

DEPLOYMENT GUIDE

Fortinet FortiGate and FireMon



Fortinet FortiGate and FireMon

Overview	3
Deployment Prerequisites	3
FireMon Configuration	4
Fortinet Configuration	7
Summary	12

Overview

The FireMon Security Manager Core Platform provides detailed, customizable IT risk analytics that allows network and security management to respond quickly to changing business demands and ensure protection, with real-time assessment of policy enforcement spanning from the specific rules and configurations of every individual device to the combined effectiveness of all defenses.

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks No. 1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

Deployment Prerequisites

- 1. Fortinet FortiGate version 4.x or newer
- 2. FireMon FMOS version 8.15.x or newer





Figure 1: Architecture overview.

FireMon Configuration

1. From the Administration screen, click Device.



- 2. From the Devices screen, click Create > Fortinet.
- 3. Choose FortiGate Firewall or FortiGate Firewall VDOM if your deployment has VDOMs.
- 4. For VDOMs, be sure to input the correct VDOM name in the device property section.



5. Under General Properties, give the device a name and enter the IP Address.

evices Management Stations Device Groups	Device Packs Clusters Normalization Status	
Device Devices Create		
roduct: Fortigate Firewall		
General Properties		
>Device Name		
FortiGate		
Management IP Address	Data Collector	
10.101.32.59	firemon.fortinet.com	
Central Syslog Server	Syslog Match Name	
	\$	
External ID ①		

- 6. Under Device Settings, enter the password for the Admin user then re-enter the password.
- 7. Click Save when done.
- 8. Please note: The Admin user will need to be configured with the super_admin profile on the FortiGate.

Device Sectings	
Managed By	
Credentials	
>User Name	>Password
admin	
	Re-enter Password 🕲
Retrieval	
Protocol	Port
Protocol	
ssh	22
Log Monitoring Change Monitoring	22
Solution Solution Solution Log Monitoring Change Monitoring Advanced	22

The next screen should look like this.

(AC	MINISTRATIC	DN 🚽							1	FireMon Fire	Mon 🝷
Syst	em 🗄 Device	PAccess 💐 FireMo	n Objects 🛛 🛇 Compliance	• Workflow	👭 Settings 🕺 K Tools						0.
Device	s Management	Stations Device Grou	ps Device Packs Cluster	rs Normalization	n Status						
Dev O Cre	rice Devic ate CImport C	Actions -					0	Device sa	ve: FortiGate.		×
0/	Add Filter						Factors		1	results 0.19 seconds	
	Name *	Description	Managemen	t IP Address V	endor	Retrieval	Change	Log	Security Manager	Policy Optimizer	
1	FortiGate		10.101.32.59	F	ortinet		•	۰	۲	0	=
Show	10 20 50 100			< 1	>					Viewing	1-1 of 1

If you plan on using Policy Optimizer, make sure to check the box to enable the License.

🭳 A I	C ADMINISTRATION -									
Sys	tem 🔡 Device	PAccess 🥄 FireMon Object	cts 🕏 Compliance 🔊 Workflow	w 🚻 Settings 🗙 Tools						0 -
Device	Management	t Stations Device Groups De	evice Packs Clusters Normaliz	ation Status						_
Dev Ocre	vice Devi	Ces Lactions -				ø	Device say	ve: FortiGate.		×
0	Add Filter							1 in	results 0.19 seconds	
						Status		ü	cense	
	Name *	Description	Management IP Address	Vendor	Retrieval	Change	Log	Security Manager	Policy Optimizer	
1	FortiGate		10.101.32.59	Fortinet		•				=
Show	10 20 50 100		<						Viewing	1-1 of 1

9. Then go to Workflow.

10. Under Policy Planner, click Create > Access Request.

	IISTRATIO	Л	•						
🌣 System	📑 Device	P Access	😍 FireMon Objects	🕑 Compliance	o ^o Workflow	i!i† Settings			
Workflows Workflow Packs									
Workflo ▼ Policy F	OW W Planner	orkflow	S						
Create Access	Request		In Process Tic	kets	Workflow	Pack Version ()			

11. Give it a Name, then click Save.

Create Workflow (Access Request)	×
>Name Fortinet	
	Save

The Workflow screen shout now look like the image below.

	NISTRATIO	N	*				1 FireMo	n FireMon
🗘 System	Device	P Access	😍 FireMon Objects	Compliance of Workfl	ow III Settings	* Tools		0
Workflows	Workflow P	Packs						
 Policy 	IOW W	orktiow	S					
• Creat	te		In Process Tickets	Workflow Park Version	Workflow ID	Process Definition Key	Created By	
1 F0	ortinet		0	9.12.3	1	fortinet-9.12.3-1	FireMon FireMon	=
Show 1	0 20 50 10	0		<	1. >		View	ing 1-1 of 1

12. Do the same for the Policy Optimizer configuration.

Note: If adding FortiGate firewalls via FortiManager, do this from Devices > Management Stations. The Admin user will need access to all VDOMs enabled.



