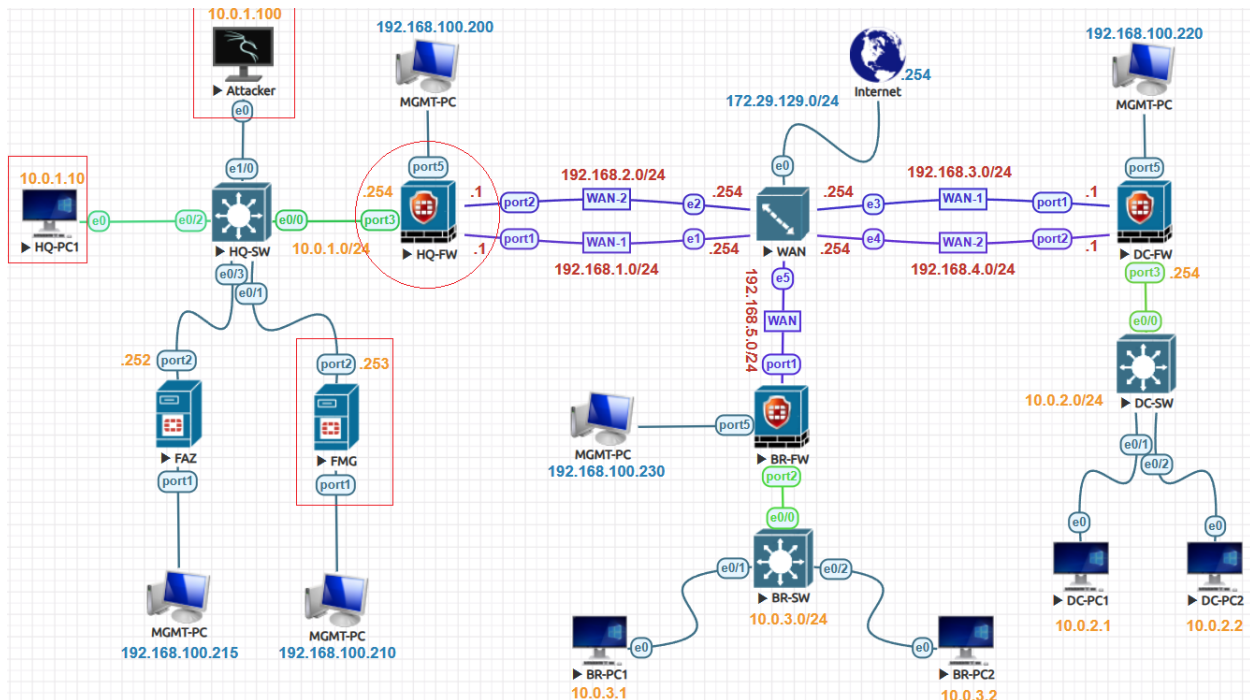


File Filter Lab:



Configure the Filter Profile:

Go to **Policy & Objects > Object Configurations > Security Profiles > File Filter Profile** and click **Create New**. Select a **Feature set**. In the Rules table, click **Create New**. Configure the settings as required.

+ Create New Edit Delete More		Create New File Filter Profile	
<input type="checkbox"/>	Name	Comments	Custom-File
<input type="checkbox"/>	default		
<input type="checkbox"/>	sniffer-profile		
Scan archive contents		<input checked="" type="checkbox"/>	
Feature Set		<div>Flow-based</div> <div>Proxy-based</div>	

Edit File Filter Profile

Name

Comments

Scan archive contents ☒

Feature Set Flow-based Proxy-based

Rules

<div><div><div>+ Create New</div><div> Edit</div><div> Delete</div><div> Move Up</div><div> Move Down</div></div><div><div> Column Settings</div><div>Search...</div><div></div></div></div>							
<input type="checkbox"/>	Rule	Comment	Traffic	Protocol	Match Files	Action	File Types
<input type="checkbox"/>	Block-PDF		any	CIFS, FTP, HTTP, IMAP, POP3, SMTP	any	block	pdf

Create New Rules

Name

Comments

Protocol

CIFS

FTP

HTTP

IMAP

MAPI

POP3

SMTP

SSH

8 entries selected

Traffic Incoming Outgoing Any

Match Files ☒

Password protected only ☐

File types

Portable Document Format (pdf)

OK Cancel

Finally, File Filter has been created to block PDF file on both directions.

