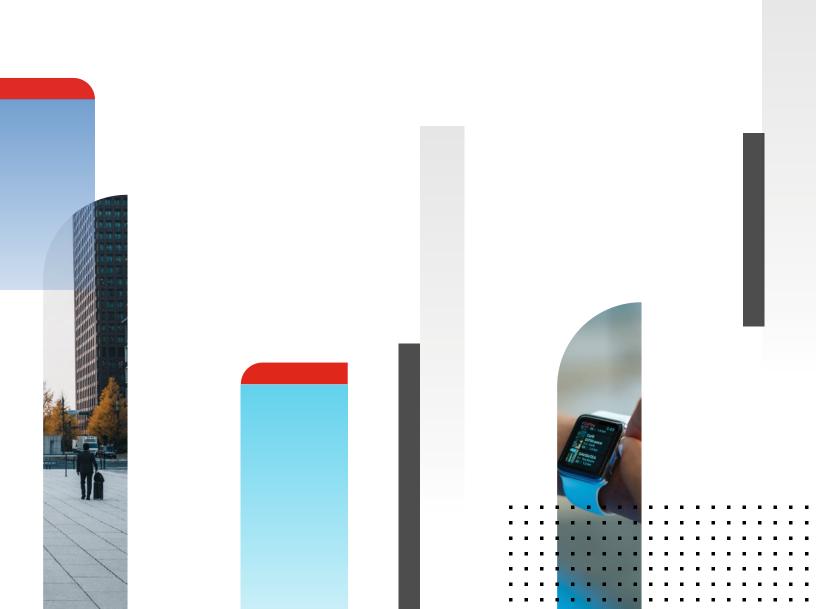


**DEPLOYMENT GUIDE** 

# Fortinet FortiGate and IBM QRadar



# Fortinet FortiGate and IBM QRadar

Overview
Deployment Prerequisites 3
About IBM QRadar 3
QRadar Configuration 4
Fortinet Configuration
Display Dashboards
Threat Dashboards
Traffic Dashboards 8
System Dashboards
Wireless Dashboards
VPN Dashboards 10
Summary

# Overview

The Fortinet FortiGate App for QRadar provides visibility of FortiGate logs on traffic, threats, system logs and performance statistics, wireless AP, and VPN. It displays top contributors to threats and traffic based on subtypes, service, user, IP, etc. The app also shows system, wireless, VPN events, and performance statistics. Users can dive into each view to show the relevant logs by clicking on the charts. Thirty-five customized properties, some of which may already exist in Fortinet Content Pack, have been defined/redefined to better interpret FortiGate logs.

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 <a href="https://www.fortinet.com">https://www.fortinet.com</a>, the Fortinet Blog, or FortiGuard Labs.

#### **Prerequisites**

- 1. Fortinet FortiGate version 5.4 or newer
- 2. Fortinet FortiAnalyzer Content Pack for QRadar
- 3. Fortinet FortiGate App for QRadar
- 4. QRadar version 7.2.8 or newer (tested with 7.2.8 Build 20160920132350)
- 5. IBM X-Force (formerly App Exchange) username and password



# About IBM QRadar

IBM (NYSE: IBM) Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM® QRadar® SIEM detects anomalies, uncovers advanced threats and removes false positives. It consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network. It then uses an advanced Sense Analytics engine to normalize and correlate this data and identifies security offenses requiring investigation. As an option, it can incorporate IBM X-Force® Threat Intelligence which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats. QRadar SIEM is available on premises and in a cloud environment.

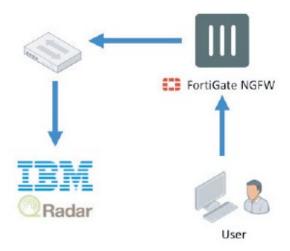


Figure 1: Architecture overview.

# **QRadar Configuration**

Add a Log Source from Admin > Data Sources > Events > Log Sources.

