Integration Guide

Micro Focus Common Event Format Integration Guide

Palo Alto Networks

Next-Generation Firewall (PAN-OS® 10.0)

Date: March 25, 2021

Table of Contents

ArcSight Integration Guide
This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to Micro Focus. Micro Focus does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Certified Integration:
The integration complies with the requirements of the Micro Focus Technology Alliance Partner program. For inbound integrations, the Micro Focus ArcSight CEF connector will be able to process the events correctly and the events will be available for use within Micro Focus' ArcSight product. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. For action and outbound integrations, the integration establishes outbound communications from Micro Focus ArcSight to a third party platform. The integration has been tested and demonstrated to Micro Focus by the third party.

Revision History

Date	Description
2/25/2011	First edition of this Configuration Guide.
3/2/2011	Version 4.0 Certified by Micro Focus
2/6/2012	Version 4.1 Certified by Micro Focus.
5/14/2014	Version 6.0.0 Certified by Micro Focus
3/16/2016	Version 7.0 Certified by Micro Focus
12/11/2019	Version 9.0 Certified by Micro Focus
3/2/2020	Version 9.1 Certified by Micro Focus
6/22/2021	Version 10.0 Certified by Micro Focus

Palo Alto Networks NGFW Integration Guide

This guide provides information for configuring the Palo Alto Networks next-generation firewalls for CEF-formatted Syslog event collection. There are several fields referenced in this document that are only available in PAN-OS 8.0 and higher. If you are using a PAN-OS version older than 8.0, please use the appropriate CEF guide that aligns with your software version.

Joint Solution Overview

Palo Alto Networks next-generation firewalls provide network security by enabling enterprises to see and control applications, users, and content—not just ports, IP addresses, and packets—using three unique identification technologies: App-ID, User-ID, and Content-ID. These technologies enable enterprises to create business-relevant security policies that safely enable adoption of new applications, instead of the traditional "all-or-nothing" approach offered by traditional port-blocking firewalls used in many security infrastructures. With CEF integration Palo Alto Networks firewalls can generate Traffic, Threat, System, Config, and HIP Match logs in CEF format. Micro Focus has tested these CEF logs to ensure accuracy and format compliance, thus, enabling ArcSight customers to seamlessly utilize the rich data generated by PAN-OS gateways.

Use Cases

This section contains use cases supported by this integration

- Identify targets of new malware campaigns by investigating Palo Alto Networks WildFire malicious verdict logs.
- Build trending reports showing threat, user, and application activity, generated from Palo Alto Networks CEF logs, over rolling time windows.
- Investigate connections to suspicious domains by leveraging Palo Alto Networks Threat URL logs of category unknown or parked.

CEF Integration

1. Configuration of Palo Alto Networks NGFW to output CEF events

Perform the following steps to configure the Palo Alto Networks firewall for ArcSight CEF-formatted Syslog events. The PAN-OS Administrator's Guide provides additional information about Syslog configuration. Please refer to the latest PAN-OS Administrator's Guide to ensure that you have configured log forwarding correctly for all the log types that you would like to forward to your ArcSight platform. The following steps only cover configuration of the custom log schema (CEF) for a given syslog server. They do not replace the administrator guide's configuration coverage of log forwarding. ⚙

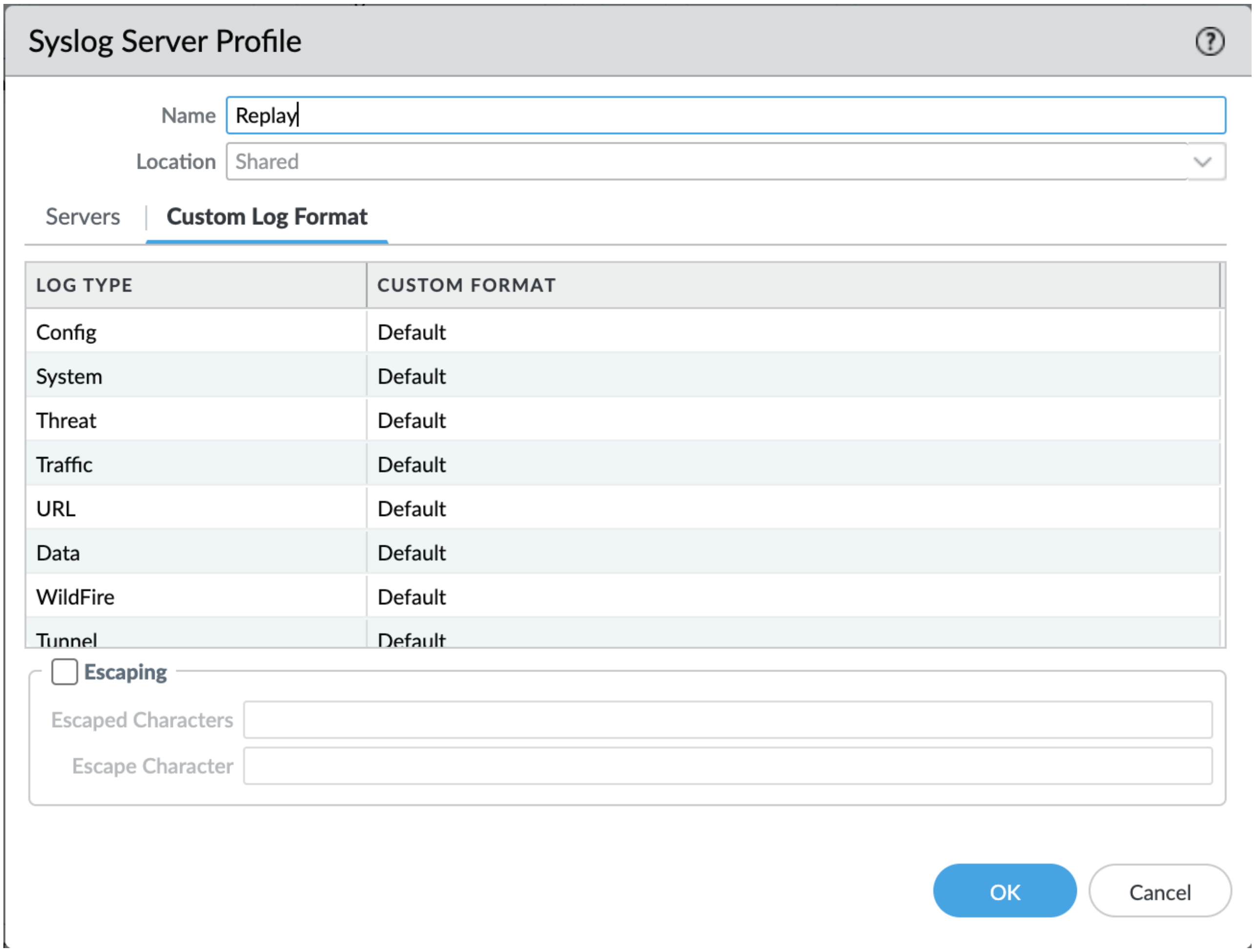
1. To configure the device to include its IP address in the header of Syslog messages, select **Panorama/Device > Setup > Management**, click the Edit icon in the **Logging and Reporting Settings** section and navigate to the **Log Export and Reporting** tab. In the **Syslog HOSTNAME Format** drop-down select **ipv4-address** or **ipv6-address**, then click **OK**.
2. Select **Device > Server Profiles > Syslog** and click **Add**.
3. Enter a server profile **Name** and **Location** (location refers to a virtual system, if the device is enabled for virtual systems).

4. In the **Servers** tab, click **Add** and enter a **Name**, IP address (**Syslog Server** field), **Transport**, **Port** (default 514 for UDP), and **Facility** (default LOG_USER) for the Syslog server.
5. Select the **Custom Log Format** tab and click any of the listed log types (Config, System, Threat, Traffic, URL, Data, WildFire, Tunnel, Authentication, User-ID, HIP Match) to define a custom format based on the ArcSight CEF for that log type (see CEF-style Log Formats). On Panorama and on higher-end appliance platforms, such as the PA-3000, PA-5000, PA-5200, and PA-7000 Series, an additional log type (Correlation) is available.

NOTE: Customers define their own CEF-style formats using the event mapping table provided in the ArcSight document "Implementing ArcSight CEF". The **Custom Log Format** tab supports escaping any characters defined in the CEF as special characters. For instance, to use a backslash to escape the backslash and equal characters, select the **Escaping** check box, specify \=as the **Escaped Characters** and \as the **Escape Character**.

NOTE: Due to PDF formatting, do not copy/paste the message formats directly into the PAN-OS web interface. Instead, paste into a text editor, remove any carriage return or line feed characters, then copy and paste into the web interface.

NOTE: Starting with release 10.0, the log format documented for log types (Traffic, Threat, URL, Decryption) exceeds the maximum supported 2048 characters in the Custom Log Format tab on the firewall and Panorama. Please select the CEF keys and values to limit the number of characters to 2048 as per your requirements.



