DEPLOYMENT GUIDE

Fortinet FortiGate and Splunk

Fortinet FortiGate and Splunk

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.

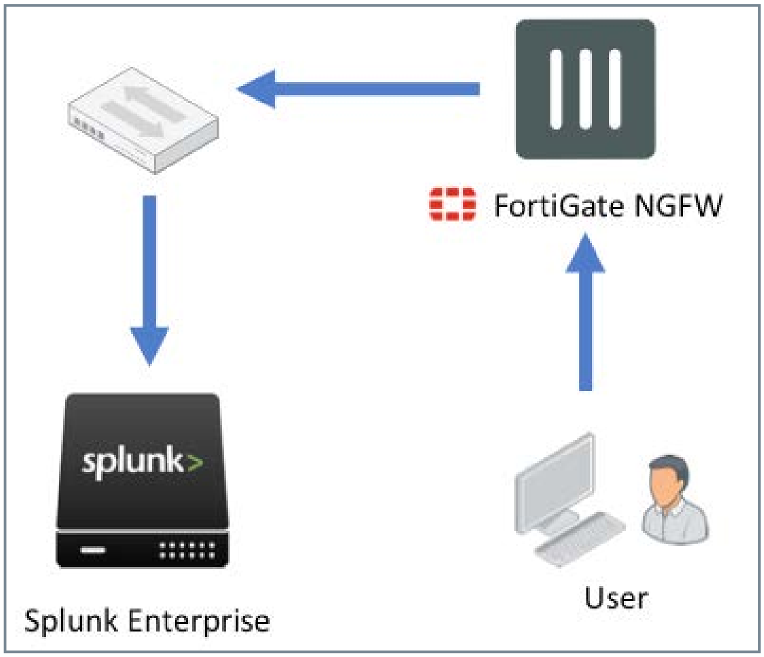


Figure 1: Architecture Overview.

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:

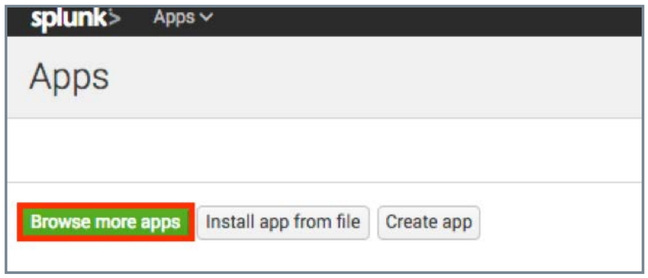
https://splunkbase.splunk.com/app/2800/#/details

