Ministry of Communications and Information Technology

DIGITAL EGYPT GENERATIONS

Digital Egypt Pioneers

Digital Egypt Pioneers Initiative (DEPI)

Firewall Policies in Fortigate

Name: Amr Ehab Mohamed Salama

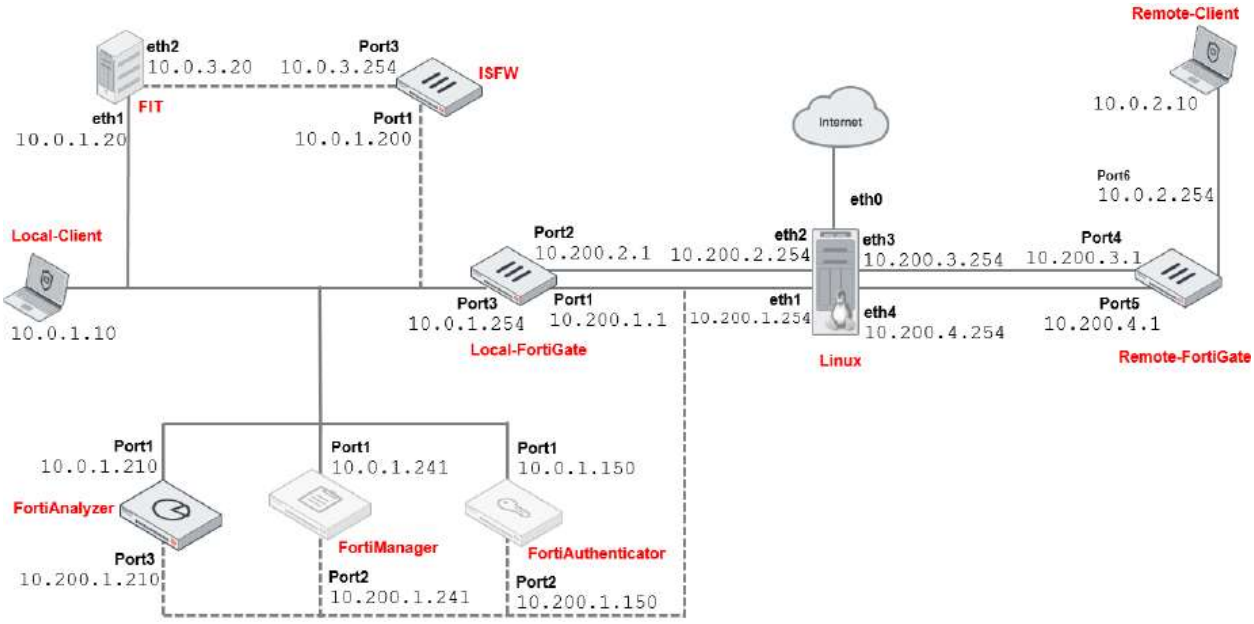
Track: Fortinet cybersecurity

Phone number: 01064988991

Email: ehabamr473@gmail.com

Group name: DEPI_1_CAI1_ISS8_S1e Fortinet Cybersecurity Engineer

Network Topology



Objectives

- Configure firewall objects and firewall policies

- Configure source and destination matching in firewall policies

- Apply service and schedule objects to a firewall policy

- Configure firewall policy logging options

- Reorder firewall policies

- Read and understand logs

- Use policy lookup to find a matching policy

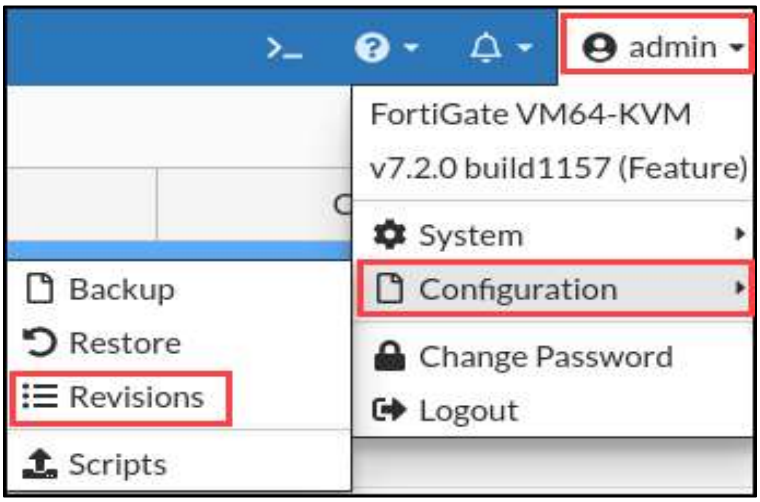
In this project, we will configure firewall policies on Local-FortiGate, and then perform various tests on the Local-Client VM to confirm that traffic is matching the appropriate firewall policies based on the configuration.

