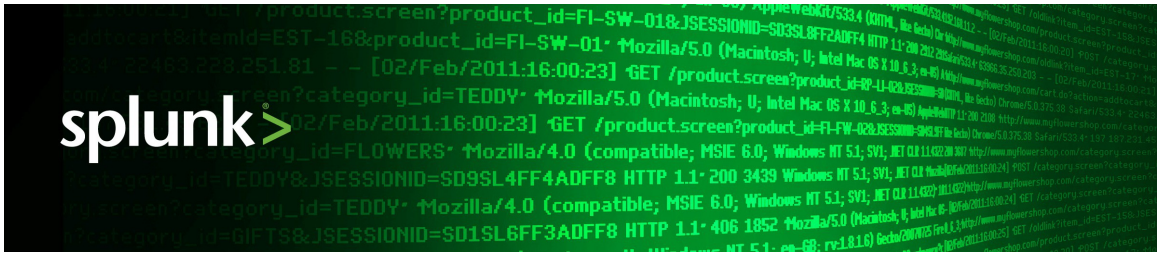

Splunk® Enterprise Add Palo Alto Networks data: Single instance 8.0.1

Configure a syslog-ng server to send Palo Alto Networks data to your Splunk Enterprise deployment

Generated: 1/02/2020 10:38 pm

Configure a syslog-ng server to send Palo Alto Networks data to your Splunk Enterprise deployment

1. Navigate to `/etc/syslog-ng/syslog-ng.conf` and save a copy of `syslog-ng.conf` as a backup before making any additional configurations.
2. Navigate to `/etc/syslog-ng/conf.d/`, and create a file called `pan.conf`.
3. Open `pan.conf`, and paste the following information in order to configure your server to listen on UDP port 514:

```
# syslog-ng config to receive syslog messages from  Palo Alto
Networks devices

options{
        create-dirs(yes);
};

#Listen on UDP port 514
source s_net{
        udp(port("514"));
};


#Destinations where syslog-ng should write to
destination d_threat            {
file("/var/log/syslog/pan/$HOST/threat/$YEAR-$MONTH-$DAY-threat.log");
};
destination d_traffic           {
file("/var/log/syslog/pan/$HOST/traffic/$YEAR-$MONTH-$DAY-traffic.log");
};
destination d_system            {
file("/var/log/syslog/pan/$HOST/system/$YEAR-$MONTH-$DAY-system.log");
};
destination d_config            {
file("/var/log/syslog/pan/$HOST/config/$YEAR-$MONTH-$DAY-config.log");
};
destination d_hipmatch          {
file("/var/log/syslog/pan/$HOST/hipmatch/$YEAR-$MONTH-$DAY-hipmatch.log");
};
destination d_endpoint          {
file("/var/log/syslog/pan/$HOST/endpoint/$YEAR-$MONTH-$DAY-endpoint.log");
};
destination d_wildfire          {
file("/var/log/syslog/pan/$HOST/wildfire/$YEAR-$MONTH-$DAY-wildfire.log");
};
destination d_correlation       {
file("/var/log/syslog/pan/$HOST/correlation/$YEAR-$MONTH-$DAY-correlation.log");
};
```

```
destination d_aperture          {
file("/var/log/syslog/pan/$HOST/aperture/$YEAR-$MONTH-$DAY-aperture.log");
};


#Filters to route sourcetypes to sepearate files
filter f_threat         { message("THREAT"); };
filter f_traffic        { message("TRAFFIC"); };
filter f_system         { message("SYSTEM"); };
filter f_config         { message("CONFIG"); };
filter f_hipmatch       { message("HIPMATCH") };
filter f_endpoint       { message("ENDPOINT"); };
filter f_wildfire       { message("WILDFIRE"); };
filter f_correlation    { message("CORRELATION"); };
filter f_aperture       { message("APERTURE"); };

#Log definitions
log { source(s_net); destination(d_threat); filter(f_threat); };
log { source(s_net); destination(d_traffic); filter(f_traffic);
};
log { source(s_net); destination(d_system); filter(f_system); };
log { source(s_net); destination(d_config); filter(f_config); };
log { source(s_net); destination(d_hipmatch); filter(f_hipmatch);
};
log { source(s_net); destination(d_endpoint); filter(f_endpoint);
};
log { source(s_net); destination(d_wildfire); filter(f_wildfire);
};
log { source(s_net); destination(d_correlation);
filter(f_correlation); };
log { source(s_net); destination(d_aperture); filter(f_aperture);
};
```

4. Save your changes. To optionally change your port, replace the `source s_net{ udp(port("514"));` with the desired port number.
5. Restart syslog-ng to apply updates.

```
sudo service syslog-ng restart
```