IBM QRadar Security I	ntelligence				-	
Dashboard Offenses L	og Activity Network Activity	Assets Reports	Risks Vulnerabilities	Admin Fortinet FortiGet.		
Admin	Deployment Ecilion	oy Changes Advanced ¥				
► System Configuration	(1) There are no changes to	deploy.				
* Data Sources	Data Sources					
Events     Flows	Events					
Vulnerability     Remote Networks and	<b>.</b>			-		
Remote Networks and Services Configuration	DSM Editor	WinCollect	Log Sources	Log Source Extensions	Log Source Groups	Log Source Parsing Ordering
► Plug-ins	100					
	Data Obfuscation Management					

- 1. Configure the Log Source.
- 2. For the Log Source Name, enter a unique name.
- 3. For the Log Source Type, select Fortinet FortiGate Security Gateway.
- 4. For the Log Source Identifier, enter the FortiGate IP address.

		6
Log Source Name	FortiGate	
Log Source Description		
Log Source Type	Fortinet FortiGate Security Gateway	
Protocol Configuration	Syslog ¢	
Log Source Identifier	192.188.1.99	
Enabled	0	
Credibility	5 \$	
Target Event Collector	eventcollector0 :: gradar \$	
Coalescing Events	0	
incoming Payload Encoding	UTF-8 \$	
Store Event Payload	0	
lease select any groups you would like t	his log source to be a member of:	

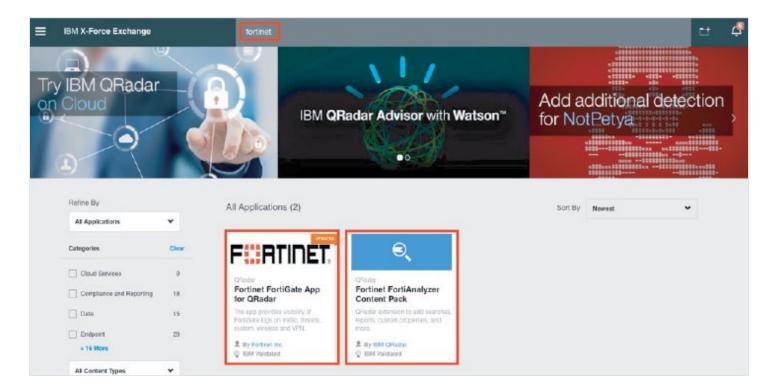
5. From the Admin screen, select Extensions Management.

Dashboard Offenses L	og Activity Network Activ	rity Assets Reports	Riska Vulnerabilities A	dmin Fortinet FortiGet					
Admin	🚱 Deployment Ecitor 🔞 D	eploy Changes Advanced ¥							
* System Configuration	U There are no changes to deploy.								
<ul> <li>User Management</li> <li>Forensics</li> <li>Assets</li> </ul>	System Configuration								
+ Data Sources			4	144 A	Gmi	ň			
<ul> <li>Events</li> <li>Flows</li> <li>Vulnerability</li> </ul>	Auto Update	Backup and Recovery	Global System Notifications	Index Management	Aggregated Data Management	Network Hierarchy			
Remote Networks and Services Configuration	<b>\$</b>	置守	ul.	2		<u></u>			
Try it out	System Settings	Asset Profiler Configuration	Custom Offense Close Reasons	Store and Forward	Reference Set Management	Centralized Credentia			
		*	6						
	Domain Management	Extensions Management	Resource Restrictions						

6. Click IBM Security App Exchange to launch the X-Force/App Exchange portal.

Extensions Man	agement		Search by extension name	٩		IBM Security App Exchange	0
ALL ITEMS	INSTALLED	NOT INSTALLED				Add	
Name				Status	Author	Added On +	

- 7. Search the "Fortinet."
- 8. Download the Fortinet Content Pack for QRadar.
- 9. Download the Fortinet FortiGate App for QRadar.



