LAB-1- NETWORK ADSRESS TRANSLATION

JAY VASANI

8885487

INFO-2280

HAUSAM SAMARA

JUNE 12, 2024

# Table of Contents

[Table of Contents 2](#_Toc48746339)

[Lab 1 – Network address translation 3](#_Toc48746340)

[Part 1- configure base firewall parameters 3](#_Toc48746341)

[Description 3](#_Toc48746342)

[Preparation 3](#_Toc48746343)

[Observations 3](#_Toc48746344)

[Screenshots 3](#_Toc48746345)

[Reflection 4](#_Toc48746346)

[Part 2- configuring the firewall policies 3](#_Toc48746341)

[Description 3](#_Toc48746342)

[Preparation 3](#_Toc48746343)

[Observations 3](#_Toc48746344)

[Screenshots 3](#_Toc48746345)

[Reflection 4](#_Toc48746346)

[Part 1- configuring the NAT policies 3](#_Toc48746341)

[Description 3](#_Toc48746342)

[Preparation 3](#_Toc48746343)

[Observations 3](#_Toc48746344)

[Screenshots 3](#_Toc48746345)

[Reflection 4](#_Toc48746346)

[References 4](#_Toc48746347)

# Lab 1 – NETWORK ADDRESS TRANSLATION

**Part 1- configure base firewall parameters.**

**DESCRIPTION:**

This part of the lab is all about the basic configuration needed for the future polices which will include the zone creation. Firewall configuration as well as the router configuration. This is the part it is required to set up the IP addresses as per the schematics. Where I will also show the IP routing and the static route set in both firewall and router. There are screenshots which will provide evidence to all this configuration done in the firewall and router.

**PREPARATION:**

For this part of lab, I connected all the devices as per the schematics. And I reloaded all the equipment’s. For the router I took 2811 router. For the switches I used 2 switches where VM-1 is connected to the 2960m switch and VM-2& VM-3 are connected to 3750 switches. For the VM-4 I connected it to the router interface. I securely logged in to the PALOALTO firewall for this activity.

**OBSERVATION:**

* Firstly, I opened the router and gave Ip address to the router interfaces as per schematics.
* Where I gave Ip address 172.17.54.1/24 to the interface 0/0 and Ip address of 172.17.54.17/24 to the interface 0/1
* After that I have set the IP route on the router where I chose 172.17.54.2 as the next hope because this is the interface connected with my firewall.
* After that I opened the PALO-ALTO firewall where I gave IP addresses to all the firewall interfaces which are as under

E1/1- 172.17.54.2

E1/2- 172.16.54.1

E1/3- 172.18.54.1

* After that I have created the virtual router where I chose all the interfaces for that
* I also edited the static route where I chose 0.0.0.0/0 as the destination and the 172.17.54.1/28 as my next hope which relates to the router interface
* I also made 2 management profiles where first one is named as jvasani5487-allow-mgmt having services like HTTP, HTTPS, SSH and ping. Second management profile named jvasani5487-allow-ping only have service of ping in it.
* After this step I have created 3 zones and connected to the designated interfaces as under

INTERNET- E1/1

INTERNAL- E1/2

DMZ-E1/3

* After that I have assigned this management profiles to the interfaces.
* By creating the different zones, we can have different policies in each of that which will provide more security and control the traffic flow with efficiency. By default, there are no packets allowed o to translate between zones and there is no communication between these zones. It also ensures that only the authorized traffic can move from one zone to different zone.

**SCREENSHOTS:**

Ip address assigned to the router interfaces as per the schematicsA screenshot of a computer screen

Description automatically generated

IP route has been set and the route is indicating the IP address of the firewall interface.

