DEPLOYMENT GUIDE

Fortinet FortiGate and IBM QRadar

Fortinet FortiGate and IBM 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. 35 customized properties, some of which may already exist in Fortinet Content Pack, have been defined/re-defined 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 #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 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)
3. IBM X-Force (formerly App Exchange) username and password

FORTINET Fabric-Ready

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.

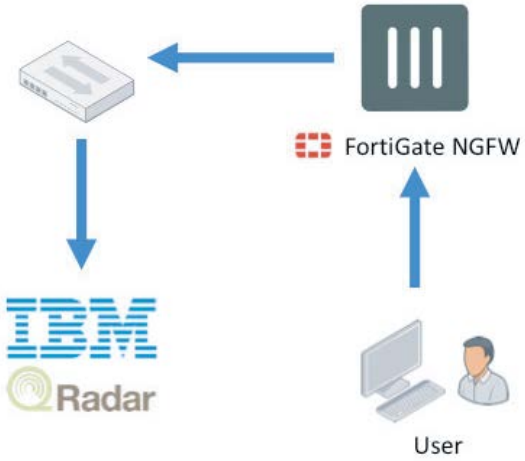
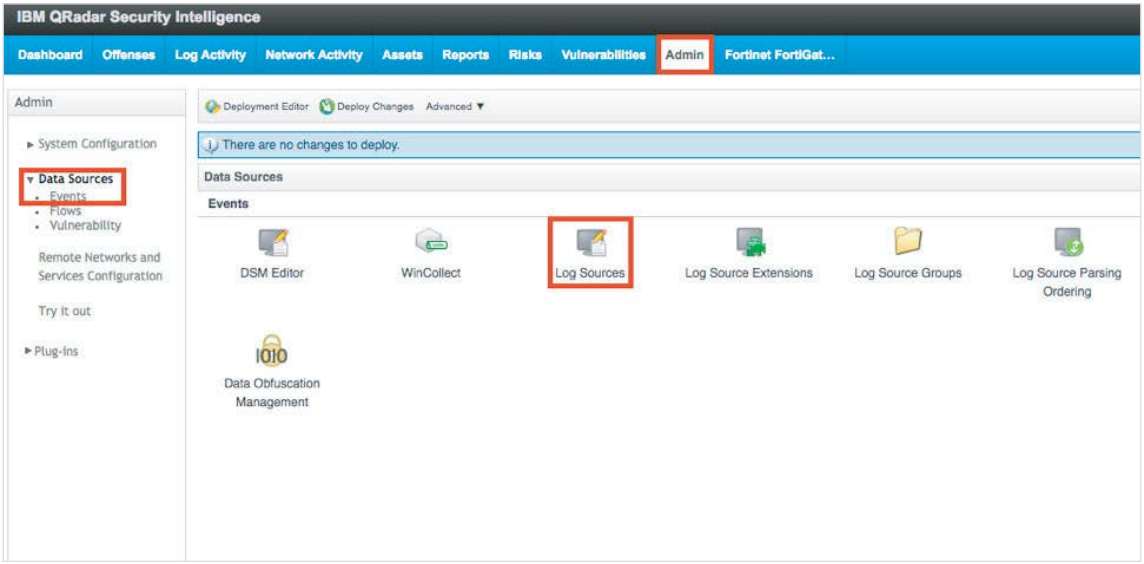


