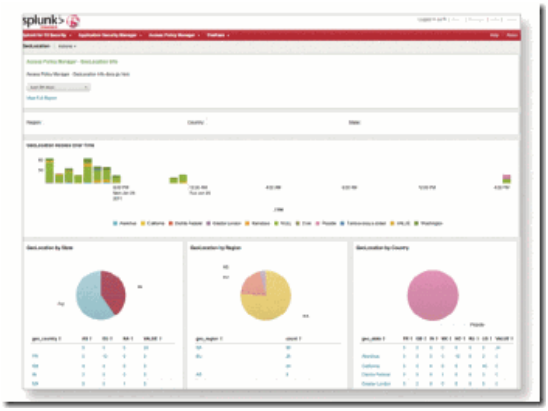
Do You Splunk 2.0

Peter Silva, 2011-19-04

A little over two years ago I blogged Do you Splunk? about the reporting integration with our FirePass SSL VPN and BIG-IP ASM. The Splunk reports have provided customers valuable insight into application access and user behavior along with deep analysis of application violations, web attacks and other key metrics. Recently, Splunk and F5 have been working behind the scenes and now you can also get 22 different templates for detailed reporting on the BIG-IP Access Policy Manager. BIG-IP APM is a flexible, high-performance access and security solution that runs as a module on BIG-IP LTM.

Splunk is the data engine for IT. It collects, indexes and harnesses the fast-moving IT data generated by all of your IT systems and infrastructure - whether physical, virtual or in the cloud and correlates various pieces of data sources to provide new views and new insights. Splunk makes it possible to search and navigate data from any application, server or network device from a web browser, in real time. Logs, configurations, messages, traps, alerts, and scripts: if a machine generates it, Splunk will index it. The Splunk for F5 App provides real-time dashboards for monitoring key performance metrics. Reports from Splunk support long-term trending and can be downloaded in PDF or Excel formats or scheduled for email delivery. The F5 App supports core Splunk functionality such as deep drill-down from graphical elements, robust role-based access controls and Splunk's award-winning search capabilities.

The following are a sample of the reports available in this version of Splunk for F5 using ASM, APM and FirePass data:



- Request Status Over Time
- Top Attacker
- Top Sites
- Top Violations
- Active Sync by Device Type
- Top Device Type
- Top User
- Geo-location Reports
- Session Duration and Throughput
- Authentication Success/Failure
- Connections by User
- Failed Connections by User
- All Connections Over Time

Splunk also has the unique ability to augment data from FirePass and ASM by connecting to and gathering data from Active Directory or LDAP and asset management databases that can highlight asset or application owner information.

Businesses are faced with competing challenges when it comes to granting their mobile workforce access to company data. The data must be readily accessible to users on the go but at the same time companies must protect and safeguard their internal systems that contain sensitive information. Robust monitoring controls are a must for maintaining auditing access, enabling dynamic application access and preventing data loss and availability issues.

Resources:

- Splunk for F5
- F5 Networks Partner Spotlight - Splunk
- Knowledgebase: Splunk for Use with F5 Networks Solutions
- Video: Splunk for Use with F5 Networks Solutions
- Splunk Templates for BIG-IP Access Policy Manager (pdf)
- Splunk for FirePass SSL VPN (pdf)
- Splunk for Application Security Manager (pdf)
- ASM & Splunk integration
- F5 Security Community Group on DevCentral
- Do you Splunk?

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com