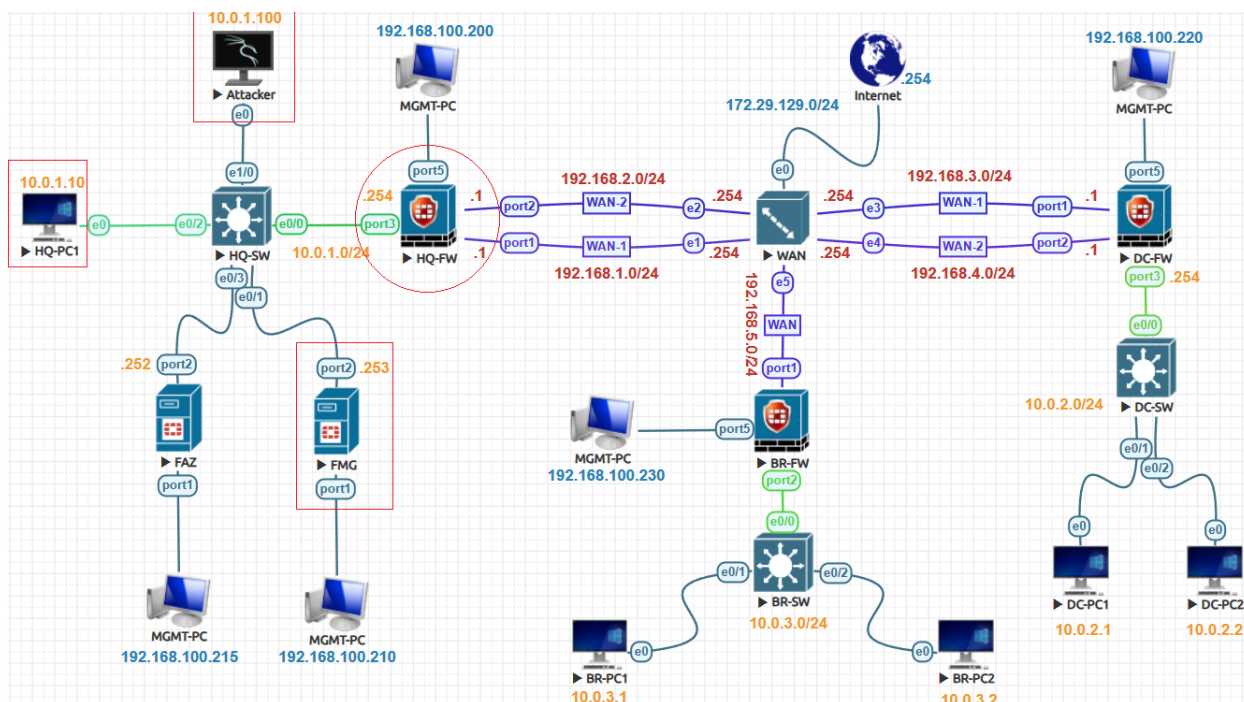


## Web Filter Profile Lab:



Go to **Policy & Objects > Object Configurations > Security Profiles > Web Filter** there are preloaded four predefined web filters.

**Policy & Objects**

Policy Package | Install | ADOM Revisions | Tools

Policy Packages >

**Object Configurations**

- Normalized Interface
- Firewall Objects
- Security Profiles
  - AntiVirus
  - Web Filter**

Name	Comments	Feature Set
default	Default web filtering.	Flow-based
sniffer-profile	Monitor web traffic.	Flow-based
wifi-default	Default configuration for offloading WiFi	Flow-based
monitor-all	Monitor and log all visited URLs, flow-ba	Flow-based

## Custom URL Filter:

To create URL filter, go to **Policy & Objects > Object Configurations > Security Profiles > Web Filter** and go to the **Static URL Filter** section. Enable **URL Filter**.

The screenshot shows the FortiGate web interface. The left sidebar has a tree view with 'Policy Packages' and 'Object Configurations'. Under 'Object Configurations', 'Web Filter' is selected. The main area shows a table of existing web filter profiles. A yellow box highlights the '+ Create New' button.