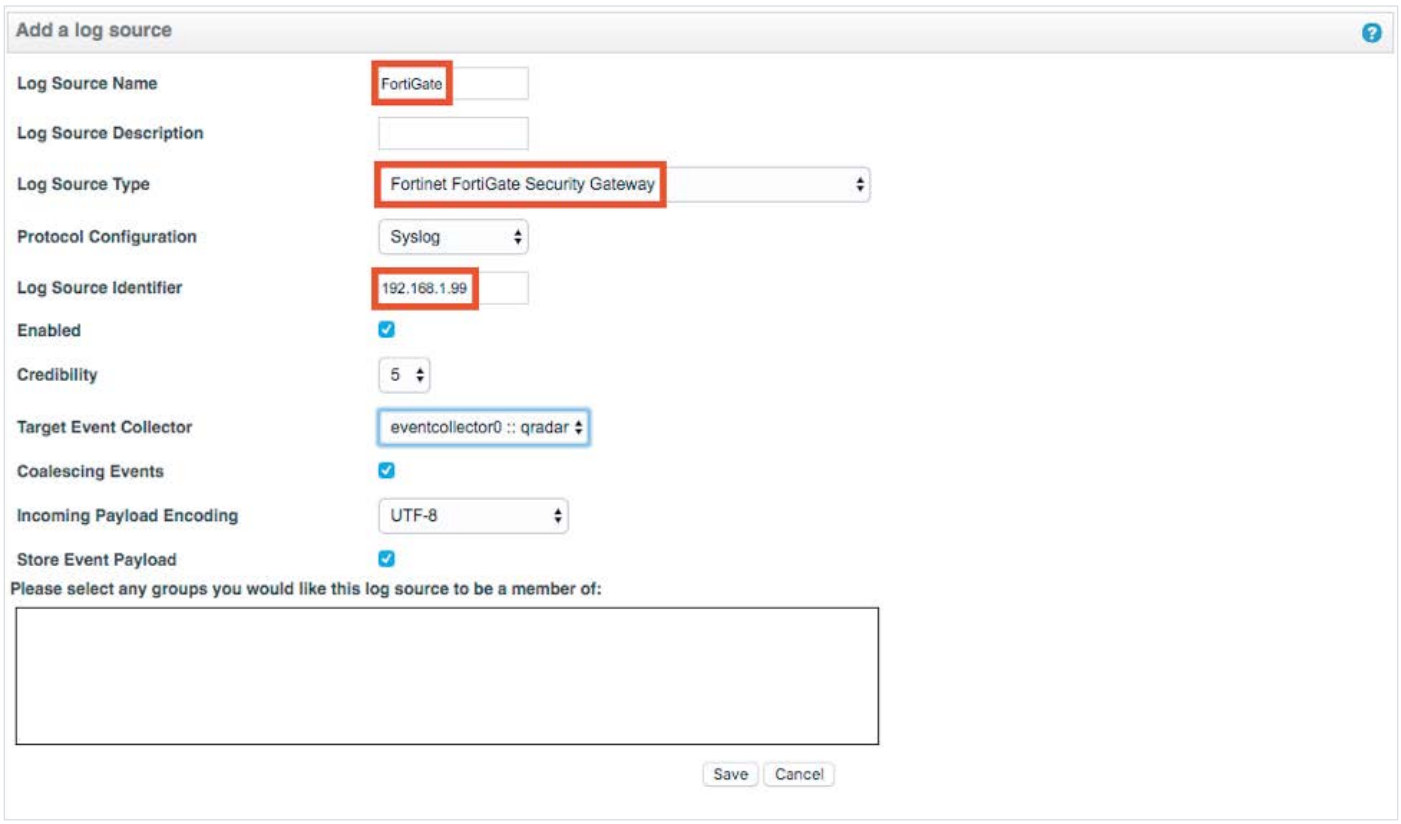
Figure 1: Architecture Overview.