FORTINET Fabric-Ready

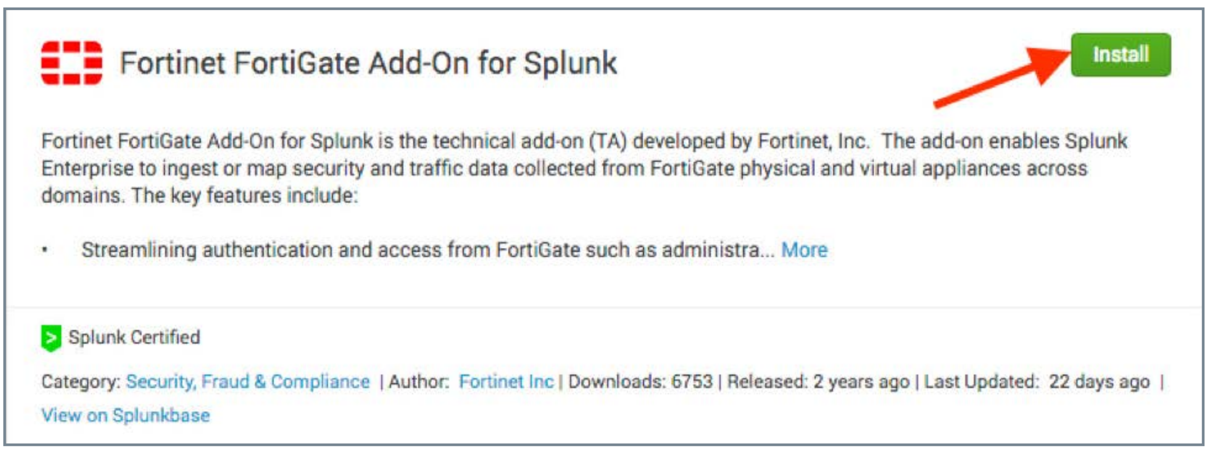
Splunk Configuration

1. To install Splunk Apps, click the gear.

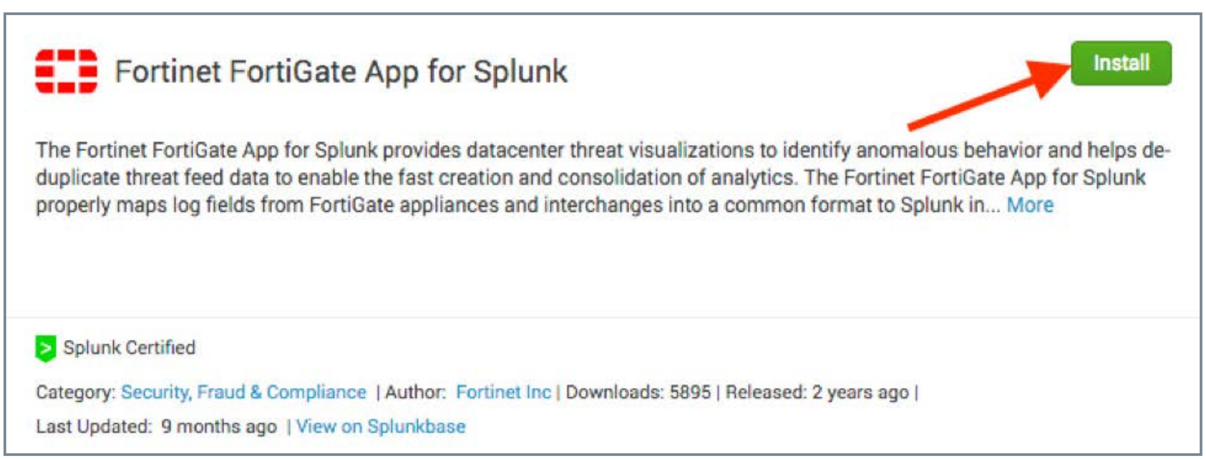
2. To install Splunk Apps, click the gear. Click Browse more apps and search for “Fortinet”



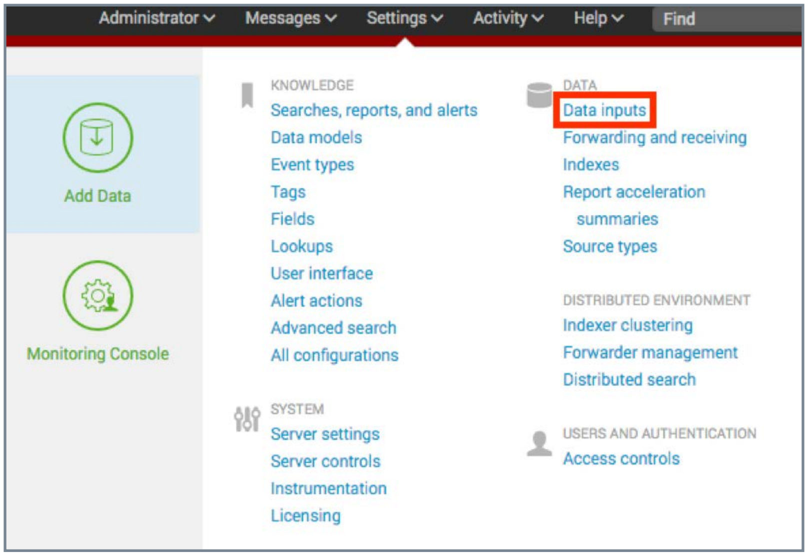
3. Install the Fortinet FortiGate Add-On for Splunk. Enter your splunk.com username & password.



