Contents

Sara Wageh AbdEl-Salam

Student ID:- 21005583

Gmail :- sarawageh78@gmail.com

DEPI Fortinet CyberSecurity

Lab [NAT]

Objective of The Lab

In this lab, you will learn how to configure and manage Network Address Translation (NAT) on FortiGate devices, focusing on both Source NAT (SNAT) and Destination NAT (DNAT) to optimize traffic flow and enhance network security. By the end of the lab, you will gain the following skills:

Configuring DNAT using Virtual IP (VIP):

Learn how to map an external IP address to an internal server using VIP to ensure that incoming traffic is correctly directed.

Configuring SNAT using IP Pools:

Understand how to translate internal device IPs into a shared external IP using Overload IP Pools to optimize IP address usage.

Setting up a Central NAT Policy for SNAT:

Gain expertise in managing SNAT configurations centrally, making it easier to handle traffic policies.

Using DNAT and VIPs to Route Traffic:

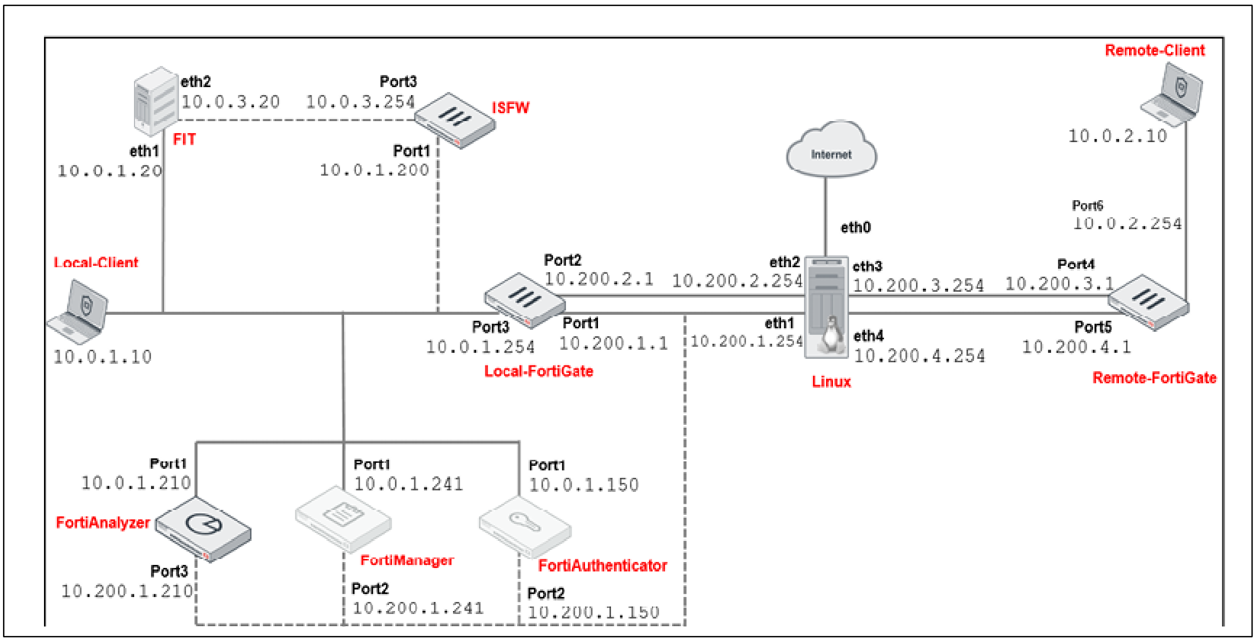
Learn how to create and manage DNAT policies using VIPs to direct external traffic to specific internal services or devices.

Final Goal:

By completing this lab, you will be equipped to configure NAT on FortiGate effectively, enhancing both the functionality and security of your network.

Topology

This is The Topology of The Lab:-



Components Used

In this topology, the components used are as follows:

FortiGate Firewalls:

Local-FortiGate: The primary device managing traffic between the local networks and the internet.

Remote-FortiGate: Handles traffic and management for the remote network.

FortiAnalyzer:

A device used for analyzing and logging network traffic, monitoring events, and ensuring performance.

FortiManager:

A centralized management device for configuring and managing other devices like FortiGate and FortiAnalyzer, as well as enforcing policies.

FortiAuthenticator:

Provides identity management and authentication for users on the network.

Clients:

Local Client: A computer in the local network (IP: 10.0.1.10).