QRadar Configuration

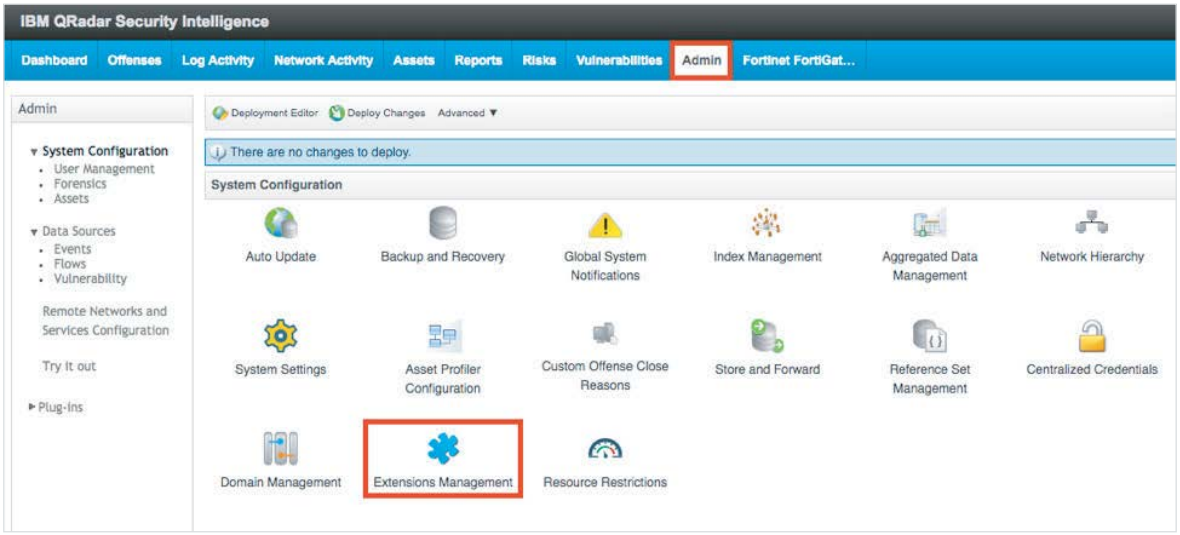
Add a Log Source from Admin > Data Sources > Events > Log Sources.



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.

