

DEPLOYMENT GUIDE

# Fortinet FortiGate and Splunk

## Fortinet FortiGate and Splunk

Overview
Deployment Prerequisites
Architecture Overview
Splunk Configuration4
Fortinet Configuration
Troubleshooting
Summary

### FERTINET

#### **Overview**

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.

#### **About Splunk**

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. Splunk Enterprise makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results.

The FortiGate App for Splunk combines the best security information and event management (SIEM) and threat prevention by aggregating, visualizing and analyzing hundreds of thousands of log events and data from FortiGate physical and virtual firewall appliances. The App dramatically improves the detection, response and recovery from advanced threats by providing broad security intelligence from data that is collected across the cloud.



Figure 1: Architecture Overview.

#### **Deployment Prerequisites**

- 1. Fortinet FortiGate version 5.6
- 2. Fortinet FortiGate App for Splunk version 1.4
- 3. Fortinet FortiGate Add-On for Splunk version 1.5
- 4. Splunk version 6.x (tested with 6.6.2)
- 5. A splunk.com username and password

**Note:** If using an older version of Fortinet FortiGate App for Splunk see the Troubleshooting Section at the end of this article:

https://splunkbase.splunk.com/ app/2800/#/details



#### **Splunk Configuration**

1. To install Splunk Apps, click the gear.



2. To install Splunk Apps, click the gear. Click Browse more apps and search for "Fortinet"

splunk> App	sƳ		
Apps			
Browse more apps	Install app from file	Create app	

3. Install the Fortinet FortiGate Add-On for Splunk. Enter your splunk.com username & password.

Fortinet FortiGate Add-On for Splunk
Fortinet FortiGate Add-On for Splunk is the technical add-on (TA) developed by Fortinet, Inc. The add-on enables Splunk Enterprise to ingest or map security and traffic data collected from FortiGate physical and virtual appliances across
Streamlining authentication and access from FortiGate such as administra More
> Splunk Certified
Category: Security, Fraud & Compliance   Author: Fortinet Inc   Downloads: 6753   Released: 2 years ago   Last Updated: 22 days ago   View on Splunkbase

4. Then install the Fortinet FortiGate App for Splunk. Enter your splunk.com username & password.

Fortinet FortiGate App for Splunk	Install
The Fortinet FortiGate App for Splunk provides datacenter threat duplicate threat feed data to enable the fast creation and consolid properly maps log fields from FortiGate appliances and interchan	visualizations to identify anomalous behavior and helps de- dation of analytics. The Fortinet FortiGate App for Splunk ages into a common format to Splunk in More
Splunk Certified	
Splunk Certified Category: Security, Fraud & Compliance   Author: Fortinet Inc   Downloa	ads: 5895   Released: 2 years ago

5. From Settings click Data Inputs.



6. Under Data Inputs create a new UDP input by clicking Add new on the right.

splunk> Appa ~	Administrator 🗸 Messages	✓ Settings ✓ Activity ✓ Help ✓
Data inputs		
Local inputs Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.		
Type	Inputs	Actiona
Local event log collection Collect event logs from this machine.	83	Edit
Remote event log collections Callect event logs from remote hosts. Note: this uses WMI and requires a domain account.	843	Add new
Files & directories Index a local file or monitor an entire directory.	6	Add new
Local performance monitoring Collect performance data from local machine.	0	Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	Add new
TCP Lister on a TCP port for incoming data, e.g. syslog.	٥	Add new
UDP Listen on a UDP port for incoming data, e.g. systog	0	Add new
Registry monitoring Have Splunk index the local Windows Registry, and menitor it for changes.	0	Add new

7. Create a UDP Data Source on Port 514.

	TCP	UDP
Port?	514	
Source name override?	optional	
	host:port	
nly accept connection from?	optional	



8. Click New.



 Under Input Settings set the Source Type to "fgt\_log". Set the Source Type Category to Custom.

Optionally set additional input parameters for this data input as follows:	
Source type	
The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.	Select New
	Source Type fgt_log
	Source Type Category
	Source Type

#### **Fortinet Configuration**

- 1. Configure FortiGate to send syslog to the Splunk IP address.
- 2. Under Log & Report click Log Settings.



- 3. Enable Send Logs to Syslog.
- 4. Enter the IP Address or FQDN of the Splunk server.
- 5. Select the desired Log Settings.
- 6. Click Save.

Security Fabric Audit Security Audit Events Learning Report	Send Logs to Syslog  IP Address/FQDN
Log Settings 🏠	Log Settings
Threat Weight Alert E-mail	Event LoggingAllCustomizeLocal Traffic LogAllCustomize

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.



#### Troubleshooting

What to do if data doesn't show up in the Dashboards?

- 1. Go to Settings > Data Inputs. Verify that you have a UDP data input enabled on port 514.
- 2. Go to Settings > Indexes.
- 3. Verify that your Index (typically main) is receiving data and that the Latest Event is recent. If not, verify the FortiGate Syslog settings are correct and that it can reach the Splunk server.

#### Summary

The Fortinet FortiGate App for Splunk solution delivers advanced security reporting and analysis in the datacenter that benefits operational reporting, as well as providing simplified and configurable dashboard views across Fortinet firewall appliances, physical and virtual. The FortiGate add-on enables Splunk Enterprise and Enterprise Security to ingest or map security and traffic data collected from FortiGate physical and virtual appliances across domains.

Solution Brief: https://www.fortinet.com/content/dam/fortinet/assets/alliances/SolutionBrief-Fortinet-Splunk.pdf

Fortinet FortiGate App for Splunk: https://splunkbase.splunk.com/app/2800/

Fortinet FortiGate Add-On for Splunk: https://splunkbase.splunk.com/app/2846/



www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. FortiGate®, FortiGate®, FortiGate®, and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective womers. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet enters a binding written contract, signed by Fortinet's General Coursel, with a purchaser that expressly warrants that the identified product will performance in the same ideal conditions as in Fortinet's and, in such event, only the specific performance metrics expressly identified performance there with a purchaser that expressly warrants that the identified product will performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

170843-A-0-EN

D:\Fortinet\Deployment Guide\Fortinet and Splunk\DG - Fortinet FortiGate and Splunk