Syslog Server Profile

Name: Replay

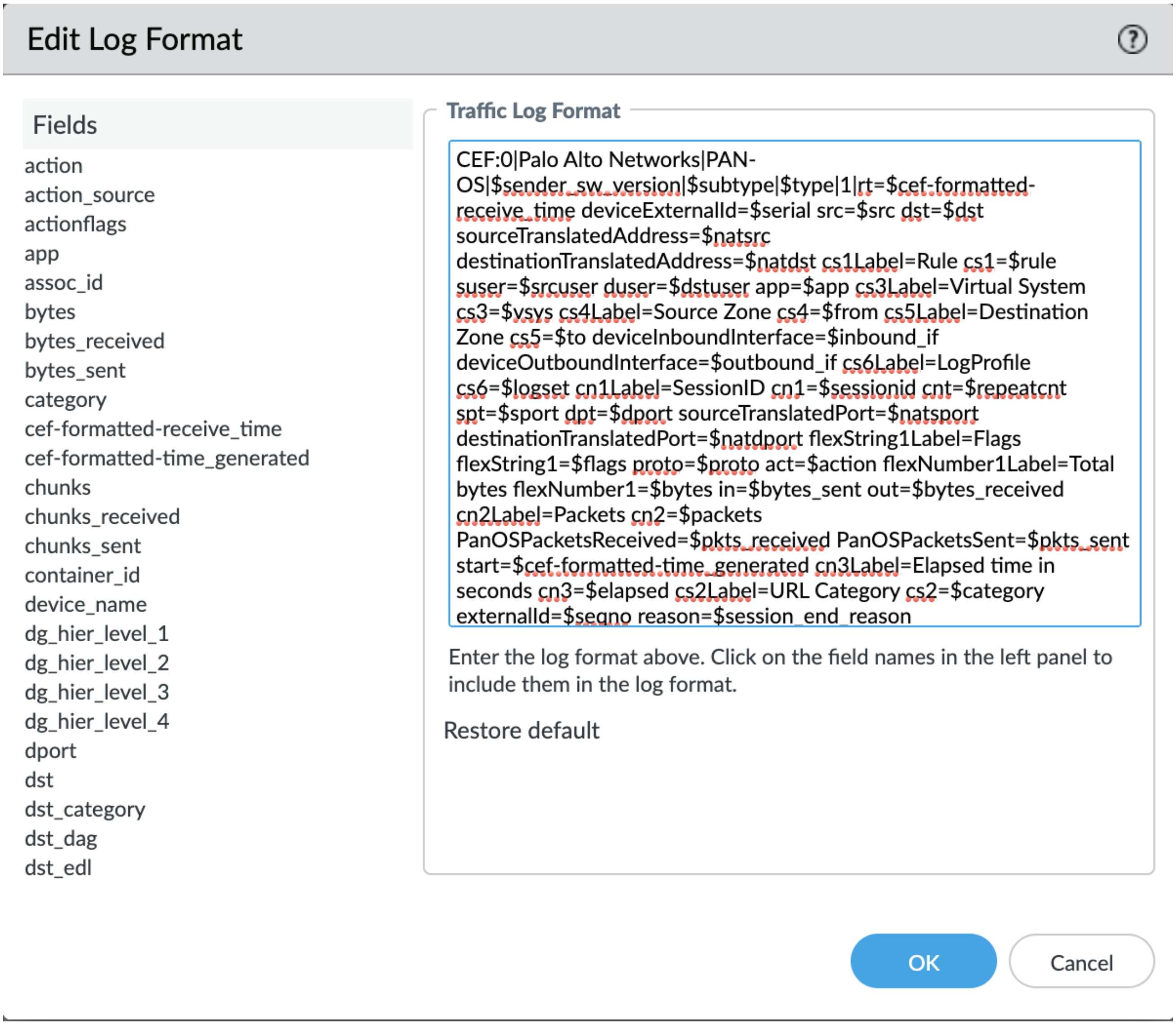
Location: Shared

LOG TYPE	CUSTOM FORMAT
Config	Default
System	Default
Threat	Default
Traffic	Default
URL	Default
Data	Default
WildFire	Default
Tunnel	Default

☐ Escaping

Escaped Characters

Escape Character



Fields

action
action_source
actionflags
app
assoc_id
bytes
bytes_received
bytes_sent
category
cef-formatted-receive_time
cef-formatted-time_generated
chunks
chunks_received
chunks_sent
container_id
device_name
dg_hier_level_1
dg_hier_level_2
dg_hier_level_3
dg_hier_level_4
dport
dst
dst_category
dst_dag
dst_edl

Traffic Log Format

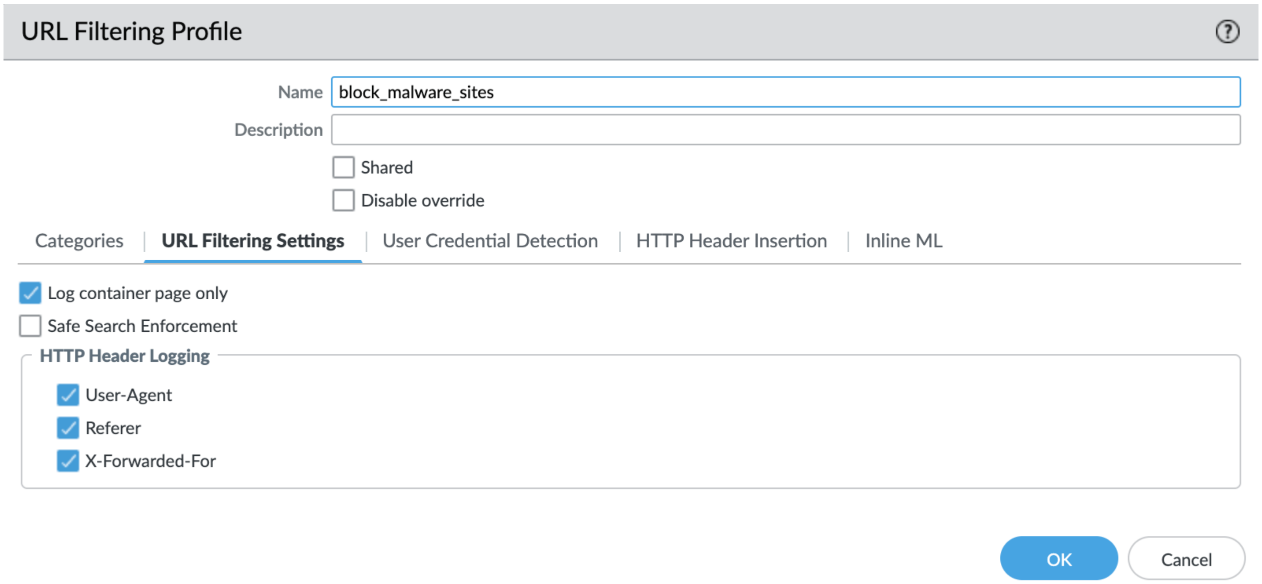
```
CEF:0|Palo Alto Networks|PAN-
OS|$sender_sw_version|$subtype|$type|1|rt=$cef-formatted-
receive_time deviceExternalId=$serial src=$src dst=$dst
sourceTranslatedAddress=$natsrc
destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule
suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System
cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination
Zone cs5=$to deviceInboundInterface=$inbound_if
deviceOutboundInterface=$outbound_if cs6Label=LogProfile
cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt
spt=$sport dpt=$dport sourceTranslatedPort=$natsport
destinationTranslatedPort=$natdport flexString1Label=Flags
flexString1=$flags proto=$proto act=$action flexNumber1Label=Total
bytes flexNumber1=$bytes in=$bytes_sent out=$bytes_received
cn2Label=Packets cn2=$packets
PanOSPacketsReceived=$pkts_received PanOSPacketsSent=$pkts_sent
start=$cef-formatted-time_generated cn3Label=Elapsed time in
seconds cn3=$elapsed cs2Label=URL Category cs2=$category
externalId=$seqno reason=$session_end_reason
```

Enter the log format above. Click on the field names in the left panel to include them in the log format.

Restore default

1. Click **OK** twice to save your entries, then click **Commit**.

1. (Optional) To include User-Agent, Referer, and X-Forwarder-For values for Threat logs of subtype URL, select Objects -> URL Filtering -> [profile_name] -> URL Filtering Settings and check the three boxes under HTTP Header Logging.



URL Filtering Profile

Name: block_malware_sites

Description:

□ Shared

□ Disable override

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

☑ Log container page only

□ Safe Search Enforcement

HTTP Header Logging

☑ User-Agent

☑ Referer

☑ X-Forwarded-For

CEF- style Log Formats:

The following table shows the CEF-style format that was used during the certification process for each log type. These custom formats include all the fields, in a similar order, that the default format of the syslogs display.

