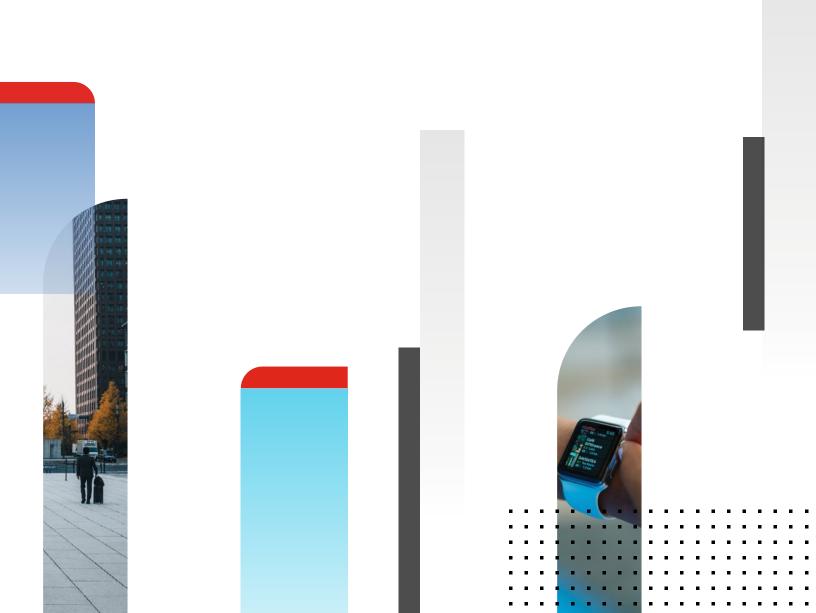


DEPLOYMENT GUIDE

Fortinet FortiGate App for QRadar



Fortinet FortiGate App for QRadar

Overview
Installation
Prerequisites
Top Three Reasons Fortinet Is Better
Display Dashboard
Threat Dashboard4
Traffic Dashboard
System Dashboard
Wireless Dashboard
VPN Dashboard6
Troubleshooting

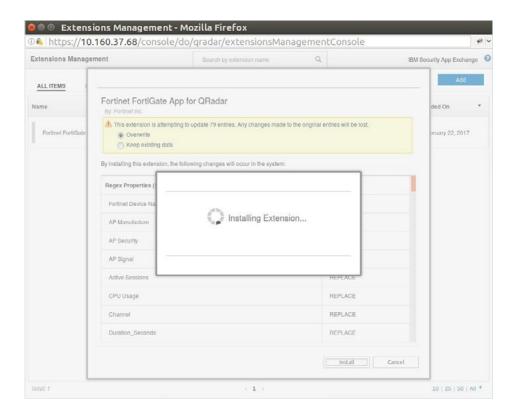


Overview

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 custom properties, some of which may already exist in Fortinet Content Pack, have been defined/redefined to better interpret FortiGate logs.

Installation

- 1. Download the extension from App Exchange.
- 2. Go to the Admin tab and click extension management.
- 3. Upload the zip file and confirm to install.
- 4. Select Overwrite if some custom properties already exist.



Prerequisites

1. 1. IBM QRadar 7.2.8 or newer

It may overwrite some custom properties defined in Fortinet Content Pack, but they are either unchanged or kept backward compatible with existing regex.

Supported Browsers:

- 2. Chrome (Verified on 56.0.x)
- 3. IE (IE10 or later)
- 4. Firefox (Verified on 50.1.0)
- 5. Logs from FortiGate FOS 5.0 or later



Top Three Reasons Fortinet is Better

1. Add a Log Source.

Add a log source		
Log Source Name	FortiGate 123	
Log Source Description		
Log Source Type	Fortinet FortiGate Security Gateway	1
Protocol Configuration	Syslog	
Log Source Identifier	10.160.38.95	
Enabled	3	
Credibility	5	
Target Event Collector	eventcollector0 :: qradar -	
Coalescing Events		
Incoming Payload Encoding	UTF-8	
Store Event Payload		
Please select any groups you would li	ke this log source to be a member of:	
	Save	ancel

2. Send Log to QRadar

On FortiGate, enable logging on firewall policies and ship logs via syslog. Log in to FortiGate and make the following configurations:

```
config global
config log syslogd setting
set status enable
set server <QRadar IP address>
```

Display Dashboard

Threat Dashboard

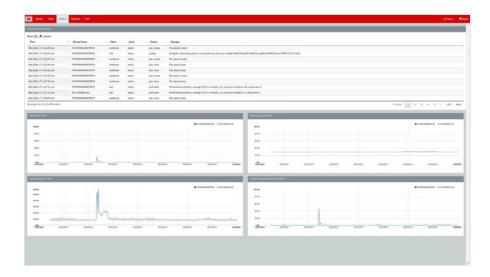




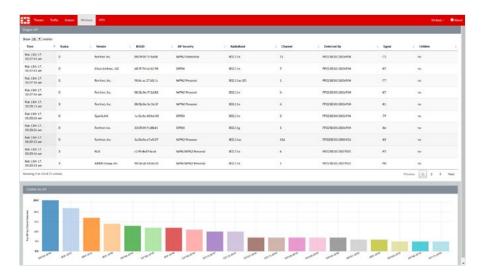
Traffic Dashboard



System Dashboard

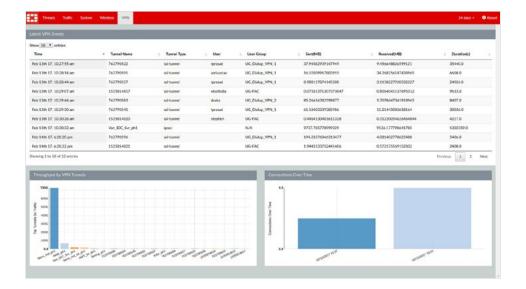


Wireless Dashboard





VPN Dashboard



The user can select different time ranges up to the 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 the last 30 days are cached for 12 hours, other ranges by the hours cached for two hours, and shortest is five minutes.

Troubleshooting

If no data can be found for the charts, no matching data found in the range will be displayed. Adjust the time range or make sure FortiGate is sending logs to QRadar by visiting Log Activities and filter FortiGate log source.

If still no data, please check /var/log/gradar.error and send any suspicious error to us at gradar_app@fortinet.com.



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 may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet ideals in all warranties, whether express or implied, except to the extent Fortinet enterts a binding written contract, signal of the 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 internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.