DEPLOYMENT GUIDE

Fortinet FortiGate App for QRadar
Fortinet FortiGate App for QRadar

Overview .............................................................. 3
Prerequisites .......................................................... 3
Installation ............................................................. 3
Top Three Reasons Fortinet is Better .............................. 4
Display Dashboard ................................................... 4
  Threat Dashboard .................................................. 4
  Traffic Dashboard .................................................. 5
  System Dashboard .................................................. 5
  Wireless Dashboard ............................................... 5
  VPN Dashboard ..................................................... 6
Troubleshooting ....................................................... 6
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. 35 custom properties, some of which may already exist in Fortinet Content Pack, have been defined/re-defined to better interpret FortiGate logs.

Installation

1. Download the extension from App Exchange.
2. Go to 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. 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:
   1. Chrome (Verified on 56.0.x)
   2. IE (IE10 or later)
   3. Firefox (Verified on 50.1.0)
   4. Logs from FortiGate FOS 5.0 or later.
Top Three Reasons Fortinet Is Better

1. Add a Log source.

![Add a log source](image)

- Log Source Name: FortiGate 123
- Log Source Type: FortiGate Security Gateway
- Protocol Configuration: Syslog
- Log Source Identifier: [QRadar IP address]
- Enabled
- Credibility
- Target Event Collector: eventcollector01:qradar
- Compression Events
- Ingress Payload Encoding
- Store Event Payload

2. Send Log to QRadar.

On FortiGate, enabling logging on firewall policies and ship logs via syslog. Login FortiGate and make following configurations:

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

Display Dashboard

Threat Dashboard
Traffic Dashboard

System Dashboard

Wireless Dashboard
VPN Dashboard

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.

Troubleshooting

If no data can be found for the charts, No matching data found in the range will be displayed. Adjusting 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/qradar.error and send any suspicious error to us at qradar_app@fortinet.com.