CONTENTS

Overview .................................................. 3
Deployment Prerequisites ............................... 3
Architecture Overview .................................. 4
QRadar Configuration .................................... 4
Fortinet Configuration ................................. 7
Summary .................................................. 11
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) is a global provider of high-performance network security and specialized security solutions that provide our customers with the power to protect and control their IT infrastructure. Our purpose-built, integrated security technologies, combined with our FortiGuard security intelligence services, provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape.

The Fortinet Security Fabric brings together all components in your network. It is Broad, Powerful and Automated. In addition to Fortinet products, the Security Fabric also integrates with 3rd Party partners to extend the power of the Security Fabric to other parts of an organization. For more information regarding our Security Fabric Partners, please refer to our Technology Alliances here: https://www.fortinet.com/partners/partnerships/alliance-partners.html

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.

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)
5. IBM X-Force (formerly App Exchange) username and password
DEPLOYMENT GUIDE: FORTINET FORTIGATE AND IBM QRADAR

Architecture Overview

QRADAR CONFIGURATION
ADD a Log Source from Admin > Data Sources > Events > Log Sources
Configure the Log Source
For the Log Source Name enter a unique name
For the Log Source Type Select Fortinet FortiGate Security Gateway
For the Log Source Identifier enter the FortiGate IP address

From the Admin screen select Extensions Management
Click IBM Security App Exchange to launch the X-Force/App Exchange portal

Search for “Fortinet”
Download the Fortinet Content Pack for QRadar
Download the Fortinet FortiGate App for QRadar

Install the Content Pack and then the FortiGate App from the Extensions Management screen by clicking Add
Browse for the Content Pack file downloaded previously then click Add
Select Overwrite if some customized properties already exist

Do the same for the FortiGate App

**FORTINET CONFIGURATION**

Configure FortiGate to send Syslog to the QRadar IP address

Under Log & Report click Log Settings
Enable Send Logs to Syslog
Enter the IP Address or FQDN of the QRadar server
Select the desired Log Settings
Click Save

Note: If the primary Syslog is already configured you can use the CLI to configure additional Syslog servers

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 DASHBOARD

TRAFFIC DASHBOARD
SYSTEM DASHBOARD

WIRELESS DASHBOARD
VPN DASHBOARD

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](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.