Fortinet Configuration

1. Ensure all Firewall rules are set to Log All Sessions.

+ c	reate New 🥒 🗄	Edit 📋 Dele	ete Q Policy Look	Q Search					Interfa	ce Pair View By Sequence
Seq.#	T Name	T Source	T Destination	T Schedule	▼ Service	T Action	T NAT	T Security Profiles	T Log	T Bytes
🖃 la	n - wan1 (1 - 1)								-	
1	Default-Policy	IIe 🗉	🗐 all	Co always	ALL	✓ ACCEPT	Enabled	AV WEB APP IPS 552	O All	482.11 GB
🗆 vs	w.dmz - wan1 (2 - :	2)			-		1			
2	FSW	🖻 all	🗐 all	Co always	ALL	✓ ACCEPT	Enabled	AV WEB APP IPS SSL	O All	9.37 GB
	an1 - Ian (3 - 3)									
3	RDP	🔳 əll	RDP_Server	Ce always	RDP	- ACCEPT	Enabled		O All	OB
	plicit (4 - 4)								-	
4	Implicit Deny	🗿 all	💷 all	Co always	ALL	Ø DENY			O Disable	ed 229.40 MB

If not, enable this for each rule under Logging Options.

Logging Options			
Log Allowed Traffic	0	Security Events	All Sessions
Generate Logs when Session Starts	0		
Capture Packets	0		

- 2. Configure FortiGate to send Syslog to the FireMon IP address.
- 3. Under Log & Report, click Log Settings.



- 4. Enable Send Logs to Syslog.
- 5. Enter the IP Address or FQDN of the FireMon server.
- 6. Select the desired Log Settings.
- 7. Click Save.



Note: If the primary Syslog is already configured, you can use the CLI to configure additional Syslog servers.

- FortiGate-ESX2 # config log syslogd2 setting FortiGate-ESX2 (setting) # set status enable FortiGate-ESX2 (setting) # set server 1.2.3.4 FortiGate-ESX2 (setting) # end FortiGate-ESX2 #
- 8. The configuration is now complete. Go back to the Devices screen in the FireMon interface. It should look like the image below once logs are received and the configuration has been retrieved.

ADMINISTRATION .							1	FireMon Fire	don •
system El Device Access	Compliance of workt								0 -
Devices Management Stations De	vice Groups Device Packs Clusters Normal	nization Status							
Device Devices Create Cimport CActions - Add Filter				_	Status			results 0.21 seconds	
Name •	Description	Management IP Address	Vendor	Retrieval	Change	Log	Security Manager	Policy Optimizer	
1 M FortiGate		10.101.32.59	Fortinet				0	٥	
Show 10 20 50 100		< <u>-</u> 2						Viewing	I+1 of 1

9. You can initiate a manual retrieval of the configuration by clicking the box on the far right.

						L FireMon FireMon
O System El Device PAccess	Compliance & Workflow	🔢 Settings 🔺 Tools				0
Devices Management Stations	Device Groups Device Packs Clusters Normalization	n Status				
Oevice Devices • Create I Import I Actions • • Add Filter					Status	Edit Retrieve Configuration Import Configuration Files
Name *	Description	Management IP Address	Vendor	Retrieval	Change Log	Delete
1 BB FortiGate		10.101.32.59	Fortinet			0 0
Show 10 20 50 100		(C) ()	>			Viewing 1-1 of

Security Manager Dashboard Views.

transpran (* bach	Devroes	compriance Occhange	P Map - P File Province				stappen - Kines -		
nterprise Ove	erview Dashboard								
Key Performance Ind	licators								
2. Besice Inventory		Ø	100% Devices Revised (Last 7 days)	Φ	© 50% Unuted Bules (Latr 50 days)		2.52 Average Security Concern Index Net encough Netter Kul data		
			2 Devices Revised			4 Unused Rules			
Devices Recently Revi	ised turn ist			Vev All	Rule Search				
Device Name	Last Revision	5010 	S. Change (Dand)		LOURCE	Search for 20-6 Ped address (24 Senseric Sectoral)	Onclude *Any (
E fundament	11/21/2017 12:56 PM	245	Net enough homoroul data		DESTRUTION	Justifi for Polithie address Of Sensorio Sensoria	Orchole. *Any (
					LABORE R	Search for prossurgions	Ondade: "Way d		
					APPLICATION	Search for approxime name analy workly	Ondvde: *Any (
					uniter-	Search for user same (interl match)	Citedade: May (
							lan an a		
Average Security Concern Index Trend on numming					Rules Contributing to Control Failures				
Inde Unage Inc Corecul	tative Coverity (D)				Most Severa Con	trad Fallward on in	10		



