labbook=3

Name = Jay Vasani

Student ID =8885487

Course code =INFO1435

Professor name =Manpreet Kaur

Due date = 2023-08-01

# Table of Contents

[Table of Contents 2](file:///C:\Users\jayv2\Downloads\jvasani-5487-INFO1435-labbook-2%20(1).docx#_Toc48746339)

NETWORK ADDRESS TRANSLATION [3](file:///C:\Users\jayv2\Downloads\jvasani-5487-INFO1435-labbook-2%20(1).docx#_Toc48746340)

[Description 3](file:///C:\Users\jayv2\Downloads\jvasani-5487-INFO1435-labbook-2%20(1).docx#_Toc48746342)

[observation 3](file:///C:\Users\jayv2\Downloads\jvasani-5487-INFO1435-labbook-2%20(1).docx#_Toc48746344)

[screenshots 4](file:///C:\Users\jayv2\Downloads\jvasani-5487-INFO1435-labbook-2%20(1).docx#_Toc48746344)

[reflection 12](file:///C:\Users\jayv2\Downloads\jvasani-5487-INFO1435-labbook-2%20(1).docx#_Toc48746344)

**DESCRIPTION:**

This lab is all about creating policies between zones and control the traffic flow through firewall. Where I need to create three zones which are internet, internal and DMZ zones. After applying the security policies, we need to confirm the traffic flow between zones. For this lab we will apply this policies and set up limitation of the packet flow.

**OBSERVATION:**

**PART-1 CONFIGURE BASE FIREWALL PARAMETERS.**

* First, I patch the cables as per the schematics. And for that I used vm2-5 and made connection with the firewall, router and both the switches.
* I opened putty and loaded the base config to the firewall and gave my management Ip address to that. After that I launched my PALO ALTO firewall on browser.
* I created my interfaces on firewall and gave IP according to the schematics and for that I chose layer 3interface type.
* I went to the virtual router’s options and setup all the interfaces over there. I also set static route on my firewall and chose my router interface as next hope for that. And I have taken 0.0.0.0/0 as my default destination.
* After giving static route I have created 3 different zones which are internet on ethernet1/1, internal on ethernet1/2, and DMZ on ethernet 1/3 interface of my firewall.
* By creating zones, we put the networks in separate areas according to the criteria. Each zone has their borders which decide to allow or deny the traffic flow coming from other zones and traffic flow going out to the other zone.

**PART-2 CONFIGURING THE FIREWALL POLICIES.**

* For this part I went to the interface management and created 2 management profiles
* I created profile named jvasani5487-allow management which allows ssh, http and https so that web-based packets can simply flow.
* I also created the jvasani5487-allow ping profile which only allows pinging.
* After that I have attached these profiles with the interfaces as needed.
* After that I have created 3 security policies
* 1 is internal to DMZ, 2 is internal to internal and 3 is internet to DMZ. By creating the security rules, I made sure the packets can only flow in the given way.
* For confirmation of internal to DMZ I ping from vm 1 to vm 2 and confirmed the packet flow
* For confirmation of internal to internet I ping from vm 1 to vm 4 and confirmed the packet flow
* For confirmation of internet to DMZ I ping from vm 4 to vm 2 and confirmed the packet flow

**PART-3 CONFIGURING NAT POLICY.**

* For this part I have configured 2 NAT policies to control the packet flow.
* First, I have created internal to internal policy for that I chose internal as my source and internet as destination zone and chose ethernet 1/1 ads the interface.
* For translated packets I have chose dynamic ip and port as the translation type and gave ip address of the firewall interface connected to the router on ethernet 1/1 interface.
* After that I sent packets from vm 1 to vm 4 and get the tcp dump for that.
* After that have created internet to internet policy for that I chose internet as my source and internet as destination zone and chose ethernet 1/1 as the interface.
* For translated packets I chose dynamic ip as translation type and gave the ip of firewall interface connected to the router.
* For destination translation I chose dynamic-destination-translation option and gave Ip of my vm 2 on that so that only packets coming for that have access to the zone.
* After that I sent packets from vm 4 to vm 2 and get the tcp dump for that.

**SCREENSHOTS:**

Screenshot showing Ip on the correct interfaces.

A screenshot of a computer

Description automatically generated

Screenshot of virtual routersA screenshot of a computer

Description automatically generated

Screenshot of correct next hope on firewallA screenshot of a computer

Description automatically generated

Screenshots of zone creationA screenshot of a computer

Description automatically generated

Screenshot of management profilesA screenshot of a computer

Description automatically generated

Creation of security policies on correct interfaces A screenshot of a computer

Description automatically generated

Creation of NAT policiy 1A screenshot of a computer

Description automatically generated

A screenshot of a mail box

Description automatically generated

A screenshot of a computer

Description automatically generated

Creation of NAT poliy 2 where I took internet to internet not DMZ (I lost the right screenshot)A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**REFLECTION:**

After completing the lab, I got the basic knowledge of NAT and security policies where security policies can only allow or deny the traffic according to the source and destination as given. Where NAT policies are for communication with the external network where it uses the public ip as the private ip after applying some restriction on it.