10. Install the Content Pack and then the FortiGate App from the Extensions Management screen by clicking Add.

Extensions Management		Search by extension name	٩		IBM Security App Exch	ange (	
ALL ITEMS	INSTALLED	NOT INSTALLED				Add	
Name			1	Status	Author	Added On	•

- 11. Browse for the Content Pack file downloaded previously, then click Add.
- 12. Select Overwrite if some customized properties already exist.

rom local storage:	
FortinetFortiGateForQRadar-Content	Browse
Install immediately	

13. Do the same for the FortiGate App.

# **Fortinet Configuration**

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

B Dashboard	>	System Inform	nation	:
FortiView  Network  System  Policy & Objects  Security Profiles  VPN  User & Device  WIEL& Switch Controller	> > > > > >	Hostname Serial Number Firmware Mode System Time Uptime	FGVM040000101072 FGVM040000101072 v5.6.0 build1449 (GA) NAT (Proxy-based)	-
III Log & Report Forward Traffic Local Traffic	~	Administrator	California, United States)	:
System Events AntiVirus Web Filter Application Control		1 Logged in		
Security Fabric Audit Security Audit Events		3		
Learning Report		Sessions		

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

Security Fabric Audit Security Audit Events Learning Report	Send Logs to Syslog  IP Address/FQDN
Log Settings 🖒 🏠	Log Settings
Threat Weight Alert E-mail	Event LoggingAllCustomizeLocal Traffic LogAllCustomize

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	#

7. The configuration is now complete

### **Display Dashboards**

The user can select different time ranges up to last 30 days, which may take longer to display, but progress will be shown during the wait. The server will cache the result for a while for revisit. Results of last 30 days are cached for 12 hours, other ranges by the hours cached for 2 hours, and shortest is 5 minutes.

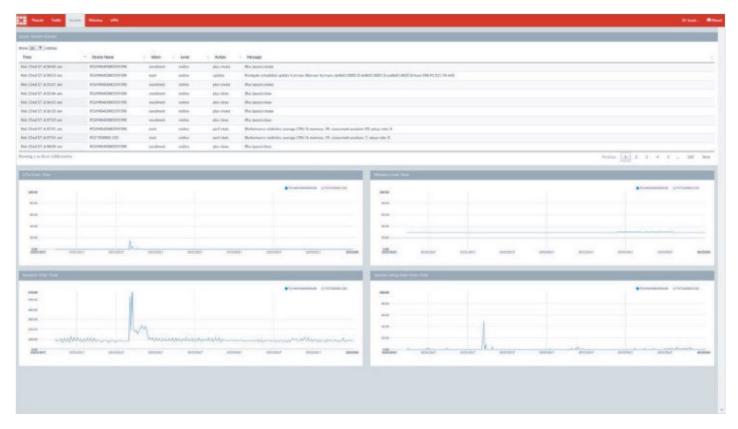
#### **Threat Dashboards**



#### **Traffic Dashboards**



#### **System Dashboards**



#### **Wireless Dashboards**

ew <u>10 Y</u> exch	* \$205	· Mender	8550	AF Security	RadioBand	Charant	Outsetted By	Send	OHWIN
vis 130 17. 02741 am	0	Fortheat leve.	00:09:0f 7: 5abi	WPA2 Enterprise	802.151	11	FF22183+13025404	71	10
vis-13th 17 0:27:41 am	0	Correlations, BIC	687774086178	OPEN	802.11#	7	PP22183813375994	-87	-
ele 5305 17. 1/27.56 am	0	Forticet, Inc.	904ca:27d15i	WFR2 Personal	H02 15er-26	3	PP22582+1335+904	-39	-
o 13th 17. 127:55 am	n	Forthert, #w.	08.56-0676.58.83	WHILE Personal	NG2 134		FP22383833328936	-47	-
5 130 17. 120 11 am	0	Fortinut, Inc.	08560e5e360f	WFA2 Percend	002.159	4	FP22183×1333×904	41	-
136 17 (28:25 am	0	Spariel APA	1e0e8e401648	OPEN	802.15%	2	FP22183x5332x404	-39	-
1 13n 17. (38.25 am	8	Fortinet los.	10-09-09-21-888-41	OPEN	900 11g	3	10/22580×5.835×904	-86	-
130117. 29113 an	6	Fortmet, Ave.	31340ec7e837	WHILE Personal	802.15a	116	P32083453005456	-65	-
130 17. (30 15 am	3	103	42.95.8877.5kp4	WEA/WEA2 Personal	#52.15e		FP22103413327625	-42	
1205 17.	a	ARRES Group, Inc.	10.0eab.5ciate.0	WPA/WPA2 Presidual	602:154	4	FP22103×13027021	:40	-
ning the Starf 2 Secret Sty Add	Poble			_	_	_			Provinsion 1 2 3 Har
11 11 12 12 12 14								_	