Prerequisites

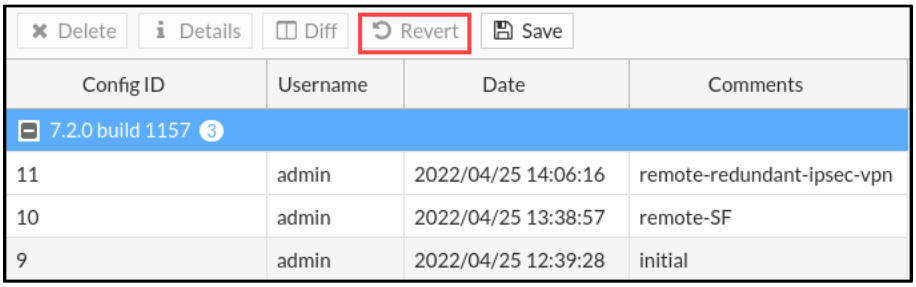
Before beginning this lab, we must restore configuration files to Remote-FortiGate, ISFW, and Local-FortiGate.

To restore the Remote-FortiGate configuration file

1. Connect to the Remote-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**.



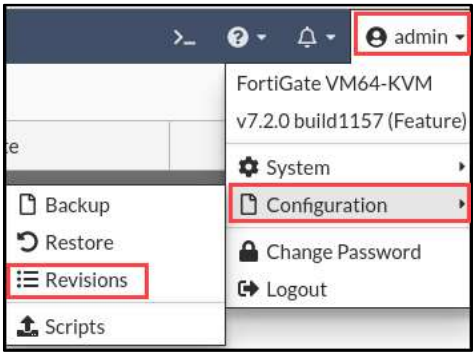
3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



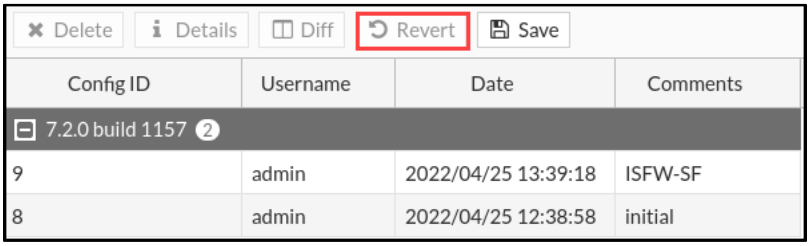
5. Click **OK** to reboot.

To restore the ISFW configuration file

1. Connect to the ISFW 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**.



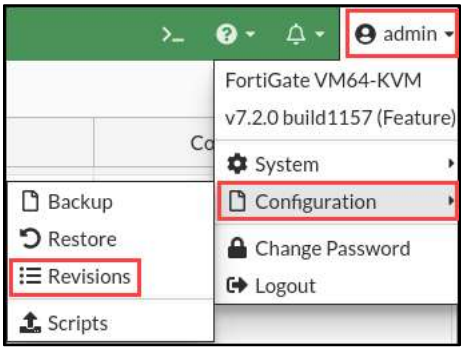
3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



