DEPLOYMENT GUIDE

Fortinet FortiGate App for QRadar

Fortinet FortiGate App for QRadar

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.

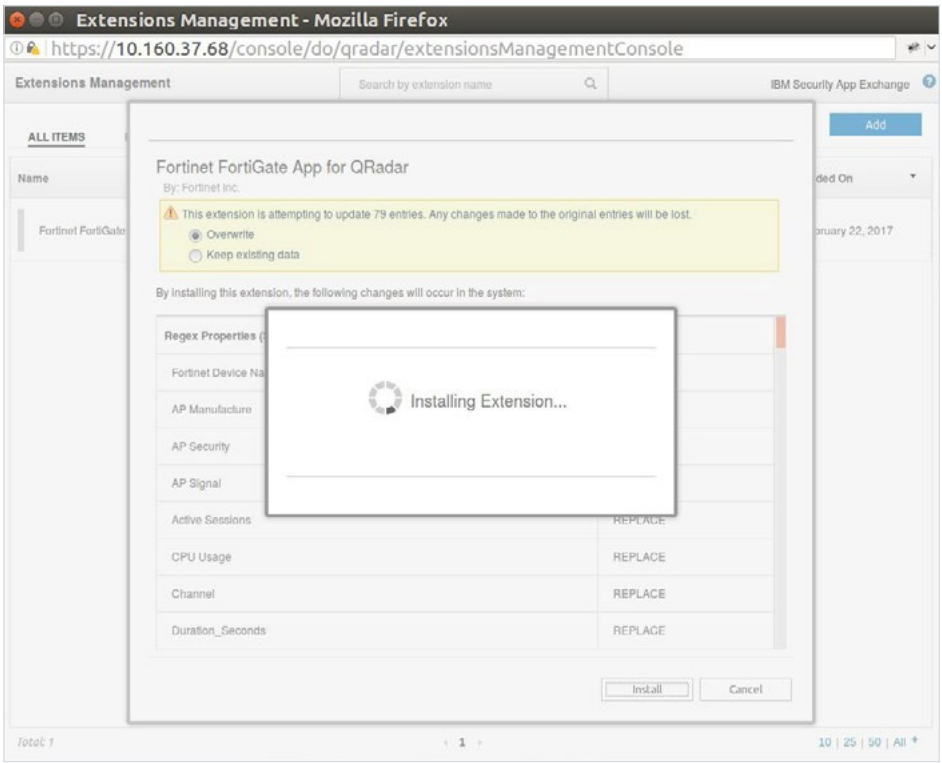
Prerequisites

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.

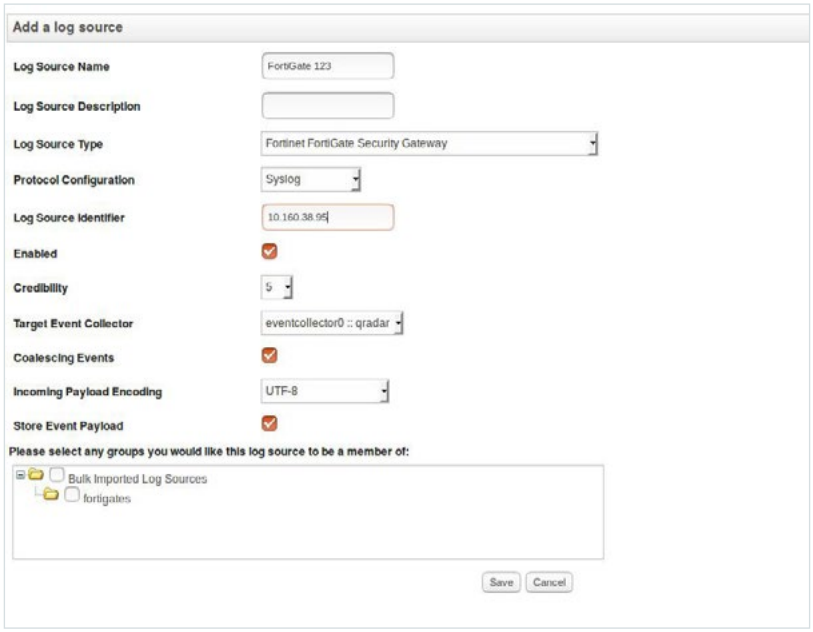
Supported Browsers:

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.