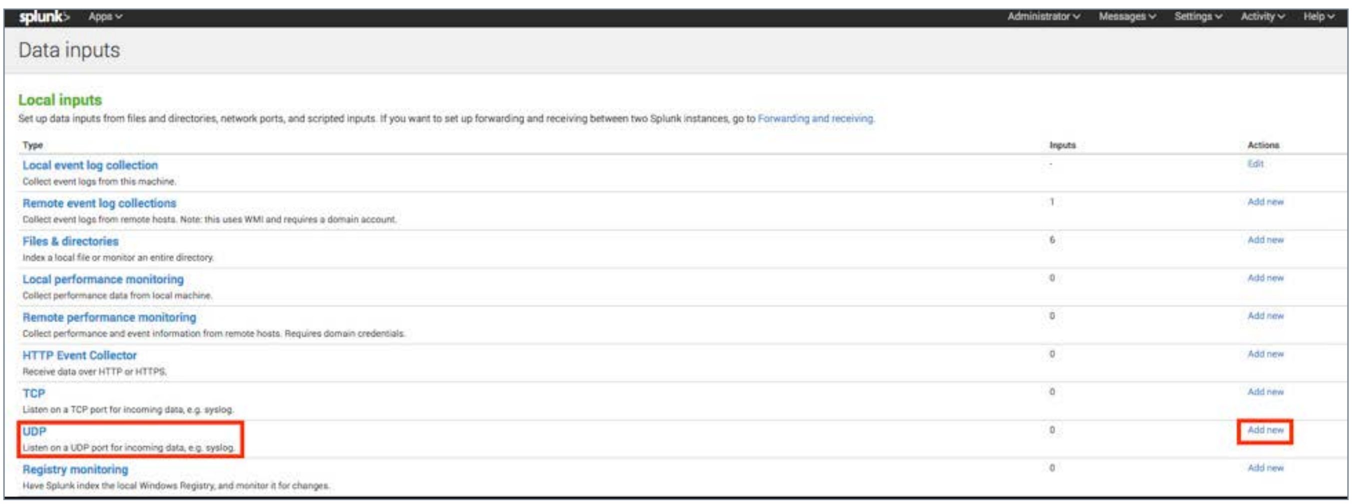
4. Then install the Fortinet FortiGate App for Splunk. Enter your splunk.com username & password.



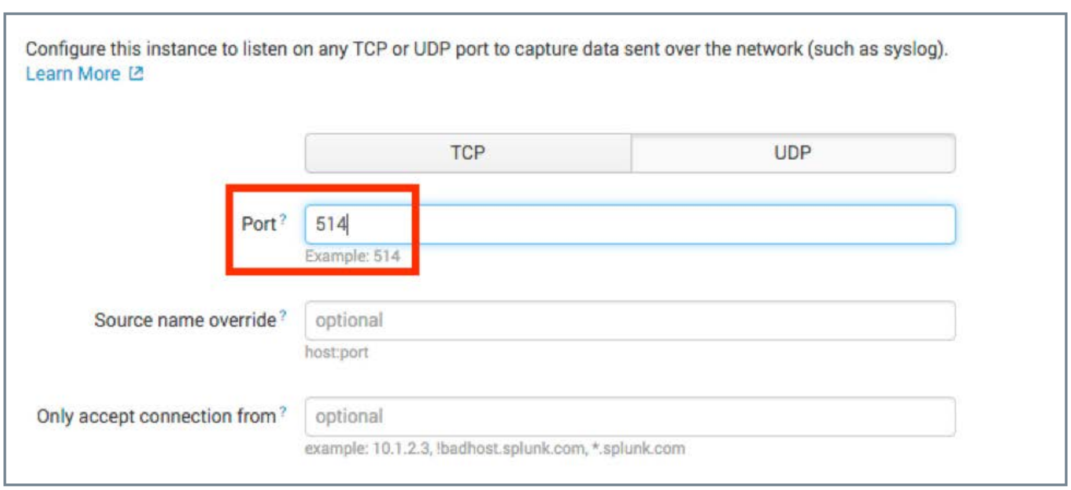
5. From Settings click Data Inputs.



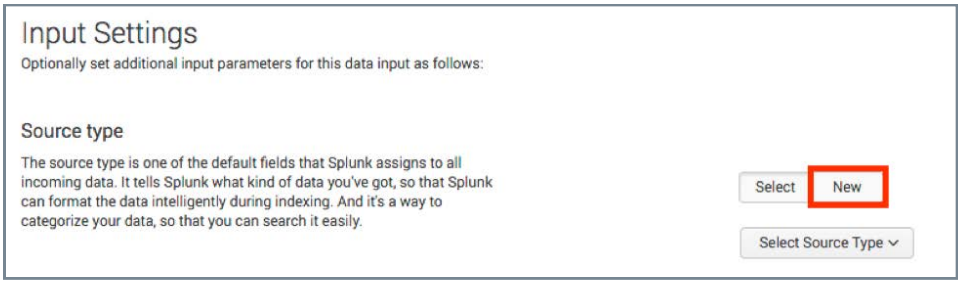
6. Under Data Inputs create a new UDP input by clicking Add new on the right.



