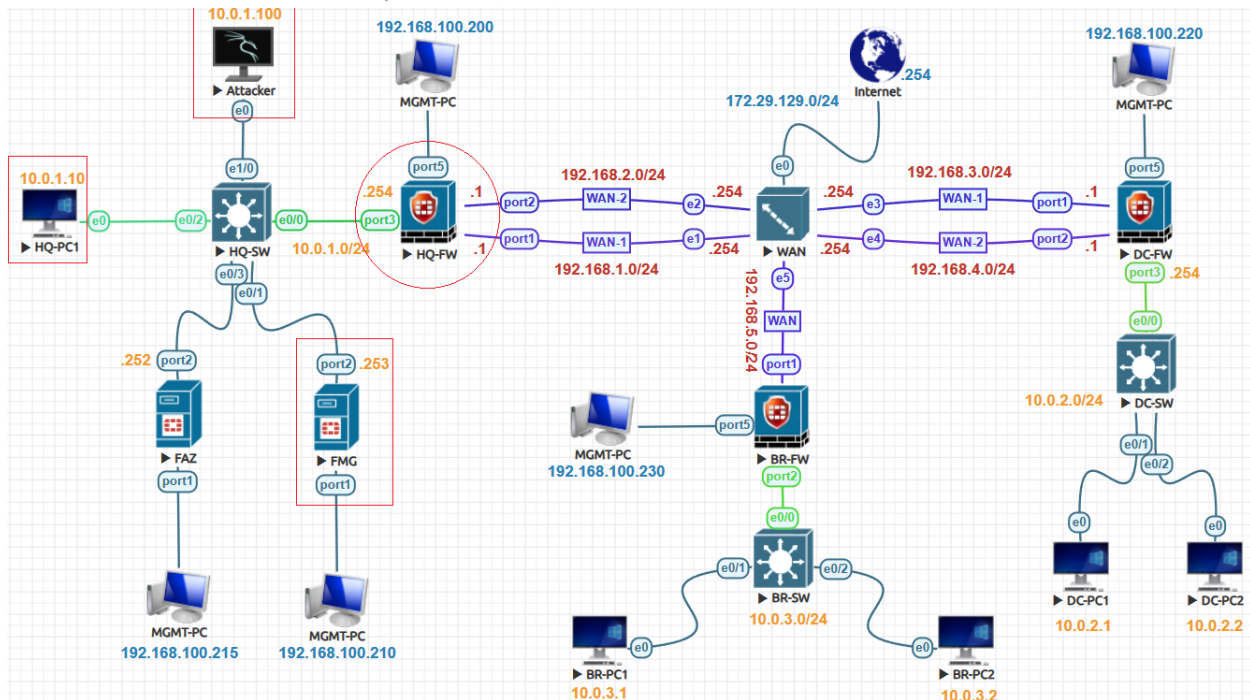


Intrusion Prevention System (IPS) Lab:



Block Malicious URL:

Block Malicious URLs, Go to **Policy & Objects > Object Configurations > Security Profiles > Intrusion Prevention**. Edit an existing sensor or create a new one. Enable **Block malicious URLs**. Configure other settings as needed. Click **OK**.

Policy & Objects

Policy Package

Install

ADOM Revisions

Tools

Policy Packages

Object Configurations

Normalized Interface

Firewall Objects

Security Profiles

AntiVirus

Web Filter

Application Control

Intrusion Prevention

Create New

Edit

Delete

More

Column Settings

Name	Comments
all_default	All predefined signatures with
all_default_pass	All predefined signatures with
default	Prevent critical attacks.
high_security	Blocks all Critical/High/Medi
protect_client	Protect against client-side vul
protect_email_server	Protect against email server-s
protect_http_server	Protect against HTTP server-
sniffer-profile	Monitor IPS attacks.

Create New IPS Sensor

Name: Custom-IPS

Comments:
 0/255

Block malicious URLs: ☐

IPS Signatures and Filters

+ Create New

<input type="checkbox"/>	Details	Exempt IPs	Action	Packet Logging
No record found.				

