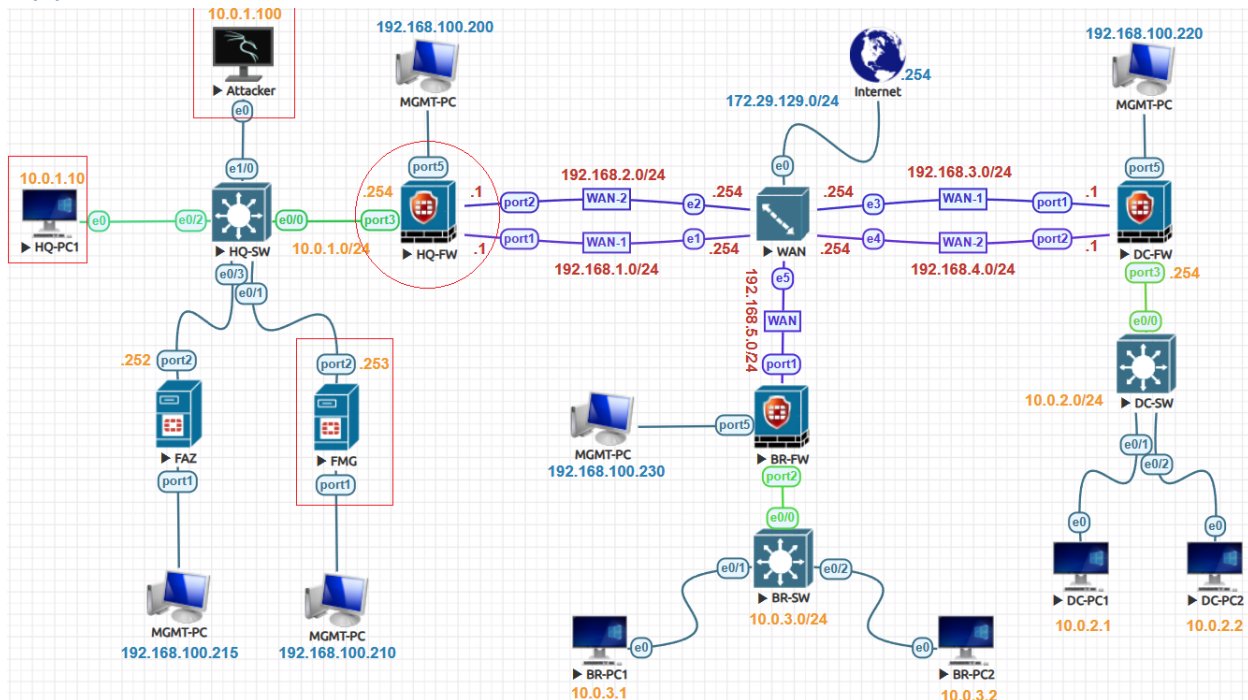


Application Control Lab:



Verify updated Application Control signatures and database navigate to **System>FortiGuard**.

Firmware & General Updates Application Control Signatures Device & OS Identification Internet Service Database Definitions	Licensed (Expiration Date: 2022/07/25) Version 20.00319 Version 1.00135 Version 7.02423	Actions
--	--	---------