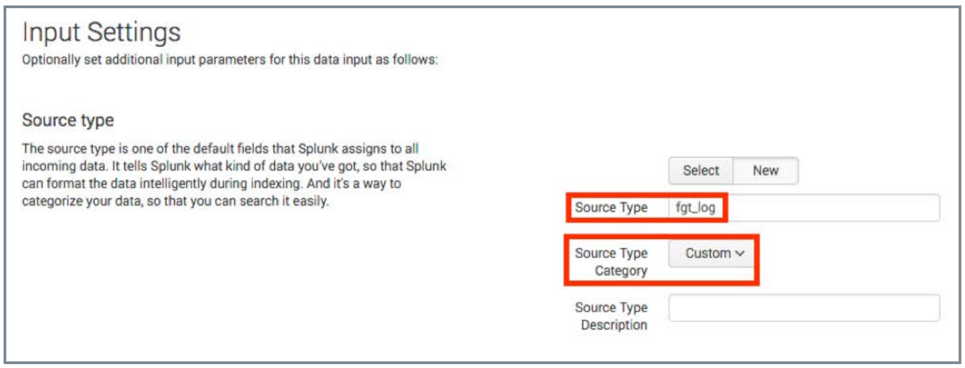
7. Create a UDP Data Source on Port 514.