Botnet C&C

Scan Outgoing Connections to Botnet Sites: Block Disable Monitor

Advanced Options >

Deviation

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					
<div> <div>Policy Packages</div> <div> <div>Search...</div> <div>HQ-FW_root</div> <div>Firewall Policy</div> <div>Installation Targets</div> <div>default</div> </div> <div>Object Configurations</div> </div>					
<div> <div>Create New</div> <div>Edit</div> <div>Delete</div> <div>Section</div> <div>Policy Lookup</div> <div>Collapse All</div> </div>					
<input type="checkbox"/>	#	Name	From	To	Source
<input checked="" type="checkbox"/>	1	LAN-to-WAN	LAN-Port	<div>WAN1-Port</div> <div>WAN2-Port</div>	all
<input type="checkbox"/>	▼ Implicit (2-2 / Total: 1)				
<input type="checkbox"/>	2	Implicit Deny	any	any	all

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

Security Profiles



Profile Type

Use Standard Security Profiles

Use Security Profile Group

AntiVirus Profile

 default 

Web Filter Profile



Application Control

 g-default 

IPS Profile

 all_default 


DNS Filter



SSL/SSH Inspection

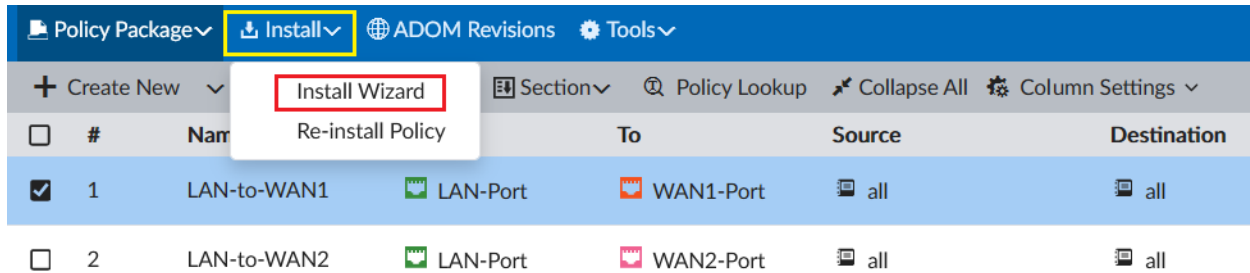
 deep-inspection 

Decrypted Traffic Mirror



Install the Policy:

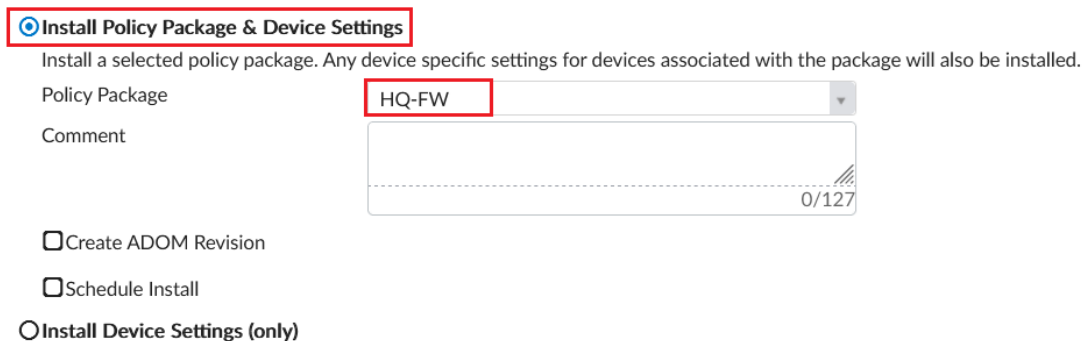
Continue on the FortiManager GUI, click **Install>Install Wizard**.