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

Policy & Objects | Policy Package | Install | ADOM Revisions | Tools

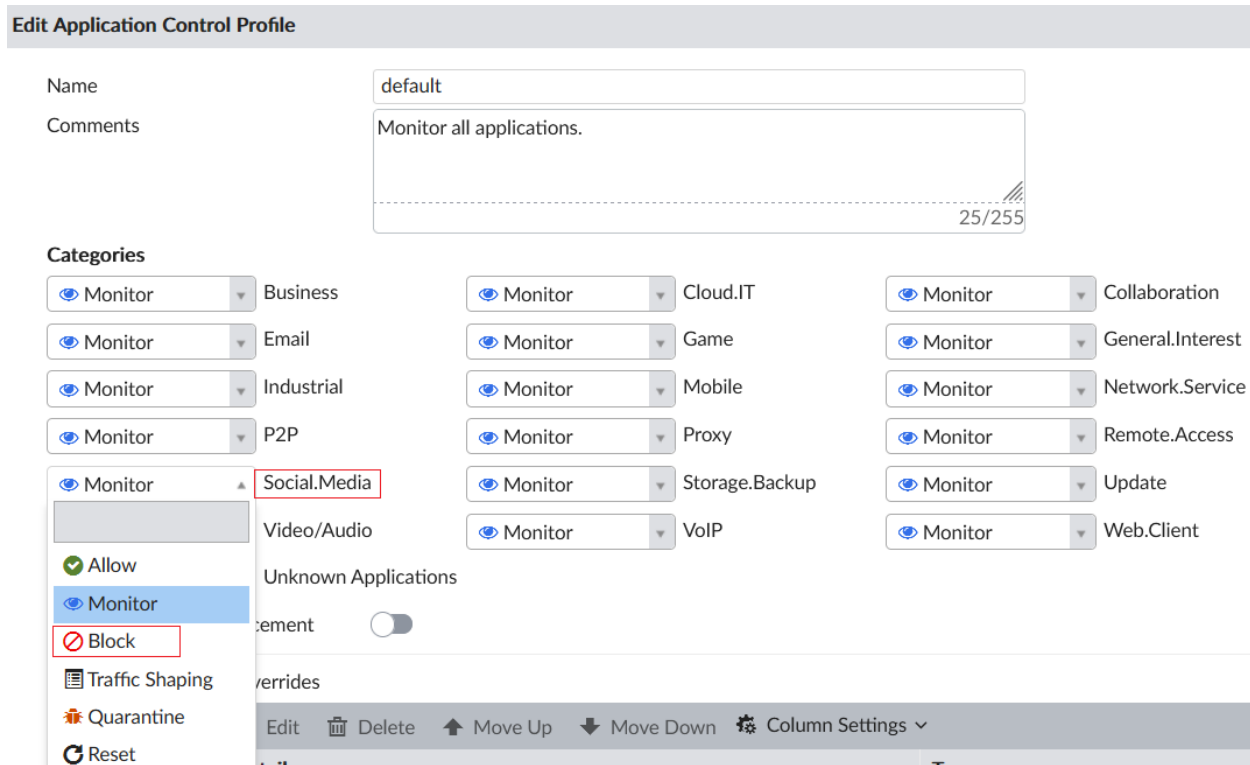
Object Configurations

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

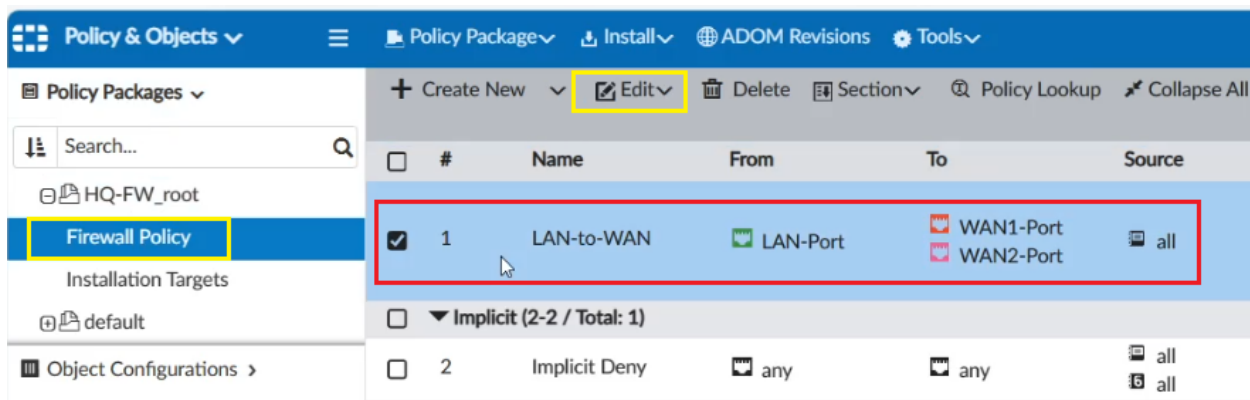
Name	Comments
block-high-risk	
default	Monitor all applications.
sniffer-profile	Monitor all applications.
wifi-default	Default configuration for

Application Control Category:

Go to **Policy & Objects > Object Configurations > Security Profiles > Application Control**. Under Categories, left click the icon next to the category name to view a dropdown of actions, Allow, Monitor, Block, Quarantine, and View signatures and Select **OK**. In this case let's **Block Social Media**.