Remote Client: A computer in the remote network (IP: 10.0.2.10).

Linux Server:

A server included in the topology for handling traffic and possibly for testing purposes (connected via eth0, eth1, eth3, eth4).

Network Interfaces and Ports:

Ports such as Port1, Port2, Port3, etc., are used for connecting devices.

Interfaces like eth0, eth1 on the Linux server manage the connections.

Overall Functionality:

Local Client and Remote Client communicate through FortiGate firewalls.

Forti Analyzer and Forti Manager are used for network monitoring, logging, and management.

Forti Authenticator ensures secure access through authentication.

Steps of The Lab

Prerequisites

1. ConnecttotheRemote-FortiGate GUI, and then log in with the username admin and password password .

2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.

3. Click +to expand the list.

4. Select the configuration with the comment initial, and then click Revert.

5. Click OK to reboot.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.

2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.

3. Click +to expand the list.

4. Select the configuration with the comment local-Nat, and then click Revert.

5. Click Ok to reboot

Configuring DNAT Settings Using a VIP Steps

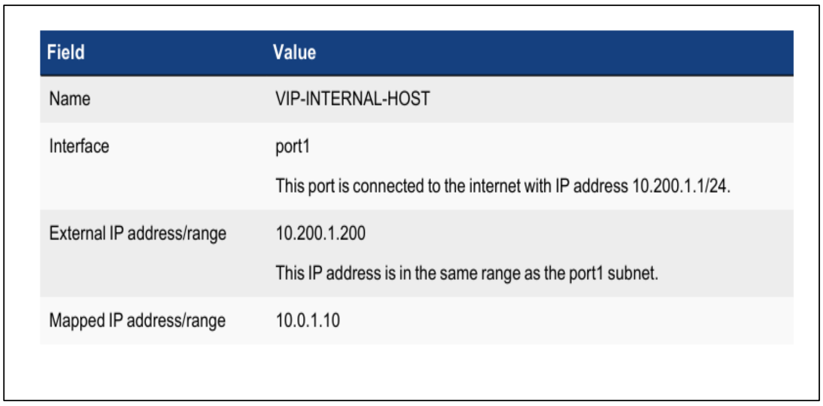
To create a VIP

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.

2. Click Policy & Objects>Virtual IPs.

3. Click Create New , and then select Virtual IP.

4. Configure the following settings:

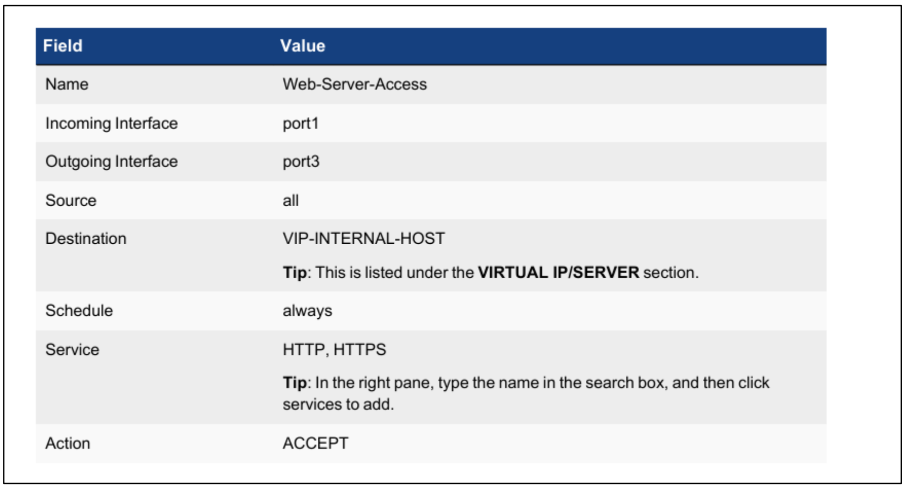


Field	Value
Name	VIP-INTERNAL-HOST
Interface	port1 This port is connected to the internet with IP address 10.200.1.1/24.
External IP address/range	10.200.1.200 This IP address is in the same range as the port1 subnet.
Mapped IP address/range	10.0.1.10

1. On the Local – FortiGate GUI , click Policy&Objects >Firewall Policy.

2. Click Create New.

3. Configure the following settings:



Field	Value
Name	Web-Server-Access
Incoming Interface	port1
Outgoing Interface	port3
Source	all
Destination	VIP-INTERNAL-HOST **Tip**: This is listed under the **VIRTUAL IP/SERVER** section.
Schedule	always
Service	HTTP, HTTPS **Tip**: In the right pane, type the name in the search box, and then click services to add.
Action	ACCEPT

4. In the Firewall/Network Options section, disable NAT.

5. In the Logging Options section, enable Log Allowed Traffic, and then select All Sessions.

6. Click OK.

Testing

Now that you have configured a firewall policy with the VIP as the destination, you can test your VIP by accessing

it from the Remote-Client VM, which is behind the Remote-FortiGate internal network. A Linux machine acts as a

router between the two FortiGate devices, and routes the traffic from the Remote-FortiGate to the Local-FortiGate.