#### **VPN Dashboards**

ow 10 · entries				1 Hours Brance			Provide Alt	
Time etc 13th 17, 10.27.55 am	<ul> <li>Tunnel Name</li> <li>763790522</li> </ul>	Turenel Type	t Uver	US Duko VPN.1	<ul> <li>Sent(ME)</li> <li>37.94582939347949</li> </ul>	8. Received(M8) 9.456648826599121	35440.0	
eb 12th 17, 10:28:14 am	763790591	ssi-bannel	asrivatav	UG Diskp VPN 1	16.10509967800955	34.268256187438945	4506.0	
eb 1365 17, 10:28:44 am	763290557	eu-canvel	toracad	UG, Diako, VPN, 1	8.900117874145508	3.1198227920533227	24026.0	
eb 13th 17, 10,29,07 am	1535014017	ed-bannel	ebortolla	UG-FAC	0.07331371307373047	0.0054041137095212	9633.0	
eb 130:17, 10:29:44 am	763790583	sti-tunnel	duha	UG Diske VPN 2	0526616382590877	5.7028447341918945	8407.0	
eb 13th 17, 10:29:50 am	763790545	eci-tumnol	teracad	UG_Distap_VPN_1	61 184022290385996	11,216/19083619364	0.40006	
eb 13th 17, 10:30 26 am	1535834820	ssi-tannel	stephen	UG-FAC	0.4464130401611328	0.31220054625464844	4217.0	
eb 13th 17, 10:30:32 am	Van IDC Svr ah1	lanec		NA	9737.785770999329	9126177790641705	1302359.0	
ib 54th 17, 438:20 pm	763290596	sci-tunnel		UG Dake VPN 1	194.23376846313077	4.083403778625488	5406.0	
da 148117, 62622 pm	1535814821	ed-tanent		UG-FAC	1.9445533752441406	0.572575569152822	2408.0	
Proughput by VPN Tunnels				Connection	ta Over Time			
		1 1 1 1 1	1.1.1.1					
7395								
8096				1				
				1				
8090 5096				these Ower Trees				
806 806 406				Connection Coll Time				

### Summary

The Fortinet FortiGate App for QRadar has been designed to improve the capabilities and user experience for IBM QRadar users within environments using Fortinet FortiGate solutions. The app provides additional visibility into FortiGate logs in the QRadar Ariel DB including traffic, threats, and system logs through a series of tabs and dashboards from within the QRadar GUI. The app displays top contributors to threats and traffic based on variables including service, user, IP address, and subtypes (e.g., Web Filter, Antivirus, IPS, and Application Control). The app also displays performance statistics for the FortiGate system including Wireless Access Points and VPN events. QRadar users can drill down into each view to show the relevant logs by clicking on the charts, with the ability to select different time ranges up to the last 30 days. The app includes 35 customized properties, some of which were already available in Fortinet QRadar Content Pack; however, these have been defined/redefined to better interpret FortiGate logs.

Solution Guide: https://www.fortinet.com/content/dam/fortinet/assets/alliances/user-guide-fortigate-app.pdf

IBM X-Force (formerly App Exchange): https://www.fortinet.com/content/dam/fortinet/assets/alliances/user-guide-fortigate-app.pdf

**Note:** The Fortinet FortiGate App for QRadar version 1.0.0 supports FortiGate versions 5.4 and older. Version 1.0.1 supports FortiGate versions 5.6 and older.



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. Mohine yources are integrated trademarks of every service in their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results. Mohine yources are integrated commitment by Fortinet. All other product and performance results. Nothine previne prevens or implied, except to the extent Fortine enternes a binding written contract, signal by Fortinet Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclams in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revises the publication without notice, and the most current version in shall be applicable.

October 1, 2021 1:34 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group S:DG-FortiGate-IBM-QRadar-102021:DG-FortiGate-IBM-QR