<input type="checkbox"/>	Name	Comments	Feature Set
<input type="checkbox"/>	default	Default web filtering.	Flow-based
<input type="checkbox"/>	sniffer-profile	Monitor web traffic.	Flow-based
<input type="checkbox"/>	wifi-default	Default configuration for offloading WiFi	Flow-based
<input type="checkbox"/>	monitor-all	Monitor and log all visited URLs, flow-ba:	Flow-based

### Create New Web Filter Profile

Name: Custom-WF

Comment:   
0/255

Feature Set: **Flow-based** Proxy-based

☐ FortiGuard Category Based Filter

☐ Allow Users to Override Blocked Categories

**Static URL Filter**

☐ Block Invalid URLs

☐ URL Filter

☐ Block Malicious URLs Discovered by FortiSandbox

☐ Web Content Filter

**Rating Options**

☐ Allow Websites When a Rating Error Occurs

☐ Rate URLs by Domain and IP Address

**Proxy Options**

HTTP POST Action: **Allow** Block

☐ Remove Cookies

Under URL Filter, click **Create New** to display New URL Filter pane. Enter **\*facebook.com**, select **Wildcard**, and select Action **Block** Also Status **Enable** finally, click **OK** button.

URL Filter Type	Description
Simple	FortiGate tries to strictly match the full context. <a href="http://www.facebook.com">www.facebook.com</a> in the URL field, it only matches traffic with <a href="http://www.facebook.com">www.facebook.com</a> . It won't match <a href="http://facebook.com">facebook.com</a> or <a href="http://message.facebook.com">message.facebook.com</a> .
Regular Expression or Wildcard	FortiGate tries to match the pattern based on the rules of regular expressions or wildcards. if enter <b>*fa*</b> in the URL field, it matches all the content that has fa such as <a href="http://www.facebook.com">www.facebook.com</a> , <a href="http://message.facebook.com">message.facebook.com</a> , <a href="http://fast.com">fast.com</a> , etc.

Action	Description
Block	Denies or blocks attempts to access any URL matching the URL pattern. FortiGate displays a replacement message.
Allow	The traffic is passed to the remaining FortiGuard web filters, web content filters, web script filters, antivirus proxy operations, and DLP proxy operations. If URL does not appear in the URL list, the traffic is permitted.
Monitor	Traffic is processed the same way as the Allow action. For the Monitor action, a log message is generated each time a matching traffic pattern.
Exempt	Traffic is allowed to bypass the remaining FortiGuard web filters, web content filters, web script filters, antivirus scanning, DLP proxy operations

☒ URL Filter

Select an URL Filter

[Create New]

+ Add   Edit   Delete   Move Up   Move Down				
<input type="checkbox"/>	#	URL	Type	Action
<input checked="" type="checkbox"/>	1	*facebook.com	wildcard	block

Continue on the FortiManager GUI, click **Policy Packages**, Click **HQ-FW>Firewall Policy**. Select the first policy at the top of the list, and then click **Edit**.

Policy & Objects   Policy Package   Install   ADOM Revisions   Tools					
+ Create New   Edit   Delete   Section   Policy Lookup   Collapse All					
<input type="checkbox"/>	#	Name	From	To	Source
<input type="checkbox"/>	1	LAN-to-WAN	LAN-Port	WAN1-Port WAN2-Port	all
<input type="checkbox"/>	▼ Implicit (2-2 / Total: 1)				
<input type="checkbox"/>	2	Implicit Deny	any	any	all all

Click the Security Profiles check box. Configure **Web Filter Profile** and SSL/SSH Inspection and click **OK**.

