PAN-OS Syslog Integration

Tech Note

Revision M

Contents

Log Formats

There are five log types that PAN-OS can generate: traffic, threat, host information profile (HIP) match, config, and system. All are formatted as comma-separated value (CSV) strings. Below are the field definitions for each log type. The fields flagged as FUTURE_USE do not currently have predictable, useful information in them.

TRAFFIC

FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Source IP, Destination IP, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Ingress Interface, Egress Interface, Log Forwarding Profile, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Bytes, Bytes Sent, Bytes Received, Packets, Start Time, Elapsed Time, Category, FUTURE_USE, Sequence Number, Action Flags, Source Location, Destination Location, FUTURE_USE, Packets Sent, Packets Received.

Descriptions

Note: The Field column shows the full name of the field and the field name as it appears in PAN-OS.

Field	Meaning
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Specifies type of log; Values are traffic, threat, config, system and hip-match.
Subtype (subtype)	Subtype of traffic log; Values are start, end, drop, and deny. See Subtype Field table for meaning of each value.
Generated Time (time_generated)	Time the log was generated on the data plane
Source IP (src)	Original session source IP address
Destination IP (dst)	Original session destination IP address
NAT Source IP (natsrc)	If Source NAT performed, the post-NAT Source IP address
NAT Destination IP (natdst)	If Destination NAT performed, the post-NAT Destination IP address
Rule Name (rule)	Name of the rule that the session matched
Source User (srcuser)	User name of the user that initiated the session

Field	Meaning
Destination User (dstuser)	User name of the user to which the session was destined
Application (app)	Application associated with the session
Virtual System (vsys)	Virtual System associated with the session
Source Zone (from)	Zone the session was sourced from
Destination Zone (to)	Zone the session was destined to
Ingress Interface (inbound_if)	Interface that the session was sourced form
Egress Interface (outbound_if)	Interface that the session was destined to
Log Forwarding Profile (logset)	Log Forwarding Profile that was applied to the session
Session ID (sessionid)	An internal numerical identifier applied to each session
Repeat Count (repeatcnt)	Number of sessions with same Source IP, Destination IP, Application, and Subtype seen within 5 seconds; Used for ICMP only.
Source Port (sport)	Source port utilized by the session
Destination Port (dport)	Destination port utilized by the session
NAT Source Port (natsport)	Post-NAT source port
NAT Destination Port (natdport)	Post-NAT destination port
Flags (flags)	32 bit field that provides details on session; See Flags Field table for meaning of each value. This field can be decoded by AND-ing the values with the logged value.
Protocol (proto)	IP protocol associated with the session
Action (action)	Action taken for the session; Values are allow or deny. See Action Field table.
Bytes (bytes)	Number of total bytes (transmit and receive) for the session
Bytes Sent (bytes_sent)	Number of bytes in the client-to-server direction of the session. Available from PAN-OS 4.1.0 on all models except the PA-4000 series.

Field	Meaning
Bytes Received (bytes_received)	Number of bytes in the server-to-client direction of the session. Available from PAN-OS 4.1.0 on all models except the PA-4000 series.
Packets (packets)	Number of total packets (transmit and receive) for the session
Start Time (start)	Time of session start
Elapsed Time (elapsed)	Elapsed time of the session
Category (category)	URL category associated with the session (if applicable)
Sequence Number (seqno)	A 64bit log entry identifier incremented sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama. Available from PAN-OS 4.0.0.
Source Location (srcloc)	Source country or Internal region for private addresses. Maximum length is 32 bytes. Available in PAN-OS 4.0.0 and above.
Destination Location (dstloc)	Destination country or Internal region for private addresses. Maximum length is 32 bytes. Available in PAN-OS 4.0.0 and above.
Packets Sent (pkts_sent)	Number of client-to-server packets for the session. Available from PAN-OS 4.1.0 on all models except the PA-4000 series.
Packets Received (pkts_received)	Number of server-to-client packets for the session. Available from PAN-OS 4.1.0 on all models except the PA-4000 series.