Traffic	*CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$subtype|$type\|1\|rt=$cef-formatted-receive_time deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags proto=$proto act=$action flexNumber1Label=Total bytes flexNumber1=$bytes in=$bytes_sent out=$bytes_received cn2Label=Packets cn2=$packets PanOSPacketsReceived=$pkts_received PanOSPacketsSent=$pkts_sent start=$cef-formatted-time_generated cn3Label=Elapsed time in seconds cn3=$elapsed cs2Label=URL Category cs2=$category externalId=$seqno reason=$session_end_reason PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name cat=$action_source PanOSActionFlags=$actionflags PanOSSrcUUID=$src_uuid PanOSDstUUID=$dst_uuid PanOSTunnelID=$tunnelid PanOSMonitorTag=$monitortag PanOSParentSessionID=$parent_session_id PanOSParentStartTime=$parent_start_time PanOSTunnelType=$tunnel PanOSSCTPAssocID=$assoc_id PanOSSCTPChunks=$chunks PanOSSCTPChunkSent=$chunks_sent PanOSSCTPChunksRcv=$chunks_received PanOSRuleUUID=$rule_uuid PanOSHTTP2Con=$http2_connection PanLinkChange=$link_change_count PanPolicyID=$policy_id PanLinkDetail=$link_switches PanSDWANCluster=$sdwan_cluster PanSDWANDevice=$sdwan_device_type PanSDWANClustype=$sdwan_cluster_type PanSDWANSite=$sdwan_site PanDynamicUsrgrp=$dynusergroup_name PanXFFIP=$xff_ip PanSrcDeviceCat=$src_category PanSrcDeviceProf=$src_profile PanSrcDeviceModel=$src_model PanSrcDeviceVendor=$src_vendor PanSrcDeviceOS=$src_osfamily PanSrcDeviceOSv=$src_osversion PanSrcHostname=$src_host PanSrcMac=$src_mac PanDstDeviceCat=$dst_category PanDstDeviceProf=$dst_profile PanDstDeviceModel=$dst_model PanDstDeviceVendor=$dst_vendor PanDstDeviceOS=$dst_osfamily PanDstDeviceOSv=$dst_osversion PanDstHostname=$dst_host PanDstMac=$dst_mac PanContainerName=$container_id PanPODNamespace=$pod_namespace PanPODName=$pod_name PanSrcEDL=$src_edl PanDstEDL=$dst_edl PanGPHostID=$hostid PanEPSerial=$serialnumber PanSrcDAG=$src_dag PanDstDAG=$dst_dag PanHASessionOwner=$session_owner PanTimeHighRes=$high_res_timestamp PanASServiceType=$nssai_sst PanASServiceDiff=$nssai_sd*

<table>
<tr><td>Threat</td><td>CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version|$threatid|$type|$number-of-severity|rt=$cef-formatted-receive_time deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags proto=$proto act=$action request=$misc cs2Label=URL Category cs2=$category flexString2Label=Direction flexString2=$direction PanOSActionFlags=$actionflags externalId=$seqno cat=$subtype fileId=$pcap_id PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSSrcUUID=$src_uuid PanOSDstUUID=$dst_uuid PanOSTunnelID=$tunnelid PanOSMonitorTag=$monitortag PanOSParentSessionID=$parent_session_id PanOSParentStartTime=$parent_start_time PanOSTunnelType=$tunnel PanOSThreatCategory=$thr_category PanOSContentVer=$contentver PanOSAssocID=$assoc_id PanOSPPID=$ppid PanOSHTTPHeader=$http_headers PanOSURLCatList=$url_category_list PanOSRuleUUID=$rule_uuid PanOSHTTP2Con=$http2_connection PanDynamicUsrgrp=$dynusergroup_name PanXFFIP=$xff_ip PanSrcDeviceCat=$src_category PanSrcDeviceProf=$src_profile PanSrcDeviceModel=$src_model PanSrcDeviceVendor=$src_vendor PanSrcDeviceOS=$src_osfamily PanSrcDeviceOSv=$src_osversion PanSrcHostname=$src_host PanSrcMac=$src_mac PanDstDeviceCat=$dst_category PanDstDeviceProf=$dst_profile PanDstDeviceModel=$dst_model PanDstDeviceVendor=$dst_vendor PanDstDeviceOS=$dst_osfamily PanDstDeviceOSv=$dst_osversion PanDstHostname=$dst_host PanDstMac=$dst_mac PanContainerName=$container_id PanPODNamespace=$pod_namespace PanPODName=$pod_name PanSrcEDL=$src_edl PanDstEDL=$dst_edl PanGPHostID=$hostid PanEPSerial=$serialnumber PanDomainEDL=$domain_edl PanSrcDAG=$src_dag PanDstDAG=$dst_dag PanPartialHash=$partial_hash PanTimeHighRes=$high_res_timestamp PanReasonFilteringAction=$reason PanJustification=$justification PanASServiceType=$nssai_sst</td></tr>
<tr><td>URL</td><td>CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version|$subtype|$type|$number-of-severity|rt=$cef-formatted-receive_time deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags proto=$proto act=$action request=$misc cs2Label=URL Category cs2=$category flexString2Label=Direction flexString2=$direction PanOSActionFlags=$actionflags externalId=$seqno requestContext=$contenttype cat=$threatid fileId=$pcap_id requestMethod=$http_method requestClientApplication=$user_agent PanOSXForwarderfor=$xff PanOSReferer=$referer PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSSrcUUID=$src_uuid PanOSDstUUID=$dst_uuid PanOSTunnelID=$tunnelid PanOSMonitorTag=$monitortag PanOSParentSessionID=$parent_session_id PanOSParentStartTime=$parent_start_time PanOSTunnelType=$tunnel PanOSThreatCategory=$thr_category PanOSContentVer=$contentver PanOSAssocID=$assoc_id PanOSPPID=$ppid PanOSHTTPHeader=$http_headers PanOSRuleUUID=$rule_uuid PanOSURLCatList=$url_category_list PanOSHTTP2Con=$http2_connection PanDynamicUsrgrp=$dynusergroup_name PanXFFIP=$xff_ip PanSrcDeviceCat=$src_category PanSrcDeviceProf=$src_profile PanSrcDeviceModel=$src_model PanSrcDeviceVendor=$src_vendor PanSrcDeviceOS=$src_osfamily PanSrcDeviceOSv=$src_osversion PanSrcHostname=$src_host PanSrcMac=$src_mac PanDstDeviceCat=$dst_category PanDstDeviceProf=$dst_profile PanDstDeviceModel=$dst_model PanDstDeviceVendor=$dst_vendor PanDstDeviceOS=$dst_osfamily PanDstDeviceOSv=$dst_osversion PanDstHostname=$dst_host PanDstMac=$dst_mac PanContainerName=$container_id PanPODNamespace=$pod_namespace PanPODName=$pod_name PanSrcEDL=$src_edl PanDstEDL=$dst_edl PanGPHostID=$hostid PanEPSerial=$serialnumber PanDomainEDL=$domain_edl PanSrcDAG=$src_dag PanDstDAG=$dst_dag PanPartialHash=$partial_hash PanTimeHighRes=$high_res_timestamp PanReasonFilteringAction=$reason PanJustification=$justification PanASServiceType=$nssai_sst</td></tr>
</table>

Data	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$subtype|$type\|$number-of-severity|rt=$cef-formatted-receive_time deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags proto=$proto act=$action request=$misc cs2Label=URL Category cs2=$category flexString2Label=Direction flexString2=$direction PanOSActionFlags=$actionflags externalId=$seqno cat=$threatid fileId=$pcap_id PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSSrcUUID=$src_uuid PanOSDstUUID=$dst_uuid PanOSTunnelID=$tunnelid PanOSMonitorTag=$monitortag PanOSParentSessionID=$parent_session_id PanOSParentStartTime=$parent_start_time PanOSTunnelType=$tunnel PanOSThreatCategory=$thr_category PanOSContentVer=$contentver PanOSAssocID=$assoc_id PanOSPPID=$ppid PanOSHTTPHeader=$http_headers PanOSRuleUUID=$rule_uuid
WildFire	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$subtype|$type\|$number-of-severity|rt=$cef-formatted-receive_time deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags proto=$proto act=$action request=$misc cs2Label=URL Category cs2=$category flexString2Label=Direction flexString2=$direction PanOSActionFlags=$actionflags externalId=$seqno cat=$threatid filePath=$cloud fileId=$pcap_id fileHash=$filedigest fileType=$filetype suid=$sender msg=$subject duid=$recipient oldFileId=$reportid PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSSrcUUID=$src_uuid PanOSDstUUID=$dst_uuid PanOSTunnelID=$tunnelid PanOSMonitorTag=$monitortag PanOSParentSessionID=$parent_session_id PanOSParentStartTime=$parent_start_time PanOSTunnelType=$tunnel PanOSThreatCategory=$thr_category PanOSContentVer=$contentver PanOSAssocID=$assoc_id PanOSPPID=$ppid PanOSHTTPHeader=$http_headers PanOSRuleUUID=$rule_uuid
Config	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$result|$type\|1\|rt=$cef-formatted-receive_time deviceExternalId=$serial shost=$host cs3Label=Virtual System cs3=$vsys act=$cmd duser=$admin destinationServiceName=$client msg=$path externalId=$seqno PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSActionFlags=$actionflags cs1Label=Before Change Detail cs1=$before-change-detail cs2Label=After Change Detail cs2=$after-change-detail PanOSFWDeviceGroup=$dg_id PanOSPolicyAuditComment=$comment
System	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$subtype|$type\|$number-of-severity|rt=$cef-formatted-receive_time deviceExternalId=$serial cs3Label=Virtual System cs3=$vsys fname=$object flexString2Label=Module flexString2=$module msg=$opaque externalId=$seqno cat=$eventid PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSActionFlags=$actionflags anOSTimeGeneratedHighResolution=$high_res_timestamp

