Vendor - Juniper

Product - Juniper JunOS

Ref	Link
Splunk Add-on	https://splunkbase.splunk.com/app/2847/
Author	https://www.juniper.net/documentation/en_US/junos/topics/
Technology Library	https://apps.splunk.com/apps-configuring-q-exchange-series.html

Sourcetypes

sourcetype	notes
juniper:junos:firewall	None
juniper:junos:firewall:structured	None
juniper:junos:idp	None
juniper:junos:idp:structured	None
juniper:junos:aamw:structured	None
juniper:junos:secintel:structured	None

Sourcetype and Index Configuration

key	sourcetype	index	notes
juniper:junos:flow	juniper:junos:firewall	netfw	none
juniper:junos:idp	juniper:junos:idp	netids	none
juniper:junos:out	juniper:junos:firewall	netfw	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 CIM is exclusively used then the add-on is not required on the indexer.
- Review and update the splunk_index.csv file and set the index as required.
- Follow vendor configuration steps referenced under Input Manual.

Options

Variable	default	description
SC4S_LISTEN_JUNIPER_JUNOS_UDP_PORT	empty	Enable a TCP port for this specific vendor product using a comma separated list of ports syslog 3514 format
SC4S_LISTEN_JUNIPER_JUNOS_TCP_PORT	empty	Enable a TCP port for this specific vendor