Vendor - Forcepoint

Product - Webprotect (Websense)

Ref	Link
Splunk Add-on	https://splunkbase.splunk.com/app/2968/
Product Manual	http://www.websense.com/content/support/library/web/v85/siem/siem.pdf

Sourcetypes

sourcetype	notes
websense:c:kv	None

Sourcetype and Index Configuration

key	sourcetype	index	notes
forcepoint_webprotect	websense:c:kv	netproxy	none

Filter type

MSG Parse: This filter parses message content

Setup and Configuration

- Install the Splunk Add-on on the search head(s) for the user communities interested in this data source. If CC35 is exclusively used the add-on is not required on the indexer.

- Review and update the splunk_index.csv file and set the index and sourcetype as required for the data source.

- Refer to the admin manual for specific details of configuration to send Reliable syslog using RFC 3195 format, a typical logging configuration will include the following features.

Options

Variable	default	description
SC4_LISTEN_FORCEPOINT_WEBPROTECT_TCP_PORT	empty string	Enable a TCP port for this specific vendor product using the number defined
SC4_LISTEN_FORCEPOINT_WEBPROTECT_UDP_PORT	empty string	Enable a UDP port for this specific vendor product using the number defined
SC4_ARCHIVE_FORCEPOINT_WEBPROTECT	no	Enable archive to disk for this specific source
SC4_DISABLE_FORCEPOINT_WEBPROTEC	no	When splunk IDS is ...