**Security Profiles**



Profile Type

AntiVirus Profile

Web Filter Profile

Application Control

IPS Profile

DNS Filter

SSL/SSH Inspection

Decrypted Traffic Mirror

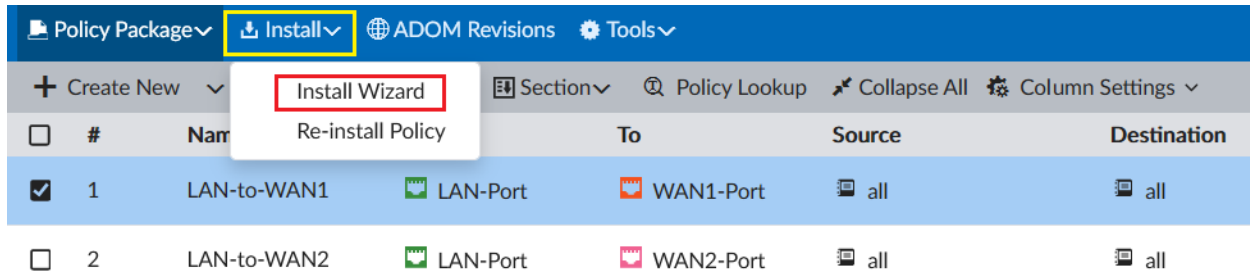
Use Standard Security Profiles

Use Security Profile Group

default	✕
default	✕
+	
+	
+	
deep-inspection	✕
+	

## Install the Policy:

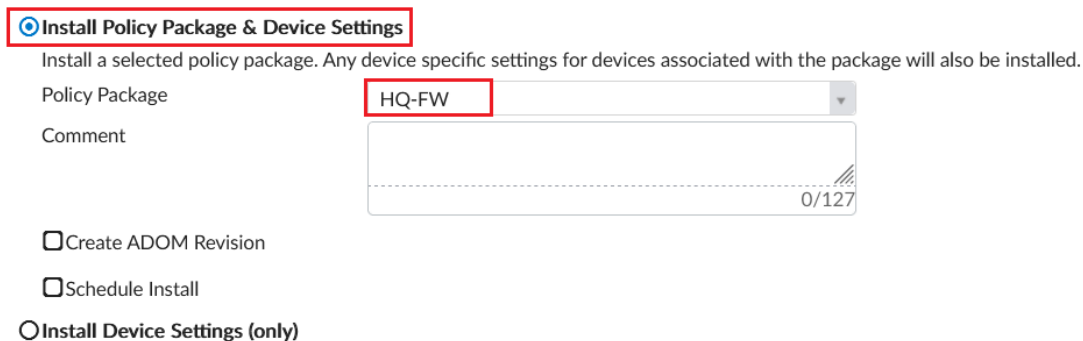
Continue on the FortiManager GUI, click **Install>Install Wizard**.



	#	Name	To	Source	Destination
<input checked="" type="checkbox"/>	1	LAN-to-WAN1	LAN-Port	WAN1-Port	all
<input type="checkbox"/>	2	LAN-to-WAN2	LAN-Port	WAN2-Port	all

Select Install Policy Package & Device Settings. Conform that the HQ-FW policy package is selected. And then click **Next**.

### Install Wizard



☒ **Install Policy Package & Device Settings**

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: **HQ-FW**

Comment:

☐ Create ADOM Revision

☐ Schedule Install


☐ Install Device Settings (only)

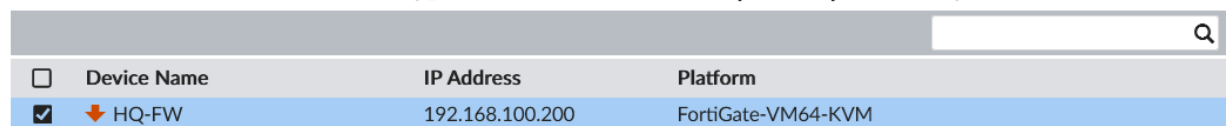
Next >

Cancel

Confirm that the **HQ-FW** device is selected, and then click **Next**.

### Install Wizard - Policy Package and Device Setting (HQ-FW)

Please select one or more devices to install (  Use checkbox or Ctrl or Shift key for multiple selections)



<input type="checkbox"/>	Device Name	IP Address	Platform
<input checked="" type="checkbox"/>	HQ-FW	192.168.100.200	FortiGate-VM64-KVM


< Back




Next >




Cancel

Click Install Preview to see changes that will be applied to FortiGate. Click Close on the Install Preview page. Click **Install**.

## Install Wizard - Policy Package (HQ-FW)

Installation Preparation Total: 3/3,  Success: 3,  Warning: 0,  Error: 0 

-  Interface Validation
-  Policy and Object Validation
-  Ready to Install.