Subtype Field

Value	Meaning
Start	session started
End	session ended
Drop	session dropped before application is identified and there is no rule to allow session
Deny	session denied after application is identified and there is a rule to block or no rule to allow the session

Action Field

Value	Meaning
Allow	session was allowed by policy
Deny	session was denied by policy

Flags Field

Value	Meaning
0x80000000	session has a packet capture (PCAP)
0x02000000	IPv6 session
0x01000000	SSL session was decrypted (SSL Proxy)
0x00800000	session was denied via URL filtering
0x00400000	session has a NAT translation performed (NAT)
0x00200000	user information for the session was captured via the captive portal (Captive Portal)
0x00080000	X-Forwarded-For value from a proxy is in the source user field
0x00040000	log corresponds to a transaction within a http proxy session (Proxy Transaction)
0x00008000	session is a container page access (Container Page)
0x00002000	session has a temporary match on a rule for implicit application dependency handling. Available in PAN-OS 5.0.0 and above.
0x00000800	symmetric return was used to forward traffic for this session. Available in PAN-OS 5.0.0 and above.

THREAT

FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Source IP, Destination IP, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Ingress Interface, Egress Interface, Log Forwarding Profile, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Miscellaneous, Threat ID, Category, Severity, Direction, Sequence Number, Action Flags, Source Location, Destination Location, FUTURE_USE, Content Type

Descriptions

Note: The Field column shows the full name of the field and the field name as it appears in PAN-OS.

Field	Meaning
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Specifies type of log; Values are traffic, threat, config, system and hip-match.
Subtype (subtype)	Subtype of threat log; Values are URL, virus, spyware, vulnerability, file, scan, flood, data, and wildfire.
Generated Time (time_generated)	Time the log was generated on the data plane
Source IP (src)	Original session source IP address
Destination IP (dst)	Original session destination IP address
NAT Source IP (natsrc)	If Source NAT performed, the post-NAT Source IP address
NAT Destination IP (natdst)	If Destination NAT performed, the post-NAT Destination IP address
Rule Name (rule)	Name of the rule that the session matched
Source User (srcuser)	User name of the user that initiated the session
Destination User (dstuser)	User name of the user to which the session was destined
Application (app)	Application associated with the session

Field	Meaning
Virtual System (vsys)	Virtual System associated with the session
Source Zone (from)	Zone the session was sourced from
Destination Zone (to)	Zone the session was destined to
Ingress Interface (inbound_if)	Interface that the session was sourced form
Egress Interface (outbound_if)	Interface that the session was destined to
Log Forwarding Profile (logset)	Log Forwarding Profile that was applied to the session
Session ID (sessionid)	An internal numerical identifier applied to each session
Repeat Count (repeatcnt)	Number of logs with same Source IP, Destination IP, and Threat ID seen within 5 seconds; Applies to all Subtypes except URL.
Source Port (sport)	Source port utilized by the session
Destination Port (dport)	Destination port utilized by the session
NAT Source Port (natsport)	Post-NAT source port
NAT Destination Port (natdport)	Post-NAT destination port
Flags (flags)	32 bit field that provides details on the session; See Flags Field table for meaning of each value.
Protocol (proto)	IP protocol associated with the session
Action (action)	Action taken for the session; Values are alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url. See Action Field table below for meaning of each value.
Miscellaneous (misc)	The actual URI when the subtype is URL; File name or file type when the subtype is file; and File name when the subtype is virus; File name when the subtype is wildfire. Length is 63 characters in PAN-OS versions before 4.0. From version 4.0, it is variable length with a maximum of 1023 characters.

Field	Meaning
Threat ID (threatid)	Palo Alto Networks identifier for the threat. It is a description string followed by a numerical identifier in parenthesis for some Subtypes. The numerical identifier is a 64 bit number from PAN-OS 5.0 onwards.
Category (category)	For URL Subtype, it is the URL Category; For Wildfile subtype, it is the verdict on the file and is either 'malicious' or 'benign'; For other subtypes the value is 'any'
Severity (severity)	Severity associated with the threat; Values are informational, low, medium, high, critical
Direction (direction)	Indicates the direction of the attack, 'client-to-server' or 'server-to-client'
Sequence Number (seqno)	A 64bit log entry identifier incremented sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama. Available in PAN-OS 4.0.0 and above.
Source Location (srcloc)	Source country or Internal region for private addresses. Maximum length is 32 bytes. Available in PAN-OS 4.0.0 and above.
Destination Location (dstloc)	Destination country or Internal region for private addresses. Maximum length is 32 bytes. Available in PAN-OS 4.0.0 and above.
Content Type (contenttype)	Content type of the HTTP response data. Maximum length 32 bytes. Applicable only when Subtype is URL. Available in PAN-OS 4.0.0 and above.

