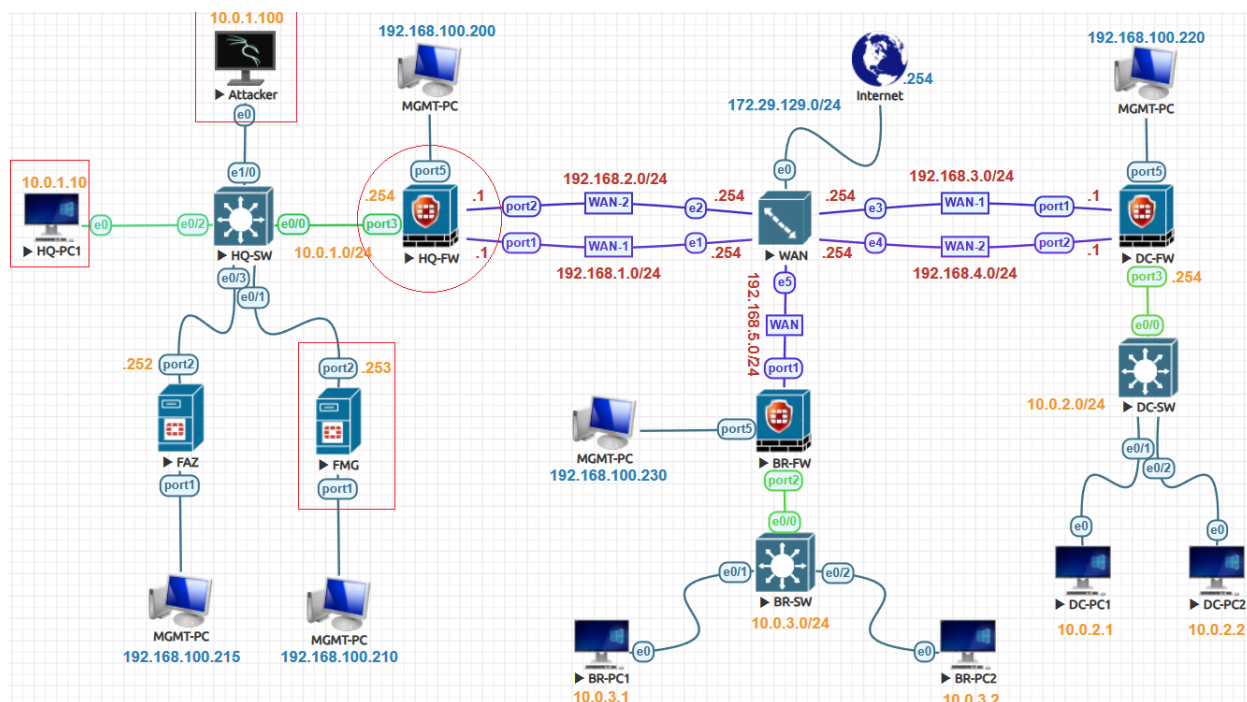



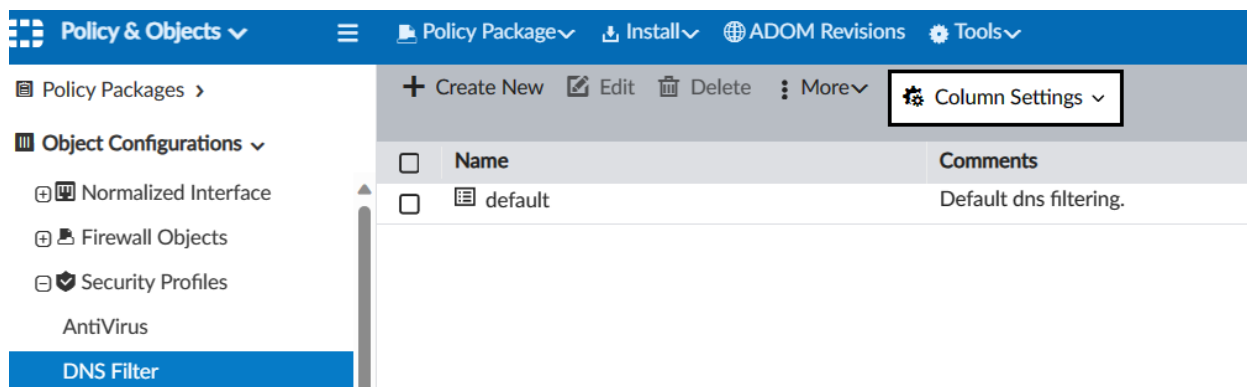
DNS Filter Lab:



