonging to the 172.16.0.0/16 network.

Step 2: Configure a pool of address for NAT.

Configure **R2** with a NAT pool that uses two addresses in the 209.165.200.232/30 address space. (You may choose any name for the pool.)

Step 3: Associate ACL 20 with the NAT pool.

Enter the command that associates ACL 20 with the NAT pool that you just created.

Step 4: Configure the NAT interfaces.

Configure **R2** interfaces with the appropriate inside and outside NAT commands.

Notice in the topology there are 3 devices that would have their addresses translated based on the ACL created.

QUESTION 4 What will happen if more than 2 devices attempt to access the Internet at the same time?

Before proceeding, return to the quiz on the Moodle page and enter your answer for question 4. Leave the quiz open while you complete the rest of the lab sheet.

Part 5: Verify NAT Implementation

Step 1: Access services across the internet.

From the web browser of **LA**, **PCA**, or **PCB**, access the web page for **Server2**.

Step 2: View NAT translations.

View the NAT translations on **R2**. Identify the internal source address of the PC and the translated address from the NAT pool in the command output.

```
R2# show ip nat translations
```

If you have correctly configured all parts of the lab your activity score should now be showing as 100%. If so, click on "check results" in the activity window. Return to the Moodle quiz one last time and enter the code into the appropriate question box (Q5) of the quiz.

You have completed the lab – please submit the Moodle quiz.