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:

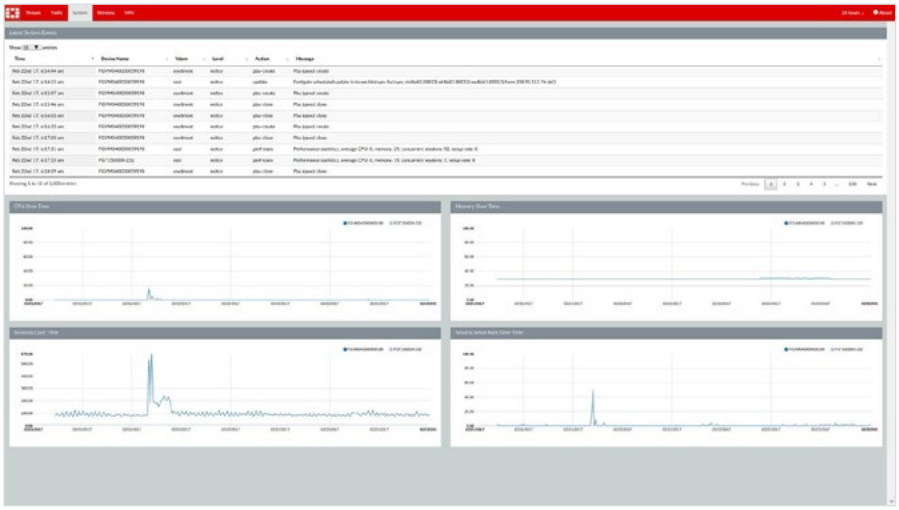
```
config global
config log syslogd setting
set status enable
set server <QRadar IP address>
```

Display Dashboard

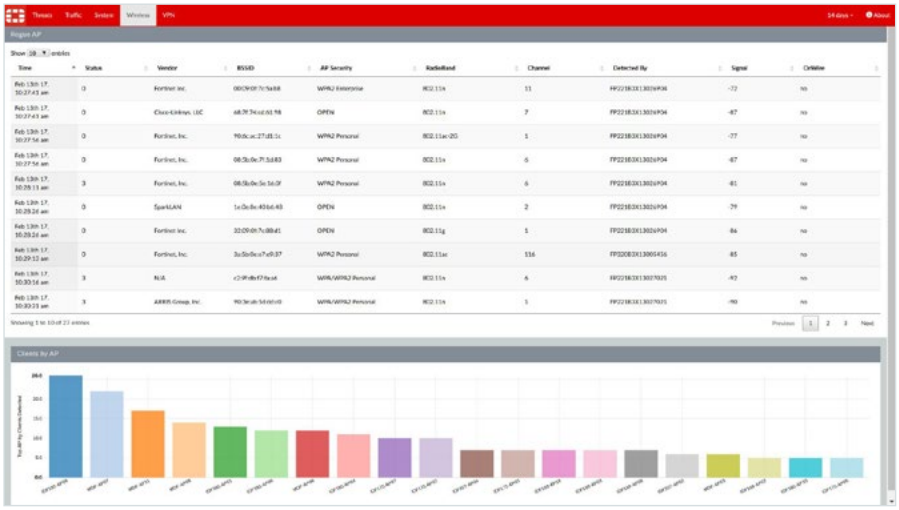
Threat Dashboard

Traffic Dashboard

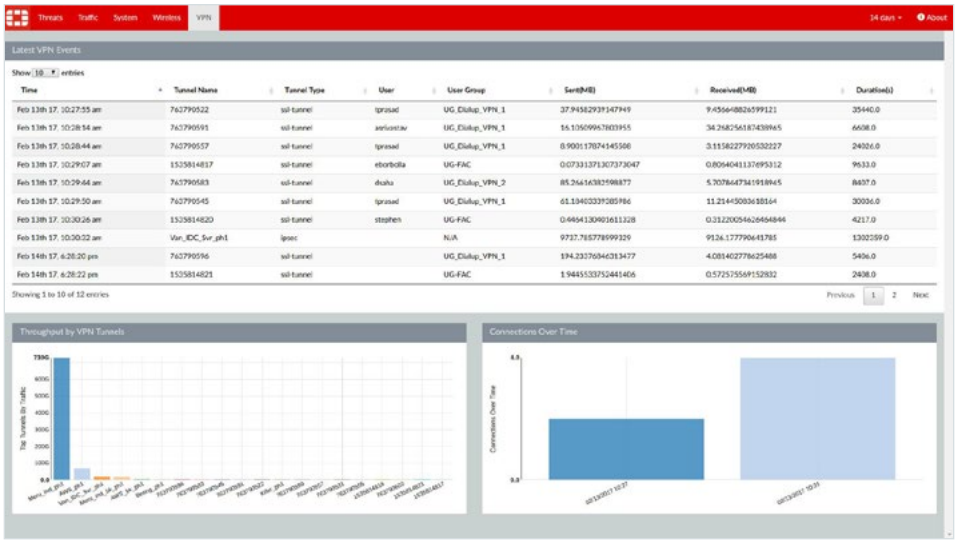
System Dashboard



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/qradar.error and send any suspicious error to us at qradar_app@fortinet.com.

September 30, 2021 2:59 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 5:DG-FortiGate-App-for-QRadar-102021:DG-FortiGate-App-for-QRadar-102021

441152-0-0-EN