Security Manager Policy Views





Security Manager Security & Compliance Views



Security Manager Security & Change Views

	Y MANAGER - Q									1 FireMon Fir	reMon 👻
		Security & Compliance									Tools - 0
erview Revi	isions Changes										
terpris	e Change Overv	iew									
ey Perform	mance Indicators										
			0					0			0
	0				FortiCato				•		
			FC	ortiGate	rtiGate		8				
	Revis		Device M	fost Recently Re	vised		Rules with Changes				
	7 Cont		At 11/21/2017 1:09 PM by admin@1					Last 7 days			
SECURIT	Y MANAGER . Q	Search by Name or IP Address								FireMon Fire	ireldon *
		Corunti E Compliance	Ocharge Palar	2011/2012						discourse \$1	Tools -
Page Page	sines Chapters	· second a compliance	Country Country								
stiew nev	nswis charges										
tevisions a	Last 10)				View A	UI Devi	ces Recently Revis	ed assist			View Al
Revision	Date/Time	User	No. of Changes	Device Name		Devi	ce Name	Last Revision	50 0	% Change (Trend)	
CI 15	11/21/2017 1:09 PM	admin@10.101.32.254	3	FortiGate	-		FortiGate	11/21/2017 1:09 PM	2.41	 Not enough historical data 	=
CI 14	11/21/2017 1:07 PM	admin@10.101.32.254	0	M FortiGate	=		FortiGate-Lab	11/21/2017 12:56 PM	2.63	Not enough historical data	=
13	11/21/2017 1:07 PM	admin@10.101.32.254	2	FortiGate	=						
12	11/21/2017 1:06 PM	admini@10.101.32.254	2	E FortiGate	=						
1 11	11/21/2017 1:05 PM	admin@10.101.32.254	0	M FortiGate	=						
10 10	11/21/2017 12:56 PM	firemon	0	B FortiGate-Lab	-						
0.9	11/21/2017 12:55 PM	firemon	0	FortiGate-Lab	-						
H C	11/21/2017 10:36 AM	tremon	0	BE FortiGate							
	10202017 1035 806	10 CONT		IN POLIGIE	-						
Changes sa	er 20)										View Al
Device Name	Revis	on Action	User	Date/Time		Object Type	Object			Summary	
FortiGate		5 A Modified	admin@10.101.3	2.254 11/21/2017 1	:09 PM	Security Rule	2			Disabled changed from [true] to [false], Log changed fro	rom (false) _
Il FortiGate		5 A Modified	admin@10.101.3	254 11/21/2017 1:09 PM		Security Rule	1	1		Rule order changed in policy (Policy) from (1) to (2)	
FortiGate	· 🖬 :	5 A Modified	.admin@10.101.3	2.254 11/21/2017 1	09 PM	Policy	Policy	sky		Security rule(s) modified	
B FortiGate	. 🖬	Modified	admin@10.101.3	2.254 11/21/2017 1	:07 PM	Security Rule	1			Disabled changed from [true] to [failse]	
M FortiGate	e 🚺 1	3 A Modified	admin@10.101.3	admin@10.10132.254 11/21/2017 1:07 PM		Policy	Policy	cy.		Security rule(s) modified	
		Z A Modified	admin@10.101.3	2.254 13/21/2017 1	254 13/23/2017 1:06 PM		1	1		Disabled changed from (failed) to (true)	
M FortiGate	1000	A Manufalland	admin@10.101.3	2.254 11/21/2017 1	:06 PM	Policy	Policy			Security rule(s) modified	
B FortiGate	. 🖬	a woomed									
FortiGate	y User (7-Day History)	a woomed									View Al
FortiGate FortiGate Changes by User	e 🚺 1 y User (7-Day Hotory)	c Mooned		No	. of Changes	Last Revision	Ser	mmary			View All
 FortiGate FortiGate Changes by User admin@10.10 	e 🖬 1 y User (7-0xy History) 21.32.254	A Moarrea		No 2	. of Changes	Last Revision 11/21/2017 1:09	PM 1 p	mmary solicies changed, 2 security rules chan	ged		View All

Summary

FireMon helps keep Fortinet firewalls running smoothly with a complete configuration management solution, including full support for the FortiGate line of network security platforms and appliances. FireMon monitors each appliance, capturing event and traffic logs in real time. All change events trigger a full configuration capture including detailed change history and a full audit trail of operations. Fortinet devices can be monitored directly or indirectly if another event collection system is in place.

Solution Guide: <u>https://www.fortinet.com/content/dam/fortinet/assets/alliances/firemon-integration-brief-for-fortinet.pdf</u> FortiGate 5.6 Handbook: https://docs.fortinet.com/uploaded/files/3999/fortios-handbook-56.pdf



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet*, FortiGate*, FortiCare* and FortiGuard*, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results. Nothing metric persons or implied, except to the extent Fortine etness a binding written contract, signal by Fortinet. Supersons or implied, except to the extent Fortine etness a binding written contract, signal by Fortinet. Supersons or implied, except to the extent Fortine etness a binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions hall be applicable.

October 7, 2021 3:55 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 5:DG-Fortinet-and-Firemon-102021:DG-