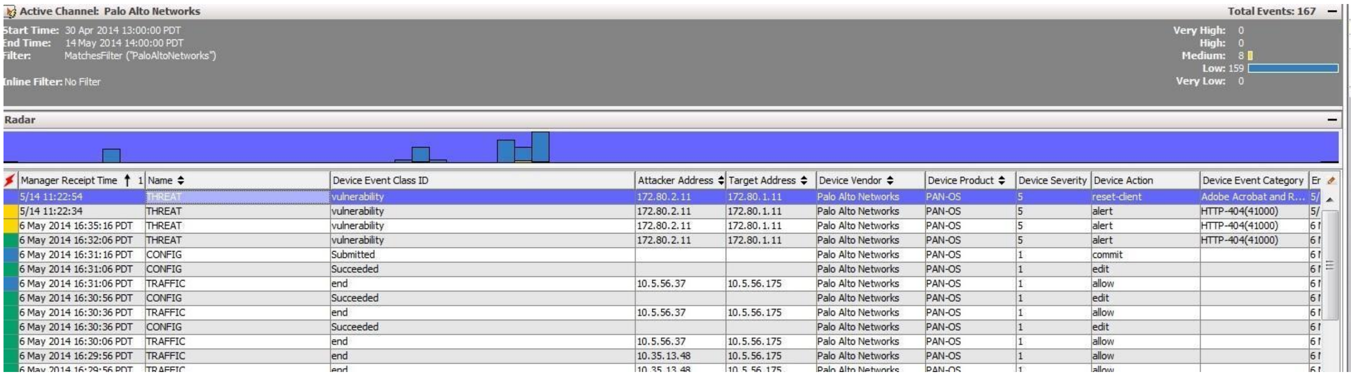
HIP Match	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$matchtype|$type\|1\|rt=$cef-formatted-receive_time deviceExternalId=$serial suser=$srcuser cs3Label=Virtual System cs3=$vsys shost=$machinename src=$src cnt=$repeatcnt externalId=$seqno cat=$matchname start=$cef-formatted-time_generated cs2Label=Operating System cs2=$os PanOSActionFlags=$actionflags PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name cn2Label=Virtual System ID cn2=$vsys_id c6a2Label=IPv6 Source Address c6a2=$srcipv6 PanOSHostID=$hostid PanOSEndpointSerialNumber=$serialnumber PanOSEndpointMac=$mac PanOSTimeGeneratedHighResolution=$high_res_timestamp
Authentication	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$subtype|$type\|1\|rt=$cef-formatted-receive_time deviceExternalId=$serial cs1Label=Server Profile cs1=$serverprofile cs2Label=Normalize User cs2=$normalize_user cs3Label=Virtual System cs3=$vsys cs4Label=Authentication Policy cs4=$authpolicy cs5Label=Client Type cs5=$clienttype cs6Label=Log Action cs6=$logset fname=$object cn1Label=Factor Number cn1=$factorno cn2Label=Authentication ID cn2=$authid src=$ip cnt=$repeatcnt duser=$user flexString2Label=Vendor flexString2=$vendor msg=$event externalId=$seqno PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSActionFlags=$actionflags PanOSDesc=$desc PanOSRuleUUID=$rule_uuid PanOSTimeGeneratedHighResolution=$high_res_timestamp PanOSSourceDeviceCategory=$src_category PanOSSourceDeviceProfile=$src_profile PanOSSourceDeviceModel=$src_model PanOSSourceDeviceVendor=$src_vendor PanOSSourceDeviceOSFamily=$src_osfamily PanOSSourceDeviceOSVersion=$src_osversion PanOSSourceHostname=$src_host PanOSSourceMac=$src_mac PanOSTrafficOriginRegion=$region PanOSHTTPUserAgent=$user_agent PanOSTrafficSessionID=$sessionid
User-ID	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$subtype|$type\|1\|rt=$cef-formatted-receive_time deviceExternalId=$serial cs1Label=Factor Type cs1=$factortype cs3Label=Virtual System cs3=$vsys cs4Label=Data Source Name cs4=$datasourcename cs5Label=Data Source cs5=$datasource cs6Label=Data Source Type cs6=$datasourcetype cn1Label=Factor Number cn1=$factorno cn2Label=Virtual System ID cn2=$vsys_id cn3Label=Timeout Threshold cn3=$timeout src=$ip spt=$beginport dpt=$endport cnt=$repeatcnt duser=$user externalId=$seqno cat=$eventid end=$factorcompletiontime PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSActionFlags=$actionflags PanOSUGFlags=$ugflags PanOSUserBySource=$userbysource PanOSTimeGeneratedHighResolution=$high_res_timestamp
IP Tag	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$subtype|$type\|1\|rt=$cef-formatted-receive_time deviceExternalId=$serial cs3Label=Virtual System cs3=$vsys src=$ip PanOSTagName=$tag_name PanOSEventID=$event_id cnt=$repeatcnt PanOSTimeout=$timeout PanOSDataSourceName=$datasourcename PanOSDataSourceType=$datasource_type PanOSDataSourceSubType=$datasource_subtype externalId=$seqno PanOSActionFlags=$actionflags PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOsVsysName=$vsys_name dvchost=$device_name cn2Label=Virtual System ID cn2=$vsys_id PanOSTimeGeneratedHighResolution=$high_res_timestamp

