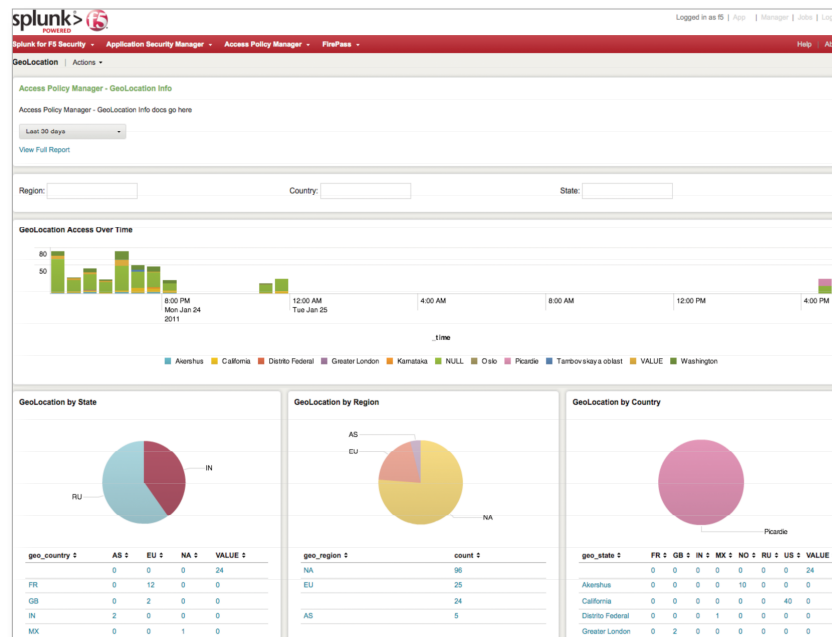


Splunk for F5

Enabling dynamic application access while preventing application level attacks.



The Challenges

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 their internal systems that contain sensitive information. From intellectual property and financial data to business processes and customer information, this data needs to be safeguarded. Robust monitoring controls are a must for maintaining auditing access and preventing data loss and availability issues. The network infrastructure supporting web service-based business service deployments needs to be constantly monitored in today's always-on business. Availability, often overlooked as a security issue, needs to be constantly monitored and linked to user access and system identities.

F5 Solutions

The F5 BIG-IP® Access Policy Manager™ (APM) is a flexible, high-performance access and security solution that runs as a module on BIG-IP® Local Traffic Manager™ (LTM). With BIG-IP APM you can provide policy-based, context-aware access to users while simplifying authentication, authorization, and accounting management. Reports are grouped into geo-location, session and access categories.

BIG-IP ASM delivers comprehensive protection for Web applications and operational infrastructure. BIG-IP ASM employs an auto-adaptive approach to application delivery security, where the security policy is automatically updated based on observed traffic patterns. This automatic policy-building feature makes it easier to implement and maintain security policies and reduces the total cost of ownership.

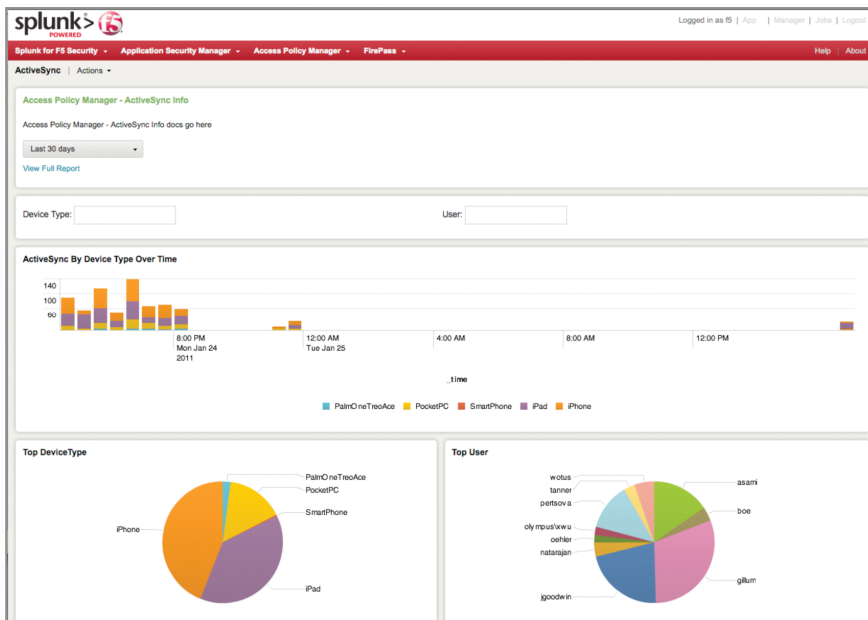
The F5 FirePass SSL VPN provides both security and ease of use. It grants users secure remote access to corporate applications using a technology that everyone understands: a Web browser. Users have secure access from any Internet connection—while FirePass ensures that connected computers are fully patched and protected. FirePass provides robust, secure SSL VPN remote access to business applications from a wide range of client devices, including Apple iPhone and Windows Mobile devices.

Using full-tunnel SSL technology and client access policies defined by system administrators, remote clients can log on to corporate business applications under pre-defined access permissions and client directory control. In the course of protecting web applications and providing robust SSL VPN capabilities, ASM and FirePass respectively produce detailed log files about each transaction. While both products come with detailed reporting capabilities, you may need to conduct even more advanced searches, reports and alerts on the data using a specially-designed analysis tool.

Incident response, threat analysis, event correlation from multiple network devices or compliance audits are common examples of activities that can require advanced investigation. For users with these advanced needs, F5 has partnered with Splunk to offer a solution specifically tailored to ASM.

Why Splunk for F5

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.



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 scales to accept tens of terabytes of data per day and, using a proprietary search and analysis language, can correlate disparate data sources to provide new views and new insights.

The Splunk for F5 App presents ASM data with FirePass data that allows for a comprehensive view of application access and attacks. Here are four examples of how Splunk and F5 can enhance security:

- Correlate access attempts by an unapproved device with correct credentials in FirePass and see attacks from the same IP address in the ASM data
- Get a more complete view of user behavior over time to understand and profile behaviors that can lead to theft of sensitive data
- View long-term user behaviors to determine access patterns and watch for outliers
- Correlate network access from geos with FirePass data and local AD log data to pinpoint fraudulent activity

Splunk gives your security team access to all IT data for investigations and root cause analysis. Comprehensive security dashboards can be created to deliver the essential metrics or key performance indicators (KPIs) that you need to maintain security best practices. Splunk also has the unique ability to augment data from FirePass and ASM by connecting to and gather data from Active Directory or LDAP and asset management databases that can highlight asset or application owner information.

The Splunk for F5 App

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. Reports can also be 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.

Features

- Visualize key performance indicators (KPIs) using prebuilt dashboards for monitoring configuration changes, malicious websites and bandwidth usage
- Leverage the Splunk scheduled reporting service
- Add and create your own graphics and dashboards
- Search and investigate with Splunk's award-winning IT data engine for universal real-time data collection and indexing from any application, server, network or security device
- Utilize an intuitive, easy-to-use interface that facilitates the communication of status and issues across your infrastructure
- Deploy with flexibility across a scalable distributed architecture

Get Started Today !

- Website: www.splunk.com
- Address: 250 Brannan St, San Francisco, CA, USA, 94107
- Email: info@splunk.com | sales@splunk.com
- Phone: +1 866-438-7758 | +1 415-848-8400
- Free Download: www.splunk.com/download
- Community: Splunk Answers | community@splunk.com