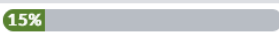
 Install Preview  Policy Package Diff			
<input type="checkbox"/>	Device Name	Status	Action
<input checked="" type="checkbox"/>	HQ-FW[root]	 Connection Up	

Install

Cancel

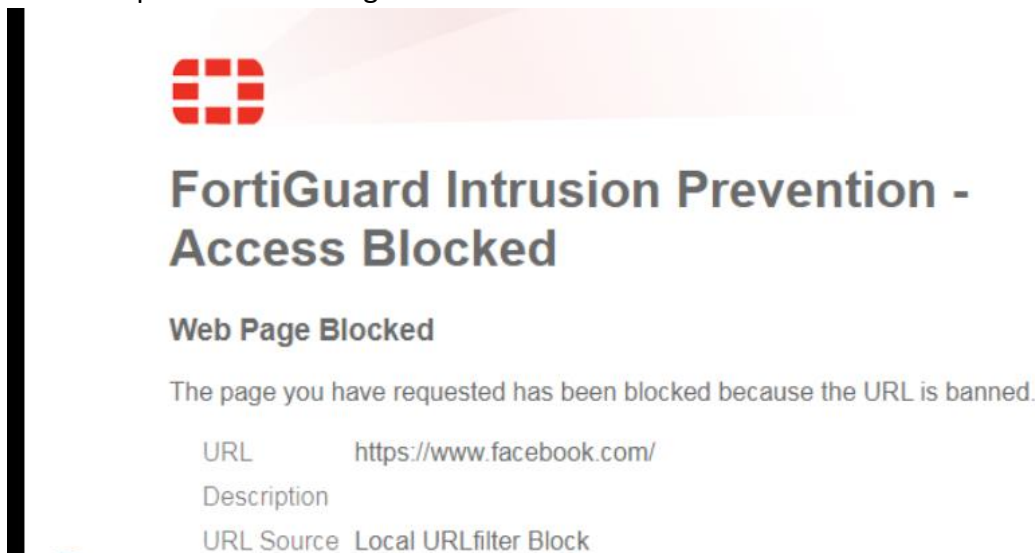
Once done click **Finish**.

## Install Wizard - Policy Package (HQ-FW)

22%			
Total: 0/1,  Pending: 0,  In Progress: 1,  Completed: 0 			
 View Installation Log  View Progress Report  Column Settings ▾			Search... 
#	Name	Time Used	Status
1	HQ-FW	N/A	 15%

## Verification & Testing:

Validate the URL filter results by going to a blocked website. Go to the **Facebook** website, you see the replacement message.



To check web filter logs in the GUI, Go to **Log & Report > Web Filter**.

		<div> Add Filter</div>		
Date/Time	User	Source	Action	URL
47 minutes ago		10.0.1.10	blocked	https://www.facebook.com/
51 minutes ago		10.0.1.10	blocked	https://www.facebook.com/
51 minutes ago		10.0.1.10	blocked	https://www.facebook.com/
52 minutes ago		10.0.1.10	blocked	https://www.facebook.com/favicon.ico
52 minutes ago		10.0.1.10	blocked	https://www.facebook.com/

All FortiGate ▾ Last 1 Hour ▾ 10:37:57 To 11:37:56								
<input type="button" value="Add Filter"/>								
#	▼ Date/Time	Device ID	User	Source	Destination IP	Service	Host Name	Action
1	11:36:49	FGVM01TM23...		10.0.1.10	31.13.69.35	HTTPS	www.facebook.c...	blocked
2	11:36:47	FGVM01TM23...		10.0.1.10	31.13.69.35	HTTPS	www.facebook.c...	blocked
3	11:36:47	FGVM01TM23...		10.0.1.10	31.13.69.35	HTTPS	www.facebook.c...	blocked
4	11:36:36	FGVM01TM23...		10.0.1.10	31.13.69.35	HTTPS	www.facebook.c...	blocked
5	11:36:36	FGVM01TM23...		10.0.1.10	31.13.69.35	HTTPS	www.facebook.c...	blocked
6	10:48:36	FGVM01TM23...		10.0.1.10	31.13.69.35	HTTPS	www.facebook.c...	blocked
7	10:44:22	FGVM01TM23...		10.0.1.10	31.13.69.35	HTTPS	www.facebook.c...	blocked
8	10:44:21	FGVM01TM23...		10.0.1.10	31.13.69.35	HTTPS	www.facebook.c...	blocked