<table>
<tr><td>Tunnel</td><td><i>CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version|$subtype|$type|1|rt=$cef-formatted-receive_time deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=Log Action cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags proto=$proto act=$action externalId=$seqno PanOSActionFlags=$actionflags PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name PanOSTunnelID=$tunnelid PanOSMonitorTag=$monitortag PanOSParentSessionID=$parent_session_id PanOSParentStartTime=$parent_start_time cs2Label=Tunnel Type cs2=$tunnel flexNumber1Label=Total bytes flexNumber1=$bytes in=$bytes_sent out=$bytes_received cn2Label=Packets cn2=$packets PanOSPacketsSent=$pkts_sent PanOSPacketsReceived=$pkts_received flexNumber2Label=Maximum Encapsulation flexNumber2=$max_encap cfp1Label=Unknown Protocol cfp1=$unknown_proto cfp2Label=Strict Checking cfp2=$strict_check PanOSTunnelFragment=$tunnel_fragment cfp3Label=Sessions Created cfp3=$sessions_created cfp4Label=Sessions Closed cfp4=$sessions_closed reason=$session_end_reason cat=$action_source start=$cef-formatted-time_generated cn3Label=Elapsed time in seconds cn3=$elapsed PanOSTunneInspectionRule=$tunnel_insp_rule PanOSRmtUserIP=$remote_user_ip PanOSRmtUserID=$remote_user_id PanOSRuleUUID=$rule_uuid PanOSPcapID=$pcap_id PanDynamicUsrgrp=$dynusergroup_name PanOSSourceEDL=$src_edl PanOSDestinationEDL=$dst_edl PanOSTimeGeneratedHighResolution=$high_res_timestamp</i></td></tr>
<tr><td>Correlation</td><td><i>CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version|$category|$type|$severity|rt=$cef-formatted-receive_time deviceExternalId=$serial start=$cef-formatted-time_generated src=$src suser=$srcuser cs3Label=Virtual System cs3=$vsys severity=$severity PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name cn2Label=Virtual System ID cn2=$vsys_id fname=$object_name cn3Label=Object ID cn3=$object_id msg=$evidence</i></td></tr>
<tr><td>GTP</td><td><i>CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version|$subtype|$type|1|rt=$cef-formatted-receive_time deviceExternalId=$serial start=cef-formatted-time_generated src=$src dst=$dst cs1Label=Rule cs1=rule app=$app cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid spt=$sport dpt=$dport proto=$proto act=$action PanOSGTPEventType=$event_type PanOSMSISDN=$msisdn PanOSAPName=$apn PanOSRadioTech=$rat PanOSGTPMsgType=$msg_type PanOSEndUserIP=$end_ip_addr PanOSTunnelEndptID1=$teid1 PanOSTunnelEndptID2=$teid2 PanOSGTPInterface=$gtp_interface PanOSGTPCause=$cause_code PanOSSeverity=$severity PanOSServingCntryMCC=$mcc PanOSServingNetMNC=$mnc PanOSAreaCode=$area_code PanOSCellID=$cell_id PanOSGTPEventCode=$event_code PanOSTunnelID=$imsi PanOSMonitorTag=$imei cat=$action_source PanOSTunnelInspectionRule=$tunnel_insp_rule PanOSRmtUserIP=$remote_user_ip PanOSRmtUserID=$remote_user_id PanOSRuleUUID=$rule_uuid fileId=$pcap_id PanOSTimeGeneratedHighResolution=$high_res_timestamp</i></td></tr>
<tr><td>SCTP</td><td><i>CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version|$type|rt=$cef-formatted-receive_time deviceExternalId=$serial start=$cef-formatted-time_generated src=$src dst=$dst cs1Label=Rule cs1=$rule cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inboudn_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$$sessionid cnt=$repeatcnt spt=$sport dpt=$dport $proto=$proto act=$action PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_level_4 PanOSVsysName=$vsys_name dvchost=$device_name externalId=$seqno PanOSAssocID=$assoc_id PanOSPayloadProtID=$ppid PanOSChunkType=$sctp_chunk_type PanOSSCTPVerTag1=$verif_tag_1 PanOSSCTPVerTag2=$verif_tag_2 PanOSSCTPCauseCode=$sctp_cause_code PanOSDiameterApp=$diam_app_id PanOSDiameterCmdCode=$diam_cmd_code PanOSDiameterAVPCode=$diam_avp_code PanOSSCTPStreamID=$stream_id PanOSSCTPAssocEndReason=$assoc_end_reason PanOSOpCode=$op_code PanOSSCCPCallingPartySSN=$sccp_calling_ssn PanOSSCCPCallingGT=$sccp_calling_gt PanOSSCTPFilter=$sctp_filter PanOSSCTPChunks=$chunks PanOSSCTPChunkSent=$chunks_sent PanOSSCTPChunkRcv=$chunks_received PanOSRuleUUID=$rule_uuid PanOSTimeGeneratedHighResolution=$high_res_timestamp</i></td></tr>
</table>

GlobalProtect	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$type|$subtype\|rt=$receive_time PanOSDeviceSN=$serial PanOSLogTimeStamp=$time_generated PanOSVirtualSystem=$vsys PanOSEventID=$eventid PanOSStage=$stage PanOSAuthMethod=$auth_method PanOSTunnelType=$tunnel_type PanOSSourceUserName=$srcuser PanOSSourceRegion=$srcregion PanOSEndpointDeviceName=$machinename PanOSPublicIPv4=$public_ip PanOSPublicIPv6=$public_ipv6 PanOSPrivateIPv4=$private_ip PanOSPrivateIPv6=$private_ipv6 PanOSHostID=$hostid PanOSDeviceSN=$serialnumber PanOSGlobalProtectClientVersion=$client_ver PanOSEndpointOSType=$client_os PanOSEndpointOSVersion=$client_os_ver PanOSCountOfRepeats=$repeatcnt PanOSQuarantineReason=$reason PanOSConnectionError=$error PanOSDescription=$opaque PanOSEventStatus=$status PanOSGPGatewayLocation=$location PanOSLoginDuration=$login_duration PanOSConnectionMethod=$connect_method PanOSConnectionErrorID=$error_code PanOSPortal=$portal PanOSSequenceNo=$seqno PanOSActionFlags=$actionflags PanOSTimeGeneratedHighResolution=$high_res_timestamp PanOSGatewaySelectionType=$selection_type PanOSSSLResponseTime=$response_time PanOSGatewayPriority=$priority PanOSAttemptedGateways=$attempted_gateways PanOSGateway=$gateway
Decryption	CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version\|$type|$subtype\|rt=$receive_time PanOSDeviceSN=$serial PanOSConfigVersion=$config_ver PanOSLogTimeStamp=$time_generated src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset PanOSTimeReceivedManagementPlane=$time_received cn1Label=SessionID cn1=$sessionid PanOSCountOfRepeats=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport =$flags proto=$proto act=$actionflags PanOSTunnel=$tunnel =$ =$ PanOSSourceUUID=$src_uuid PanOSDestinationUUID=$dst_uuid PanOSRuleUUID=$rule_uuid PanOSClientToFirewall=$hs_stage_c2f PanOSFirewallToServer=$hs_stage_f2s PanOSTLSVersion=$tls_version PanOSTLSKeyExchange=$tls_keyxchg PanOSTLSEncryptionAlgorithm=$tls_enc PanOSTLSAuth=$tls_auth PanOSPolicyName=$policy_name PanOSEllipticCurve=$ec_curve PanOSErrorIndex=$err_index PanOSRootStatus=$root_status PanOSChainStatus=$chain_status PanOSProxyType=$proxy_type PanOSCertificateSerial=$cert_serial PanOSFingerprint=$fingerprint PanOSTimeNotBefore=$notbefore PanOSTimeNotAfter=$notafter PanOSCertificateVersion=$cert_ver PanOSCertificateSize=$cert_size PanOSCommonNameLength=$cn_len PanOSIssuerNameLength=$issuer_len PanOSRootCNLength=$rootcn_len PanOSSNILength=$sni_len PanOSCertificateFlags=$cert_flags PanOSCommonName=$cn PanOSIssuerCommonName=$issuer_cn PanOSRootCommonName=$root_cn PanOSServerNameIndication=$sni_len PanOSErrorMessage=$error PanOSContainerID=$container_id PanOSContainerNameSpace=$pod_namespace PanOSContainerName=$pod_name PanOSSourceEDL=$src_edl PanOSDestinationEDL=$dst_edl PanOSSourceDynamicAddressGroup=$src_dag PanOSDestinationDynamicAddressGroup=$dst_dag PanOSTimeGeneratedHighResolution=$high_res_timestamp PanOSSourceDeviceCategory=$src_category PanOSSourceDeviceProfile=$src_profile PanOSSourceDeviceModel=$src_model PanOSSourceDeviceVendor=$src_vendor PanOSSourceDeviceOSFamily=$src_osfamily PanOSSourceDeviceOSVersion=$src_osversion PanOSSourceDeviceHost=$src_host PanOSSourceDeviceMac=$src_mac PanOSDestinationDeviceCategory=$dst_category PanOSDestinationDeviceProfile=$dst_profile PanOSDestinationDeviceModel=$dst_model PanOSDestinationDeviceVendor=$dst_vendor PanOSDestinationDeviceOSFamily=$dst_osfamily PanOSDestinationDeviceOSVersion=$dst_osversion PanOSDestinationDeviceHost=$dst_host PanOSDestinationDeviceMac=$dst_mac PanOSLogTypeSeqNo=$seqno PanOSActionFlags=$actionflag

Screen Shot: Active Channel Page

Shown below is a screenshot of the Active Channel page showing the events that a Palo Alto Networks device generated.



Active Channel: Palo Alto Networks

Total Events: 167

Start Time: 30 Apr 2014 13:00:00 PDT
End Time: 14 May 2014 14:00:00 PDT
Filter: MatchesFilter ("PaloAltoNetworks")

