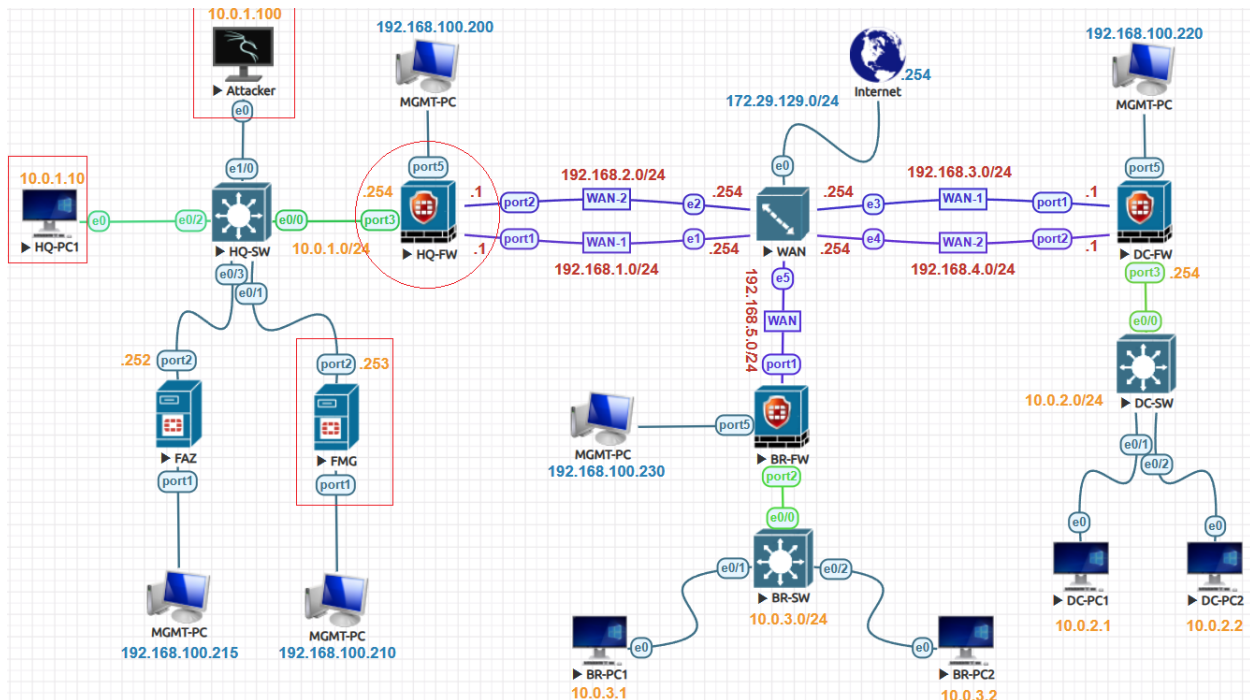


## IPS Filters Lab:



## IPS Filters:

Let's create IPS Filters to add All Severity level to block. Go to **Policy & Objects > Object Configurations > Security Profiles > Intrusion Prevention**. Edit an existing sensor or create a new one. In the IPS Signatures and Filters section, click **Create New**. Select the Type to Filter, Action Block, Packet logging Enable, set the status to enable while in Filter choose all Severity Level and click **OK**.

### IPS Signatures and Filters

+ Create New				
<input type="checkbox"/>	Details	Exempt IPs	Action	Packet Logging
<input type="checkbox"/>		0	Default	Disabled

### Create New IPS Signatures and Filters

Type: **Filter** Signature

Action: **Default**

Packet Logging: **Enable** Disable

Status: **Enable** Disable Default

Filter: **+ Add Filter**

Advanced Options >

## Add Filter

☐ Severity = Information
 ☐ Severity = Low
 ☐ Severity = Medium
 ☐ Severity = High
 ☐ Severity = Critical

Column Settings ▾

ID	Name	On-Hold Until	Severity
▼ Custom IPS Signature (0)			
▼ IPS Signature (16825)			
47306	10-Strike.LANState.Local.Buffer.Overflow.Exploit		medium
25536	1024CMS.Standard.PHP.File.Inclusion		high

## Add Filter

☐ Severity = Information
 ☐ Severity = Low
 ☐ Severity = Medium
 ☐ Severity = High
 ☐ Severity = Critical

Column Settings ▾ View Packages ▾

ID	Name	On-Hold Until	Severity	Target	OS	Default Ac	CV
▼ Custom IPS Signature (0)							
▼ IPS Signature (16825)							
47306	10-Strike.LANState.Local.Buffer.Overflow.Exploit		medium	server,client	Windows	⊘ block	
25536	1024CMS.Standard.PHP.File.Inclusion		high	server	Windows, Linux, BSD, Solaris, macOS	⊘ block	
28273	2Wire.Wireless.Router.XSRF.Password.Reset		medium	server,client	Linux	⊘ block	CV
52796	3CX.DesktopApp.SupplyChain.Backdoor		critical	server	Windows, macOS	⊘ block	CV
43545	3CX.Phone.System.VAD_Deploy.Arbitrary.File.Upload		high	server	Windows	⊘ block	
30316	3Com.3CDAemon.FTP.Server.Buffer.Overflow		high	server	Windows	⊘ block	CV
10174	3Com.3CDAemon.FTP.Server.Information.Disclosure		low	client	Windows	⊘ block	CV
26815	3Com.Intelligent.Management.Center.Information.Disclosure		medium	server	Windows	⊘ block	
27309	3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS		medium	server	Linux	⊘ block	
48622	3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution		high	server	Linux	⊘ block	

Version: 26.701 DB: Regular, Extended, Inc

Export to CSV

Check On-Hold Status

Use Filters

Finally, IPS Filters has been created to Block all Severity levels.

