FORTINET FORTIGATE AND IBM QRADAR

DEPLOYMENT GUIDE

CONTENTS

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.

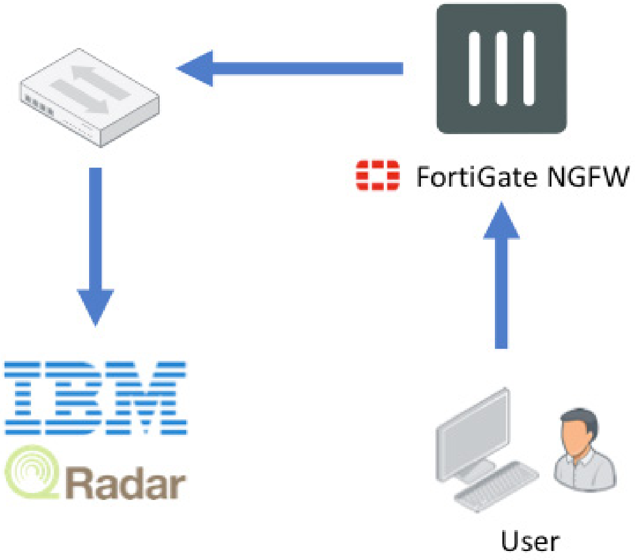
The Fortinet Security Fabric brings together all components in your network. It is Broad, Powerful and Automated. In addition to Fortinet products, the Security Fabric also integrates with 3rd Party partners to extend the power of the Security Fabric to other parts of an organization. For more information regarding our Security Fabric Partners, please refer tour 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

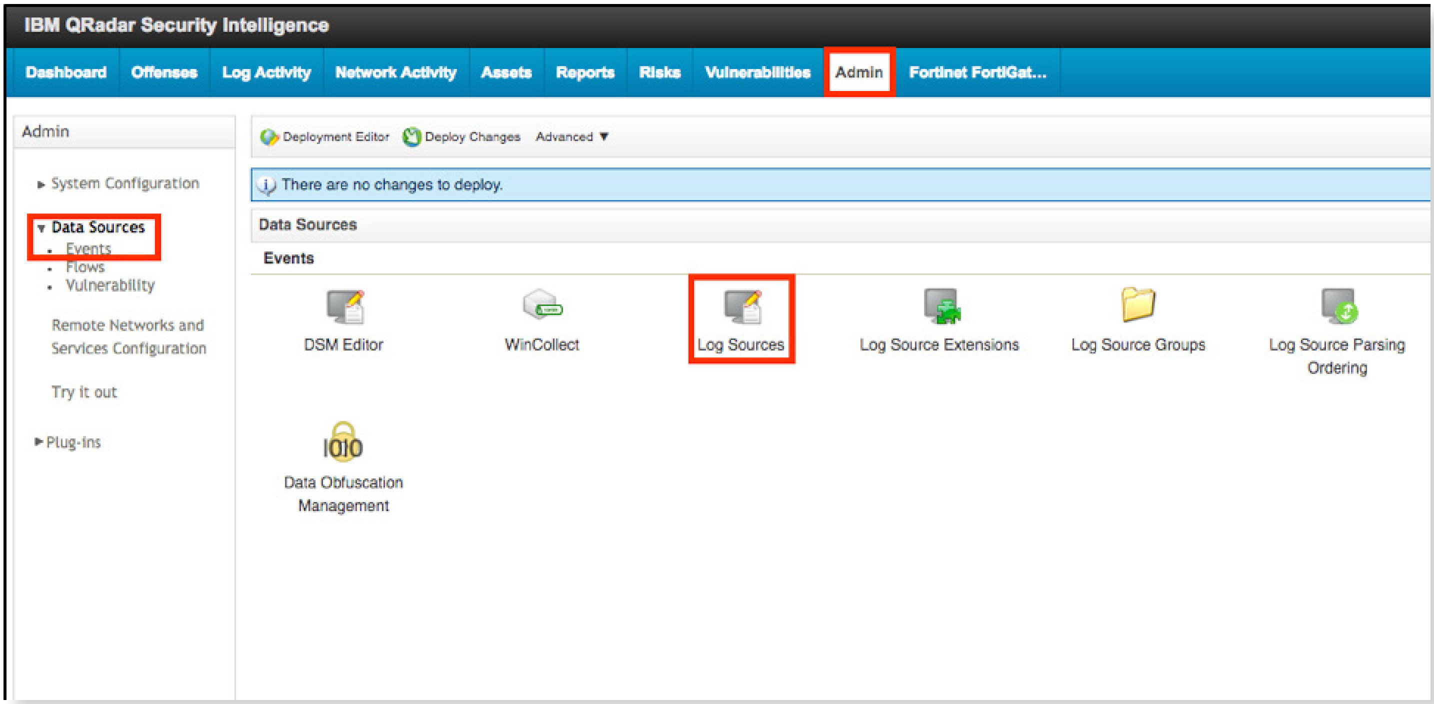
1. Fortinet FortiGate version 5.4 or newer
2. Fortinet FortiAnalyzer Content Pack for QRadar
3. Fortinet FortiGate App for QRadar
4. QRadar version 7.2.8 or newer (tested with 7.2.8 Build 20160920132350)
5. IBM X-Force (formerly App Exchange) username and password