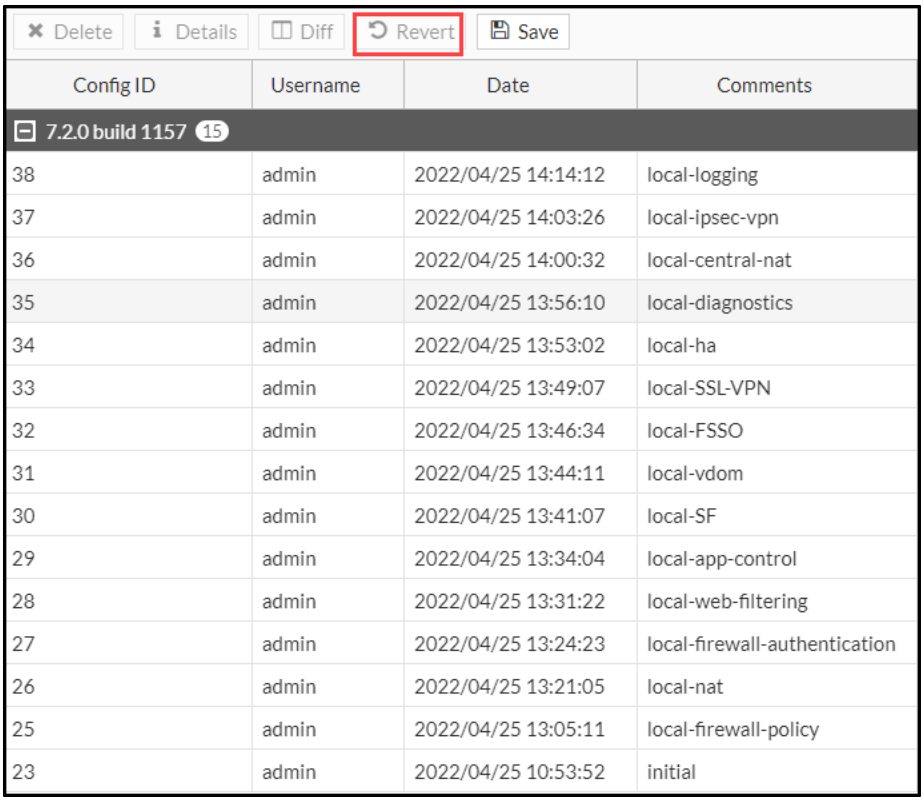
5. Click **OK** to reboot.

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 the **+** sign to expand the list.
4. Select the configuration with the comment **local-firewall-policy**, and then click **Revert**.



5. Click **OK** to reboot.

Exercise 1: Creating Firewall Address Objects and Firewall Policies

In this exercise, we will configure firewall address objects. we will also configure an IPv4 firewall policy that we will apply firewall address objects to, along with a schedule, services, and log options. Then, we will test the firewall policy by passing traffic through it and checking the logs for our traffic.

At its core, FortiGate is a firewall, so almost everything that it does to our traffic is related to our firewall policies.

Create 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 our organization, we 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

5. Click **OK**.

Create a Firewall Policy

First, we will disable the existing firewall policy. Then, we will create a more specific firewall policy using the firewall address object that we created in the previous procedure. we will also select specific services and configure log settings.

To disable an existing firewall policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Right-click the **Full_Access** firewall policy, and then in the **Set Status** field, select **Disable**.

To create a firewall policy

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>
Enable this policy	<enable>

Test the Firewall Policy and View the Generated Logs

Now that we configured the firewall policy, we will test it by passing traffic through it and viewing the generated logs.

To test and view logs for a firewall policy

1. On the Local-Client VM, open several web browser tabs, and connect to several external websites, such as:

   www.google.com
   kb.fortinet.com
   docs.fortinet.com
   www.bbc.com

2. Return to the browser tab with the Local-FortiGate GUI, and then click **Policy & Objects** > **Firewall Policy**.
3. Right-click the **Internet_Access** policy, and then click **Show Matching Logs**.

4. Identify the log entries for our internet browsing traffic.

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

When sessions close, there is a separate log entry for the amount of data that was sent and received.

5. In the **Forward Traffic** logs, click **X** to remove the **Policy UUID** filter.

When we remove the **Policy UUID** filter, the logs are displayed unfiltered. we will use the logs in upcoming labs.

Exercise 2: Reordering Firewall Policies and Firewall Policy Actions

In the applicable interface pair section, FortiGate looks for a matching policy, beginning at the top. Usually, we should put more specific policies at the top—otherwise, more general policies will match the traffic first, and more granular policies will never be applied.

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

Create a Firewall Policy

To create a firewall policy

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.

