Firewall Policies Lab

…. Contents ….

……

1_ The Objective

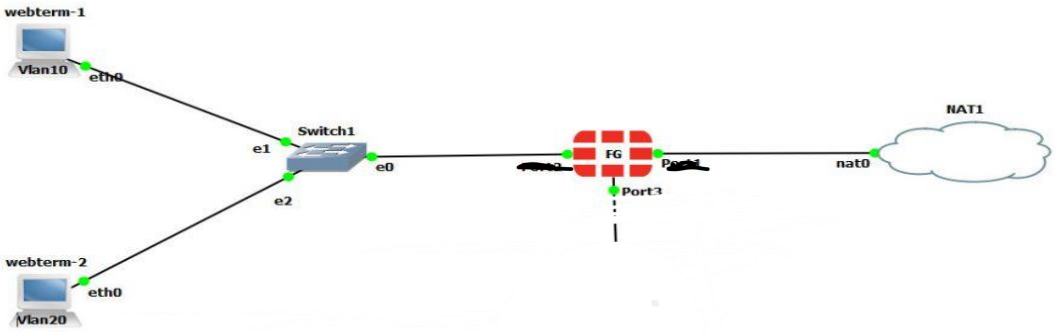
In this Lab, we will configure firewall address objects. You will also configure an IPv4 firewall policy that you will apply firewall address objects to, along with a schedule, services, and log options. Then, you will test the firewall policy by passing traffic through it and checking the logs for your traffic. At its core, FortiGate is a firewall, so almost everything that it does to your traffic is related to your firewall policies.

In this lab, we will:

- **Create Address Objects**: Define firewall address objects that will be used in the policies.
- **Configure Firewall Policies**: Set up firewall policies on the Local FortiGate device.
- **Set Up an IPv4 Firewall Policy**: Apply the created address objects to an IPv4 firewall policy, including settings for schedules, services, and logging options.
- **Test the Firewall Policy**: Conduct tests by passing traffic through the configured policy and verifying the results through log checks.

……

2_Topology



1. **Fortigate Firewall**: The main device for implementing Firewall Polices.
2. **Internal Network**: A switch connected to the Fortigate's internal interface.
3. **Internet**: Simulated internet connection for testing web access.

.....

3_Components Used

1_Fortigate Firewall: Virtual or physical device.

2_Switch: For internal network connections.

3_Router: For external network connections**.**

4_PCs or VMs: For simulating internal network users.

.....

4_Steps to configuration Lab

#Creating Firewall Address Objects

By default, FortiGate has many preconfigured, well-known address objects in the factory default configuration. However, if those objects don't meet the needs of your organization, you can configure more.

To create a firewall address object

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Addresses**.
3. Click **Create New** > **Address**.
4. Configure the following settings:

Field	Value
Name	LOCAL_SUBNET
Type	Subnet
IP/Netmask	10.0.1.0/24
Interface	any

#Creating Firewall Policy

create a more specific firewall policy using the firewall address object that you created in the previous procedure. You will also select specific services and configure log settings.

1. Continuing in the **Policy & Objects** > **Firewall Policy** section, click **Create New** to add a new firewall policy.
2. Configure the following settings:

Field	Value
Name	Internet_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL_ICMP, HTTP, HTTPS, DNS, SSH **Tip**: Type the service name in the search box to quickly find it, and then click the service object to add it to the policy.
Action	ACCEPT
NAT	<enable>
Log Allowed Traffic	<enable> and select **All Sessions**
Generate Logs when Session Starts	<enable>

$$$$Logs to this policy

-Right-click the Internet_Access policy, and then click Show Matching Logs

With the current settings, you should have a few log messages that have Accept: session start in the Result column. These are the session start logs.

#Reordering Firewall Policies and Firewall Policy Actions.

In this exercise, you will create a new firewall policy with more specific settings, such as the source, destination, and service, and you will set the action to **DENY**. Then, you will move this firewall policy above the existing firewall policies and observe the behavior that reordering the firewall policies creates.

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**, and then click **Create New**.
3. Configure the following settings:

Field	Value
Name	Block_Ping
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	LINUX_ETH1
Schedule	always
Service	PING **Tip**: Type the service name in the search box to quickly find it, and then click the service object to add it to the policy.
Action	DENY
Log Violation Traffic	<enable>
Enable this policy	<enable>

. Click **OK** to save the changes.