#	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)

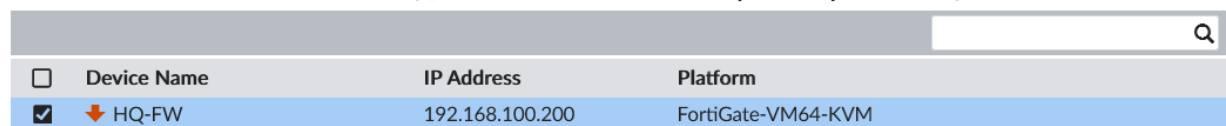
Next >

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

Install





Cancel

Once done click **Finish**.

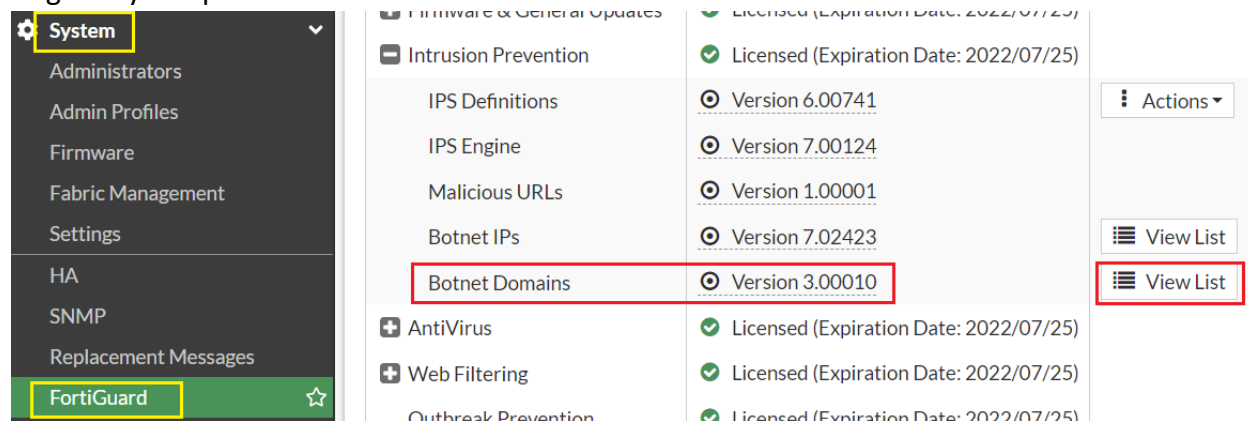
Install Wizard - Policy Package (HQ-FW)

22%

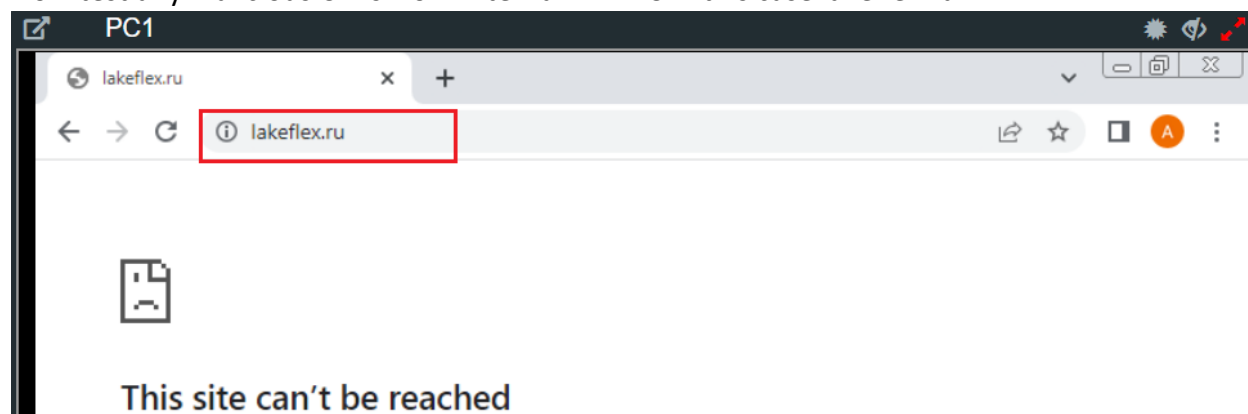
Total: 0/1,  Pending: 0,  In Progress: 1,  Completed: 0 

