ENTERPRISE SECURITY

Common Event Format Configuration Guide

Palo Alto Networks
PAN-OS 6.0
Date: May 16, 2014

paloalto
NETWORKS

ArcSight CEF
Certified
2014

CEF Connector Configuration 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 HP. HP does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Certified CEF

The event format complies with the requirements of the HP ArcSight Common Event Format (CEF). The HP ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HP's ArcSight product. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. The events will be sufficiently categorized to be used in correlation rules, reports and dashboards as a proof-of-concept (POC) of the joint solution.

Revision History

Date	Description
2/25/2011	First edition of this Configuration Guide.
3/2/2011	Certified CEF-compliant PAN-OS 4.0.0
1/9/2012	Re-map the Direction field in threat log to a string. PAN-OS 4.1.0: Added Bytes In/Out fields to traffic log.
2/6/2012	V4.1 Certified by HP Enterprise Security.
10/2/2012	Modified mapping for "msg" for system events. Added support contact information. Added configuration step for including device host information.
5/16/2014	5.0 Updates Added another threat subtype called "wildfire". Updated threat logs threat ID definition. **Re-map URL logs $misc to map to "request" instead of "msg".** **Updated threat logs to provide more event context:** **split $subtype and $threatid into their own event fields** **(deviceEventClassId and "cat" respectively).** **Updated system logs to remove $eventid from header to "cat".** **Updated config logs to remove $subtype from header.** Added optional fields for config log details.
5/16/2014	6.0 Updates Added new fields to threat logs: Cloud, PCAP-ID, and File Digest. Added OS to HIP logs.
5/14/2014	Version 6.0.0 Certified by HP Enterprise Security

CEF Connector support information when an issue is outside of the ArcSight team's ability

In some cases the ArcSight Customer Service team is unable to help with issues that lie within the configuration itself. In this 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 the preceding contact information for issues outside of the ArcSight product concerning configuration of the Palo Alto Networks firewall for exporting to a Syslog server.

PAN-OS 6.0.0 CEF Configuration Guide

This guide provides information for configuring the Palo Alto Networks next-generation firewalls for CEF-formatted Syslog event collection. PAN-OS version 4.0.0 or higher is supported.

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.

Palo Alto Networks devices include the Panorama M-100 appliance, Panorama virtual appliance, PA-7000 Series firewall, PA-5000 Series firewall, PA-4000 Series firewall, PA-2000 Series firewall, PA-500 firewall, PA-200 firewall, and the PA-VM Series firewall. The firewalls range from 250Mbps to 20Gbps of throughput capacity. Delivered as a purpose-built appliance, every Palo Alto Networks next-generation firewall uses dedicated, function-specific processing that is tightly integrated with a single-pass software engine. This unique combination of hardware and software maximizes network throughput while minimizing latency. Each hardware platform supports the same rich set of firewall features, ensuring consistent operation across the entire line.

Configuration

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.

1. To configure the device to include its IP address in the header of Syslog messages, select **Panorama/Device > Setup > Management**, in the Logging and Reporting Settings section click the Edit ⚙ icon, 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**.