Subtype Field

Value	Meaning
url	URL filtering log
virus	virus detection
spyware	spyware detection
vulnerability	vulnerability exploit detection
file	file type log
scan	scan detected via Zone Protection Profile
flood	flood detected via Zone Protection Profile
data	data pattern detected from Data Filtering Profile
wildfire	wildfire log. Available in PAN-OS 5.0.0 and above.

Action Field

Value	Meaning
alert	threat or URL detected but not blocked
allow	flood detection alert
deny	flood detection mechanism activated and deny traffic based on configuration
drop	threat detected and associated session was dropped
drop-all-packets	threat detected and session remains, but drops all packets
reset-client	threat detected and a TCP RST is sent to the client
reset-server	threat detected and a TCP RST is sent to the server
reset-both	threat detected and a TCP RST is sent to both the client and the server
block-url	a URL request was blocked because it matched a URL category that was set to be blocked

ThreatID Field

Value	Meaning
8000 – 8099	scan detection
8500 – 8599	flood detection
9999	URL filtering log
10000 – 19999	sypware phone home detection
20000 – 29999	spyware download detection
30000 – 44999	vulnerability exploit detection
52000 – 52999	filetype detection
60000 – 69999	data filtering detection
100000 – 2999999	virus detection
3000000 – 3999999	wildfire signature feed
4000000-4999999	DNS Botnet signatures. Available in PAN-OS 5.0.0 and above.

Direction Field

Value	Meaning

Value	Meaning
0	direction of the threat is client to server
1	direction of the threat is server to client

Starting with PAN-OS 3.1, the direction field will contain either “client-to-server” or “server-to-client” to directly indicate the direction of the attack.

HIP MATCH

FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, FUTURE_USE, Source User, Virtual System, Machine name, Source Address, HIP, Repeat Count, HIP Type, FUTURE_USE, FUTURE_USE, Sequence Number, Action Flags

HIP Match logs are generated in PAN-OS 4.0.0 and above.

Descriptions

Note: The Field column shows the full name of the field and the field name as it appears in PAN-OS.

Field	Meaning
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Specifies type of log; Values are traffic, threat, config, system and hip-match.
Subtype (subtype)	Subtype of hip-match log; Unused.
Source User (srcuser)	User name of the Source user
Virtual System (vsys)	Virtual System associated with the HIP Match log
Machine Name (machinename)	Name of the Users machine
Source Address (src)	IP address of the source user
HIP (matchname)	Name of the HIP Object or Profile.
Repeat Count (repeatcnt)	Number of times the HIP profile matched
HIP Type (matchtype)	Specifies whether the HIP field represents a HIP Object or a HIP Profile.
Sequence Number (seqno)	A 64bit log entry identifier incremented sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama. Available in PAN-OS 4.0.0 and above.

HIP Type Field

Value	Meaning
object	The HIP field is a HIP Object
profile	The HIP field in a HIP Profile

CONFIG

FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, FUTURE_USE, Host, Virtual System, Command, Admin, Client, Result, Configuration Path, Sequence Number, Action Flags

Descriptions

Note: The Field column shows the full name of the field and the field name as it appears in PAN-OS.

Field	Meaning
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Specifies type of log; Values are traffic, threat, config, system and hip-match.
Subtype (subtype)	Subtype of the Config log; Unused.
Host (host)	Host name or IP address of the client machine
Virtual System (vsys)	Virtual System associated with the configuration log.
Command (cmd)	Command performed by the Admin; Values are add, clone, commit, delete, edit, move, rename, set, validate.
Admin (admin)	User name of the Administrator performing the configuration
Client (client)	Client used by the Admin; Values are Web and CLI.
Result (result)	Result of the configuration action. Values are Submitted, Succeeded, Failed, and Unauthorized.
Configuration Path (path)	The path of the configuration command issued. Up to 512 bytes in length.
Sequence Number (seqno)	A 64bit log entry identifier incremented sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama. Available in PAN-OS 4.0.0 and above.

SYSTEM

FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, FUTURE_USE, Virtual System, Event ID, Object, FUTURE_USE, FUTURE_USE, Module, Severity, Description, Sequence Number, Action Flags

Descriptions

Note: The Field column shows the full name of the field and the field name as it appears in PAN-OS.

