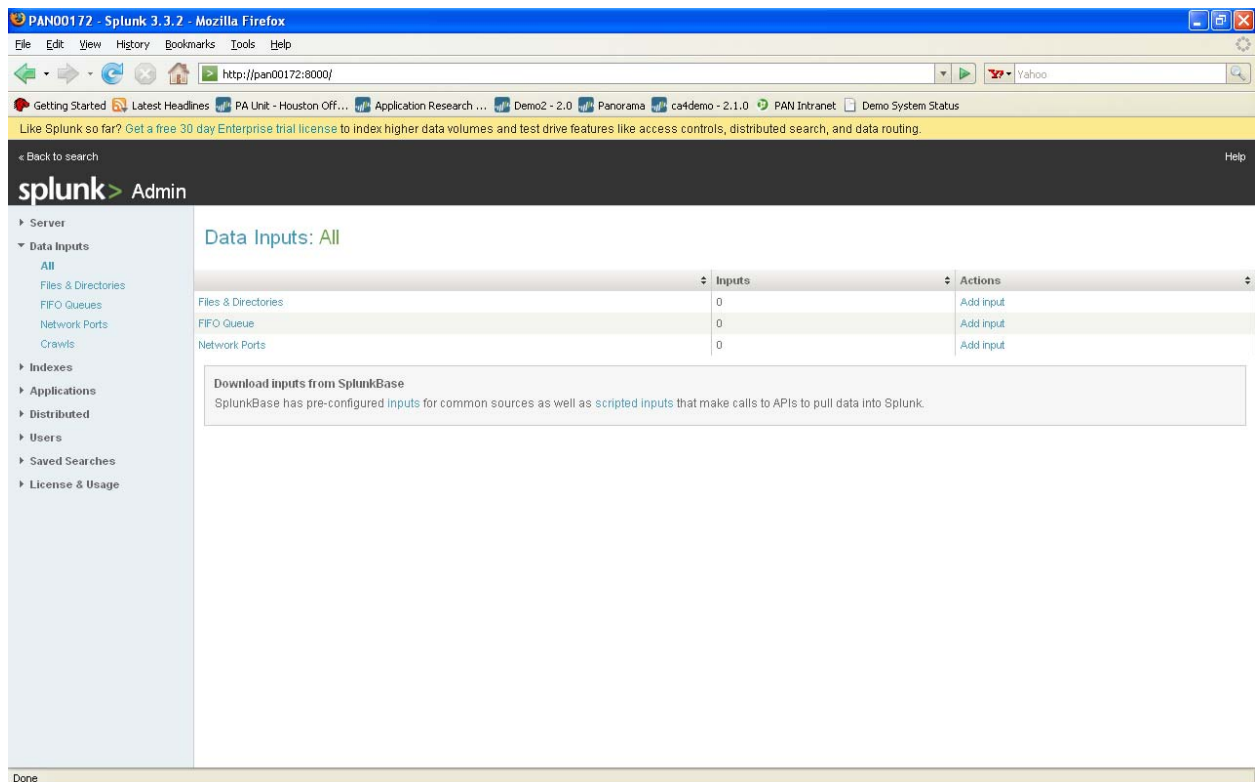




Palo Alto Networks - Integrating with Splunk

Splunk can be enhanced to support threat logs generated by Palo Alto Networks firewall. The simple procedure requires 2 configuration files to be added to Splunk. The steps below were done with Splunk version 3.3.2 and PAN-OS 2.0.5.

- Download & install splunk; installed directory will be like C:\Program Files\Splunk
- Under the \etc dir, create a new dir \PAN\default like so → C:\Program Files\Splunk\etc\apps\PAN\default
- Copy files 'props.conf' and 'transforms.conf' into the newly created directory C:\Program Files\Splunk\etc\apps\PAN\default
- edit 'props.conf' and enter the filename of the logs that splunk will process; in this sample, the filename is [threat_log_usernames]
- launch splunk, access the GUI → Admin → Data Inputs → Files & Directories and specify where the PAN log files are located

A screenshot of the Splunk Admin console interface. The browser window title is "PAN00172 - Splunk 3.3.2 - Mozilla Firefox". The address bar shows "http://pan00172:8000/". The page content shows the "Data Inputs: All" section. A table lists three input types: "Files & Directories", "FIFO Queue", and "Network Ports", each with a count of 0 and an "Add input" button. Below the table is a section titled "Download inputs from SplunkBase" with a description: "SplunkBase has pre-configured inputs for common sources as well as scripted inputs that make calls to APIs to pull data into Splunk." The left sidebar shows the navigation menu with "Data Inputs" expanded.

	Inputs	Actions
Files & Directories	0	Add input
FIFO Queue	0	Add input
Network Ports	0	Add input

Download inputs from SplunkBase
SplunkBase has pre-configured inputs for common sources as well as scripted inputs that make calls to APIs to pull data into Splunk.

The reports are available under 'threat_log_usernames' at the main menu.

The screenshot shows the Splunk 3.3.2 main dashboard in a Mozilla Firefox browser. The search bar contains 'Last 3 months' and shows '18,003 events'. Below the search bar, there are three summary cards: 'All indexed data' showing 3 sources (WinEventLog System, WinEventLog Application, threat_log_usernames.txt), 3 sourcetypes (WinEventLog System, WinEventLog Application, threat_log_usernames), and 2 hosts (localhost, PAN00172). Below these is a line chart titled 'Errors in the last hour' showing a peak around 09:08. At the bottom, there is a 'Saved searches' list including 'Daily indexing volume by server', 'Default crawl', 'Errors in the last 24 hours', etc.

Top Categories report.

The screenshot shows the 'Top Categories' report in Splunk. The search bar contains the query 'sourcetype="threat_log_usernames" | top limit=100 category - over all time - PAN00172 - Splunk 3.3.2 - Mozilla Firefox'. The report displays a bar chart titled 'top values of category for results over all time'. The x-axis lists categories like infrastructure, news, shopping, business, motor-vehicles, finance-and-investment, education, holiday-sites, chat, and download. The y-axis is 'count'. A tooltip for 'infrastructure' shows a count of 264. Below the chart is a table with columns 'category', 'count', and 'percent'.

category	count	percent
1 infrastructure	264	10.459588
2 unknown	239	9.469097
3 government	213	8.438986
4 news	204	8.082409