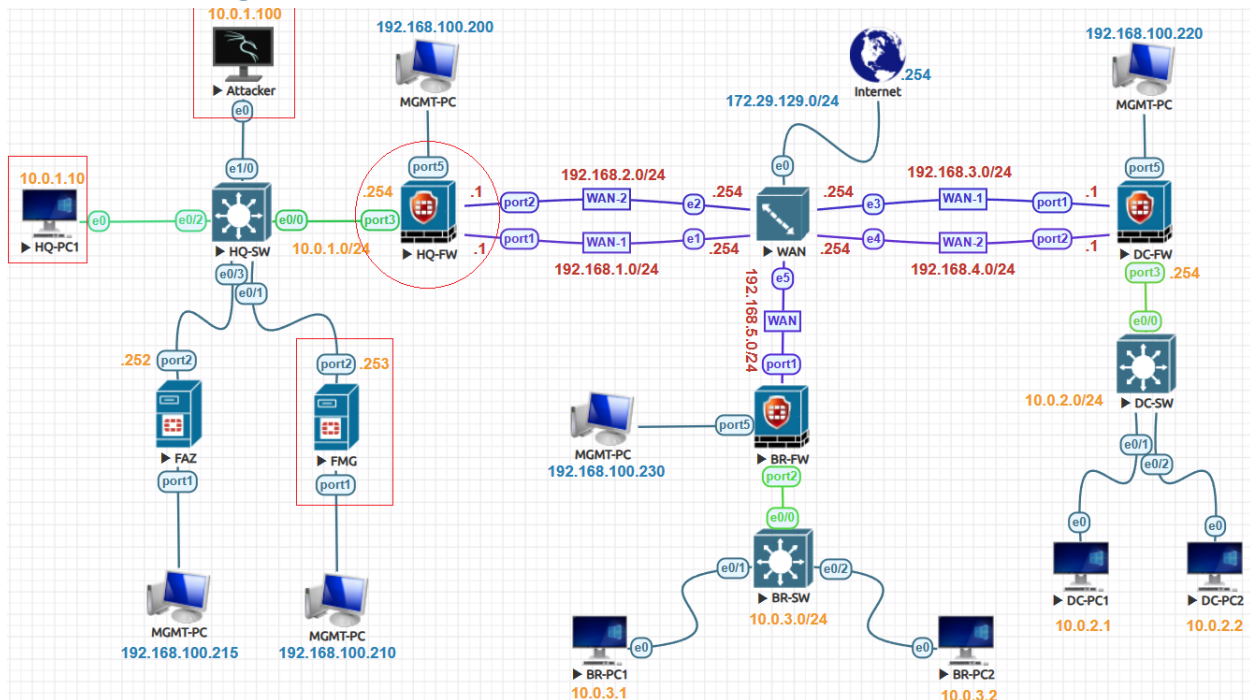


IPS Custom Signature Lab:





IPS Custom Signature:

Add IPS signatures to a sensor, 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**.

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
Rate-based Setting	Default Specify
Exempt IPs	0  Edit
Signatures	<div> + Add Signature  Delete </div>
<div>OK</div>	

A list of available signatures appears. Select the **signatures** you want to include from the list. Click **Add Selected**.

Add Signatures

Add Filter				
⚙️ Column Settings ▾		📁 View Packages ▾ eic 🔍		
<input type="checkbox"/>	ID	Name	Severity	On-Hold Until
<input type="checkbox"/>	▼ IPS Signature (16816)			
<input checked="" type="checkbox"/>	29844	Eicar.Virus.Test.File	info	
<input type="checkbox"/>	46589	Foxit.Reader.Annotations.noteicon.Use.After.Free	high	
<input type="checkbox"/>	48314	KDE.KConfig.Dreictory.ICON.File.Remote.Code.Injection	high	
<input type="checkbox"/>	13839	Knusperleicht.ShoutBox.Remote.File.Inclusion	low	