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 **Application Profile** and SSL/SSH Inspection and click **OK**.

Edit Firewall Policy

Disclaimer Options

Display Disclaimer ☐

Security Profiles ☒

Profile Type **Use Standard Security Profiles** **Use Security Profile Group**

AntiVirus Profile

Web Filter Profile

Application Control

IPS Profile

DNS Filter

SSL/SSH Inspection

Decrypted Traffic Mirror

Traffic Shaping Options

Shared Shaper

Reverse Shaper

Per-IP Shaper

Logging Options

Log Allowed Traffic **No Log** **Log Security Events** **Log All Sessions**

☐ Capture Packets

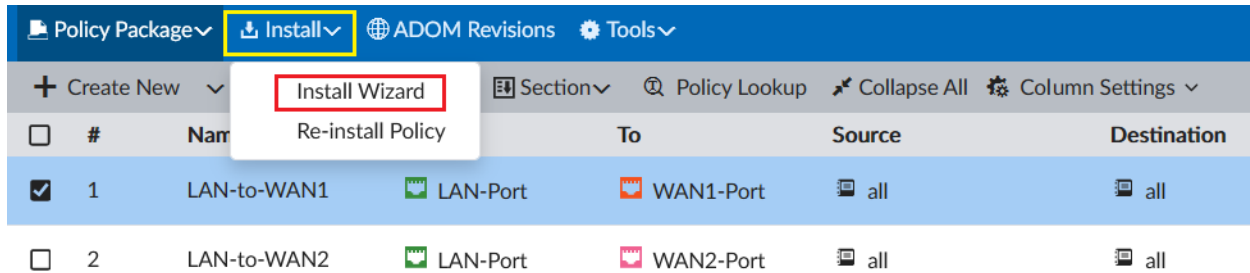
☐ Generate Logs when Session Starts

Advanced

OK **Cancel**

Install the Policy:

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



#	Name	To	Source	Destination
1	LAN-to-WAN1	LAN-Port	WAN1-Port	all
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)

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="text" value=""/>
<input type="checkbox"/>	Device Name	Status	Action
<input checked="" type="checkbox"/>	HQ-FW[root]	Connection Up	