Architecture Overview

QRADAR CONFIGURATION

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



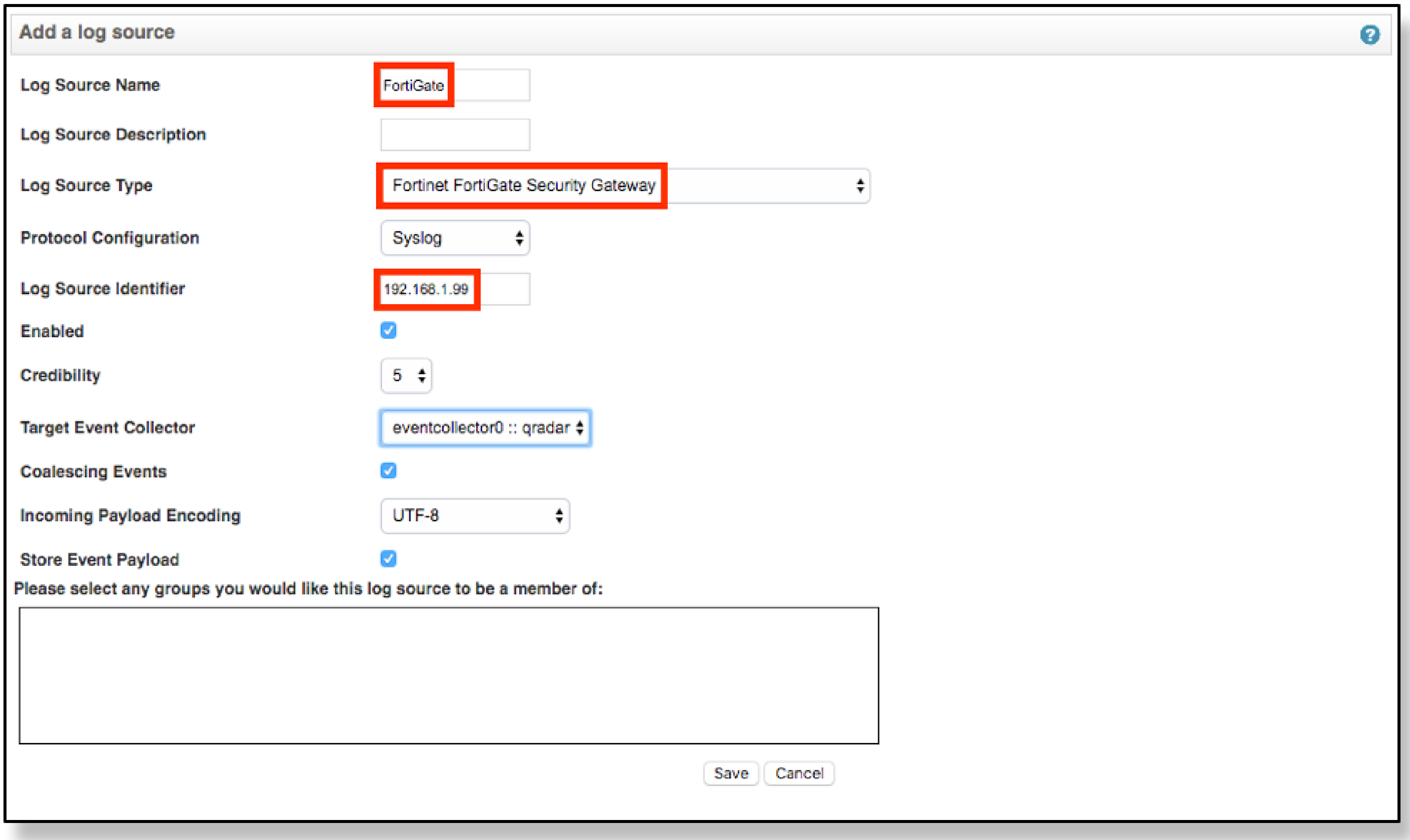
There are no changes to deploy.

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

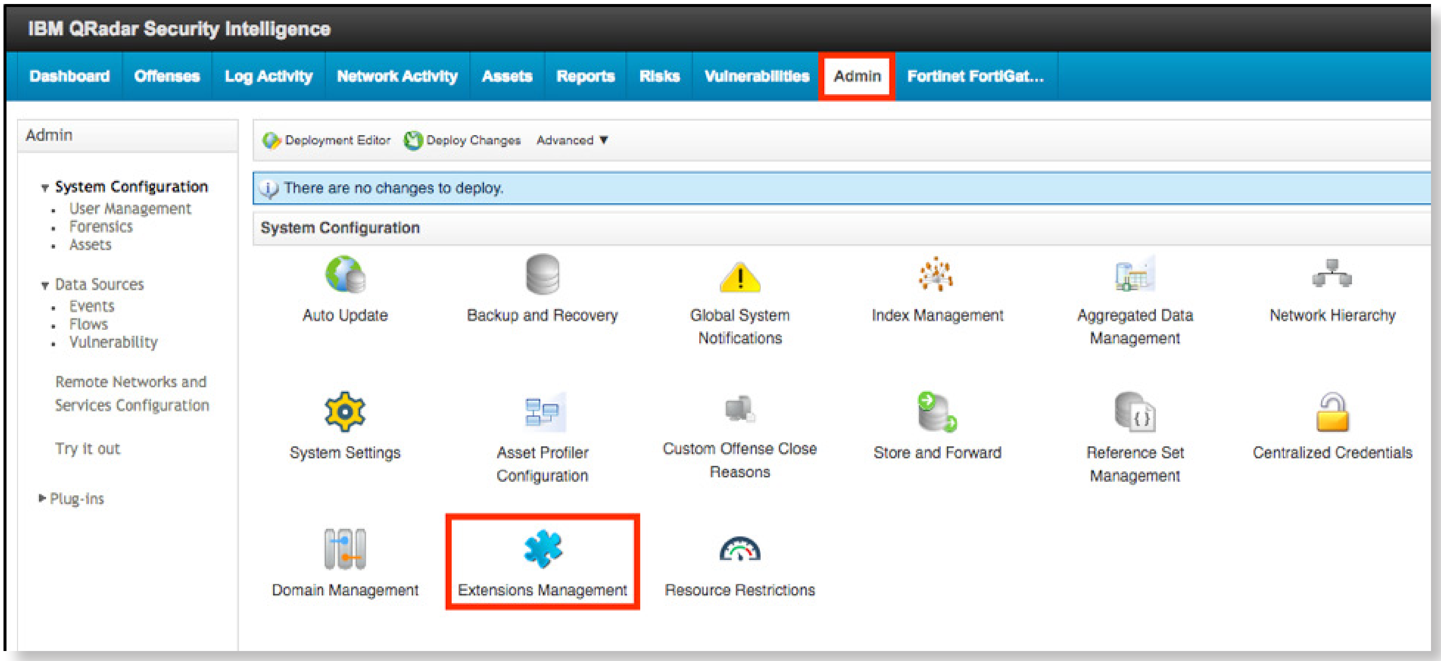


Add a log source

Log Source Name	FortiGate
Log Source Description	
Log Source Type	Fortinet FortiGate Security Gateway
Protocol Configuration	Syslog
Log Source Identifier	192.168.1.99
Enabled	☑
Credibility	5
Target Event Collector	eventcollector0 :: qradar
Coalescing Events	☑
Incoming Payload Encoding	UTF-8
Store Event Payload	☑

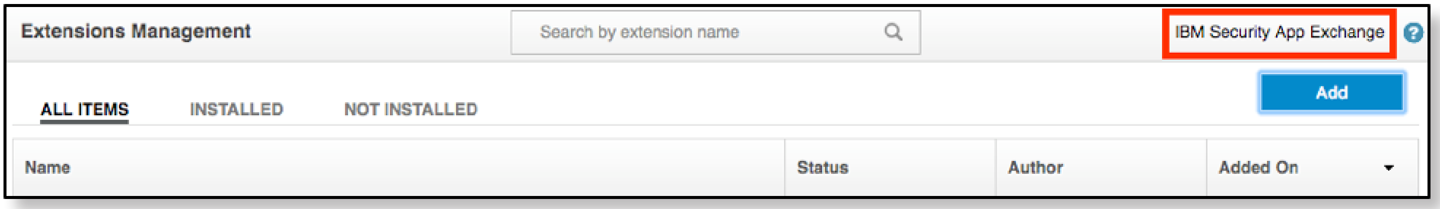
Please select any groups you would like this log source to be a member of:

From the Admin screen select Extensions Management



There are no changes to deploy.

