Vendor - pfSense

All pfSense based firewalls

Product

Ref	Link
Splunk Add-On	https://splunkbase.splunk.com/app/1527/
Product	https://docs.netgate.com/pfsense/latest/monitoring/
Manual	copying-logs-to-a-remote-host-with-syslog.html highlight=syslog

Sourcetypes

sourcetype	notes
pfsense:filterlog	None
pfsense:*	All programs other than filterlog

Sourcetype and Index Configuration

key	sourcetype	index	notes
pfsense	pfsense	netfw	none
pfsensefilterlog	pfsense:filterlog	netfw	none

Filter type

Source does not provide a hostname, port or IP based filter is required

Setup and Configuration

- Install the Splunk Add-On on the search head(s) for the user communities interface on the data source. If CCS 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.
- Configure a dedicated SCS port OR configure IP filter
- Refer to the Splunk TA documentation for the specific customer format required for proxy configuration.
  - Select TCP or SSL transport option
  - Ensure the format of the events customized per Splunk documentation.

Options

Variable	default	description
SC4S_LISTEN_PFSENSE_TCP_PORT string	Enable a TCP port this specific	protocol using the number defined