Inline Filter: No Filter

Very High: 0
High: 0
Medium: 8
Low: 159
Very Low: 0

Radar

Manager Receipt Time	Name	Device Event Class ID	Attacker Address	Target Address	Device Vendor	Device Product	Device Severity	Device Action	Device Event Category	Er
5/14 11:22:54	THREAT	vulnerability	172.80.2.11	172.80.1.11	Palo Alto Networks	PAN-OS	5	reset-client	Adobe Acrobat and R...	5/
5/14 11:22:34	THREAT	vulnerability	172.80.2.11	172.80.1.11	Palo Alto Networks	PAN-OS	5	alert	HTTP-404(41000)	5/
6 May 2014 16:35:16 PDT	THREAT	vulnerability	172.80.2.11	172.80.1.11	Palo Alto Networks	PAN-OS	5	alert	HTTP-404(41000)	6 I
6 May 2014 16:32:06 PDT	THREAT	vulnerability	172.80.2.11	172.80.1.11	Palo Alto Networks	PAN-OS	5	alert	HTTP-404(41000)	6 I
6 May 2014 16:31:16 PDT	CONFIG	Submitted			Palo Alto Networks	PAN-OS	1	commit		6 I
6 May 2014 16:31:06 PDT	CONFIG	Succeeded			Palo Alto Networks	PAN-OS	1	edit		6 I
6 May 2014 16:31:06 PDT	TRAFFIC	end	10.5.56.37	10.5.56.175	Palo Alto Networks	PAN-OS	1	allow		6 I
6 May 2014 16:30:56 PDT	CONFIG	Succeeded			Palo Alto Networks	PAN-OS	1	edit		6 I
6 May 2014 16:30:36 PDT	TRAFFIC	end	10.5.56.37	10.5.56.175	Palo Alto Networks	PAN-OS	1	allow		6 I
6 May 2014 16:30:36 PDT	CONFIG	Succeeded			Palo Alto Networks	PAN-OS	1	edit		6 I
6 May 2014 16:30:06 PDT	TRAFFIC	end	10.5.56.37	10.5.56.175	Palo Alto Networks	PAN-OS	1	allow		6 I
6 May 2014 16:29:56 PDT	TRAFFIC	end	10.35.13.48	10.5.56.175	Palo Alto Networks	PAN-OS	1	allow		6 I
6 May 2014 16:29:56 PDT	TRAFFIC	end	10.35.13.48	10.5.56.175	Palo Alto Networks	PAN-OS	1	allow		6 I

2. Events

For system events, the *$eventid* field captures the specific event associated with that log. Please refer to the latest PAN-OS Administrator's Guide for additional coverage of logging in PAN-OS.

3. Device Event Mapping to ArcSight Data Fields

The device sends information contained within vendor-specific event definitions to the ArcSight SmartConnector, and then maps the events to ArcSight data fields.

The Prefix Fields table lists definitions of the prefix fields and their values for Syslog messages that Palo Alto Networks firewalls generate. The Extension Dictionary and Custom Dictionary Extension tables list Palo Alto Networks-specific event definitions and their mapping to ArcSight CEF data fields.

Prefix Fields

CEF Name	Data Type	Meaning	Palo Alto Networks Value
Version	Integer	Identifies the version of the CEF format.	0
Device Vendor	String	Device vendor	Palo Alto Networks
Device Product	String	Device product	PAN-OS
Device Version	String	Device version	Configurable. For example, '8.0.2'
Signature ID	String	Unique identifier per event-type Note: Updated in PAN-OS 5.0	Value is event-type specific: ● Traffic: $subtype ● Threat: $subtype ● Config: $result ● System: $subtype ● HIP: $matchtype
Name	String	Represents a human-readable and understandable description of the event. Note: Updated in PAN-OS 5.0	Value is event-type specific: ● Traffic: $type ● Threat: $type

			● Config: $type ● System: $type ● HIP Match: $type
Severity	Integer	Reflects the importance of the event. Only numbers from 0 to 10 are allowed, where 10 indicates the most important event.	$number-of-severity Always 1 for traffic, config, user-id, authentication, and HIP events.

Extension Dictionary

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
act	deviceAction	String	63	Action mentioned in the event.	Value is event-type specific: ● Traffic : $action ● Threat: $action ● Config: $cmd
app	ApplicationProtocol	String	31	Application-level protocol, example values are: HTTP, HTTPS, SSHv2, Telnet, POP, IMAP, IMAPS.	$app
c6a2Label		IPv6 Address		Represents an IPv6 address	HIP Match: $srcipv6 (IPv6 address of the user's machine or device.)
cat	deviceEventCategory	String	1023	Represents the category that the originating device assigned. Devices often use their own categorization schema to classify events.	Value is event-type specific: ● System : $eventid ● Threat: $threatid ● HIP: $matchname ● Traffic, Tunnel Inspection: $action_source
cfp1	deviceCustomFloatingPoint1			Tunnel Inspection Logs: Unknown Protocol	Tunnel Inspection Logs: $unknown_proto

cfp1Label	deviceCustomFloatingPoint1	String		Tunnel Inspection Logs: Unknown Protocol	Tunnel Inspection Logs: $unknown_proto
cfp2	deviceCustomFloatingPoint2			Tunnel Inspection Logs: Strict Checking	Tunnel Inspection Logs: $strict_check
cfp2Label	deviceCustomFloatingPoint2	String		Tunnel Inspection Logs: Strict Checking	Tunnel Inspection Logs: $strict_check
cfp3	deviceCustomFloatingPoint3			Tunnel Inspection Logs: Sessions Created	Tunnel Inspection Logs: $sessions_created
cfp3Label	deviceCustomFloatingPoint3	String		Tunnel Inspection Logs: Sessions Created	Tunnel Inspection Logs: $sessions_created
cfp4	deviceCustomFloatingPoint4			Tunnel Inspection Logs: Sessions Closed	Tunnel Inspection Logs: $sessions_closed
cfp4Label	deviceCustomFloatingPoint4	String		Tunnel Inspection Logs: Sessions Closed	Tunnel Inspection Logs: $sessions_closed
cn1	deviceCustomNumber1	Long		Varies	Value is event-type specific: ● Traffic, Threat, Tunnel Inspection: $sessionid ● Auth, User-id: $factorno
cn1Label	deviceCustomNumber1 Label	String	1023	Traffic, Threat, Tunnel Inspection: Session ID Auth, User-ID: Factor Number	Value is event-type specific: ● Traffic, Threat, Tunnel Inspection: $sessionid

					● Auth, User-id: $factorno
cn2	deviceCustomNumber2	Long		Varies	Value is event-type specific: ● Traffic, Threat, Tunnel Inspection: $packets ● Correlation, HIP Match, User-ID: $vsys_id ● Authentication: $authid
cn2Label	deviceCustomNumber2Label	String	1023	Varies	Value is event-type specific: ● Traffic, Threat, Tunnel Inspection: packets ● Correlation, HIP Match, User-ID: Virtual System ID ● Authentication: Authentication ID
cn3	deviceCustomNumber3	Long		Varies	Value is event-type specific: ● Traffic: $elapsed ● User-ID: $timeout ● Correlation: $object_id
cn3Label	deviceCustomNumber3Label	String	1023	Varies	Value is event-type specific: ● Traffic, Tunnel Inspection: Elapsed Time (sec): elapsed time of the session. ● User-ID: Timeout ● Correlation: Object ID
cnt	baseEventCount	Integer		A count associated with this event: the	$repeatcnt

				number of times it was observed.	
cs1	deviceCustomString1	String	1023	Rule Config optional: before change detail	Value is event-type specific: ● Traffic, Threat, Tunnel Inspection : $rule ● Config: $before-change-detail ● User-ID: $factortype
cs1Label	deviceCustomString1Label	String	1023	Rule Config optional: before change detail Auth: Server Profile User-ID: Factor Type	Value is event-type specific: ● Traffic, Threat, Tunnel Inspection: Rule ● Config: Before Change Detail ● Auth: Server Profile ● User-ID: Factor Type
cs2	deviceCustomString2	String	1023	URL category Config optional: after change detail HIP: Operating system (Note: Added in PAN-OS 6.0) Authentication: Normalize User	Value is event-type specific: ● Traffic: $category ● Threat: $category ● Config: after-change-detail ● HIP: $os ● Authentication: $normalize_user ● Tunnel Inspection: $tunnel
cs2Label	deviceCustomString2Label	String	1023	URL category Config optional: after change detail HIP: Operating system (Note: Added in PAN-OS 6.0)	Value is event-type specific: ● Traffic: URL category ● Threat: URL category ● Config: after change detail

				Authentication: Normalize User	● HIP: operating system ● Authentication: Normalize User ● Tunnel Inspection: Tunnel Type
cs3	deviceCustomString3	String	1023	Vsys	$vsys
cs3Label	deviceCustomString3Label	String	1023	Virtual system	
cs4	deviceCustomString4	String	1023	Varies	Value is event-type specific: ● Traffic, Threat, URL, Data, WildFire, Tunnel Inspection: $from ● Authentication: $authpolicy ● User-ID: $datasourcename
cs4Label	deviceCustomString4Label	String	1023	Varies	Value is event-type specific: ● Traffic, Threat, URL, Data, WildFire, Tunnel Inspection: Source zone ● Authentication: Authentication Policy ● User-ID: Data Source Name
cs5	deviceCustomString5	String	1023	Varies	Value is event-type specific: ● Traffic, Threat, URL, Data, WildFire, Tunnel Inspection: $to ● Authentication: $clienttype