Version: 26.696 DB: Regular, Extended, Industrial Total: 5

Export to CSV

Check On-Hold Status

Use Selected Signatures

Cancel

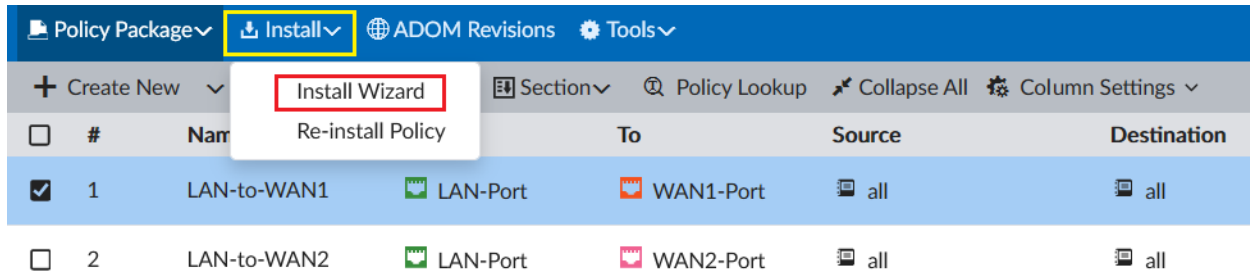
Finally, IPS Signature is added which action is blocked and logging is enabled.

IPS Signatures and Filters

+ Create New 📄 🗑️ ⬆️ ⬇️ ⚙️ ▾				
<input type="checkbox"/>	Details	Exempt IPs	Action	Packet Logging
<input type="checkbox"/>		0	🛡️ Default	🚫 Disabled
<input type="checkbox"/>	Eicar.Virus.Test.File	0	🛡️ Default	✅ Enabled

Install the Policy:

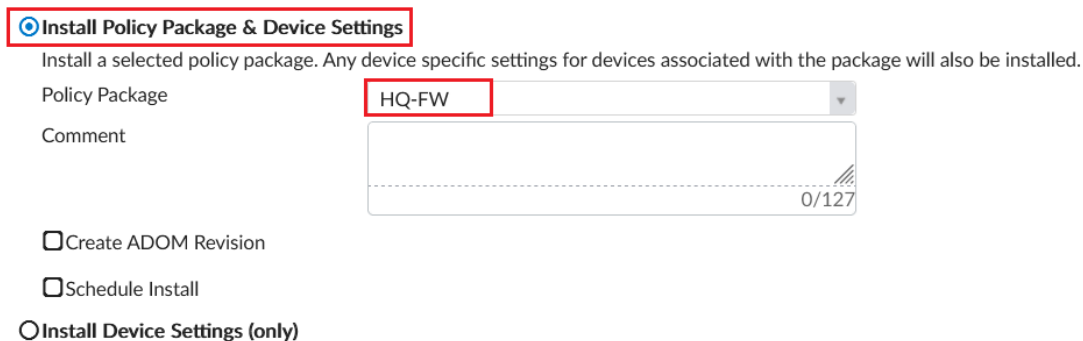
Continue on the FortiManager GUI, click **Install>Install Wizard**.



	#	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)

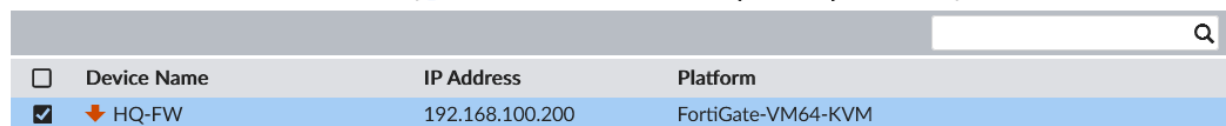
Next >

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.