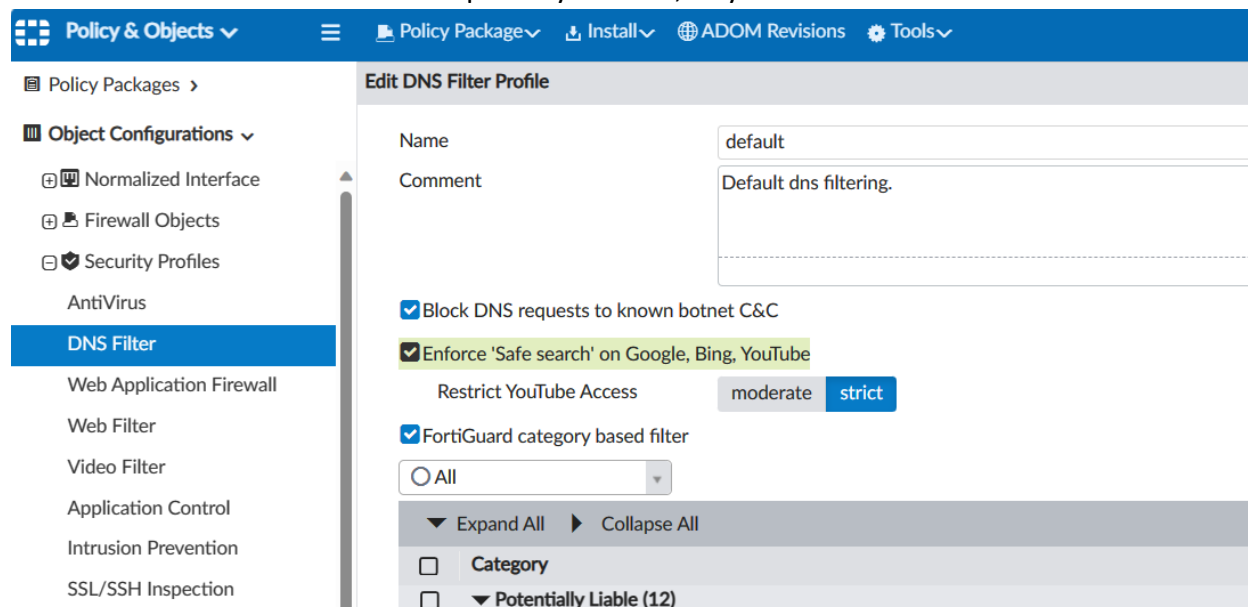
Go to **Policy & Objects > Object Configurations > Security Profiles > DNS Filter**. You can **Create New** and also there are four preloaded DNS Filter profiles to use.