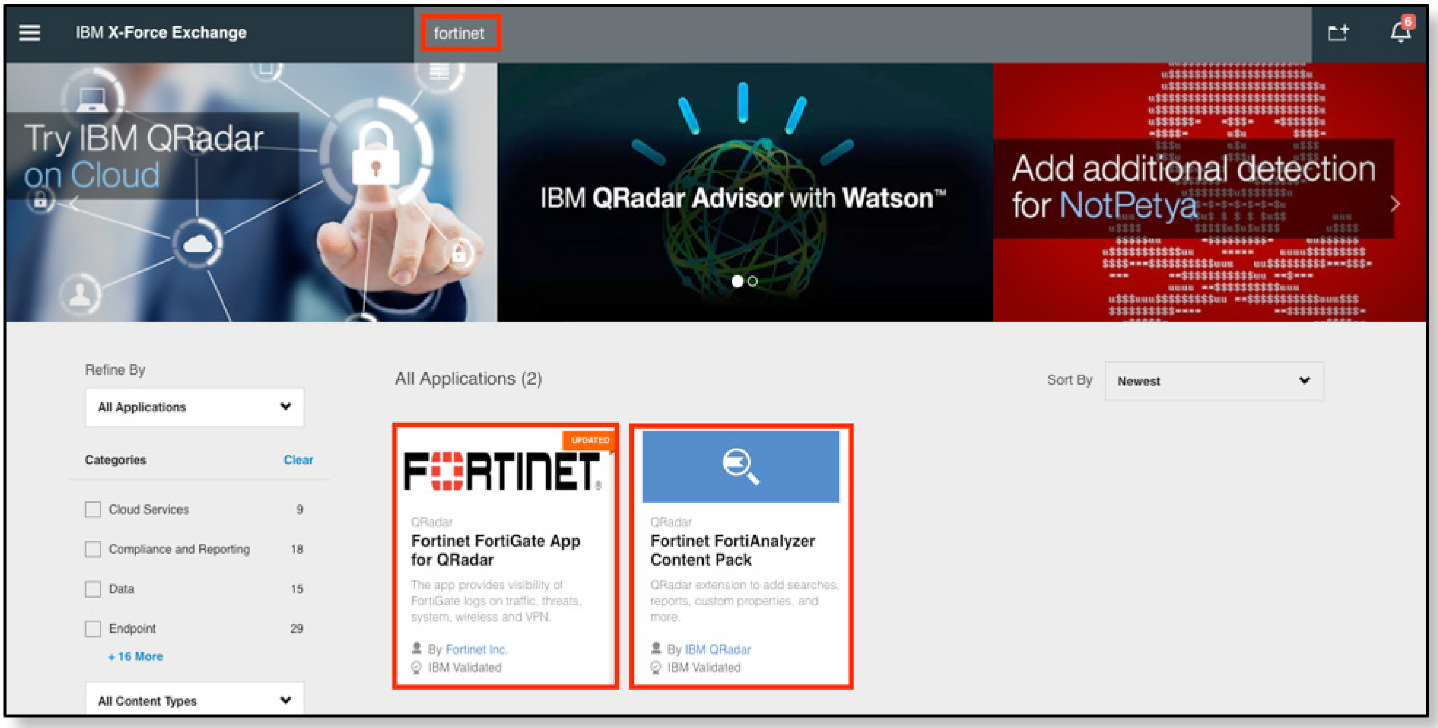
Click IBM Security App Exchange to launch the X-Force/App Exchange portal



Search for "Fortinet"

Download the Fortinet Content Pack for QRadar

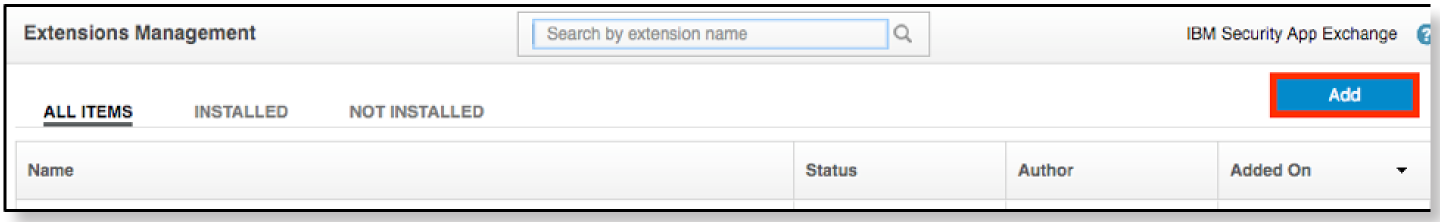
Download the Fortinet FortiGate App for QRadar



QRadar
Fortinet FortiGate App for QRadar
The app provides visibility of FortiGate logs on traffic, threats, system, wireless and VPN.
By Fortinet Inc.
IBM Validated