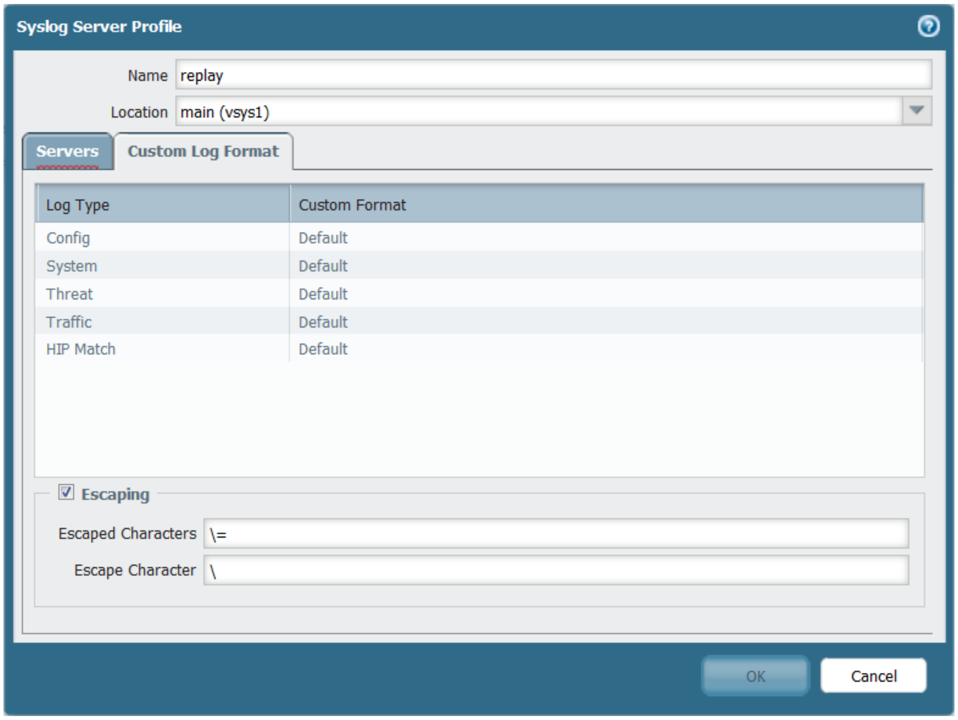
3. Enter a server profile **Name** and **Location** (location refers to a virtual system, if the device is enabled for virtual systems).

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, HIP Match) to define a custom format based on the ArcSight CEF for that log type (see CEF-style Log Formats).

   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.



Syslog Server Profile

Name: replay

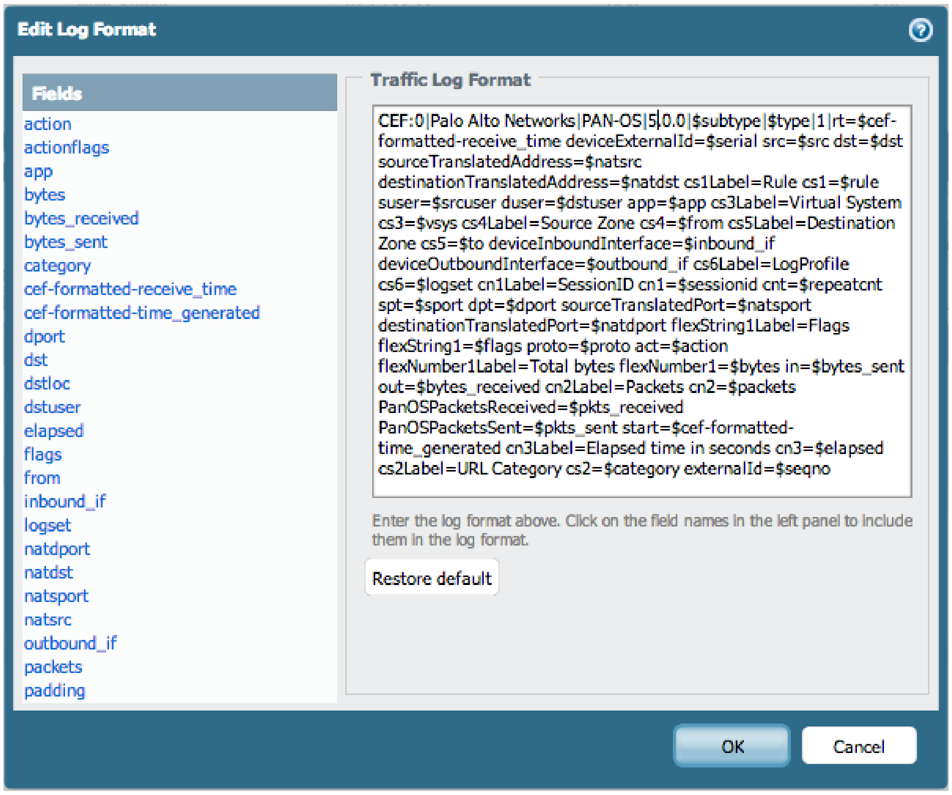
Location: main (vsys1)