A computer screen shot of a black screen

Description automatically generated

Firewall interfaces with the IP addresses assigned.A screenshot of a computer

Description automatically generated

Default route has been edited and I selected all the firewall interfaces. A screenshot of a computer

Description automatically generated

Static route has been created and the next hope is the firewall interface connected with the router.A screenshot of a computer

Description automatically generated

There are zones created named INTERNET, INTERNAL and DMZ A screenshot of a computer

Description automatically generated

This screenshot shows the management profile created and there are HTTP, HTTPS, SSH and ping services allowed in this activityA screenshot of a computer

Description automatically generatedhere is the screenshot showing all the interfaces of firewall are having the management profilesA screenshot of a computer

Description automatically generated

**REFLECTION:**

This part of the lab was mainly about the basic configuration, and it gives knowledge about the zones and management policies of the firewall. This part briefly explains the use of creating zones into the network. Basically, it was easy, and it also gives information about the next hope and static route. There are all screenshots attached for all the steps into the observation part.

**Part 2- configuring the firewall policies.**

**DESCRIPTION:**

This part is about setting up the firewall policies which will basically control the packet flow between different zones. It is all about the ICMP packets and its connectivity to the different zones. In this part of the lab management profiles are also important to create. Which will basically allow SSH and web-based management. There are 3 security policies required in this part which are as under

* Internal to DMZ
* Internal to internet
* Internet to DMZ

**PREPARATION:**

For this part of lab, I connected all the devices as per the schematics. And I reloaded all the equipment’s. For the router I took 2811 router. For the switches I used 2 switches where VM-1 is connected to the 2960m switch and VM-2& VM-3 are connected to 3750 switches. For the VM-4 I connected it to the router interface. I securely logged in to the PALOALTO firewall for this activity.

**OBSERVATION:**

* In this part I created 2 management profile 1 is allowing all SSH and web-based management. Which is named jvasani5487-allow-mgmt
* For the second profile I chose ICMP packet transfer service which will basically allow ping to the other devices. Which is named jvasani5487-allow-ping
* After that I have assigned this management profiles to the designated interfaces of the firewall.
* After this I have created 3 security policies for the packet transportation between different zones.
* First policy is internal to DMZ which will simply allow packet flow from internal zone to DMZ zone where packets can go from VM-1 to VM2&3.
* Second policy is internal to internet which will simply allow packet flow from internal zone to internet zone where packets can go from VM-1 to VM-4.
* Third policy is internet to DMZ which will simply allow packet flow from internet zone to DMZ zone where packets can go from VM-4 to VM2&3.
* After that I saved all this configuration and assigned the IP addresses to all this VMs which are as under

VM-1 = 172.16.54.10

VM-2 = 172.18.54.20

VM-3 = 172.18.54.30

VM-4 = 172.17.54.18

* To confirm the policies are working or not I started pinging the VMs in different zones and collected the successful screenshots
* This are the ping I have achieved.

1. VM-1 TO VM-2&3
2. VM-1 TO VM-4
3. VM-4 TO VM-2&3

**SCREENSHOTS:**

This screenshot shows the management profile created and there are HTTP, HTTPS, SSH and ping services allowed in this activityA screenshot of a computer

Description automatically generatedhere is the screenshot showing all the interfaces of firewall are having the management profilesA screenshot of a computer

Description automatically generated

Security policies are created in this part

A screenshot of a computer

Description automatically generated

This screenshot shows the succesfull ping from VM1 to VM4 which will prove that internal to internet policy is successful. A screen shot of a computer

Description automatically generated

this screenshot shows the suceesful ping to the internet zone where it send the traffic to all the interfaces of router.A screenshot of a computer

Description automatically generated

this screenshot shows the ping from VM-4 to VM-3 and VM-2 and it will prove that the policy internet to DMZ is working good.A screenshot of a computer program

Description automatically generated

this screenshot shows ping from VM-1 to VM-3 & VM-2 and it will show that the policy internal to DMZ is working well.A screenshot of a computer

Description automatically generated

**REFLECTION:**

This part was all about security policies where it was controlling the packet transfer between different zones. In this part I also got hands on practice to the firewall management profiles which basically control the packet type which we are sending. This policy ensures the data protection in larger organization and it also gave me hands on practice to the monitoring the packet transfer between different zones.