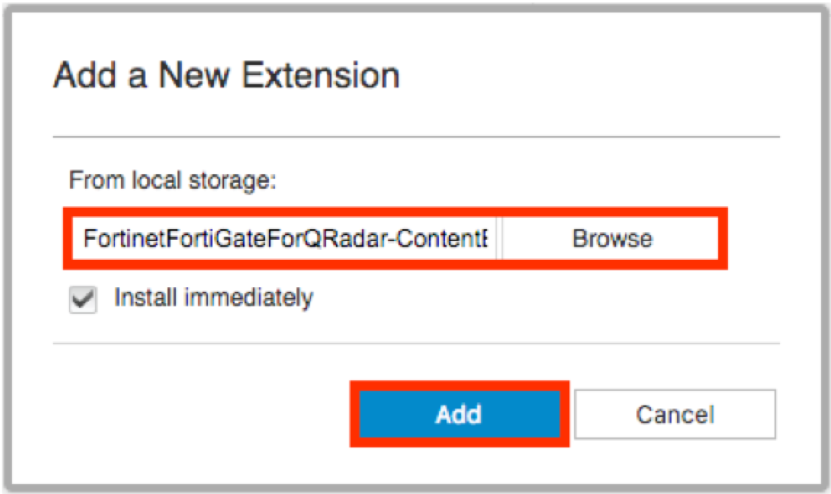
QRadar
Fortinet FortiAnalyzer Content Pack
QRadar extension to add searches, reports, custom properties, and more.
By IBM QRadar
IBM Validated

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



Add a New Extension

From local storage:

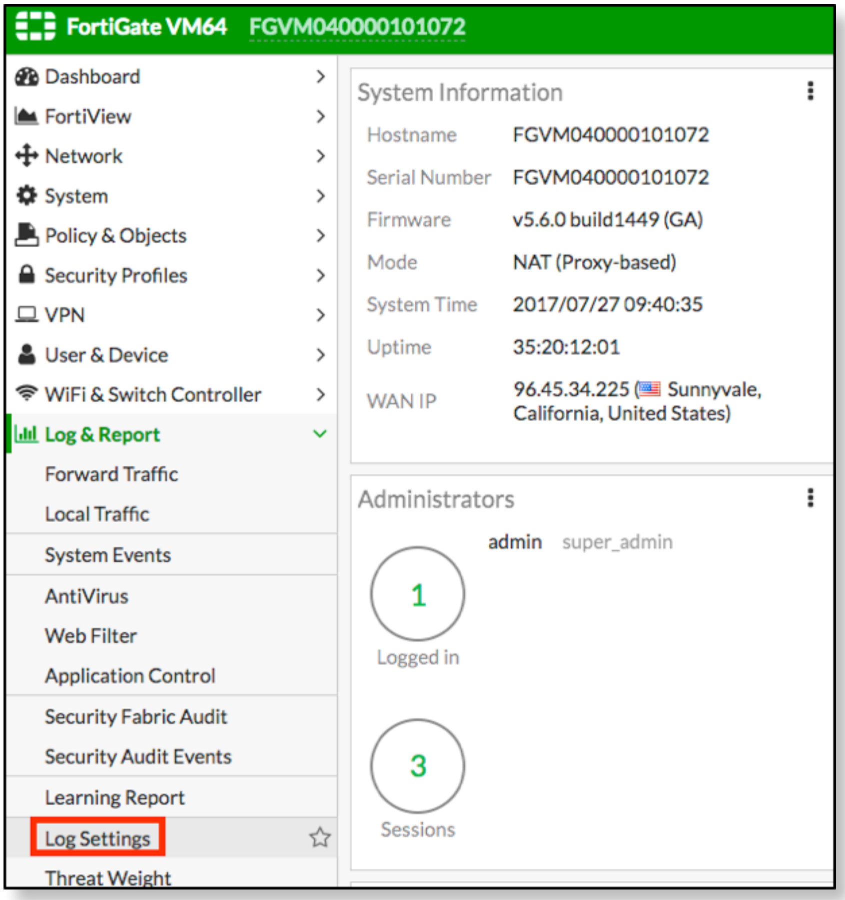
FortinetFortiGateForQRadar-ContentI

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



System Information

Hostname FGVM040000101072

Serial Number FGVM040000101072

Firmware v5.6.0 build1449 (GA)

Mode NAT (Proxy-based)

System Time 2017/07/27 09:40:35

Uptime 35:20:12:01

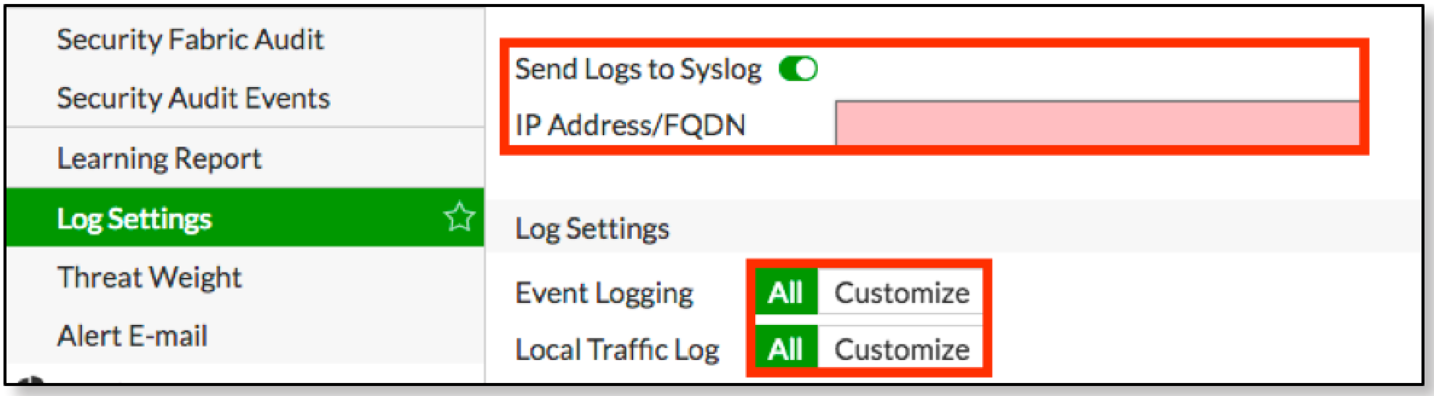
WAN IP 96.45.34.225 (Sunnyvale, California, United States)

Administrators

admin super_admin

Enable Send Logs to Syslog
Enter the IP Address or FQDN of the QRadar server
Select the desired Log Settings