## IPS Signatures and Filters

<input type="checkbox"/>	Details	Exempt IPs	Action	Packet Logging
<input type="checkbox"/>	Eicar.Virus.Test.File	0	⊘ Block	✅ Enabled
<input checked="" type="checkbox"/>	Severity: info low medium high critical	0	⊘ Block	⊘ Disabled

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 Package▼ Install▼ ADOM Revisions Tools▼						
+ Create New ▼ Edit▼ Delete Section▼ Policy Lookup Collapse All Column Settings ▼						
<input type="checkbox"/>	#	Name	From	To	Source	Destination
<input checked="" type="checkbox"/>	1	LAN-to-WAN1	LAN-Port	WAN1-Port	all	all
<input type="checkbox"/>	2	LAN-to-WAN2	LAN-Port	WAN2-Port	all	all
<input type="checkbox"/>	▼ Implicit (3-3 / Total: 1)					
<input type="checkbox"/>	3	Implicit Deny	any	any	all	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

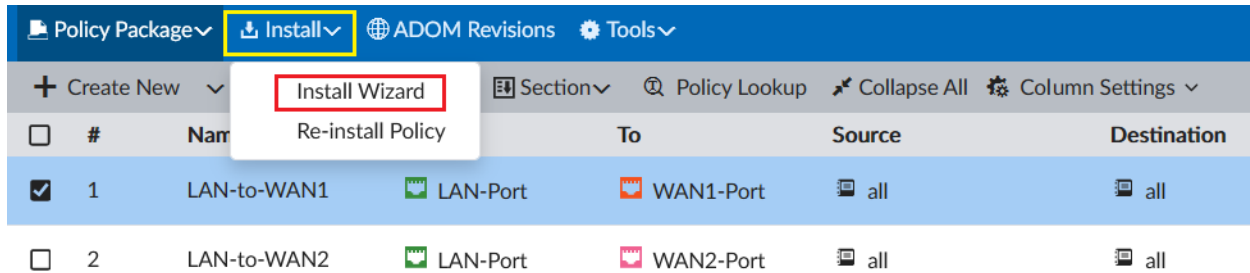
deep-inspection

Decrypted Traffic Mirror



## Install the Policy:

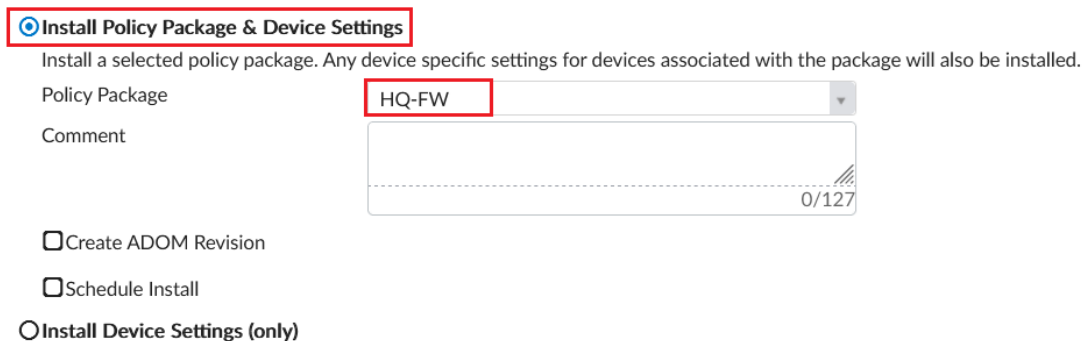
Continue on the FortiManager GUI, click **Install>Install Wizard**.



#	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)

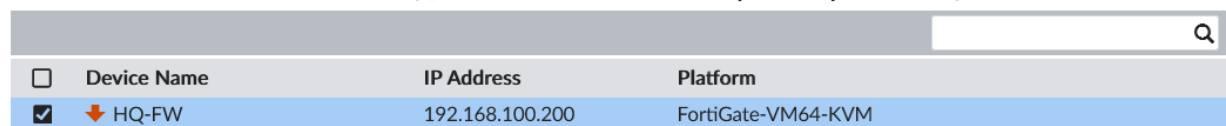
Next >

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%

## Verification & Testing:

To validate the IPS results by going to internal Attacker System and run nmap and nikto commands to generate attack on outside system. **Nmap -A 192.168.1.254** and **Nikto -host 192.168.1.254**

```
Attacker
root@kali:~# nmap -A 192.168.1.254
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-27 06:44 EDT

root@kali:~# nikto -host 192.168.1.254
- Nikto v2.1.6
```

Go to **Log & Report > Intrusion Prevention** to view the log.

Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner
19 seconds ago		■ ■ ■ ■	10.0.1.100	6		dropped		Nmap.ScriptScanner

Go to **Log & Report > Forward Traffic** to view the log.

Date/Time		Source	Device	Destination	Application Name	Result
37 seconds ago		10.0.1.100	kali	192.168.1.254	HTTPS	Deny: UTM Blocked
37 seconds ago		10.0.1.100	kali	192.168.1.254	HTTPS	Deny: UTM Blocked
38 seconds ago		10.0.1.10	DESKTOP-W10	40.81.120.44 (win10.ipv6.microsoft.com)	MMS	62.30 kB / 94.80 kB
38 seconds ago		10.0.1.100	kali	192.168.1.254	tcp/264	60 B / 0 B
38 seconds ago		10.0.1.100	kali	192.168.1.254	tcp/1247	60 B / 0 B

▼ Date/Time	Device ID	Severity	Source	Destination IP	Action	Service
14:16:57	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:57	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:57	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:57	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:56	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:56	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:50	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:50	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:50	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:49	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP
14:16:49	FGVM01TM230059...	low	10.0.1.100	192.168.1.254	dropped	HTTP