Test the Reordering of a Firewall Policy

Now that our configuration is ready, we will test it by moving the **Block_Ping** firewall policy above the **Internet_ Access** firewall policy. The objective is to confirm that, after we reorder the firewall policies, the following occurs:

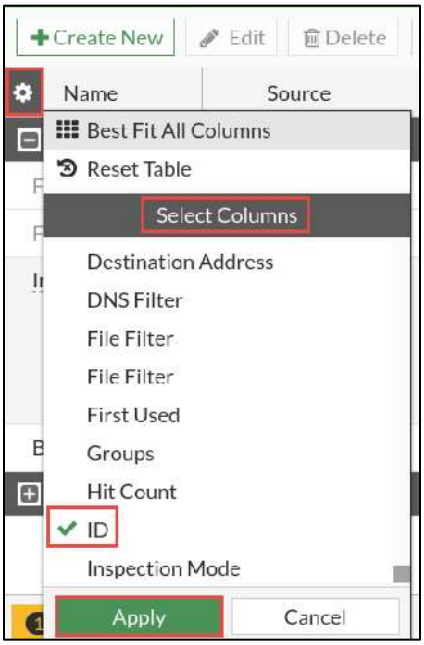
--Traffic is matched to a more specific firewall policy.

--The policy ID remains the same.

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

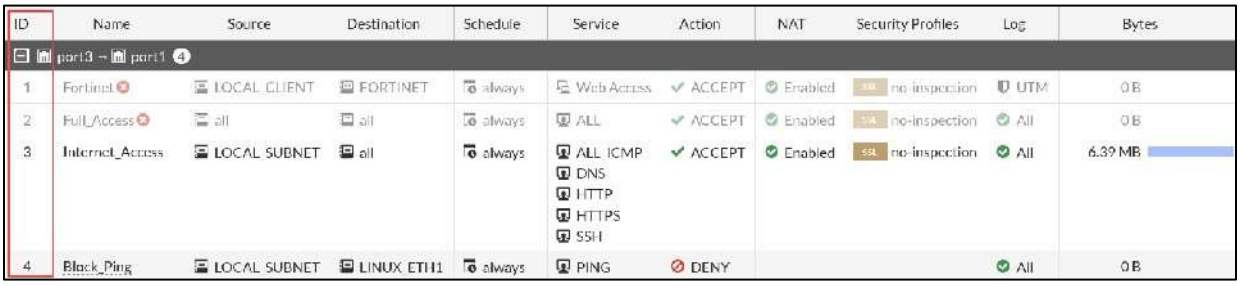
1. On the Local-Client VM, open a terminal.
2. Ping the destination address (**LINUX_ETH1**) that we configured in the **Block_Ping** firewall policy.
   `ping 10.200.1.254`
3. Leave the terminal window open and running.
4. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
5. Hover over the **Name** column.

   A settings icon appears beside **Name**.
6. Click the settings icon, scroll down to the **Select Columns** section, select the **ID** column, and then click **Apply**.



The **ID** column appears as the last column in the table.

7. Drag the **ID** column to the left of the **Name** column, so it becomes the first column in the table. Note the current **ID** values for both the **Internet_Access** and **Block_Ping** firewall policies.



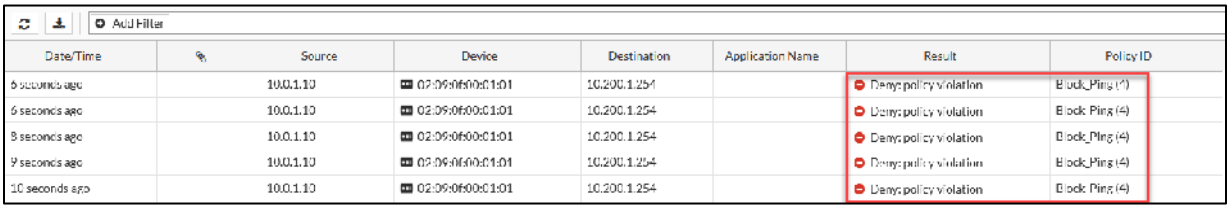
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port3 → port1 4										
1	Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT	Enabled	no-inspection	UTM	0 B
2	Full_Access	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All	0 B
3	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	ACCEPT	Enabled	no-inspection	All	6.39 MB
4	Block_Ping	LOCAL_SUBNET	LINUX_ETH1	always	PING	DENY			All	0 B