Field	Meaning
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Specifies type of log; Values are traffic, threat, config, system and hip-match.
Subtype (subtype)	Subtype of the system log. Refers to the system daemon generating the log; Values are crypto, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn.
Virtual System (vsys)	Virtual System associated with the system event
Event ID (eventid)	String showing the name of the event
Object (object)	Name of the object associated with the system log.
Module (module)	This field is valid only when the value of the Subtype field is general; It provides additional information about the sub-system generating the log. Values are general, management, auth, ha, upgrade, chassis.
Severity (severity)	Severity associated with the event; Values are informational, low, medium, high, critical
Description (opaque)	Detailed description of the event. Length is up to 512 bytes.
Sequence Number (seqno)	A 64bit log entry identifier incremented sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama. Available in PAN-OS 4.0.0 and above.

Sending the Device Hostname in the Syslog Messages

By default, the hostname field in the header of the Syslog messages is not populated and will not appear in the Syslog messages. To include the hostname, navigate to **Device > Setup > Management > Logging and Reporting Settings** and select the **Send Hostname in Syslog** check box. In PAN-OS 5.0, the device's FQDN is used when both hostname and domain are configured in the **Management > General Settings** section or just the hostname when the domain is not configured. In PAN-OS 4.1 and earlier, the device's management IP address appears in the hostname field of the Syslog header.

Syslog Facility

The syslog facility can be configured within the system when setting the syslog destination. Multiple syslog settings can be configured and referenced by the various log forwarding function if desired. The available facilities are: user, local0, local1, local2, local3, local4, local5, local6, and local7.

Syslog Severity

The syslog severity is set based on the log type and contents.

Log Type/Severity	Syslog Severity
TRAFFIC	INFO
CONFIG	INFO
THREAT/SYSTEM – Informational	INFO
THREAT/SYSTEM – Low	NOTICE
THREAT/SYSTEM – Medium	WARNING
THREAT/SYSTEM – High	ERROR
THREAT/SYSTEM – Critical	CRITICAL

Custom Log/Event Format

Palo Alto Networks provides an interface for completely customizing the log message format that can be sent from Palo Alto Networks Next Generation Firewalls. Custom message formats can be configured under Device > Server Profiles > Syslog > Syslog Server Profile > Custom Log Format. Custom Key:Value attribute pairs can be added. Log customization can facilitate and trivialize the integration with external log parsing systems. This feature can be leveraged to achieve ArcSight Common Event Format (CEF) compliant log formatting, see https://live.paloaltonetworks.com/docs/DOC-2834 for PAN-OS 4.0 and https://live.paloaltonetworks.com/docs/DOC-2835 for PAN-OS-4.1 for more information.

Custom log format is available in PAN-OS 4.0.0 and above.

Escape Sequences

Pre-PAN-OS 4.0.0: The Miscellaneous field in Threat Log is always enclosed in double quotes. This field contains either a URL or a file name. The double quotes avoid confusing any commas that may appear in this field for the comma used as a delimiter in CSV.

PAN-OS 4.0.0: Any field that contains a comma will be enclosed in double quotes. Further, a double-quote, comma, or backslash appearing in any of the fields, will be escaped by preceding it with a backslash.

PAN-OS 4.0.4 and after: Any field that contains a comma or a double-quote will be enclosed in double quotes. Furthermore, a double-quote appearing inside a field will be escaped by preceding it with another double-quote. The Misc field in threat log will always be enclosed in double-quotes to maintain backward compatibility.

Revision History

Date	Revision	Comment
February 15, 2013	M	The reference to the CEF doc - https://live.paloaltonetworks.com/docs/DOC-2775 no longer worked because they were replaced by the following two docs- https://live.paloaltonetworks.com/docs/DOC-2834 and https://live.paloaltonetworks.com/docs/DOC-2835. Fixed the links in the doc, not changing the rev since the content in this doc is not changing.
December 14, 2012	M	Updated the section "Sending Device Hostname in Syslog Messages" with more specific steps and info on the differences between PAN-OS 4.1 and 5.0.
November 5, 2012	L	Revision history log started. Revision L also reflects changes made for the PAN-OS 5.0 release. Items modified marked with PAN-OS 5.0 in the description.