Click Save

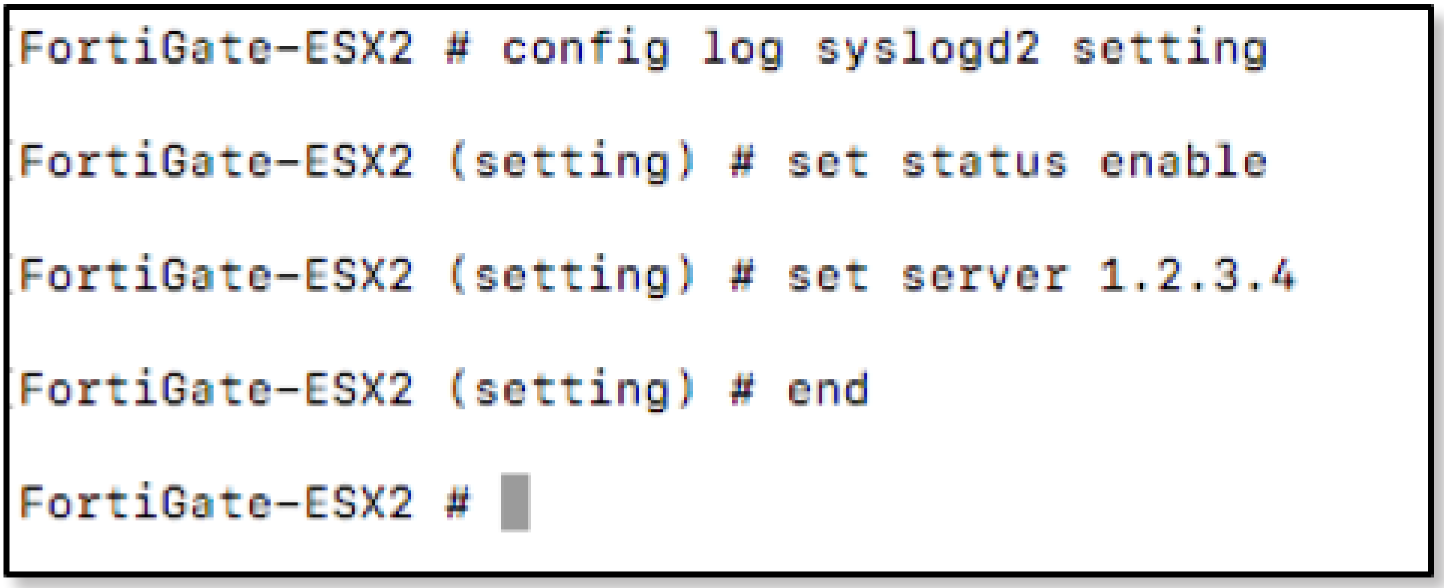


Send Logs to Syslog ●
IP Address/FQDN

Log Settings

Event Logging: All | Customize
Local Traffic Log: All | Customize

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



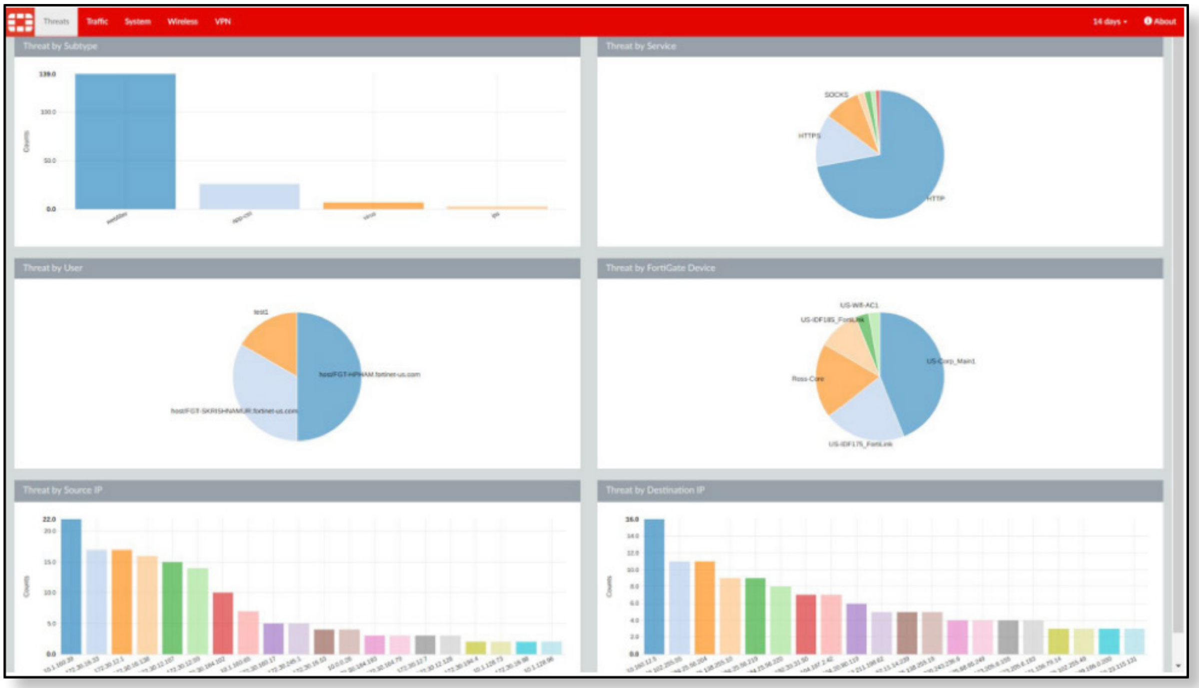
```
FortiGate-ESX2 # config log syslogd2 setting

FortiGate-ESX2 (setting) # set status enable

FortiGate-ESX2 (setting) # set server 1.2.3.4

FortiGate-ESX2 (setting) # end

FortiGate-ESX2 #
```