8. Click New.

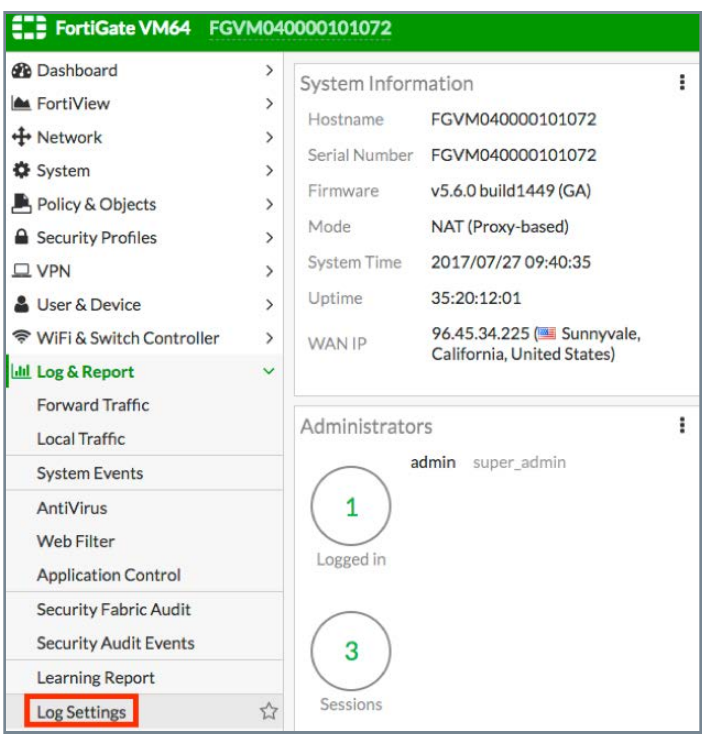


9. Under Input Settings set the Source Type to “fgt_log”.
   Set the Source Type Category to Custom.

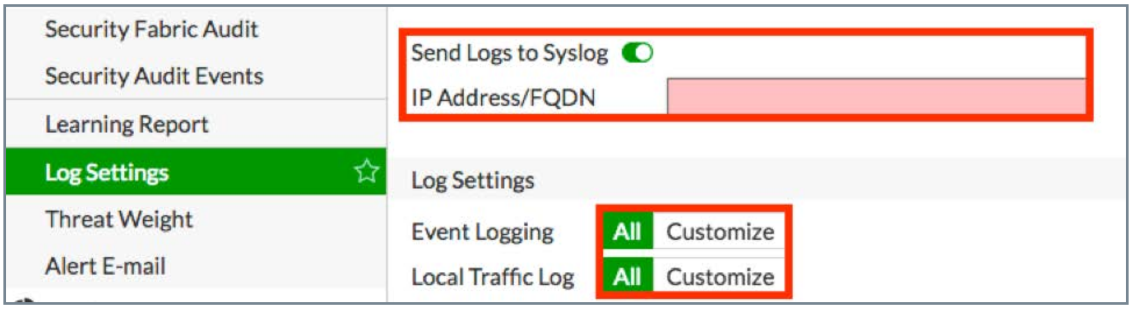


Fortinet Configuration

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



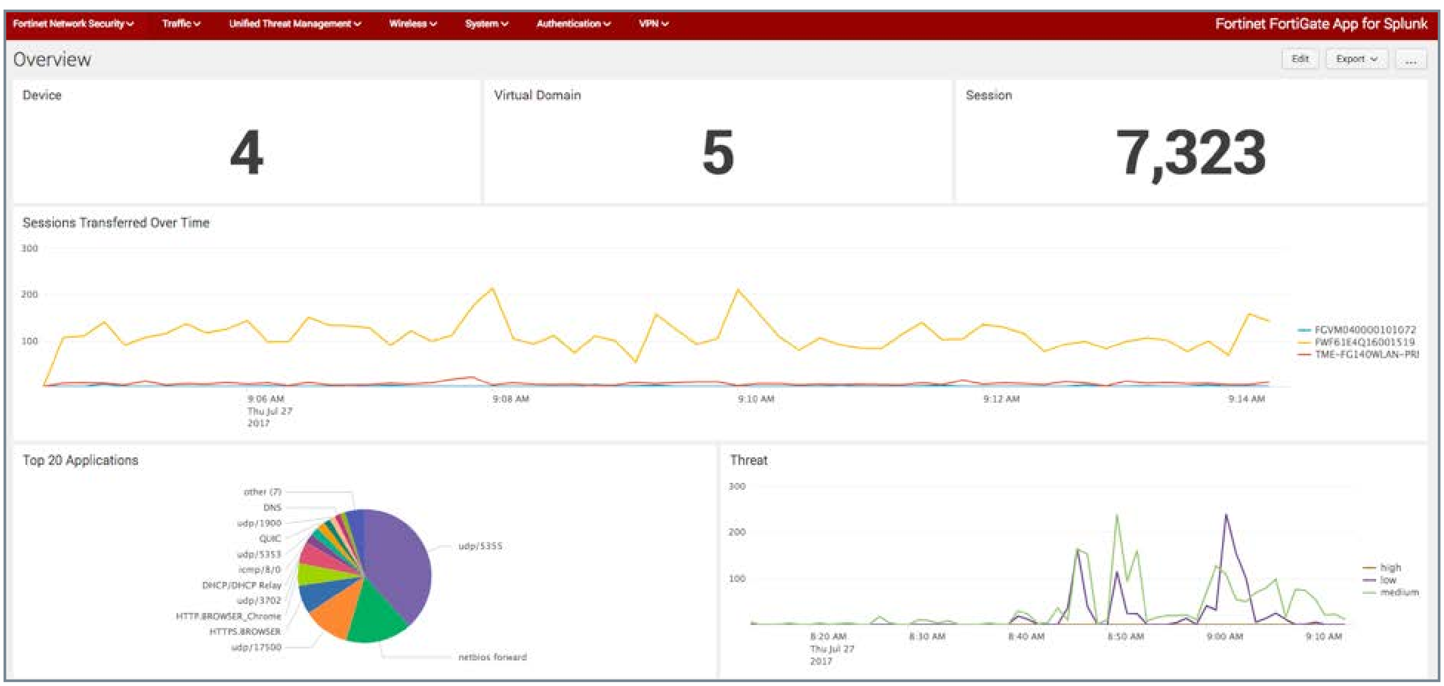
3. Enable Send Logs to Syslog.
4. Enter the IP Address or FQDN of the Splunk server.
5. Select the desired Log Settings.
6. Click Save.



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/

June 27, 2019 6:04 AM

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

170843-A-0-EN