Display Options

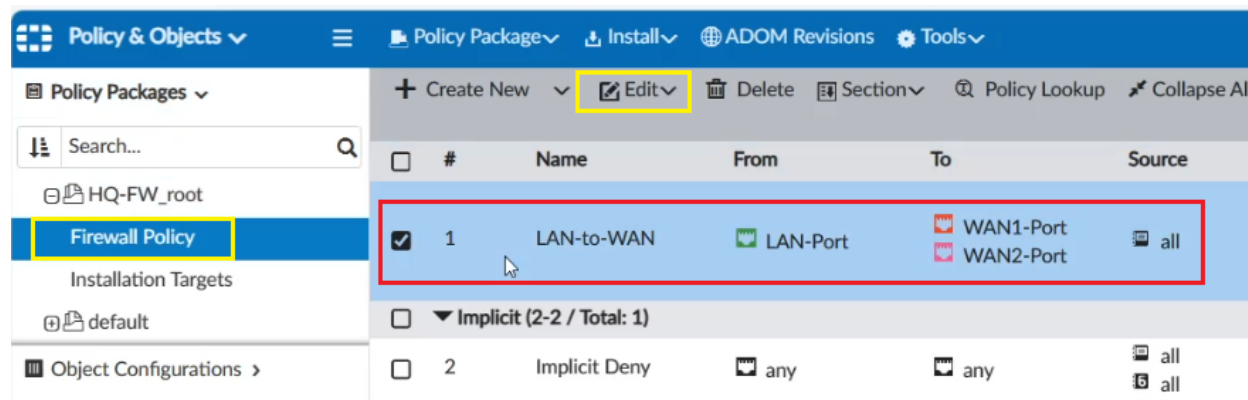
	<input checked="" type="checkbox"/> Iramic Snapers <input type="checkbox"/> Virtual Servers <input type="checkbox"/> Web Proxy Forwarding Server <input type="checkbox"/> ZTNA Server	<input checked="" type="checkbox"/> Snapping Promie <input type="checkbox"/> Health Check <input type="checkbox"/> Authentication Scheme <input type="checkbox"/> ZTNA Tag
<input checked="" type="checkbox"/>  Security Profiles	<input checked="" type="checkbox"/> AntiVirus <input checked="" type="checkbox"/> Web Application Firewall <input checked="" type="checkbox"/> Video Filter <input checked="" type="checkbox"/> Intrusion Prevention	<input checked="" type="checkbox"/> DNS Filter <input checked="" type="checkbox"/> Web Filter <input checked="" type="checkbox"/> Application Control <input type="checkbox"/> Email Filter



Go to **Policy & Objects > Object Configurations > Security Profiles > DNS Filter**, you can modify the default DNS Filter and enable the options you want, or you can create a new DNS Filter.



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**.



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

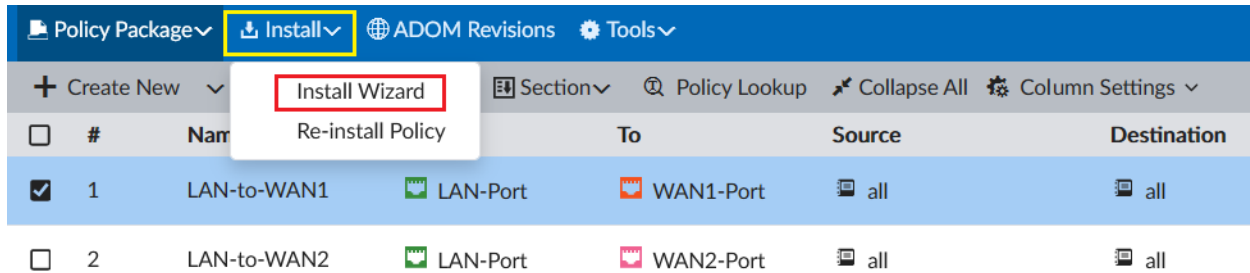
Security Profiles ☒

Profile Type

	Use Standard Security Profiles	Use Security Profile Group
AntiVirus Profile		+
Web Filter Profile		+
Application Control		+
IPS Profile	Custom-IPS	✕
DNS Filter	default	✕
SSL/SSH Inspection	deep-inspection	✕
Decrypted Traffic Mirror		+

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)