Rules

<div> + Create New Edit Delete Move Up Move Down Column Settings Search... </div>							
<input type="checkbox"/>	Rule	Comment	Traffic	Protocol	Match Files	Action	File Types
<input type="checkbox"/>	Block-PDF		any	CIFS, FTP, HTTP, IMAP, POP3, SMTP	any	block	pdf

<div> + Create New Edit Delete More Column Settings </div>				
<input type="checkbox"/>	Name	Comments	Feature Set	Created Time
<input type="checkbox"/>	Custom-File		Flow-based	2023-12-22 14:37:37
<input type="checkbox"/>	default	File type inspection.	Flow-based	2023-12-17 18:13:31
<input type="checkbox"/>	sniffer-profile	File type inspection.	Flow-based	2023-12-17 18:13:31

Apply the Filter to a Policy:

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**.

<div> Policy & Objects Policy Package Install ADOM Revisions Tools </div>					
<div> + Create New Edit Delete Section Policy Lookup Collapse All </div>					
<input type="checkbox"/>	#	Name	From	To	Source
<input checked="" type="checkbox"/>	1	LAN-to-WAN	LAN-Port	WAN1-Port WAN2-Port	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 **File Filter Profile** 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



File Filter Profile

Custom-File



DNS Filter



SSL/SSH Inspection

deep-inspection

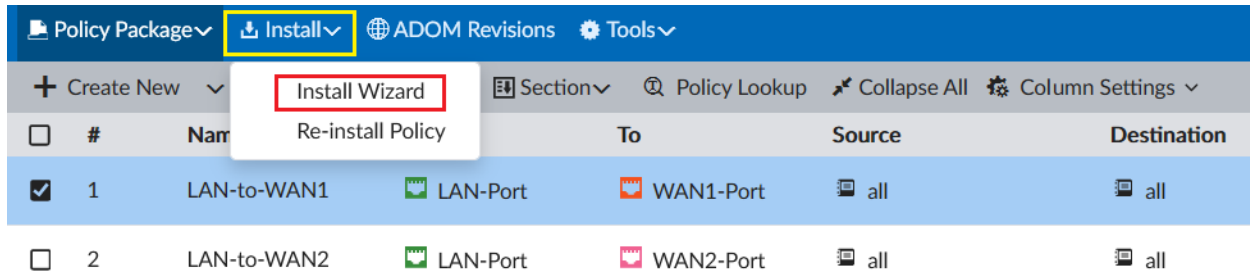


Decrypted Traffic Mirror



Install the Policy:

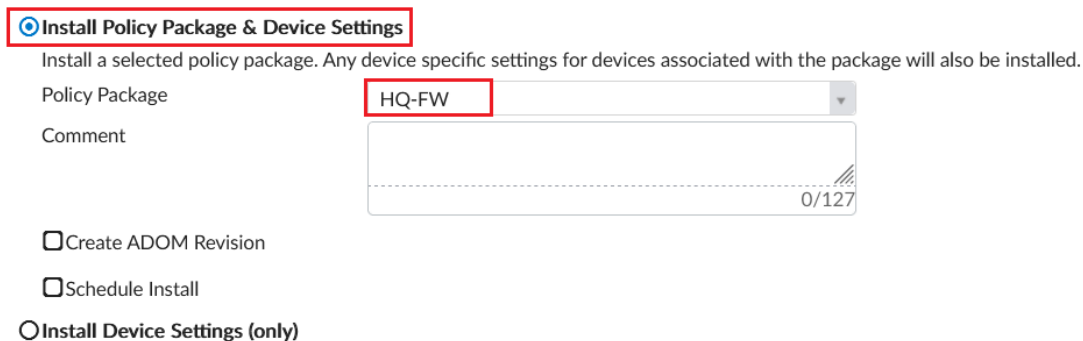
Continue on the FortiManager GUI, click **Install>Install Wizard**.