8. In the **ID** column, drag the **Block_Ping** firewall policy up, and place it above the **Internet_Access** firewall policy. When we move the **Block_Ping** policy up, the **ID** value remains the same.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port3 → port1 4										
1	Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT	Enabled	no-inspection	UTM	0 B
2	Full_Access	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All	0 B
4	Block_Ping	LOCAL_SUBNET	LINUX_ETH1	always	PING	DENY			All	0 B
3	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	ACCEPT	Enabled	no-inspection	All	6.39 MB

9. On the Local-Client VM, review the terminal window that is running the continuous ping. we should see that the pings now fail.
10. Close the terminal window.
11. On the Local-FortiGate GUI, click **Log & Report** >

Forward Traffic. we should see many policy violation logs reporting the blocked ping.



Exercise 3: Applying ISDB Objects as Destinations

FortiGate can match destination traffic using address objects or internet service database (ISDB) objects. ISDB objects are predefined entries that FortiGuard regularly updates and contain a database of IP addresses, protocols, and port numbers that the most common internet services use.

we can use ISDB objects to allow or deny traffic to well-known internet destinations, without having to configure the IP addresses, protocols, or ports that those destinations use in the firewall policy.

In this exercise, we will apply an ISDB object as the destination criteria in a firewall policy to block traffic to a well- known internet service.

Review the ISDB

we will review the entries in the ISDB.

To review the ISDB

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click Policy & Objects > Internet Service Database.
3. Expand the **Predefined Internet Services** and **IP Reputation Database** sections.
4. Double-click any entry, and then click **View/Edit Entries**.
5. we can see the corresponding IP addresses, ports, and protocols that the internet service uses.
6. Click **Return**.

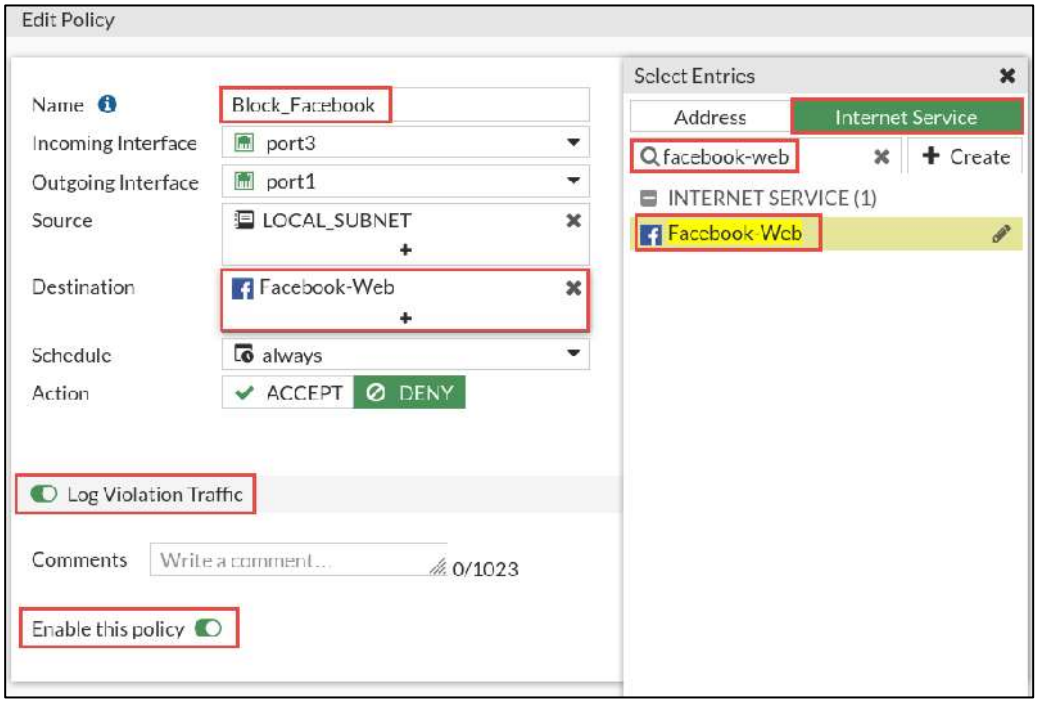
Configure a Firewall Policy Destination as an ISDB Object

we 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**.