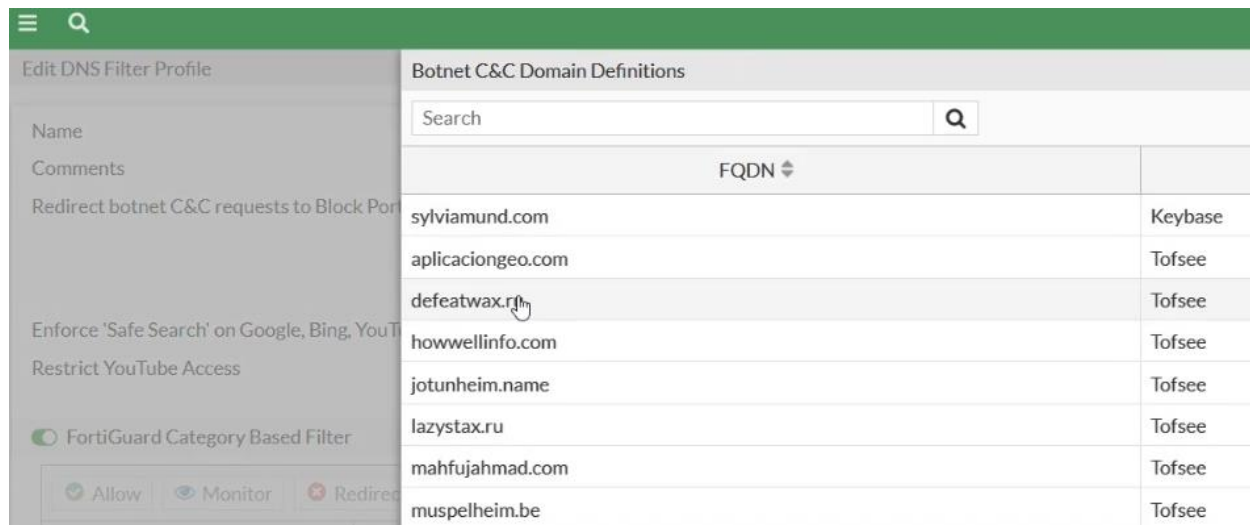
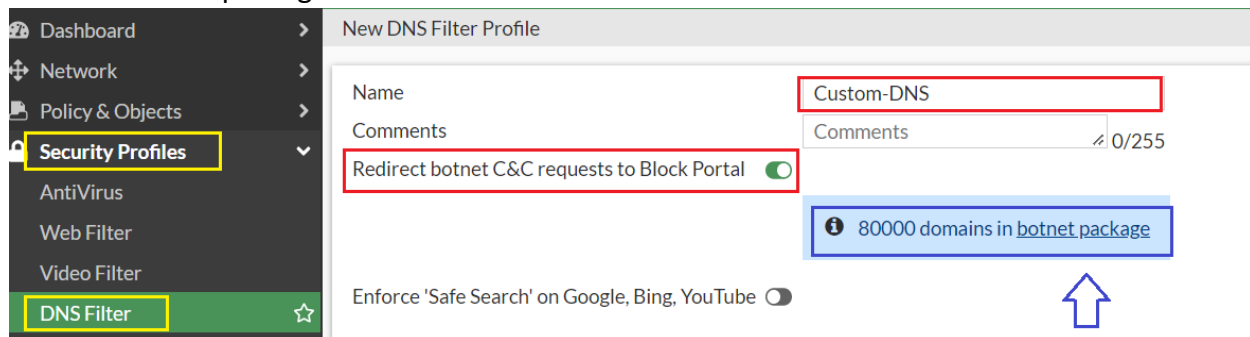
22%

Total: 0/1,  Pending: 0,  In Progress: 1,  Completed: 0 

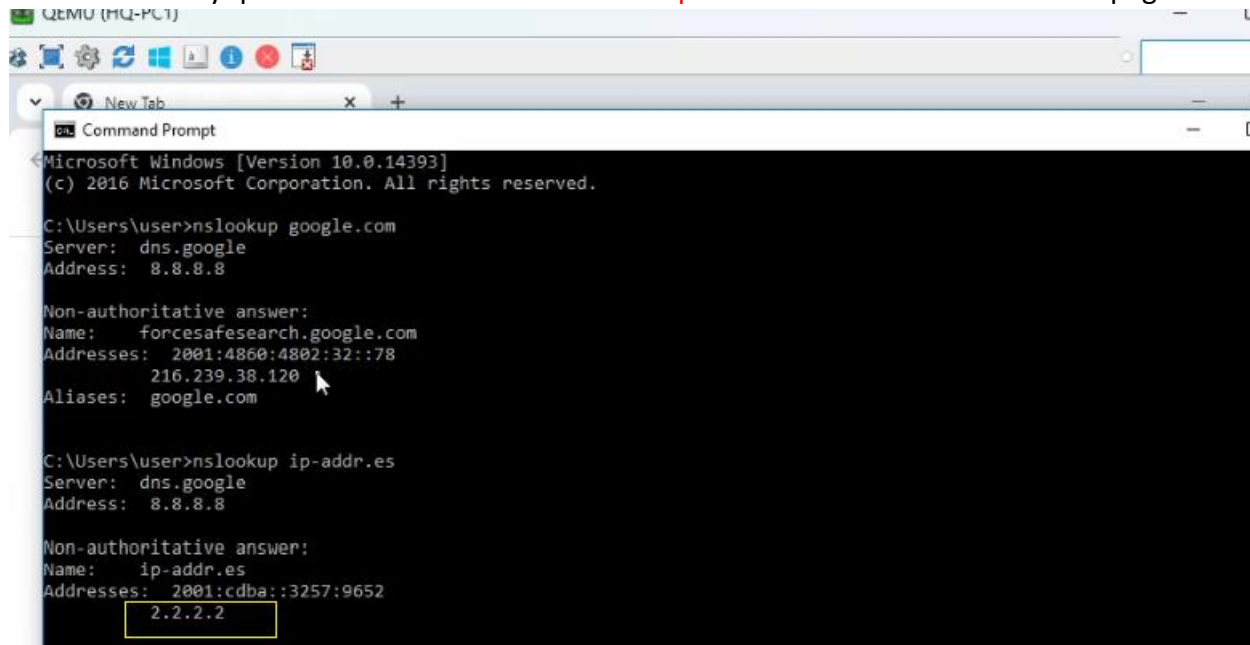
 View Installation Log  View Progress Report  Column Settings 			
#	Name	Time Used	Status
1	HQ-FW	N/A	 15%