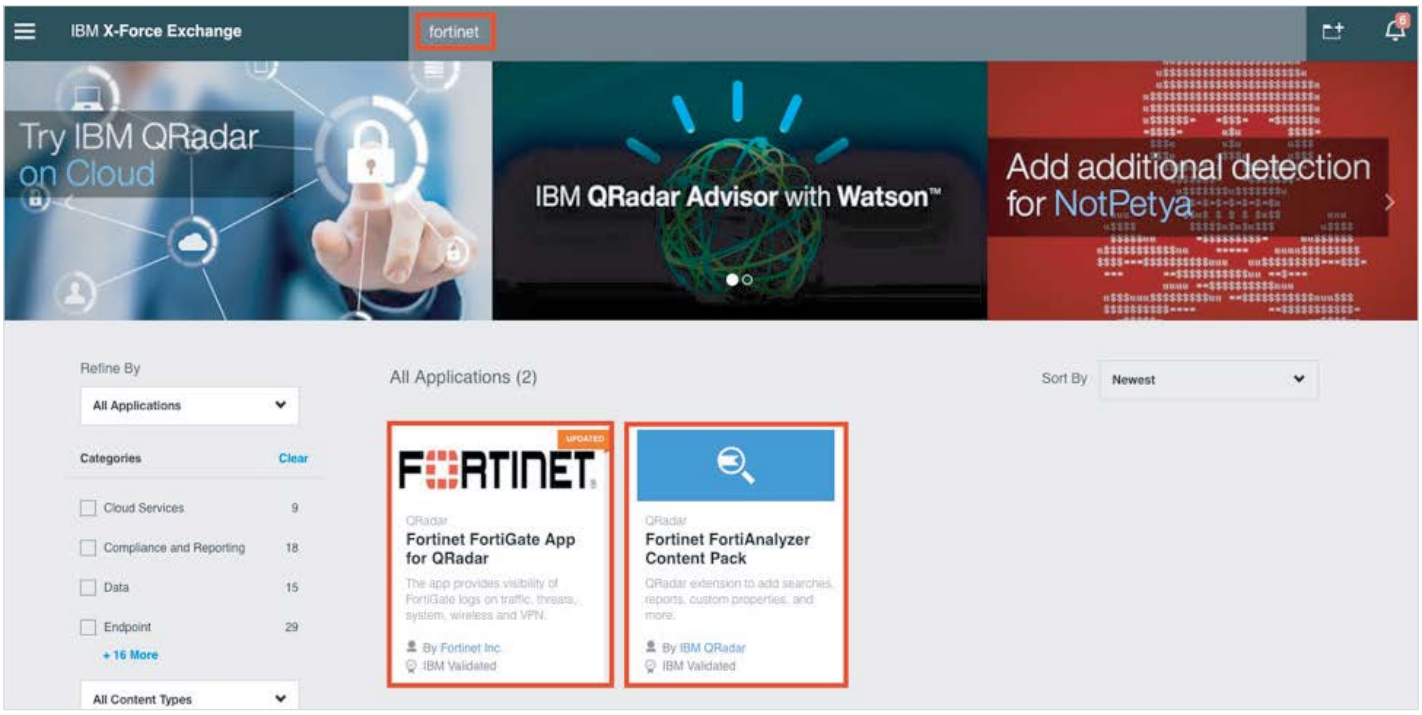


5. From the Admin screen, select Extensions Management.



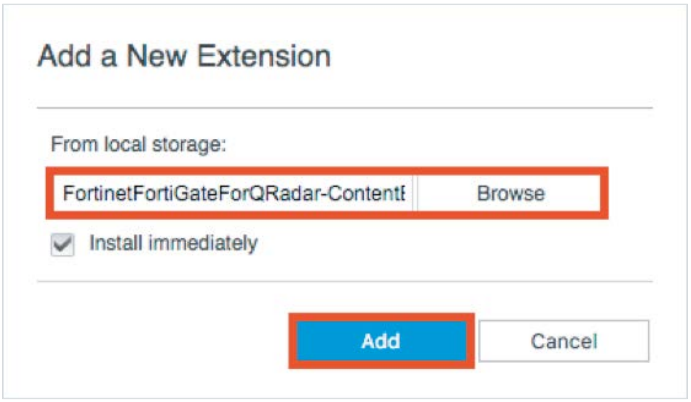
6. Click IBM Security App Exchange to launch the X-Force/App Exchange portal.

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.

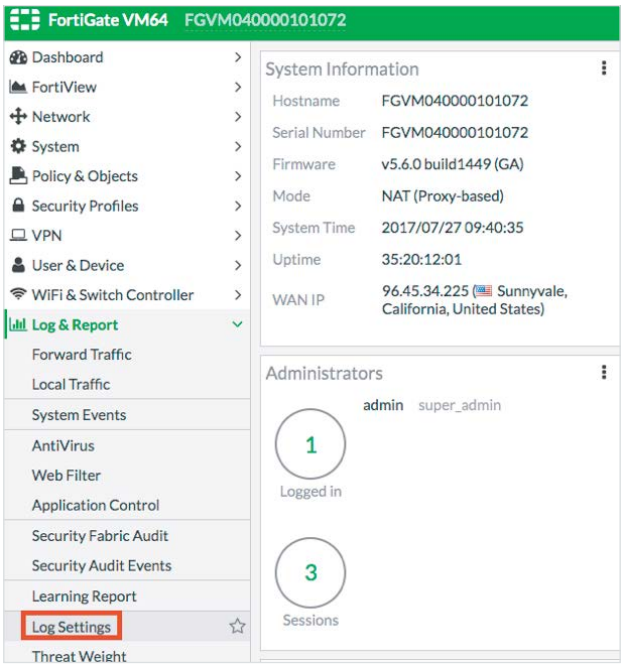
11. Browse for the Content Pack file downloaded previously then click Add.
12. Select Overwrite if some customized properties already exist.



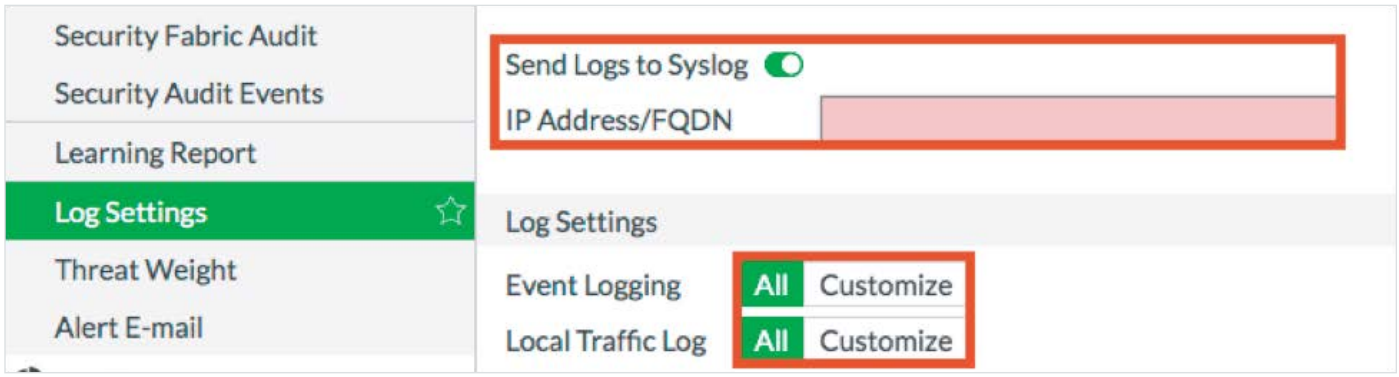
13. Do the same for the FortiGate App.