Log Type	Custom Format
Config	Default
System	Default
Threat	Default
Traffic	Default
HIP Match	Default

☑ Escaping

Escaped Characters: \=

Escape Character: \



Edit Log Format

Traffic Log Format

```
CEF:0|Palo Alto Networks|PAN-OS|5.0.0|$subtype|$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
```

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

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

CEF-style Log Formats

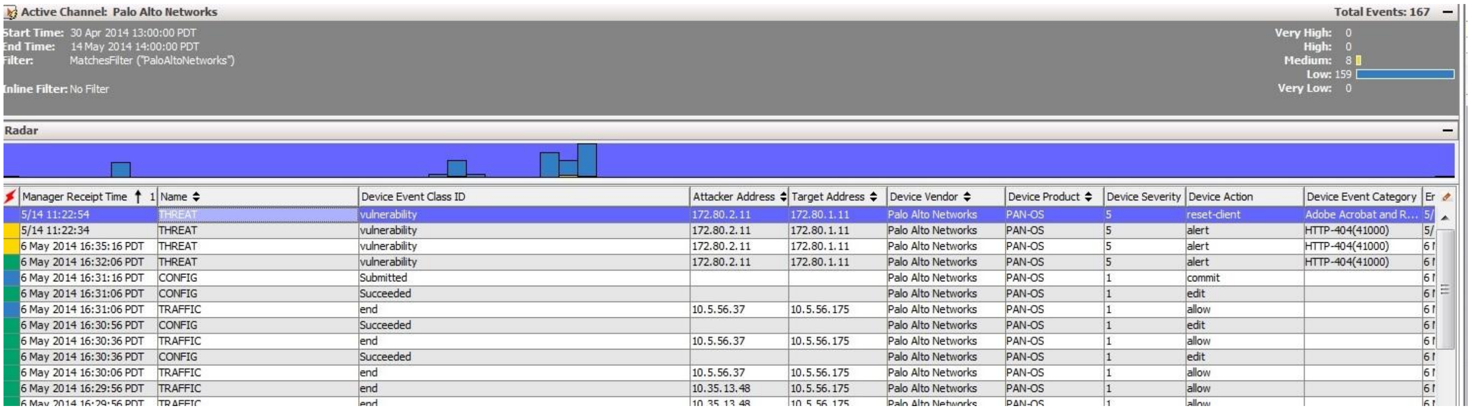
The following table shows the CEF-style format that was used during the certification process for each log type. These custom formats include all the fields, in a similar order, that the default format of the syslogs display.

<table>
<tr><td>Traffic</td><td>CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$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=$seqno</td></tr>
<tr><td>Threat</td><td>CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$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 externalId=$seqno requestContext=$contenttype cat=$threatid filePath=$cloud fileId=$pcap_id fileHash=$filedigest</td></tr>
<tr><td>Config</td><td>CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$result|$type|1|rt=$cef-formatted-receive_time deviceExternalId=$serial dvchost=$host cs3Label=Virtual System cs3=$vsys act=$cmd duser=$admin destinationServiceName=$client msg=$path externalId=$seqno
Optional: cs1Label=Before Change Detail cs1=$before-change-detail cs2Label=After Change Detail cs2=$after-change-detail</td></tr>
</table>

System	CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype\|$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=$eventid
HIP Match	CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$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 cs2Label=Operating System cs2=$os

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

	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

Events

The different log types for which the device generates syslogs include traffic, threat, config, system, and HIP match. For the system events, the *$eventid* field captures the specific event associated with that log. Refer to the System Log Events document (https://live.paloaltonetworks.com/docs/DOC-2821) for a listing of all the events grouped by the system area.

