

A graphic featuring the year '2024' in white, bold, sans-serif font, centered within a white-outlined square. The square is slightly offset to the right, creating a layered effect. The background is a dark blue gradient with a light blue geometric shape on the right side.

2024

FIREWALL POLICIES

PREPARED BY:

REEM ESSAM DOSOKY SALAM

INTERNSHIP:

DIGITAL EGYPTION PIONEER

TRACK:

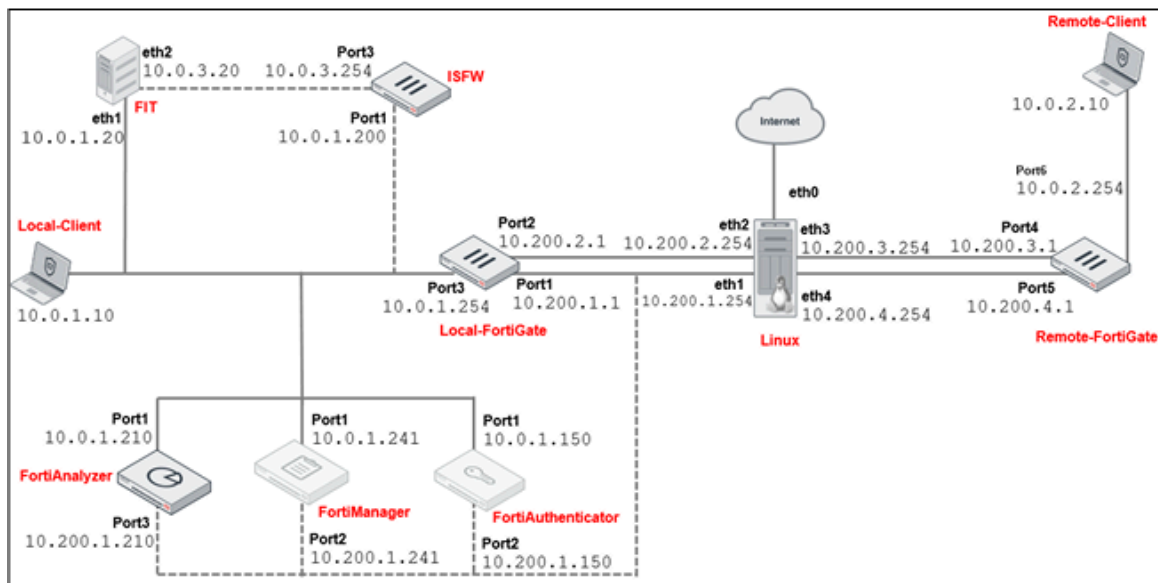
CNNA AND FORTINENT

Decorative blue geometric shapes at the bottom of the page, including a large light blue arrow pointing right and a smaller teal triangle pointing left, set against a dark blue background.

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

topology:



components used:

1. Remote client virtual machine.
2. local client virtual machine.
3. remote fortiGate virtual machine.
4. local fortigate virtual machine.
5. fortianalyzer virtual machine.
6. fortimanager virtual machine.
7. fortiauthenticator virtual machine.
8. server with linux operating system virtual machine.

steps of the lab:

- **To restore the Remote-FortiGate configuration file.**
 1. Connect to the Remote-FortiGate GUI, then log in with the username admin and password.
 2. In the screen's upper-right corner, click admin, then Configuration > Revisions.
 3. Select the configuration with the comment initial, and then click Revert.
 4. Click OK to reboot.
- **To restore the ISFW configuration file**
 5. Connect to the ISFW GUI, then log in with the username, admin, and password.
 6. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.
 7. Select the configuration with the comment initial, and then click Revert.
- **To restore the Local-FortiGate configuration file**
 8. Connect to the local- fortigate GUI, then log in with the username, admin, and password.
 9. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.
 10. Select the configuration with the comment initial, and then click Revert.
 11. Click OK to reboot.
- **To create a firewall address object**
 12. Connect to the local- fortigate GUI, then log in with the username, admin, and password.
 13. Click Policy & Objects>Addresses.
 14. Click Create New>Address.
 15. Configure the following settings:

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

- **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**

3. Continuing in the Policy&Objects > Firewall Policy section, click Create New to add a new firewall policy.
4. 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>

- **To test and view logs for a firewall policy**

1. On the Local-Client VM, open several browser tabs, and then connect to several external websites, such as:
www.google.com
www.cnn.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 your internet browsing traffic.

Reordering Firewall Policies and Firewall Policy Actions

In the applicable interface pair section, FortiGate looks for a matching policy, beginning at the top. Usually, you 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, 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.

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>

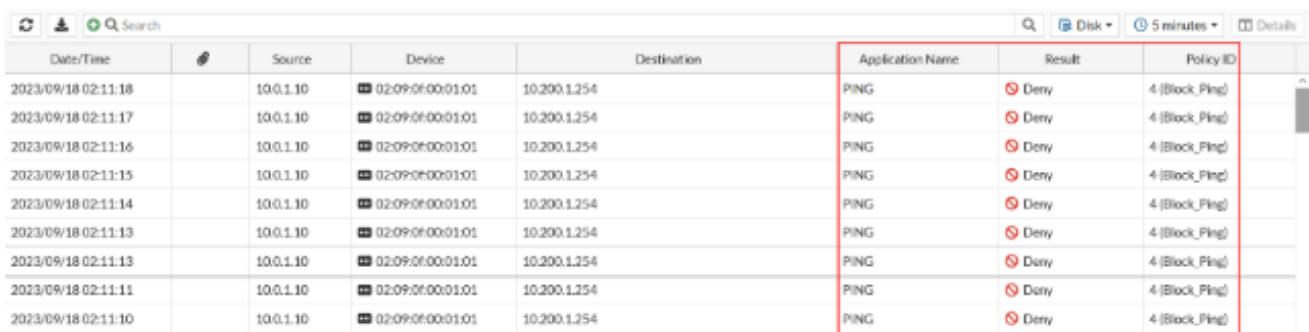
Test the Reordering of a Firewall Policy

Now that your configuration is ready, you will test it by moving the Block_Ping firewall policy above the Internet_Access firewall policy. The objective is to confirm that, after you 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 you 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.
6. Click the settings icon, scroll down to the Select Columns section, select the ID column, and then click Apply.
7. Drag the ID column to the left of the Name column, so it becomes the first column in the table.
8. In the ID column, drag the Block_Ping firewall policy up, and place it above the Internet_Access firewall policy.
9. On the Local-Client VM, review the terminal window that is running the continuous ping, You should see that the pings now fail.
10. Close the terminal window.
11. On the Local-FortiGate GUI, click Log & Report > Forward Traffic.



Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2023/09/18 02:11:18	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:17	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:16	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:15	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:14	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:13	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:13	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:11	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:10	10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)