Fortinet Configuration

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



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.



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.

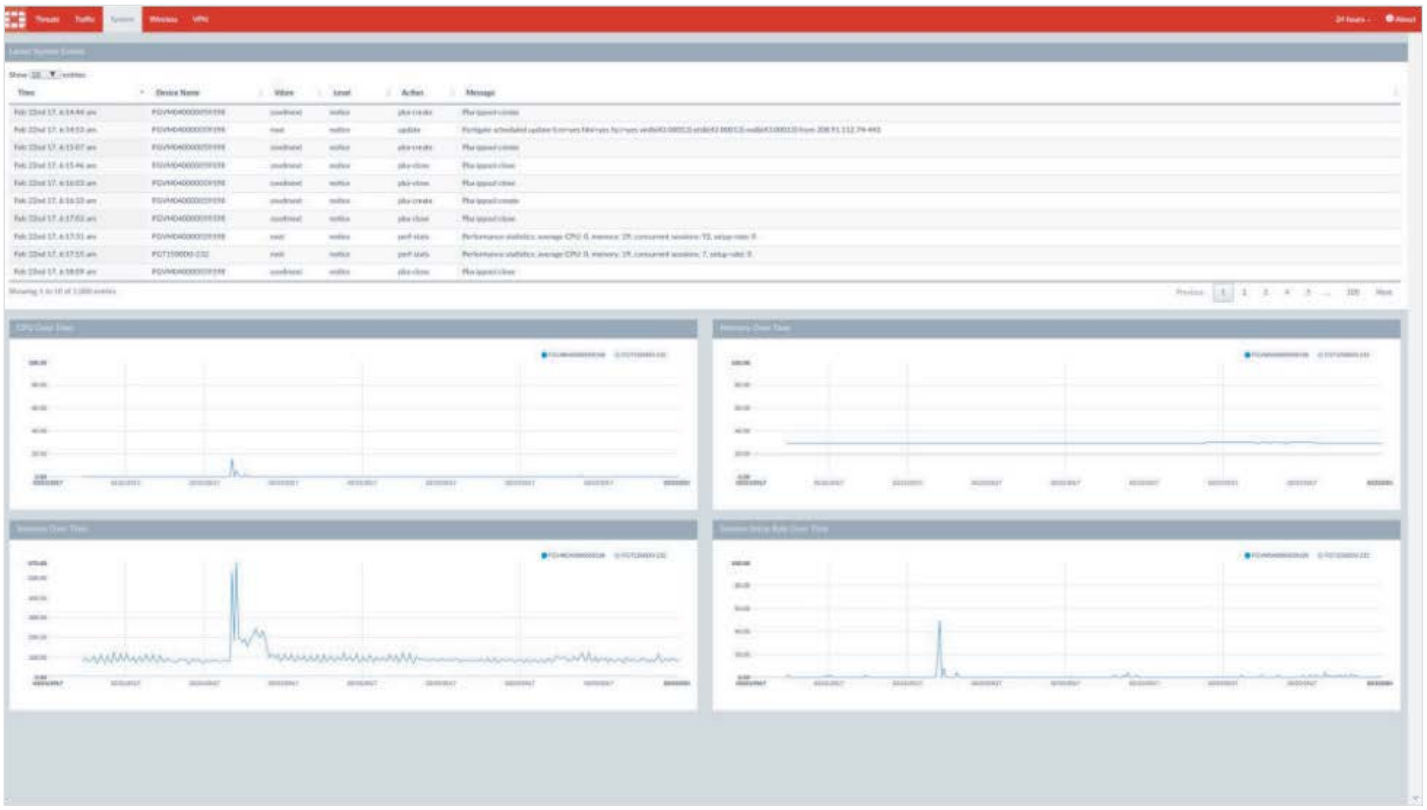
Display Dashboards

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.