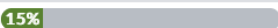
 Install Preview	 Policy Package Diff	
<input type="checkbox"/> Device Name	Status	Action
<input checked="" type="checkbox"/> HQ-FW[root]	 Connection Up	

Install

Cancel

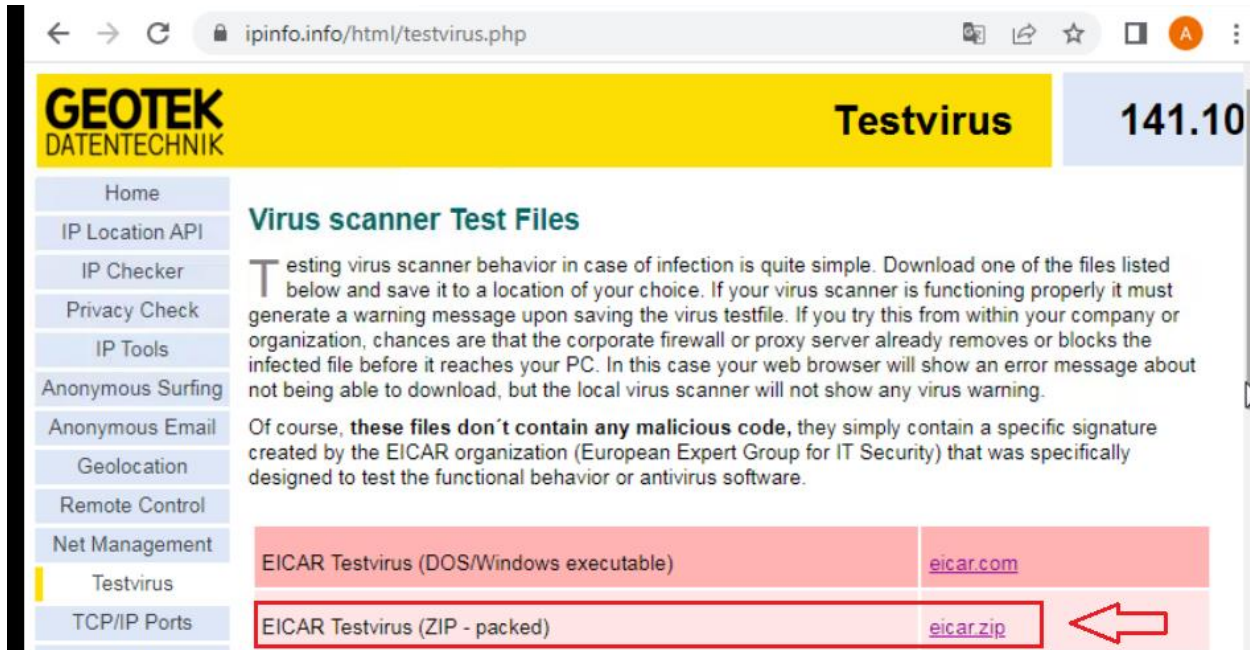
Once done click **Finish**.

Install Wizard - Policy Package (HQ-FW)

22%			
Total: 0/1,  Pending: 0,  In Progress: 1,  Completed: 0 			
#	Name	Time Used	Status
1	HQ-FW	N/A	 15%

Verification and Testing:

Try to visit ipinfo.info/html/testvirus.php and click to download EICAR TestVirus ZIP file.



File Name	Download Link
EICAR Testvirus (DOS/Windows executable)	eicar.com
EICAR Testvirus (ZIP - packed)	eicar.zip



FortiGate Intrusion Prevention

Intrusion Prevention Triggered

Your attempt to access the Internet resource is blocked by Intrusion Prevention.

URL <https://meineipadresse.de/testvirus/eicar.zip>

Navigate to **Log & Report > Intrusion Prevention**

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
18 seconds ago	■■■■■	10.0.1.10	6		dropped		Eicar.Virus.Test.File
52 seconds ago	■■■■■	10.0.1.10	6		dropped		Eicar.Virus.Test.File
10 minutes ago	■■■■■	10.0.1.10	6		dropped		DCRat