Test and Verify:

Click the botnet package link to see the latest botnet C&C domain list.



Visit botnet fully qualified Domain name or **nslookup** DNS it will show below error in page.



Go to **Log & Report > DNS Query** to view the DNS traffic that just traverse the FortiGate and the FortiGuard rating for this domain name.

Date/Time	DNS Type	Source	Domain Name	Query Type
9 seconds ago	dns-response	10.0.1.10	webegen.com	AAAA
10 seconds ago	dns-response	10.0.1.10	webegen.com	A
Minute ago	dns-response	10.0.1.10	ip-addr.es	AAAA
Minute ago	dns-response	10.0.1.10	ip-addr.es	A
Minute ago	dns-response	10.0.1.10	google.com	AAAA
Minute ago	dns-response	10.0.1.10	google.com	A

Date/Time	DNS Type	Source	Domain Name	Query Type	Policy ID	Log Details
20 seconds ago	dns-response	10.0.1.10	webegen.com	AAAA	LAN-to-WAN (1)	<div>Destination</div> <div>IP 8.8.8.8</div> <div>Port 53</div> <div>Country/Region United States</div> <div>Destination Interface WAN-2 (port2)</div> <div>Application Control</div> <div>Protocol 17</div> <div>Data</div> <div>Message Domain was blocked by dns botnet C&C</div> <div>Action</div> <div>Action redirect</div> <div>Policy ID LAN-to-WAN (1)</div> <div>Policy b1661a18-a08e-51ee-62d8-15384ae5bb59</div> <div>Policy Type Firewall</div> <div>Security</div> <div>Level ■■■■■</div> <div>DNS</div> <div>Domain Name webegen.com</div> <div>Query Type AAAA</div>
21 seconds ago	dns-response	10.0.1.10	webegen.com	A	LAN-to-WAN (1)	
Minute ago	dns-response	10.0.1.10	ip-addr.es	AAAA	LAN-to-WAN (1)	
Minute ago	dns-response	10.0.1.10	ip-addr.es	A	LAN-to-WAN (1)	
Minute ago	dns-response	10.0.1.10	google.com	AAAA	LAN-to-WAN (1)	
Minute ago	dns-response	10.0.1.10	google.com	A	LAN-to-WAN (1)	

In FortiAnalyzer, navigate to Log **View>FortiGate>Security>DNS**.

#	▼Date/Time	Sub Type	Policy ID	Source	Domain Name
1	16:43:02	dns	1	10.0.1.10	webegen.com
2	16:43:00	dns	1	10.0.1.10	webegen.com
3	16:42:02	dns	1	10.0.1.10	ip-addr.es
4	16:42:00	dns	1	10.0.1.10	ip-addr.es
5	16:41:38	dns	1	10.0.1.10	google.com
6	16:41:38	dns	1	10.0.1.10	google.com