#	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)

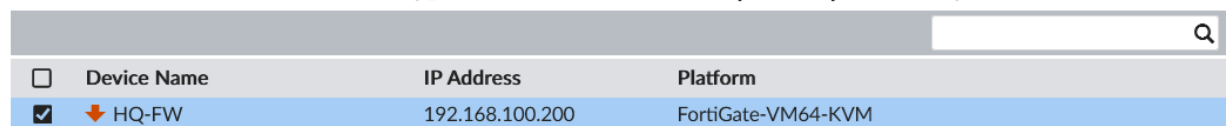
Next >

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

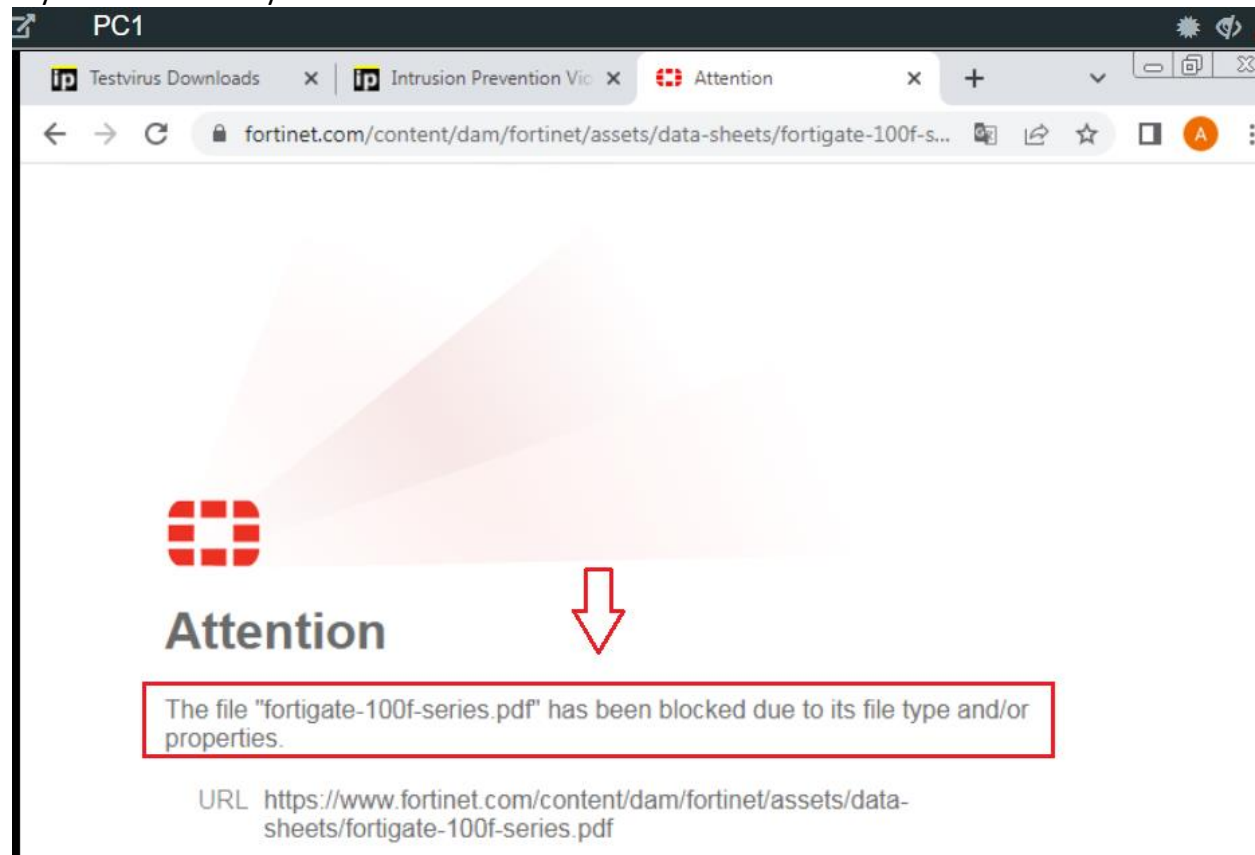
Once done click **Finish**.