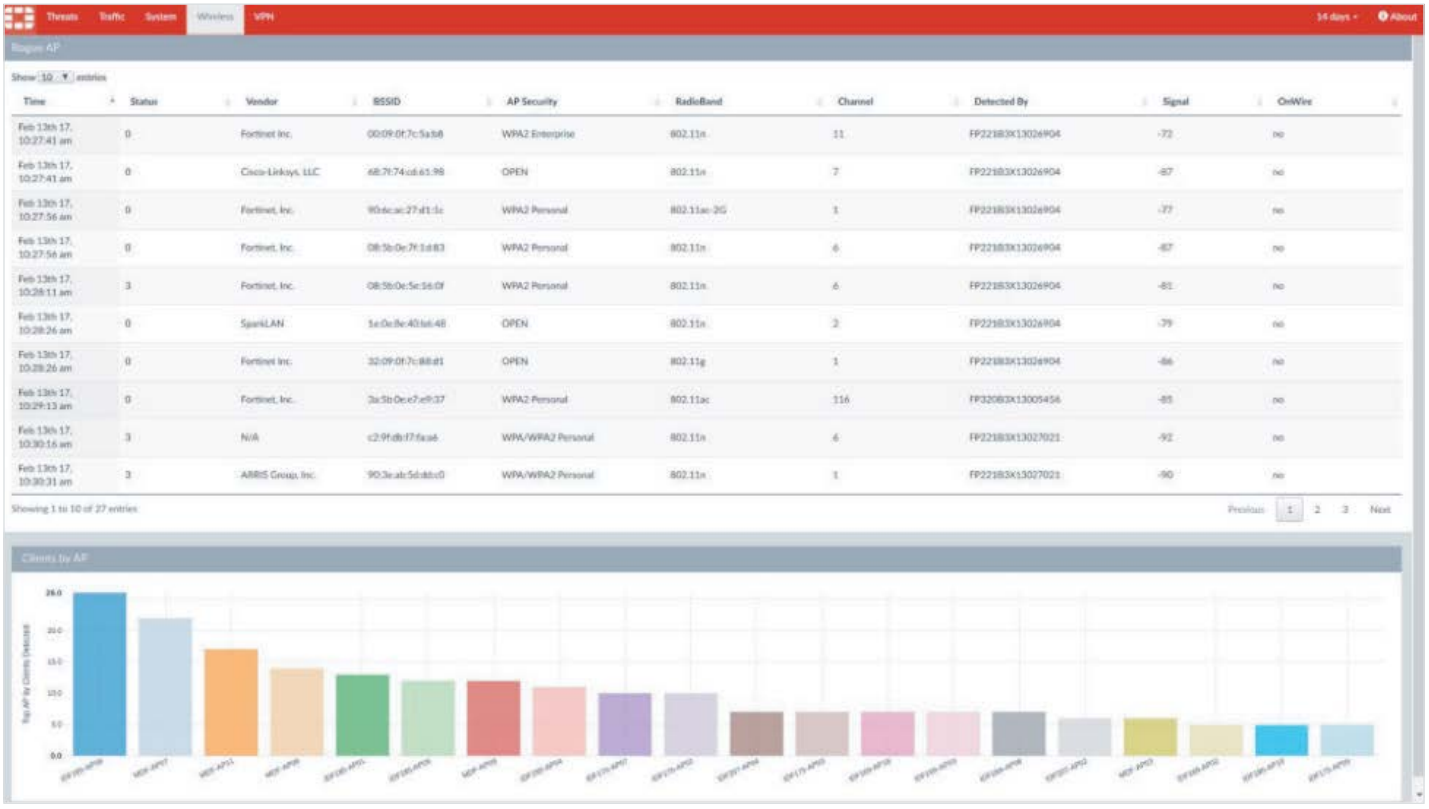
Threat Dashboards

Traffic Dashboards

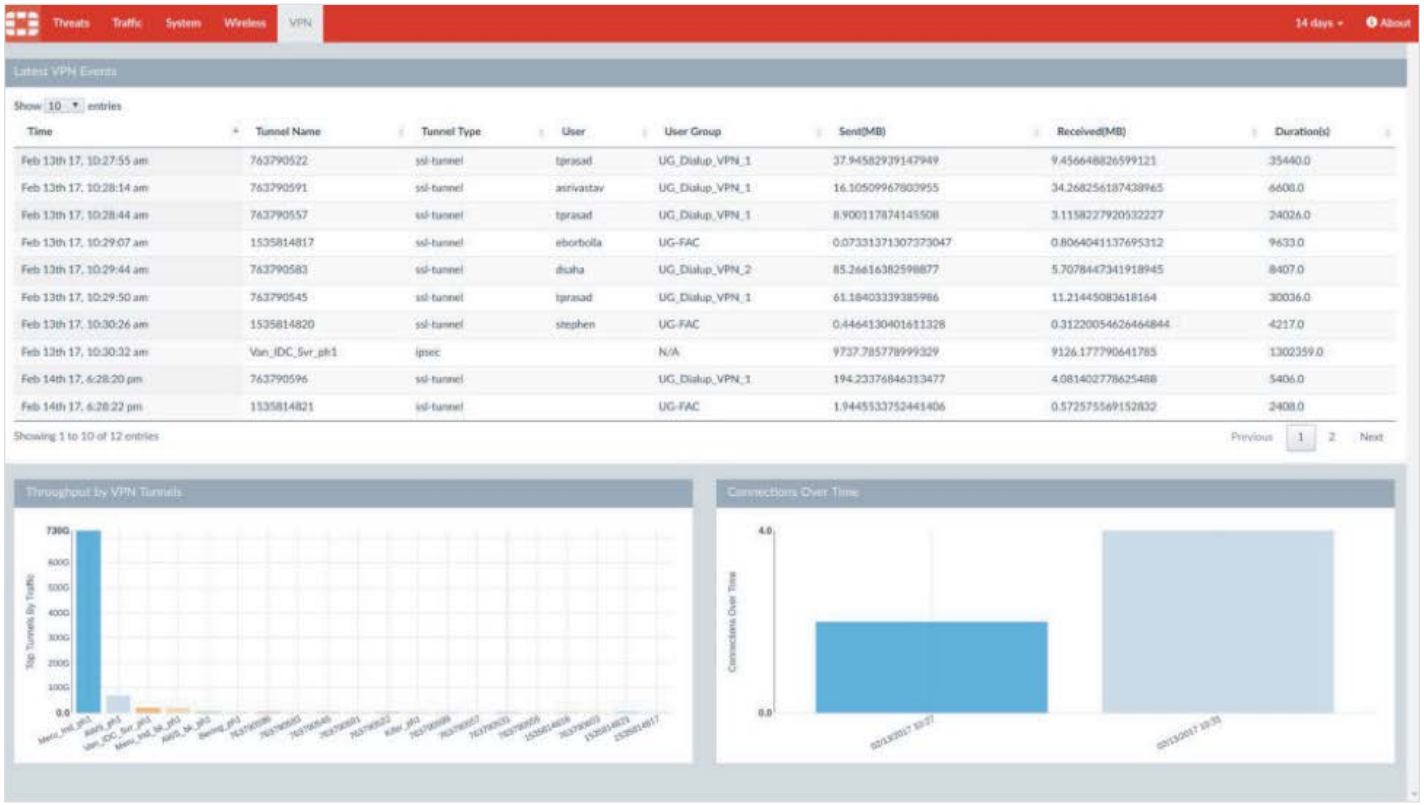
System Dashboards



Wireless Dashboards



VPN Dashboards



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, Anti-Virus, 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/re-defined 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.

July 10, 2019 1:19 AM

115271-A-0-EN

D:\Fortinet\Deployment Guide\Security Fabric and IBM QRadar\FA - DG - Fortinet FortiGate and IBM QRadar