**Firewall Policies Lab**

…. Contents ….

* The Objective
* Topology
* Components
* Steps
* Testing
* The Result

…………………………………………………

**1\_ The Objective**

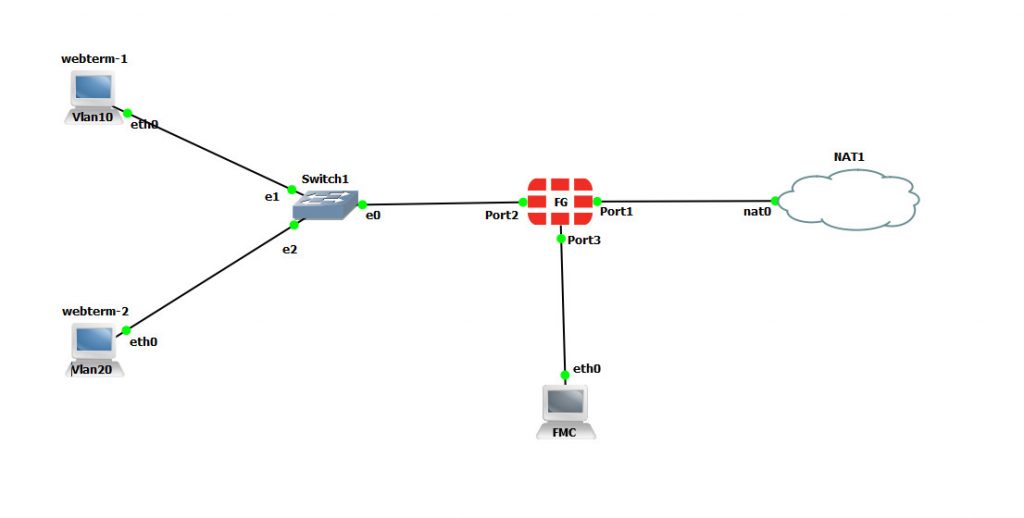
In this Lab, we will configure firewall address objects. You will also configure an IPv4 firewall policy that you will apply firewall address objects to, along with a schedule, services, and log options. Then, you will test the firewall policy by passing traffic through it and checking the logs for your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

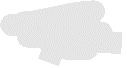
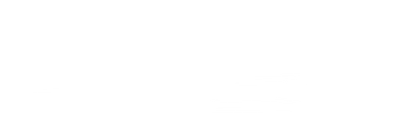
In this lab, we will:

* **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**.**

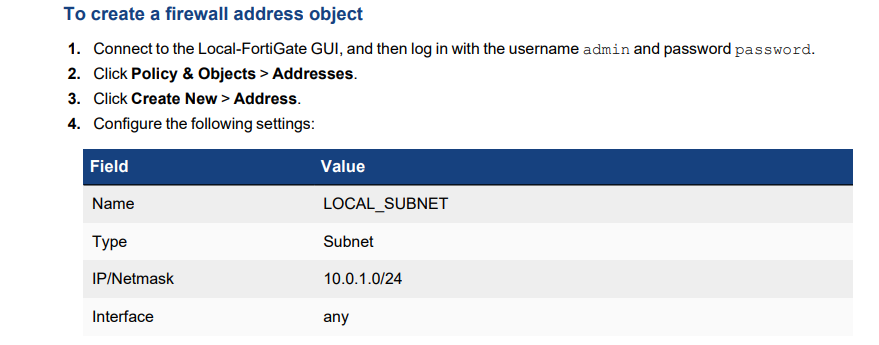
**4\_PCs or VMs:** For simulating internal network users.

……………………………………………………………………………………….

**4\_Steps to configuration Lab**

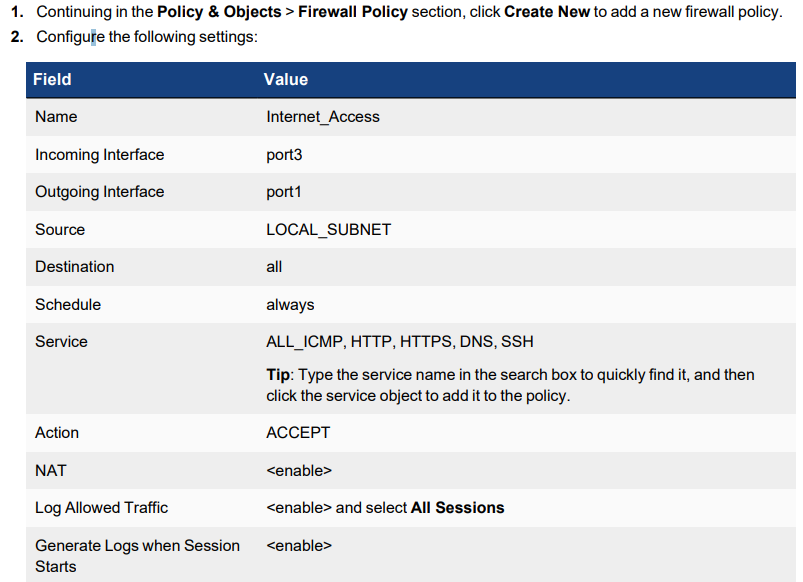
**#Creating Firewall Address Objects**

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.