For more information, see Network Topology on page 8.

You will also test how the source address is translated by the VIP when traffic leaves the Local-Client VM

To test VIPs (DNAT)

1. On the Remote-Client VM , open a browser ,and then browse to the following URL:

http://10.200.1.200

If the VIP operation is successful, a simple web page opens.

2. On the Local-FortiGate CLI, log in with the username admin and password password.

3. Enter the following command to check the destination NAT entries in the session table:

```
get system session list
```

The following example shows a sample output:

```
Local-FortiGate# get system session list

PROTO EXPIRE SOURCE SOURCE-NAT DESTINATION DESTINATION-NAT

tcp 3594 10.200.3.1:49478- 10.200.1.200:80 10.0.1.10:80
```

Result 1

You will notice that the destination address 10.200.1.200 is translated to 10.0.1.10, which is themapping you configured in the VIP.

The HTTP session may have been deleted by the time your un the get system

session listcommand.Youcanrepeatsteps1–3togenerateanewHTTP

connection and, therefore, another HTTP session through Local-FortiGate

Test SNAT

As a result of the VIP (which is a static NAT), FortiGate uses the VIP external address as the NAT IP address

When performing SNAT for the ingress-to-egress direction of the traffic, provided the matching outgoing firewall policy has NAT enabled. That is, FortiGate doesn't use the egress interface address.

To test SNAT

1. Return to the Local-FortiGate CLI session, and then enter the following command to clear any existing sessions:

```
diagnose sys session clear
```

The diagnose sys session clear CLI command clears all sessions , including

the SSH session you created. This is expected behavior .

This clears the session to the Local-FortiGate from the Local-Client VM.

1

2. Close the Local-FortiGate CLI window.

3. on the Local-Client VM, open a few browser tabs, and connect to a few websites, such as:

www.fortinet.com

www.yahoo.com

www.bbc.com

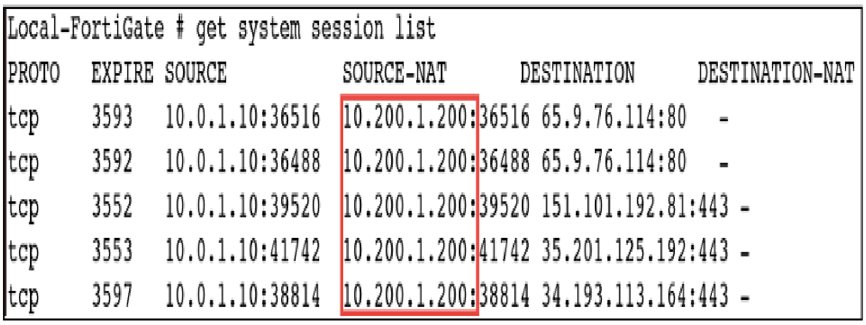
4. on the Local-FortiGate CLI, log in with the username admin and password password.

5. Enter the following command to view the session information:

```
get system session list
```

Result 2

The following example shows a sample output:-



```
Local-FortiGate # get system session list
PROTO   EXPIRE SOURCE           SOURCE-NAT        DESTINATION        DESTINATION-NAT
tcp     3593   10.0.1.10:36516  10.200.1.200:36516 65.9.76.114:80    -
tcp     3592   10.0.1.10:36488  10.200.1.200:36488 65.9.76.114:80    -
tcp     3552   10.0.1.10:39520  10.200.1.200:39520 151.101.192.81:443 -
tcp     3553   10.0.1.10:41742  10.200.1.200:41742 35.201.125.192:443 -
tcp     3597   10.0.1.10:38814  10.200.1.200:38814 34.193.113.164:443 -
```

This is a behavior for SNAT when using astatic NAT VIP. That is, when you enable NAT on a policy, the external address of a static NAT VIP takes precedence over the destination interface IP address if the source address of the connections matches the VIP internal address.