The configuration is now complete

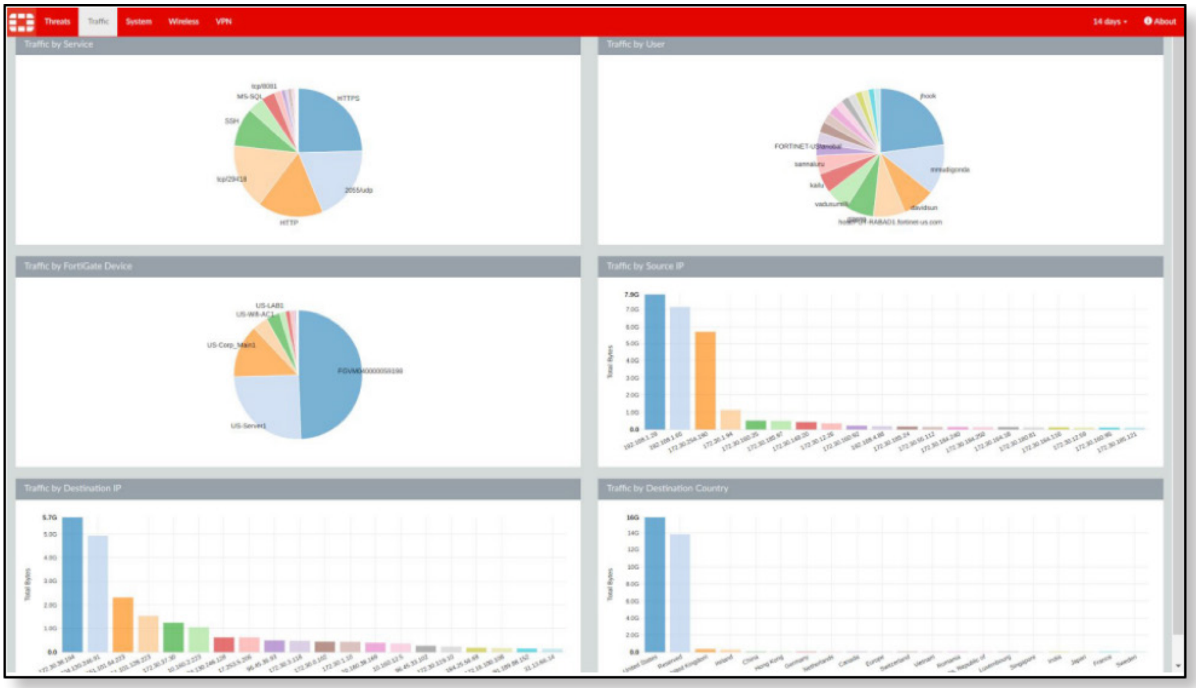
DISPLAY DASHBOARDS

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.