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

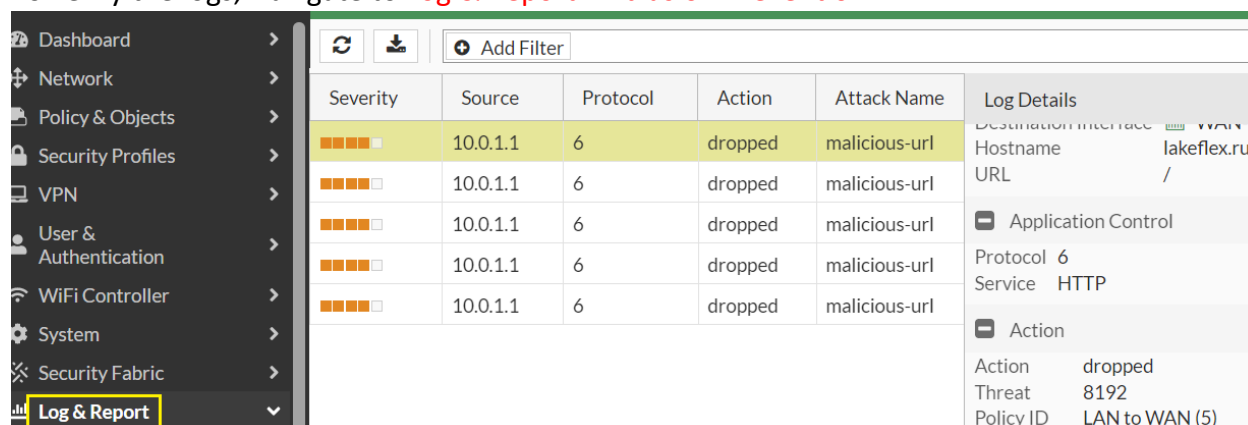
Navigate to **System>FortiGuard** click on Intrusion Prevention **Botnet Domains** and click **View List** to get any sample Malicious URLs from the list to test in Internal LAN PC.



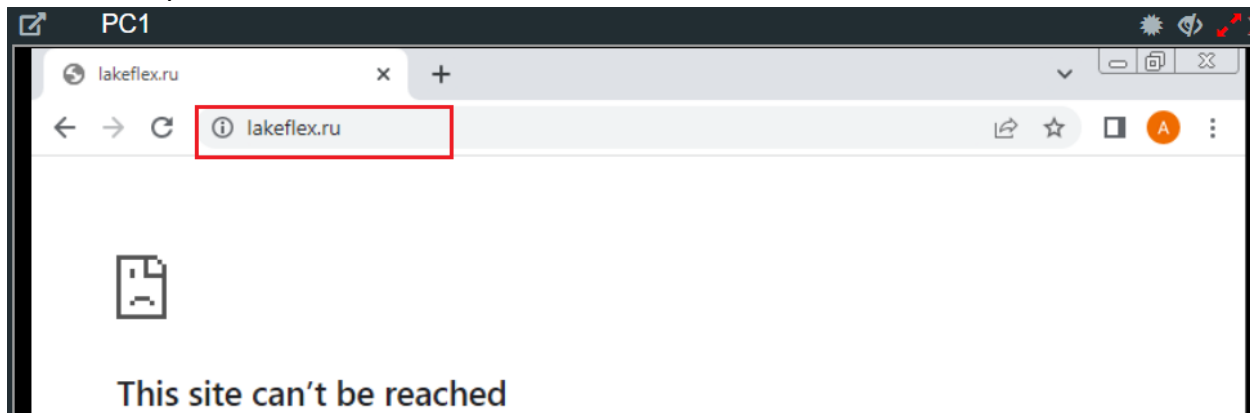
Now test any malicious URLs from Internal LAN PC in this case lakeflex.ru



To verify the logs, Navigate to **Log & Report >Intrusion Prevention**.