					● User-ID: $datasource
cs5Label	deviceCustomString5Label	String	1023	Varies	Value is event-type specific: ● Traffic, Threat, URL, Data, WildFire, Tunnel Inspection: Destination Zone ● Authentication: Client Type ● User-ID: Data Source ● (Source from which User-ID mapping information is collected)
cs6	deviceCustomString6	String	1023	Traffic, Threat, URL, Data, WildFire: LogProfile Authentication, Tunnel Inspection: Log Action User-ID: Data Source Type	Value is event-type specific: ● Traffic, Threat, URL, Data, WildFire: $logset ● Authentication, Tunnel Inspection: $logset ● User-ID: $datasourcetype
cs6Label	deviceCustomString6Label	String	1023	Traffic, Threat, URL, Data, WildFire: LogProfile Authentication, Tunnel Inspection: Log Action User-ID: Data Source Type	Value is event-type specific: ● Traffic, Threat, URL, Data, WildFire: Log Profile ● Authentication, Tunnel Inspection: Log Action ● User-ID: Data Source Type
destinationServiceName		String	1023	The service that this event targets.	Value is event-type specific: Config: $client

destinationTranslated Address		IPv4 Address		Identifies the translated destination that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”	$natdst
destinationTranslatedPort		Integer		Port after it was translated; for example, a firewall. Valid port numbers are 0 to 65535.	$natdport
deviceExternalId		String	255	A name that uniquely identifies the device generating this event. Serial number of the device.	$serial
deviceInboundInterface		String	15	Interface on which the packet or data entered the device.	$inbound_if
deviceOutboundInterface		String	15	Interface on which the packet or data left the device.	$outbound_if
dpt	destinationPort	Integer		The valid port numbers are between 0 and 65535.	• Traffic, Threat, URL, Data, WildFire: $dport • User-ID: $endport
dst	destinationAddress	IPv4 Address		Identifies the destination that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”	$dst
duid	destinationUse rId	String	1023	Only for WildFire subtype; all other	$recipient

				types do not use this field. Specifies the name of the receiver of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.	
duser	destinationUserName	String	1023	Identifies the destination user by name. This is the user associated with the event destination. Email addresses are also mapped into the UserName fields. The recipient is a candidate to put into destinationUserName.	Value is event-type specific: ● Traffic: $dstuser ● Threat: $dstuser ● Config: $admin ● Authentication, User-ID: $user
dvchost	deviceHostName	String	100	The format should be a fully qualified domain name (FQDN) associated with the device node, when a node is available. Examples: “host.domain.com” or “host”.	Value is event-type specific: All logs: $device_name Note: updated in 7.0: Remapped Config: $host to shost
end		Time Stamp		Varies	User-ID: $factorcompletiontime (Time the authentication was completed.)
externalId		Integer		An ID that the originating device used. Usually these are increasing	$seqno

				numbers associated with events.	
fileType	fileType	String	1023	Only for WildFire subtype; all other types do not use this field.Specifies the type of file that the firewall forwarded for WildFire analysis.	$fileType
flexNumber1				Total bytes (rx and tx)	$bytes
flexNumber1Label				Total bytes	
flexNumber2				Maximum Encapsulation	$max_encap
flexNumber2Label				Tunnel Inspection logs: Maximum Encapsulation (Number of packets the firewall dropped because the packet exceeded the maximum number of encapsulation levels configured in the Tunnel Inspection policy rule (Drop packet if over maximum tunnel inspection level).	$max_encap
flexString1		String		Flags	$flags
flexString1Label		String		Flags	
flexString2		String		Direction Module Vendor	Value is event-type specific: ● Threat: $direction ● System: $module ● Authentication: $vendor

flexString2Label		String		Varies: Direction Module Vendor (Vendor providing additional factor authentication.)	Value is event-type specific: ● Threat: direction ● System: module ● Authentication: Vendor
fname	filename	String	1023	Name of the file.	Value is event-type specific: ● System, Authentication: $object ● Correlation: $object_name
filePath		String	1023	The cloud string shows the FQDN of either the WildFire appliance (private) or the WildFire cloud (public) where the file was uploaded for analysis. Note: Added in PAN-OS 6.0	$cloud
fileId		String	1023	Pcap-id is a 64-bit unsigned integer denoting an identifier to correlate threat PCAP files with extended PCAPs taken as a part of that flow. Note: Added in PAN-OS 6.0	$pcap_id
fileHash		String	255	The filedigest string shows the binary hash of the file sent to the WildFire service for analysis.	$filedigest

				Note: Added in PAN-OS 6.0	
in	bytesIn	Integer		Number of bytes transferred inbound. Inbound is relative to the source-to-destination relationship, meaning that data flowed from source to destination.	$bytes_sent
msg	Message	String	1023	An arbitrary message giving more details about the event. Using \n as the new-line separator enables multi-line entries.	Value is event-type specific: ● Authentication: $event ● Config: $path ● Correlation: $evidence ● WildFire: $subject (subject of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.) ● System: $opaque ● Correlation: $evidence
oldFileId	oldFileId	String	1023	Only for WildFire subtype; all other types do not use this field. Identifies the analysis request on the WildFire cloud or the WildFire appliance.	$reportid
out	bytesOut	Integer		Number of bytes transferred outbound. Outbound is relative to the source-to-destinat	$bytes_received

				ion relationship, meaning that data flowed from destination to source.	
proto	transportProtocol	String	31	Identifies the Layer 4 protocol used. The possible values are protocol names such as TCP or UDP.	$proto
reason		String	1023	The reason an audit event was generated. For example "Bad password” or “Unknown User".	Traffic, Tunnel Inspection: $session_end_reason
request	requestURL	String	1023	URL or filename for threat logs	$misc
requestClientApplication	requestClientApplication	String	1023	Only for the URL Filtering subtype; all other types do not use this field. The User Agent field specifies the web browser that the user used to access the URL, for example Internet Explorer. This information is sent in the HTTP request to the server.	$user_agent
requestContext		String	2048	Description of the content from which the request originated.	Value is event-type specific: URL: $contenttype (Content type of the HTTP response data)
requestMethod		String		Only in URL filtering logs.	URL: $http_method

				Describes the HTTP Method used in the web request. Only the following methods are logged: Connect, Delete, Get, Head, Options, Post, Put. Note: added in PAN-OS 8.0	
rt	receiptTime	Time Stamp		The time when the event related to the activity was received. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970).	$cef-formatted-receive_time
shost	sourceHostName	String	1023	Identifies the source that an event refers to in an IP network. The format should be a fully qualified domain name associated with the source node, when a node is available. Examples: “host.domain.com” or “host”.	Value is event-type specific: ● HIP match: $machinename ● Config: $host
sourceTranslatedAddress		IPv4 Address		Identifies the translated source that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”	$natsrc
sourceTranslatedPort		Integer		Port after it was translated by, for	$natsport

				example, a firewall. The valid port numbers are 0 to 65535.	
spt	sourcePort	Integer		The valid port numbers are 0 to 65535.	● Traffic, Threat, URL, Data, WildFire: $sport ● User-ID: $beginport
src	sourceAddress	IPv4 Address		Identifies the source that an event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”	Value is event-type specific: ● Traffic, Threat, URL, Data, WildFire, HIP Match, Correlation: $src ● Authentication, User-ID: $ip
start	startTime	Time Stamp		The time when the activity the event referred to started. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970).	Traffic, HIP Match, Correlation Logs: ● $cef-formatted-time_generated (Time the log was generated on the dataplane.) ● Tunnel Inspection Logs: $start (Year/month/day hours:minutes:seconds that the session began.)
suid	sourceUserId	String	1023	Only for WildFire subtype; all other types do not use this field. Specifies the name of the sender of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.	$sender

suser	sourceUserName	String	1023	Identifies the source user by name. Email addresses are also mapped into the UserName fields. The sender is a candidate to put into sourceUserName.	Value is event-type specific: Traffic, Threat, URL, Data, WildFire, HIP Match, Correlation: $srcuser

Custom Dictionary Extensions

Extension Key Name	Data Type	Length	Meaning
PanLinkChange			Number of link flaps that occurred during the session.
PanPolicyID			Name of the SD-WAN policy.
PanLinkDetail			Contains up to four link flap entries, with each entry containing the link name, link tag, link type, physical interface, timestamp, bytes read, bytes written, link health, and link flap cause
PanSDWANCluster			Name of the SD-WAN cluster.
PanSDWANDevice			Type of device (`hub` or `branch`).
PanSDWANClustype			Type of cluster (`mesh` or `hub-spoke`).
PanSDWANSite			Name of the SD-WAN site.
PanOSPcapID			Unique packet capture ID that defines the location of the pcap file on the firewall.
PanOSRmtUserID			IMSI identity of a remote user, and if available, one IMEI identity or one MSISDN identity.
PanOSRmtUserIP			IPv4 or IPv6 address of a remote user.
PanDynamicUsrgrp			Name of the dynamic user group that contains the user who initiated the session.