Install

Cancel

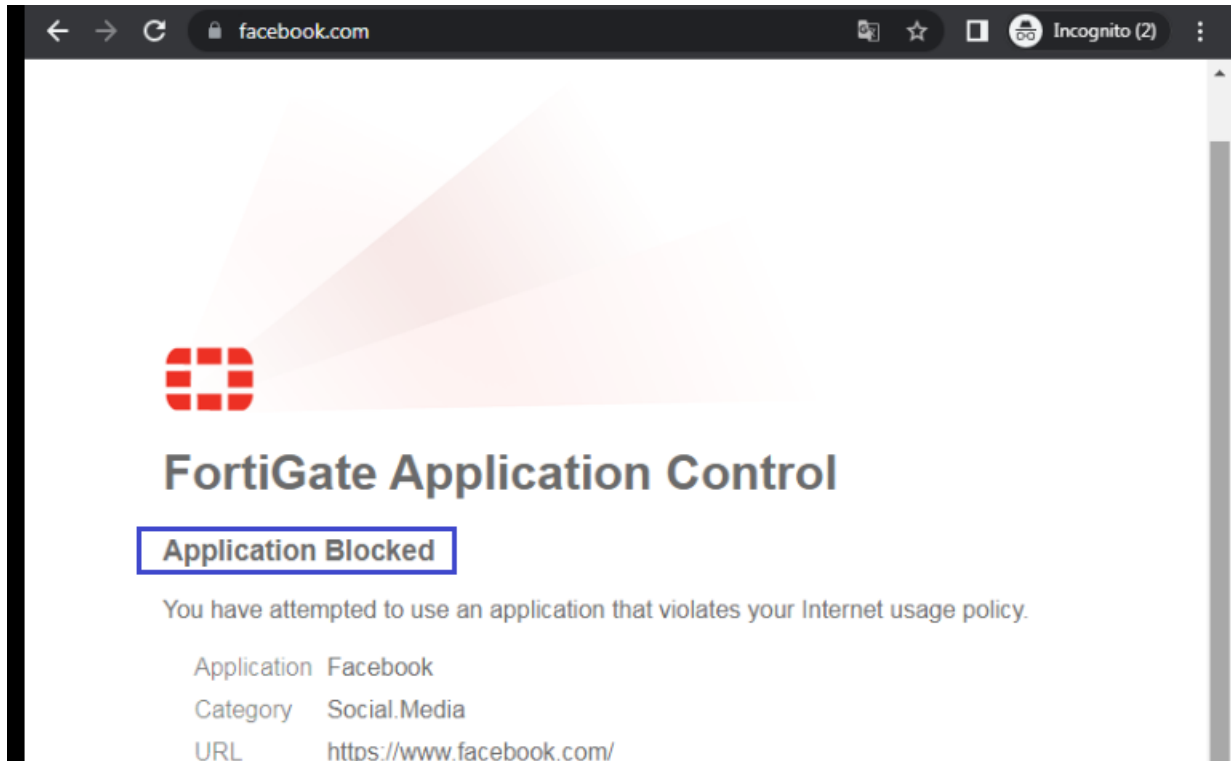
Once done click **Finish**.

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			<input type="text" value="Search..."/>
#	Name	Time Used	Status
1	HQ-FW	N/A	15%

Verification & Testing:

Go to **Facebook** website, you will see the replacement message display.



To check Application Control logs in the GUI, Go to **Log & Report > Application Control**.

Add Filter						
Date/Time		Source	Destination	Application Name	Action	
20 seconds ago		10.0.1.10	31.13.69.174 (z-p42-instagram.c10r.instagram.com)	Instagram	block	
32 seconds ago		10.0.1.10	142.250.200.238 (play.google.com)	HTTPS.BROWSER	pass	
32 seconds ago		10.0.1.10	142.250.200.238 (play.google.com)	HTTPS.BROWSER	pass	
32 seconds ago		10.0.1.10	104.244.42.129 (twitter.com)	Twitter	block	
32 seconds ago		10.0.1.10	104.244.42.129 (twitter.com)	Twitter	block	
32 seconds ago		10.0.1.10	104.244.42.129 (twitter.com)	Twitter	block	
44 seconds ago		10.0.1.10	173.194.76.84 (accounts.google.com)	Google.Accounts	pass	
44 seconds ago		10.0.1.10	173.194.76.84 (accounts.google.com)	SSL	pass	
44 seconds ago		10.0.1.10	142.251.37.238 (www.google-analytics.com)	HTTPS.BROWSER	pass	
44 seconds ago		10.0.1.10	173.194.76.84 (accounts.google.com)	Google.Accounts	pass	
45 seconds ago		10.0.1.10	2.19.24.68 (e2885.e9.akamaiedge.net)	HTTPS.BROWSER	pass	
45 seconds ago		10.0.1.10	199.232.16.157 (static.ads-twitter.com)	Twitter	block	
45 seconds ago		10.0.1.10	104.244.42.69 (t.co)	HTTPS.BROWSER	pass	
45 seconds ago		10.0.1.10	152.199.21.141 (cs510.wpc.edgecastcdn.net)	Twitter	block	
52 seconds ago		10.0.1.10	31.13.69.35 (facebook.com)	Facebook	block	
Minute ago		10.0.1.253	208.184.237.67	HTTPS.BROWSER	pass	
Minute ago		10.0.1.10	172.217.18.46 (apis.google.com)	HTTPS.BROWSER	pass	

To check Application Control logs in the GUI, Go to **Log & Report > Forward Traffic**.