**Part 3- configuring the NAT policies.**

**DESCRIPTION:**

This part is about creating the NAT policies into the firewall which will not only control the packet flow but also control the packet type. (ICMP or TCP) there are 2 required NAT policies which is internal to internet and internet to DMZ. first policy is about getting the traffic on VM-4 before and after pinging it from VM-1, second policy is about getting tcp dump on VM-2 from VM-4 before and after the NAT translations.

**PREPARATION:**

For this part of lab, I connected all the devices as per the schematics. And I reloaded all the equipment’s. For the router I took 2811 router. For the switches I used 2 switches where VM-1 is connected to the 2960m switch and VM-2& VM-3 are connected to 3750 switches. For the VM-4 I connected it to the router interface. I securely logged in to the PALOALTO firewall for this activity.

**OBSERVATION:**

* First, I have collected ICMP dump on my VM-4 for the traffic coming for VM-1 and I collected the data coming from IP address of VM-1(172.16.54.10)
* After that I have created the NAT policy named internal to internet and assigned the firewall interface IP as the source translation.
* I committed the configuration and again sent traffic from VM-1 to VM-4 and took the screenshot of the ICMP dump.
* This time the traffic was not coming from the VM-1, but it was coming from the IP address of my firewall interface which was 172.17.54.2/28
* The second policy I created is internet to DMZ where I assigned the firewall interface for the source translation
* Before I commit, I collected TCP dump on VM-2 for the traffic sent from the VM-1 and I found that the traffic is coming from the IP address of my VM-4 (172.17.54.18)
* After that I committed the NAT translation and again repeated the same action.
* But this time the traffic came from the different IP which was my firewall interface (172.17.54.2)
* This 2 screenshot and traffic source translation shows the NAT policies I have created is working well.
* For the first policy it uses the dynamic NAT policy. Where it will dynamically translate the source IP and poet for the traffic translation.
* For the second activity it uses static NAT policy. Where it will specifically allow internet users to access the external web servers in DMZ via IP address of 172.17.54.2

**SCREENSHOTS:**

in this picture all the NAT policies are there in action where internal to internet and internet to DMZ is created A screenshot of a computer

Description automatically generated

before the NAT policy 1 – internal to internet

this is the screenshot showing the icmp traffic is collected when the packet is sent from VM-1 to VM-4 which is coming from the IP address of 172.16.54.10A screenshot of a computer program

Description automatically generated

After the NAT policy 1 – internal to internet

this is the screenshot showing the icmp traffic is collected when the packet is sent from VM-1 to VM-4 which is coming from the IP address of 172.17.54.2A screenshot of a computer

Description automatically generated

before the second NAT translation internet to DMZ

this Screenshot shows the picture of TCP dump from VM-4 to VM-2 where it shows that the traffic is coming from 172.17.54.18A screenshot of a computer screen

Description automatically generated

after the second NAT translation internet to DMZ

this screenshot is after the NAT policy where it shows that the traffic is coming from 172.17.54.2A screenshot of a computer screen

Description automatically generated

**REFLECTION:**

This was the most difficult but important part of the LAB where I created NAT policies and got hands on experience on that. as well as I got knowledge on dynamic and static NAT policy and when to use those policies. I also collected ICMP and TCP traffic for both the NAT policies. At the end I found that the IP address of the traffic coming get changed after the policy has been committed. Which basically shows the success of the NAT translation. And it is used in organizations to provide security into their internal and external networks.

**REFRENCES:**

Netizzan. (n.d.). Dynamic NAT vs Static NAT - Comparison and Differences. Retrieved June 12, 2024, from <https://netizzan.com/dynamic-nat-vs-static-nat-comparison-and-differences/#:~:text=The%20choice%20between%20static%20NAT%20and%20dynamic%20NAT,when%20public%20IP%20addresses%20need%20to%20be%20managed>