5_Testing

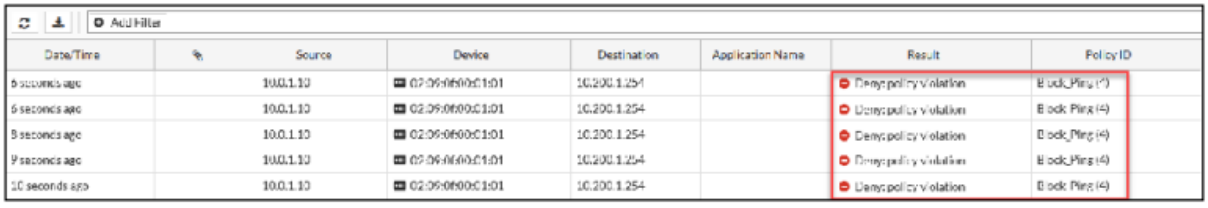
To confirm traffic matches a more granular firewall policy after reordering the policies ..

1. On the Local-Client VM,
2. open a terminal.
3. Ping the destination address (LINUX_ETH1) that you configured in the Block_Ping firewall policy. ping 10.200.1.254..

6_The Result

On the Local-Client VM, review the terminal window that is running the continuous ping. You should see that the pings now fail ..

You should see many policy violation logs reporting the blocked ping.



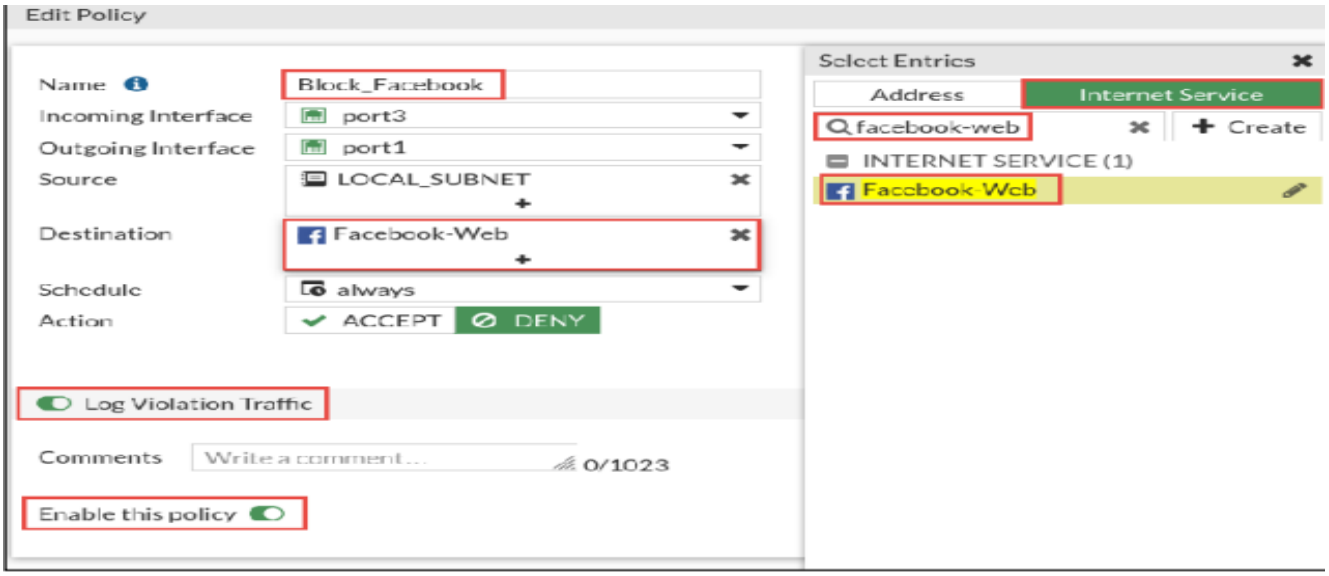
We can Try this on different Policies to permit or deny …

Configure a Firewall Policy Destination as an ISDB Object

You will modify an existing firewall policy and use an ISDB object as a destination.

To configure an internet service as a destination

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Right-click the **ID** column for the **Block_Ping** firewall policy, and then click **Edit**.
3. Change the **Name** to **Block_Facebook**.
4. Click **Destination**, and then in the right pane, click **LINUX_ETH1** to clear it.
5. Click **Internet Service**.
6. Select **Facebook-Web**.



To test the internet service firewall policy

1. On the Local-Client VM, open a few browser tabs, and go to the following websites: l www.facebook.com

Access Deny