<div> <div> <div></div> <div></div> </div> <div> <div>Application Name: twitter</div> <div>OR NOT EXACT</div> <div>Add Filter</div> </div> </div>						
Date/Time		Source	Device	Destination	Application Name	Result
5 hours ago		10.0.1.10	DESKTOP-W10	199.232.16.157 (static.ads-twitter.com)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	151.101.8.157 (platform.twitter.map.fastly.net)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	151.101.8.157 (platform.twitter.map.fastly.net)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	151.101.8.157 (platform.twitter.map.fastly.net)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	199.232.16.157 (static.ads-twitter.com)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	199.232.16.157 (static.ads-twitter.com)	Twitter	1.68 kB / 6.22 kB
5 hours ago		10.0.1.10	DESKTOP-W10	104.244.42.1 (twitter.com)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	104.244.42.67 (s.twitter.com)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	104.244.42.193 (twitter.com)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	104.244.42.193 (twitter.com)	Twitter	Deny: UTM Blocked
5 hours ago		10.0.1.10	DESKTOP-W10	104.244.42.193 (twitter.com)	Twitter	Deny: UTM Blocked

In FortiAnalyzer, navigate to **Log View>FortiGate>Application Control**.

<div> <div>Log View</div> <div></div> </div>											
<div> <div>Fabric</div> <div>All</div> <div>FortiGate</div> <div>Traffic</div> <div>Security</div> <div>Antivirus</div> <div>Application Control</div> <div>Web Filter</div> <div>Event</div> <div>FortiAnalyzer</div> <div>Log Browse</div> <div>Log Group</div> </div>											
<div> <div>All FortiGate</div> <div>Last 1 Hour</div> <div>11:15:34 To 12:15:33</div> </div>											
<div>Add Filter</div>											
#	Date/Time	Level	Device ID	Source	User	Group	Profile	Destination Port	Destination IP	Service	
1	12:14:35	warn	FGVM01...	10.0.1...				443	31.13.69.174	SSL	
2	12:14:23	inform	FGVM01...	10.0.1...				443	142.250.20...	SSL	
3	12:14:23	inform	FGVM01...	10.0.1...				443	142.250.20...	SSL	
4	12:14:23	warn	FGVM01...	10.0.1...				443	104.244.42...	SSL	
5	12:14:23	warn	FGVM01...	10.0.1...				443	104.244.42...	SSL	
6	12:14:22	warn	FGVM01...	10.0.1...				443	104.244.42...	SSL	
7	12:14:13	inform	FGVM01...	10.0.1...				443	173.194.76...	SSL	
8	12:14:11	inform	FGVM01...	10.0.1...				443	173.194.76...	HTTPS	
9	12:14:11	inform	FGVM01...	10.0.1...				443	142.251.37...	SSL	
10	12:14:11	inform	FGVM01...	10.0.1...				443	173.194.76...	SSL	
11	12:14:10	inform	FGVM01...	10.0.1...				443	2.19.24.68	SSL	
12	12:14:10	warn	FGVM01...	10.0.1...				443	199.232.16...	SSL	
13	12:14:10	inform	FGVM01...	10.0.1...				443	104.244.42...	SSL	
14	12:14:10	warn	FGVM01...	10.0.1...				443	152.199.21...	SSL	
15	12:14:05	warn	FGVM01...	10.0.1...				443	31.13.69.35	SSL	
16	12:13:50	inform	FGVM01...	10.0.1...				443	208.184.23...	SSL	
17	12:13:30	inform	FGVM01...	10.0.1...				443	172.217.18...	SSL	
18	12:13:27	warn	FGVM01...	10.0.1...				443	31.13.69.174	SSL	
19	12:13:27	inform	FGVM01...	10.0.1...				443	31.13.69.174	SSL	
20	12:13:26	warn	FGVM01...	10.0.1...				443	31.13.69.174	SSL	
21	12:13:26	inform	FGVM01...	10.0.1...				443	142.251.37...	SSL	
22	12:13:26	inform	FGVM01...	10.0.1...				443	142.250.20...	SSL	