Now test any malicious URLs from Internal LAN PC in this case lakeflex.ru



To verify the logs, Navigate to **Log & Report > Forward Traffic**.

	Date/Time	Source	Device	Destination	Result
	8 seconds ago	10.0.1.1	USER-PC	208.91.112.55	Deny: UTM Blocked
	57 seconds ago	10.0.1.1	USER-PC	8.8.8.8 (dns.google)	73 B / 89 B
	Minute ago	10.0.1.1	USER-PC	108.177.15.188 (mtalk.google.co...)	2.61 kB / 18.97 kB
	Minute ago	10.0.1.1	USER-PC	142.250.201.10 (ajax.googleapis....)	2.25 kB / 4.11 kB
	3 minutes ago	10.0.1.1	USER-PC	142.250.203.227 (clientservices....)	1.72 kB / 2.67 kB
	3 minutes ago	10.0.1.1	USER-PC	142.250.201.10 (ajax.googleapis....)	Deny: UTM Blocked
	3 minutes ago	10.0.1.1	USER-PC	108.177.15.188 (mtalk.google.co...)	2.61 kB / 18.81 kB
	4 minutes ago	10.0.1.1	USER-PC	8.8.8.8 (dns.google)	75 B / 91 B
	5 minutes ago	10.0.1.1	USER-PC	142.250.203.227 (clientservices....)	1.62 kB / 2.36 kB

Botnet C&C IP Blocking:

To configure botnet C&C IP blocking, Go to **Policy & Objects > Object Configurations > Security Profiles > Intrusion Prevention**. Edit an existing sensor or create a new one. Navigate to the **Botnet C&C** section. For Scan Outgoing Connections to Botnet Sites, click **Block** or **Monitor**.

Configure other settings as needed.

Click **Apply**. Botnet C&C is now enabled for the sensor. Add this sensor to the firewall policy.

Edit IPS Sensor

Name: all_default

Comments: All predefined signatures with default setting.

Block malicious URLs: ☐

IPS Signatures and Filters

	Details	Exempt IPs	Action
<input type="checkbox"/>		0	Default

Botnet C&C

Scan Outgoing Connections to Botnet Sites: **Block** | Disable | Monitor

Advanced Options

Now test any Botnet C&C IP from Internal LAN PC in this case 1.123.37.68

PC1

1.123.37.68

← → ↻ ⓘ 1.123.37.68

Telnet 1.123.37.68

```
C:\Users\user>telnet 1.123.37.68 80
Connecting To 1.123.37.68...
```


To verify the logs, Navigate to **Log & Report > Intrusion Prevention**.

Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
55 seconds ago		■■■■■	10.0.1.10	6		dropped		DCRat
55 seconds ago		■■■■■	10.0.1.10	6		dropped		DCRat
55 seconds ago		■■■■■	10.0.1.10	6		dropped		DCRat
5 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
5 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
5 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
6 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
6 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
6 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
7 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
7 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
7 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
7 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat
7 minutes ago		■■■■■	10.0.1.10	6		dropped		DCRat

In FortiAnalyzer, navigate to **Log View>FortiGate>Intrusion Prevention**

All FortiGate - Last 1 Hour - 12:04:34 To 13:04:33							
Add Filter							
#	▼ Date/Time	Device ID	Severity	Source	Destination IP	Action	Service
1	13:03:23	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
2	13:03:23	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
3	13:03:23	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
4	12:58:25	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
5	12:58:25	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
6	12:58:20	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
7	12:57:30	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
8	12:57:29	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
9	12:57:29	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
10	12:57:05	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
11	12:57:05	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
12	12:57:05	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
13	12:56:42	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP
14	12:56:41	FGVM01TM230059...	critical	10.0.1.10	2.59.119.56	dropped	HTTP