Select **Facebook-Web**.



Test the Internet Service Firewall Policy

Now that we configured the firewall policy, we will test it by passing traffic through it.

To test the internet service firewall policy

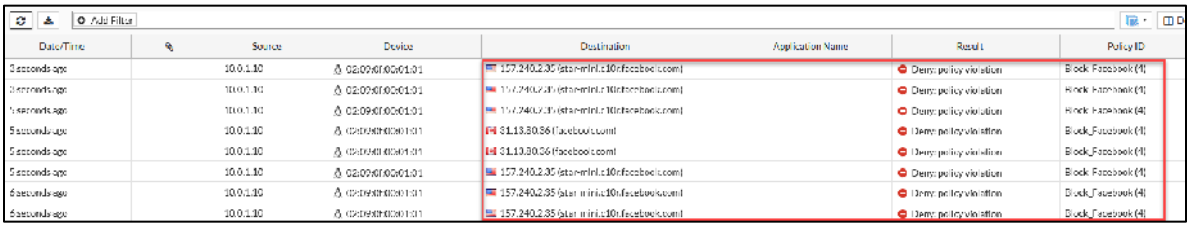
On the Local-Client VM, open a few browser tabs, and go to the following websites:

www.facebook.com

www.twitter.com

On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.

we should see many policy violation logs that the **Block_Facebook** policy reported.



On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, right-click the **Block_Facebook** firewall policy, select **Set Status**, and then click **Disable**.

Exercise 4: Using Policy Lookup

FortiGate can find a matching firewall policy based on the policy lookup input criteria. The policy lookup feature basically creates a packet flow over FortiGate without real traffic. From this packet flow, FortiGate can extract a policy ID and highlight it on the GUI policy configuration page.

In this exercise, we will use the policy lookup feature to find a matching firewall policy based on input criteria.

Enable Existing Firewall Policies

As required in the previous exercises, most of the configured firewall policies are currently disabled. Now, we will enable some of the existing firewall policies.

To enable existing firewall policies

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Right-click the **Fortinet** firewall policy, select **Set Status**, and then click **Enable**.
4. Right-click the **Full_Access** firewall policy, select **Set Status**, and then click **Enable**.

Set Up and Test the Policy Lookup Criteria

we will set up the policy lookup criteria. FortiGate searches and highlights the matching firewall policy based on our input criteria.

To set up and test the policy lookup criteria

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, and then click **Policy Lookup**.
2. Configure the following settings:

Field	Value
Protocol	TCP

Source	10.0.1.100
Source Port	<leave this field empty>
Destination	fortinet.com
Destination Port	443

Click **Search**.

The search matches the **Full_Access** policy, but does not match the more specific **Fortinet** firewall policy.

In the search criteria, the source address is set to `10.0.1.100`. This source address is not included in the **Fortinet** firewall policy; therefore, the search does not match the **Fortinet** firewall policy.
Click **Policy Lookup**, and then change the **Source** to `10.0.1.10`.

Make sure all the other settings match the settings we configured in step 2.

Click **Search**.

This time, the search matches the **Fortinet** firewall policy, in which the destination is set to the FQDN address object.

To reorder the firewall policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. From the ID column, drag the **Block_Facebook** firewall policy above the **Full_Access** firewall policy. The order of the firewall policies should match the following example:

ID	Name	Source	Destination
port3 → port1 4			
1	Fortinet	LOCAL_CLIENT	FORTINET
4	Block_Facebook	LOCAL_SUBNET	Facebook-Web
2	Full_Access	all	all
3	Internet_Access	LOCAL_SUBNET	all

Retest Policy Lookup After Reordering the Firewall Policies

we will retest the policy lookup feature after reordering the firewall policies.

To retest policy lookup after reordering the firewall policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, and then click **Policy Lookup**.
2. Configure the following settings:

Field	Value
Source Interface	port3
Protocol	TCP
Source	10.0.1.10
Destination	facebook.com
Destination Port	443

3. Click **Search**.
4. Right-click the **Block_Facebook** firewall policy, select **Set Status**, and then click **Enable**.
5. Click **Policy Lookup**.
6. Make sure all the settings match the settings we configured in step 2.
7. Click **Search**.
8. This time the search matches the more specific policy, **Block_Facebook**.