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 Extensions 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, '6.0.0'
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, 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
cat	deviceEventCategory	String	1023	Represents the category that the originating device assigned. Devices often use their own categorization schema to classify events. Note: Added in PAN-OS 5.0	Value is event-type specific: System : $eventid Threat: $threatid HIP: $matchname
cn1	deviceCustomNumber1	Long		SessionID	$sessionid
cn1Label	deviceCustomNumber1 Label	String	1023	SessionID	
cn2	deviceCustomNumber2	Long		Packets	$packets
cn2Label	deviceCustomNumber2Labe	String	1023	Packets	

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
	l				
cn3	deviceCustomNumber3	Long		Elapsed time	$elapsed
cn3Label	deviceCustomNumber3Label	String	1023	Elapsed time in seconds	
cnt	baseEventCount	Integer		A count associated with this event: the number of times it was observed.	$repeatcnt
cs1	deviceCustomString1	String	1023	Rule Config optional: before change detail	Value is event-type specific: Traffic : $rule Threat: $rule Config: $before-change-detail
cs1Label	deviceCustomString1Label	String	1023	Rule Config optional: before change detail	Value is event-type specific: Traffic : Rule Threat: Rule Config: Before Change Detail
cs2	deviceCustomString2	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: $category Threat: $category Config: after-change-detail HIP: $os

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
cs2Label	deviceCustom String2Label	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 HIP: operating system
cs3	deviceCustom String3	String	1023	Vsys	$vsys
cs3Label	deviceCustom String3Label	String	1023	Virtual system	
cs4	deviceCustom String4	String	1023	Srczone	$from
cs4Label	deviceCustom String4Label	String	1023	Source zone	
cs5	deviceCustom String5	String	1023	Dstzone	$to
cs5Label	deviceCustom String5Label	String	1023	Destination zone	
cs6	deviceCustom String6	String	1023	LogProfile	$logset
cs6Label	deviceCustom String6Label	String	1023	LogProfile	
destinationServi		String	1023	The service that	Value is event-

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
ceName				this event targets.	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
deviceOutbound Interface		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.	$dport
dst	destinationAddress	IPv4 Address		Identifies the destination that the event refers to in an	$dst

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
				IP network. The format is an IPv4 address. Example: “192.168.10.1”	
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
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: Config: $host
externalId		Integer		An ID that the originating device used. Usually these are increasing numbers associated with events.	$seqno
flexNumber1				Total bytes (rx and tx)	$bytes
flexNumber1Label		String		Total bytes	

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
flexString1		String		Flags	$flags
flexString1Label		String		Flags	
flexString2		String		Direction Module	Value is event-type specific: Threat: $direction System: $module
flexString2Label		String		Direction Module	Value is event-type specific: Threat: direction System: module
fname	filename	String	1023	Name of the file.	Value is event-type specific: System: $object
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.	$pcap_id

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
				Note: Added in PAN-OS 6.0	
fileHash		String	255	The filedigest string shows the binary hash of the file sent to the Wildfire service for analysis. Note: Added in PAN-OS 6.0	$filedigest
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. Note: 5.0 removed the mapping for threat logs and re-mapped to request.	Value is event-type specific: System: $opaque Config: $path
out	bytesOut	Integer		Number of bytes transferred outbound. Outbound is relative to the source-to-	$bytes_received

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
				destination 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
request	requestURL	String	1023	URL or filename for threat logs	$misc
requestContext		String	2048	Description of the content from which the request originated.	Value is event-type specific: Threat: $contenttype
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.	Value is event-type specific: HIP match: $machinename

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
				Examples: "host.domain.com" or "host".	
sourceTranslated Address		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
sourceTranslated Port		Integer		Port after it was translated by, for example, a firewall. The valid port numbers are 0 to 65535.	$natsport
spt	sourcePort	Integer		The valid port numbers are 0 to 65535.	$sport
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"	$src
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).	$cef-formatted-time_generated

CEF Key Name	Full Name	Data Type	Length	Meaning	Palo Alto Networks Value Field
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.	$srcuser

Custom Dictionary Extensions

Extension Key Name	Data Type	Length	Meaning
PanOSPacketsReceived	Integer		Number of packets transferred inbound, from destination to source.
PanOSPacketsSent	Integer		Number of packets transferred outbound, from source to destination