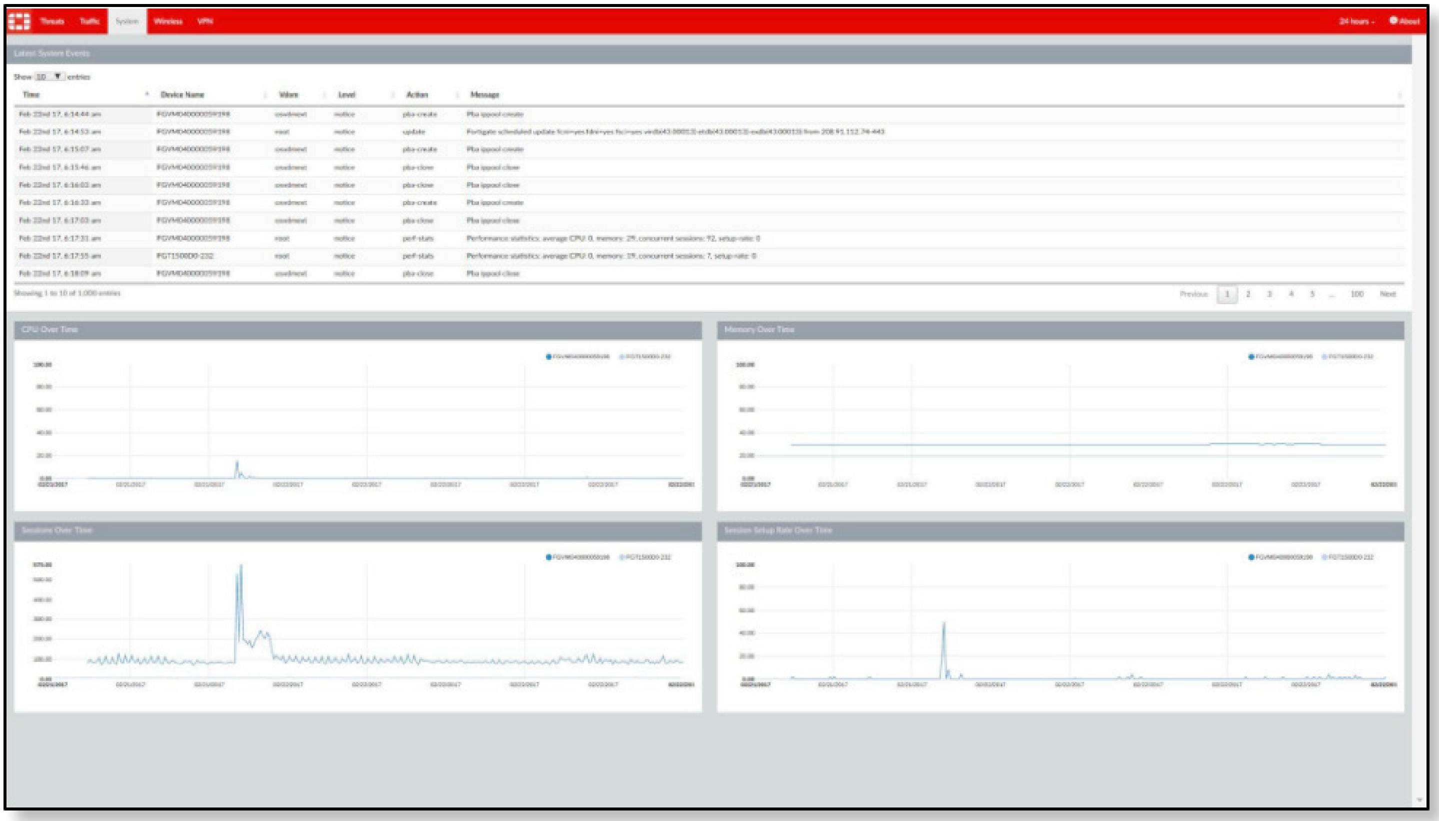
THREAT DASHBOARD



TRAFFIC DASHBOARD



SYSTEM DASHBOARD



Latest System Events

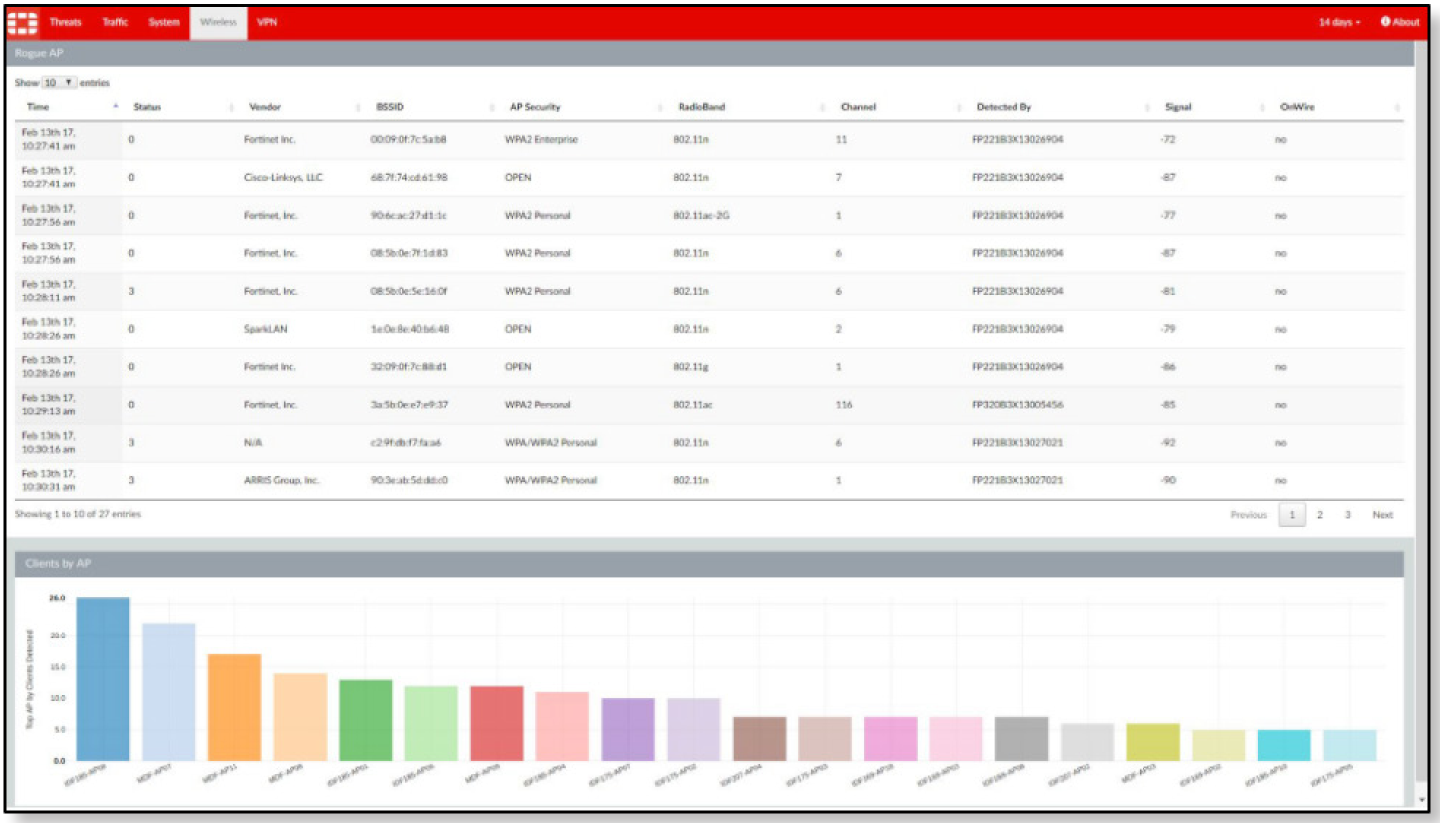
Show 10 ▼ entries

Time	Device Name	Vdom	Level	Action	Message
Feb 22nd 17, 6:14:44 am	FGVM040000059198	csvdmext	notice	pba-create	Pba ippool create
Feb 22nd 17, 6:14:53 am	FGVM040000059198	root	notice	update	Fortigate scheduled update fcni=yes fdni=yes fsci=yes virdb(43.00013) etdb(43.00013) exdb(43.00013) from 208.91.112.74:443
Feb 22nd 17, 6:15:07 am	FGVM040000059198	csvdmext	notice	pba-create	Pba ippool create
Feb 22nd 17, 6:15:46 am	FGVM040000059198	csvdmext	notice	pba-close	Pba ippool close
Feb 22nd 17, 6:16:03 am	FGVM040000059198	csvdmext	notice	pba-close	Pba ippool close
Feb 22nd 17, 6:16:33 am	FGVM040000059198	csvdmext	notice	pba-create	Pba ippool create
Feb 22nd 17, 6:17:03 am	FGVM040000059198	csvdmext	notice	pba-close	Pba ippool close
Feb 22nd 17, 6:17:31 am	FGVM040000059198	root	notice	perf-stats	Performance statistics: average CPU: 0, memory: 29, concurrent sessions: 92, setup-rate: 0
Feb 22nd 17, 6:17:55 am	FGT1500D0-232	root	notice	perf-stats	Performance statistics: average CPU: 0, memory: 19, concurrent sessions: 7, setup-rate: 0
Feb 22nd 17, 6:18:09 am	FGVM040000059198	csvdmext	notice	pba-close	Pba ippool close