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

Test and Verification:

Try to download any PDF file from Internal PC it will show the banner below.



Navigate to **Log & Report > File Filter** to see the logs.

Date/Time	Service	Action	URL	File Name	Matched file name
5 seconds ago	HTTPS	blocked	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
7 seconds ago	HTTPS	blocked	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
8 seconds ago	HTTPS	blocked	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
11 seconds ago	HTTPS	blocked	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
39 seconds ago	HTTPS	blocked	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
2 minutes ago	HTTPS	passthrough	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
2 minutes ago	HTTPS	passthrough	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
Hour ago	HTTPS	blocked	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
Hour ago	HTTPS	blocked	https://nseti-pdfs.s3.us-west-2.amazonaws.com/desc/N...	NSE4_7.0_Exam_Description.pdf	
Hour ago	HTTPS	blocked	https://nseti-pdfs.s3.us-west-2.amazonaws.com/desc/N...	nse4_fgt-7.0-pdf.pdf	
Hour ago	HTTPS	blocked	https://www.africau.edu/images/default/sample.pdf	sample.pdf	
Hour ago	HTTPS	blocked	https://www.africau.edu/images/default/sample.pdf	sample.pdf	

Navigate to **Log & Report >Forward Traffic** to see the File Block logs.

	Date/Time	Source	Device	Destination	Result
	Minute ago	10.0.1.1	USER-PC	216.239.38.120 (www.google.com)	✓ 925 B / 510 B
	Minute ago	10.0.1.1	USER-PC	3.7.210.81 (www.fortinet.com)	✗ Deny: UTM Blocked
	2 minutes ago	10.0.1.1	USER-PC	3.7.210.81 (www.fortinet.com)	✗ Deny: UTM Blocked
	3 minutes ago	10.0.1.1	USER-PC	108.177.15.188 (mtalk.google.com)	✓ 3.91 kB / 30.27 kB
	5 minutes ago	10.0.1.1	USER-PC	108.177.15.188 (mtalk.google.com)	✓ 3.91 kB / 30.12 kB
	7 minutes ago	10.0.1.1	USER-PC	108.177.15.188 (mtalk.google.com)	✓ 3.91 kB / 29.96 kB

In FortiAnalyzer, navigate to **Log View>FortiGate>File Filter**.

#	Date/Time	Sub Type	Event Type	Source	Filter Name	File Name	File Type	Service	Source IP	Destination IP	Action
1	16:35:04	file-filter	file-filter	10.0.1.10	Block-PDF	nse4_fgt-7.0-p...	pdf	HTTPS	10.0.1.10	172.66.40.114	blocked
2	16:34:23	file-filter	file-filter	10.0.1.10	Block-PDF	sample.pdf	pdf	HTTPS	10.0.1.10	34.174.121.15	blocked
3	16:34:21	file-filter	file-filter	10.0.1.10	Block-PDF	sample.pdf	pdf	HTTPS	10.0.1.10	34.174.121.15	blocked
4	16:34:19	file-filter	file-filter	10.0.1.10	Block-PDF	sample.pdf	pdf	HTTPS	10.0.1.10	34.174.121.15	blocked
5	16:34:16	file-filter	file-filter	10.0.1.10	Block-PDF	sample.pdf	pdf	HTTPS	10.0.1.10	34.174.121.15	blocked
6	16:33:48	file-filter	file-filter	10.0.1.10	Block-PDF	sample.pdf	pdf	HTTPS	10.0.1.10	34.174.121.15	blocked
7	16:32:13	file-filter	file-filter	10.0.1.10	Block-PDF	sample.pdf	pdf	HTTPS	10.0.1.10	34.174.121.15	passthrough
8	16:31:58	file-filter	file-filter	10.0.1.10	Block-PDF	sample.pdf	pdf	HTTPS	10.0.1.10	34.174.121.15	passthrough