Name : Mohamed Hossam monier el-shafey

Objectives:

* Configure DNAT settings using a VIP
* Configure SNAT settings using overload IP pools
* Configure a central NAT policy for SNAT
* Configure DNAT and VIPs for DNAT

Needs:

1-remote-fortigate vm

2-local-fortigate vm

**To restore the Remote-FortiGate configuration file:**

1.Connect to the Remote-FortiGate GUI, by using username( admin) and password (password).

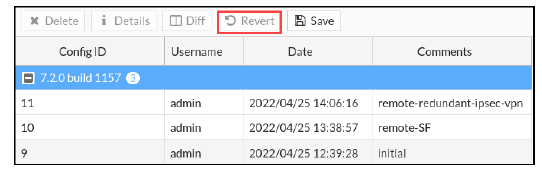
**2.** In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.

A screenshot of a computer

Description automatically generated

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).

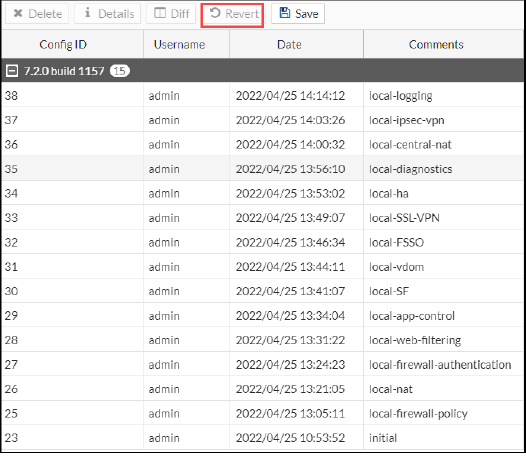
2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions

A screenshot of a computer

Description automatically generated

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:

**To create a VIP:**

1.Connect to the Local-FortiGate GUI, by using 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 |

A screenshot of a computer

Description automatically generated

**5.** Click **OK**.

You will configure a new firewall policy using the VIP that you just created as the destination address:

To create a new firewall policy:

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 |
| 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**.

A screenshot of a computer

Description automatically generated

**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.

A screenshot of a computer

Description automatically generated

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

**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

**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

A screenshot of a computer screen

Description automatically generated

Using Dynamic NAT With IP Pools:

**To create an IP pool:**

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

**2.** Click **Policy & Objects** > **IP Pools**.

**3.** Click **Create New**, and then configure the following settings:

|  |  |
| --- | --- |
| Field | Value |
| Name | NTERNAL-HOST-EXT-IP |
| Type | Overload |
| External IP address/range | 10.200.1.100-10.200.1.100 |

A screenshot of a computer

Description automatically generated

4.click ok

**To edit the firewall policy**

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

**2.** Right-click the **Full\_Access** firewall policy, and then click **Edit**.

**3.** In the **Firewall / Network Options** section, configure the following settings:

|  |  |
| --- | --- |
| Field | Value |
| NAT | <enable> |
| IP Pool Configuration | Use Dynamic IP Pool |

**4.** Click the **+** sign that appeared when you clicked **Use Dynamic IP Pool**, and then in the right pane, click **INTERNAL-HOST-EXT-IP**

A screenshot of a computer

Description automatically generated

**5.** Click **OK**.

**To test dynamic NAT with IP pools**

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

**2.** Enter the following commands to clear sessions sourced from 10.0.1.10:

diagnose sys session filter clear

diagnose sys session filter src 10.0.1.10

diagnose sys session clear

**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, enter the following command to verify the SNAT address that the sessions are using:

get system session list

A screenshot of a computer

Description automatically generated

Configuring Central SNAT:

**To restore the Local-FortiGate configuration file**

**1.** Connect to the Local-FortiGate GUI, by using username (admin) and password (password).

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

A screenshot of a computer

Description automatically generated

**3.** Click **+** to expand the list.

**4.** Select the configuration with the comment **local-central-nat**, and then click **Revert**.

A screenshot of a computer

Description automatically generated

**5.** Click **OK** to reboot.

**To configure a central SNAT policy**

**1.** On the Local-FortiGate GUI, click **Policy & Objects** > **Central SNAT**.

**2.** Click **Create New**, and then configure the following settings:

|  |  |
| --- | --- |
| Field | Value |
| Incoming Interface | Port3 |
| Outgoing Interface | Port1 |
| Source Address | All |
| Destination Address | All |
| NAT | <enable> |
| IP Pool Configuration | Use Dynamic IP Pool  Click **+**, and then select **INTERNAL-HOST-EXT-IP**. |
| Protocol | any |

A screenshot of a computer

Description automatically generated

**To verify that NAT is enabled on the firewall policy**

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

**2.** Right-click the **Full\_Access** firewall policy, and then click **Edit**.

**3.** Review the **Firewall/Network Options** of the **Full\_Access** policy.

A screenshot of a computer

Description automatically generated

**To test central SNAT**

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

**2.** Enter the following commands to clear sessions sourced from 10.0.1.10:

diagnose sys session filter clear

diagnose sys session filter src 10.0.1.10

diagnose sys session clear

**3.** Close the Local-FortiGate CLI window.

**4.** 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

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

**6.** Enter the following command to verify the SNAT IP address that those sessions are using:

get system session list

A screenshot of a computer

Description automatically generated

Configuring and Testing DNAT and VIPs

**To create DNAT and VIPs**

**1.** Connect to the Local-FortiGate GUI, by using username (admin) and password (password).

**2.** Click **Policy & Objects** > **DNAT & Virtual IPs**.

**3.** Click **Create New**, and then select **DNAT & Virtual IP**.

**4.** Configure the following settings:

|  |  |
| --- | --- |
| Field | Value |
| Name | Central-DNAT |
| Interface | Port1 |
| Type | Static NAT |
| External IP address/range | 10.200.1.150 |
| Mapped IP address/range | 10.0.1.10 |

A screenshot of a computer

Description automatically generated

**5.** Click **OK**.

**To verify the firewall policy settings**

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

**2.** Right-click the **Web-Server-Access** firewall policy, and then click **Edit**.

**3.** Review the settings of the firewall policy.

**4.** Try to select the **Central-DNAT** object in the firewall **Destination** address.

**5.** Scroll to the bottom of the page, and then ensure that **Enable this policy** is enabled.

A green and white sign

Description automatically generated

6.click ok

**To test DNAT and VIPs**

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

http://10.200.1.150

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

A close-up of a list

Description automatically generated

**4.** 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

**5.** Return to the Local-FortiGate CLI session, and then verify the SNAT IP address that those sessions are using:

get system session list