Showing 1 to 10 of 1,000 entries

Previous 1 2 3 4 5 … 100 Next

WIRELESS DASHBOARD



Rogue AP

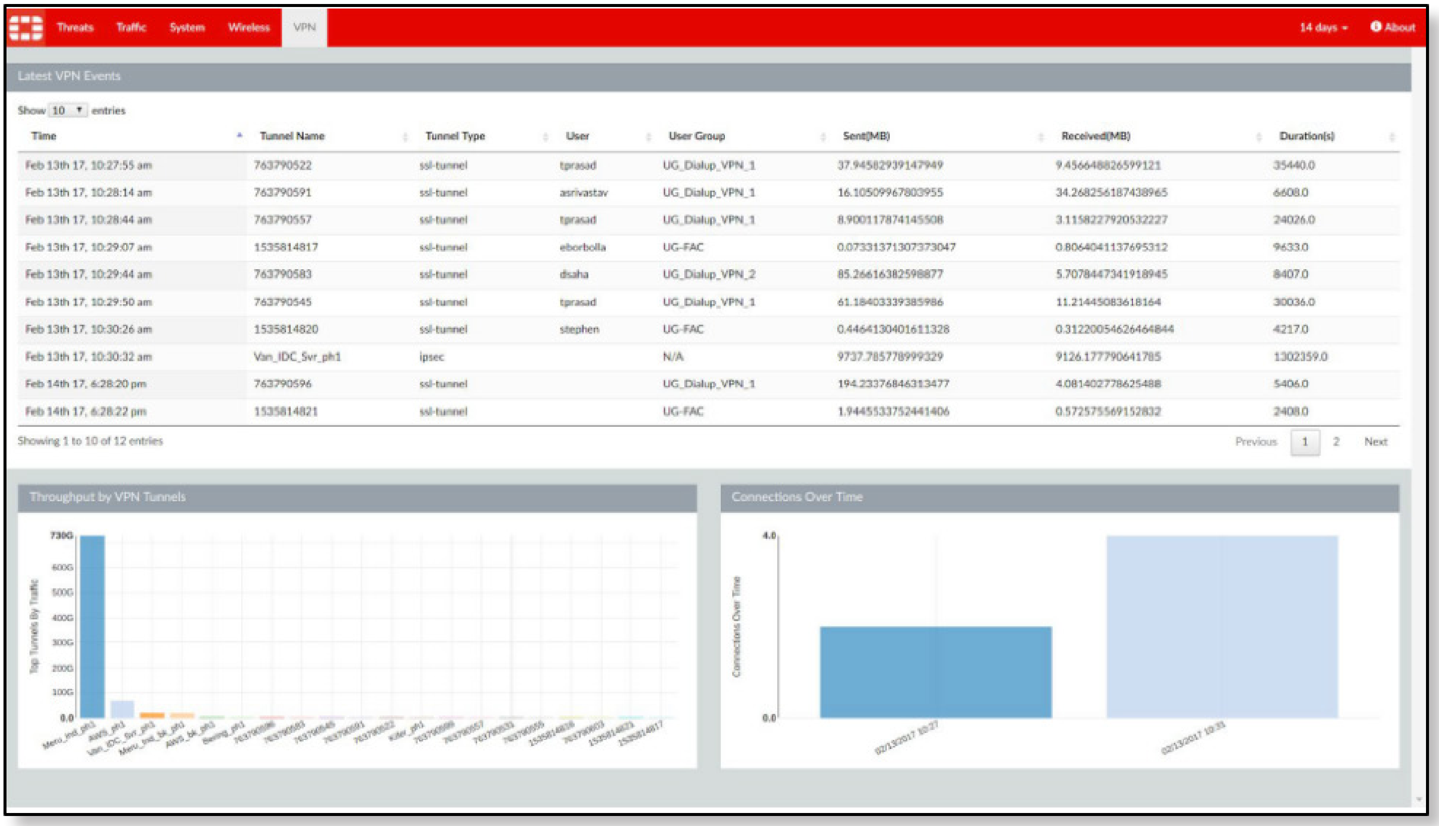
Show 10 ▼ entries

Time	Status	Vendor	BSSID	AP Security	RadioBand	Channel	Detected By	Signal	OnWire
Feb 13th 17, 10:27:41 am	0	Fortinet Inc.	00:09:0f:7c:5a:b8	WPA2 Enterprise	802.11n	11	FP221B3X13026904	-72	no
Feb 13th 17, 10:27:41 am	0	Cisco-Linksys, LLC	68:7f:74:cd:61:98	OPEN	802.11n	7	FP221B3X13026904	-87	no
Feb 13th 17, 10:27:56 am	0	Fortinet, Inc.	90:6c:ac:27:d1:1c	WPA2 Personal	802.11ac-2G	1	FP221B3X13026904	-77	no
Feb 13th 17, 10:27:56 am	0	Fortinet, Inc.	08:5b:0e:7f:1d:83	WPA2 Personal	802.11n	6	FP221B3X13026904	-87	no
Feb 13th 17, 10:28:11 am	3	Fortinet, Inc.	08:5b:0e:5e:16:0f	WPA2 Personal	802.11n	6	FP221B3X13026904	-81	no
Feb 13th 17, 10:28:26 am	0	SparkLAN	1e:0e:8e:40:b6:48	OPEN	802.11n	2	FP221B3X13026904	-79	no
Feb 13th 17, 10:28:26 am	0	Fortinet Inc.	32:09:0f:7c:88:d1	OPEN	802.11g	1	FP221B3X13026904	-86	no
Feb 13th 17, 10:29:13 am	0	Fortinet, Inc.	3a:5b:0e:e7:e9:37	WPA2 Personal	802.11ac	116	FP320B3X13005456	-85	no
Feb 13th 17, 10:30:16 am	3	N/A	c2:9f:db:f7:fa:a6	WPA/WPA2 Personal	802.11n	6	FP221B3X13027021	-92	no
Feb 13th 17, 10:30:31 am	3	ARRIS Group, Inc.	90:3e:ab:5d:dd:c0	WPA/WPA2 Personal	802.11n	1	FP221B3X13027021	-90	no

Showing 1 to 10 of 27 entries

Previous 1 2 3 Next

VPN DASHBOARD



Latest VPN Events

Show 10 ▾ entries

Time	Tunnel Name	Tunnel Type	User	User Group	Sent(MB)	Received(MB)	Duration(s)
Feb 13th 17, 10:27:55 am	763790522	ssl-tunnel	tprasad	UG_Dialup_VPN_1	37.94582939147949	9.456648826599121	35440.0
Feb 13th 17, 10:28:14 am	763790591	ssl-tunnel	asrivastav	UG_Dialup_VPN_1	16.10509967803955	34.268256187438965	6608.0
Feb 13th 17, 10:28:44 am	763790557	ssl-tunnel	tprasad	UG_Dialup_VPN_1	8.900117874145508	3.1158227920532227	24026.0
Feb 13th 17, 10:29:07 am	1535814817	ssl-tunnel	eborbolla	UG-FAC	0.07331371307373047	0.8064041137695312	9633.0
Feb 13th 17, 10:29:44 am	763790583	ssl-tunnel	dsaha	UG_Dialup_VPN_2	85.26616382598877	5.707844734191 8945	8407.0
Feb 13th 17, 10:29:50 am	763790545	ssl-tunnel	tprasad	UG_Dialup_VPN_1	61.18403339385986	11.21445083618164	30036.0
Feb 13th 17, 10:30:26 am	1535814820	ssl-tunnel	stephen	UG-FAC	0.4464130401611328	0.31220054626464844	4217.0
Feb 13th 17, 10:30:32 am	Van_IDC_Svr_ph1	ipsec		N/A	9737.785778999329	9126.177790641785	1302359.0
Feb 14th 17, 6:28:20 pm	763790596	ssl-tunnel		UG_Dialup_VPN_1	194.23376846313477	4.081402778625488	5406.0
Feb 14th 17, 6:28:22 pm	1535814821	ssl-tunnel		UG-FAC	1.9445533752441406	0.572575569152832	2408.0

Showing 1 to 10 of 12 entries

Previous 1 2 Next

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://exchange.xforce.ibmcloud.com/hub

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.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990