PanHTTP2Con			Identifies if traffic used an HTTP/2 connection by displaying one of the following values: TCP connection session ID—session is HTTP/2 0—session is not HTTP/2
PanOSActionFlags	String		A bit field indicating if the log was forwarded to Panorama. Note: Added in PAN-OS 8.0
PanOSAssocID			Number that identifies all connections for an association between two SCTP endpoints.
PanOSChunkType			Describes the type of information contained in a chunk, such as control or data.
PanOSContentVer	String		Applications and Threats version on your firewall when the log was generated. Note: Added in PAN-OS 8.0
PanOSDataSourceName			The name of the source from which mapping information is collected.
PanOSDataSourceSubType			The mechanism used to identify the IP address-to-username mappings within a data source.
PanOSDataSourceType			The source from which mapping information is collected.
PanOSDesc	String		Additional Authentication Information. Note: Added in PAN-OS 8.0
PanOSDGl1 **PanOSDGl2** **PanOSDGl3** **PanOSDGl4**	Integer		A sequence of identification numbers that indicate the device group's location within a device group hierarchy. The firewall (or virtual system) generating the log includes the identification number of each ancestor in its device group hierarchy. The shared device group (level 0) is not included in this structure. If the log values are 12, 34, 45, 0, it means that the log was generated by a firewall (or virtual system) that belongs to device group 45, and its ancestors are 34, and 12. To view the device group names that correspond to the value 12, 34 or 45, use one of the following methods: CLI command in configure mode: show readonly dg-meta-data API query: /api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>
PanOSDiameterApp			The diameter application in the data chunk which triggered the event. Diameter Application ID is assigned by Internet Assigned Numbers Authority (IANA).
PanOSDiameterAVPCode			The diameter AVP code in the data chunk which triggered the event.
PanOSDiameterCmdCode			The diameter command code in the data chunk which triggered the event. Diameter Command Code is assigned by Internet Assigned Numbers Authority (IANA)
PanOSDstUUID	String		Identifies the destination universal unique identifier for a guest virtual machine in the VMware NSX environment.

			Note: Added in PAN-OS 8.0
PanOSDstUUID			Identifies the destination universal unique identifier for a guest virtual machine in the VMware NSX environment.
PanOSEventID			A string showing the name of the event.
PanOSHostID			Unique ID GlobalProtect assigns to identify the host.
PanOSHTTPHeader			Indicates the inserted HTTP header in the URL log entries on the firewall.
PanOSMonitorTag	String		Monitor name you configured for the Tunnel Inspection policy rule or the International Mobile Equipment Identity (IMEI) ID of the mobile device. Note: Added in PAN-OS 8.0
PanOSMonitorTag			International Mobile Equipment Identity (IMEI) is a unique 15 or 16 digit number allocated to each mobile station equipment.
PanOSOpCode			Identifies the operation code of application layer SS7 protocols, like MAP or CAP, in the data chunk which triggered the event.
PanOSPacketsReceived	Integer		Number of packets transferred inbound, from destination to source.
PanOSPacketsSent	Integer		Number of packets transferred outbound, from source to destination
PanOSParentSessionID	Integer		ID of the session in which this session is tunneled. Applies to inner tunnel (if two levels of tunneling) or inside content (if one level of tunneling) only. Note: Added in PAN-OS 8.0
PanOSParentSessionID			ID of the session in which this session is tunneled. Applies to inner tunnel (if two levels of tunneling) or inside content (if one level of tunneling) only.
PanOSParentStartTime	Time Stamp		Year/month/day hours:minutes:seconds that the parent tunnel session began. Note: Added in PAN-OS 8.0
PanOSParentStartTime			Year/month/day hours:minutes:seconds that the parent tunnel session began.
PanOSPayloadProtID			Identifies the Payload Protocol ID (PPID) in the data chunk which triggered this event. PPID is assigned by Internet Assigned Numbers Authority (IANA).
PanOSPPID			ID of the protocol for the payload in the data portion of thedata chunk.
PanOSReferer	String		Only for the URL Filtering subtype; all other types do not use this field. The Referer field in the HTTP header contains the URL of the web page that linked the user to another web page; it is the source that redirected (referred) the user to the web page that is being requested.

PanOSRmtUserID			IMSI identity of a remote user, and if available, one IMEI identity and/or one MSISDN identity.
PanOSRmtUserIP			IPv4 or IPv6 address used by a remote user.
PanOSRuleUUID			The UUID that permanently identifies the rule.
PanOSSCCPCallingGT			The Signaling Connection Control Part (SCCP) calling party global title (GT) in the data chunk which triggered the event.
PanOSSCCPCallingPartySSN			The Signaling Connection Control Part (SCCP) calling party subsystem number (SSN) in the data chunk which triggered the event.
PanOSSCTPAssocEndReason			Reason an association was terminated. If the termination had multiple causes, the highest priority reason is displayed. The possible session end reasons in descending priority are: -shutdown-from-endpoint (highest)—endpoint sends out SHUTDOWN -abort-from-endpoint—endpoint sends out ABORT -unknown (lowest)—the association aged out, or association termination reason is not covered by one of the previous reasons (for example, a clear session all command).
PanOSSCTPAssocID			Number that identifies all connections for an association between two SCTP endpoints.
PanOSSCTPCauseCode			Sent by an endpoint to specify reason for an error condition to other endpoint of same SCTP association.
PanOSSCTPChunkRcv			Number of SCTP chunks received for an association.
PanOSSCTPChunks			Sum of SCTP chunks sent and received for an association.
PanOSSCTPChunkSent			Number of SCTP chunks sent for an association.
PanOSSCTPFilter			Name of the filter that the SCTP chunk matched.
PanOSSCTPStreamID			ID of the stream which carries the data chunk which triggered the event.
PanOSSCTPVerTag1			Used by endpoint1 which initiates the association to verify if the SCTP packet received belongs to current SCTP association and validate the endpoint2.
PanOSSCTPVerTag2			Used by endpoint2 to verify if the SCTP packet received belongs to current SCTP association and validate the endpoint1.
PanOSSrcUUID	String		Identifies the source universal unique identifier for a guest virtual machine in the VMware NSX environment. Note: Added in PAN-OS 8.0
PanOSSrcUUID			Identifies the source universal unique identifier for a guest virtual machine in the VMware NSX environment.
PanOSTagName			The tag mapped to the source IP address.
PanOSThreatCategory	String		Describes threat categories used to classify different types of threat signatures.

			Note: Added in PAN-OS 8.0
PanOSTimeout			The amount of time before the IP address-to-tag mapping expires for the source IP address.
PanOSTunnelFragment	Integer		Number of packets the firewall dropped because of fragmentation errors (Tunnel Inspection logs).
PanOSTunnelID	Integer		ID of the tunnel being inspected or the International Mobile Subscriber Identity (IMSI) ID of the mobile user. Note: Added in PAN-OS 8.0
PanOSTunnelID			International Mobile Subscriber Identity (IMSI) is a unique number allocated to each mobile subscriber in the GSM/UMTS/EPS system. IMSI shall consist of decimal digits (0 through 9) only and maximum number of digits allowed are 15.
PanOSTunnelInspectionRule			Name of the tunnel inspection rule matching the cleartext tunnel traffic
PanOSTunnelType	String		Type of tunnel, such as GRE or IPSec. Note: Added in PAN-OS 8.0
PanOSTunnelType	String		Type of tunnel, such as GRE or IPSec.
PanOSTunnelType			Type of tunnel, such as GRE or IPSec.
PanOSUGFlags			Displays whether the user group that was found during user group mapping. Supported values are: User Group Found—Indicates whether the user could be mapped to a group. Duplicate User—Indicates whether duplicate users were found in a user group. Displays N/A if no user group is found.
PanOSURLCatList			Lists the URL Filtering categories that the firewall used to enforce policy.
PanOSUserBySource			Indicates the username received from source through IP-User mapping.
PanOSVsysName	String		This is the full virtual system name. This can be used instead of vsys which is an id representation of the virtual system. Note: Added in PAN-OS 7.0
PanOSXforwarderfor	IPv4Address		Only for the URL Filtering subtype; all other types do not use this field. The X-Forwarder-For field in the HTTP header contains the IP address of the user who requested the web page. It allows you to identify the IP address of the user, which is useful particularly if you have a proxy server on your network that replaces the user IP address with its own address in the source IP address field of the packet header.

Support

In some cases, the ArcSight Customer Service team is unable to help with issues that are specific to the configuration. In such a case, contact the certified vendor for assistance:

Palo Alto Networks Customer Support

- **Phone**—US: (866) 898-9087. Outside the US: +1 (408) 738-7799
- **Email**—support@paloaltonetworks.com

Instructions—Use this contact information for issues outside of the ArcSight product concerning configuration of the Palo Alto Networks firewall for exporting to a Syslog server.

Additional ArcSight Documentation

For more information about the joint solution, visit the Micro Focus ArcSight Marketplace:
https://marketplace.microfocus.com/arcsight/category/partner-integrations
For more information about Micro Focus Security ArcSight ESM:
https://software.microfocus.com/en-us/software/siem-security-information-event-management