**#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.



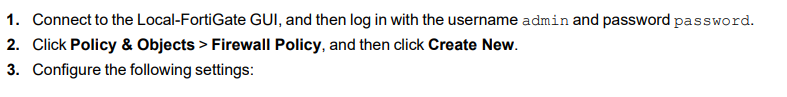
$$$$Logs to this policy

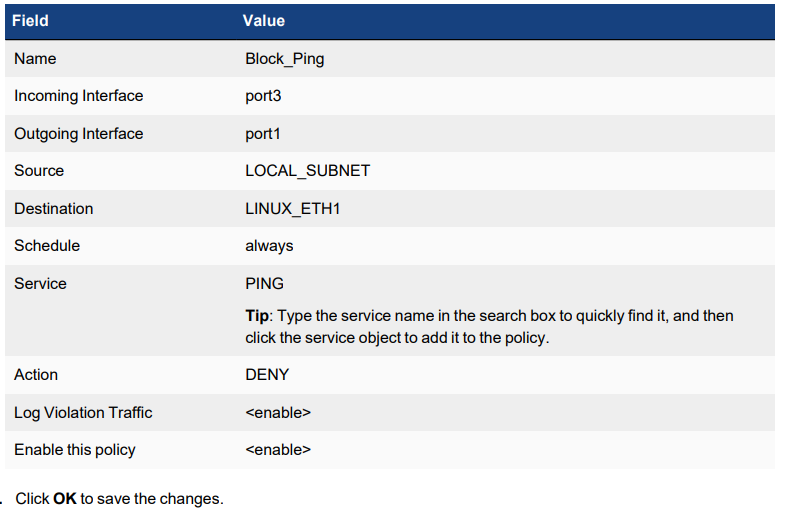
-**Right-click the Internet\_Access policy, and then click Show Matching Logs**

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.





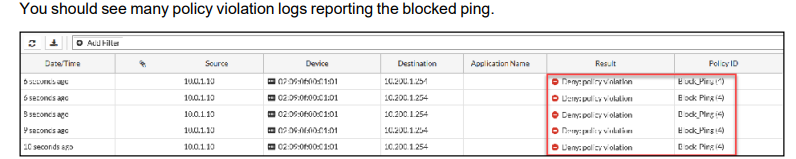
5\_Testing

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

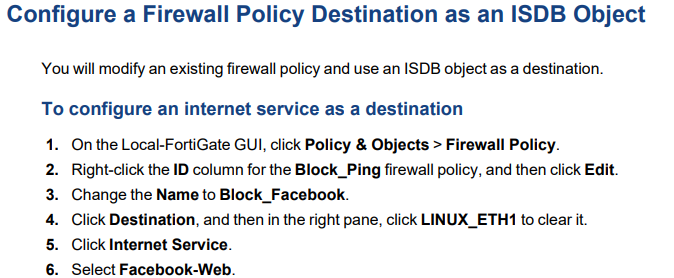
1. On the Local-Client VM,
2. open a terminal.
3. Ping the destination address (LINUX\_ETH1) that you configured in the Block\_Ping firewall policy. ping 10.200.1.254..

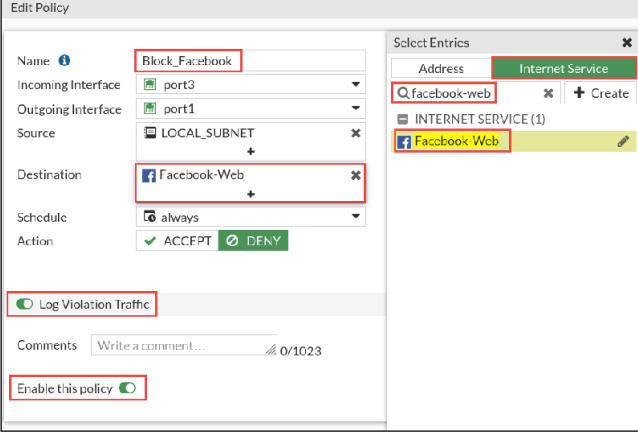
6\_The Result

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



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





**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**

