PAN-OS Syslog Integration

Tech Note

Log Formats

There are four log types that PAN-OS can generate: traffic, threat, 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, FUTURE_USE, 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, FUTURE_USE, FUTURE_USE, Packets, Start Time, Elapsed Time, Category, FUTURE_USE

Action Field

Value	Meaning
allow	session was allowed by policy
deny	session was denied by application policy
drop	session denied due to no allow rule or port-based deny rule

THREAT

FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, FUTURE_USE, 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

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

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 – 4000000	virus detection

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

Value	Meaning
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

Direction Field

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

CONFIG

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

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

General Flag Field

The traffic and threat log types have a *flag* field that contains unique information about that particular event. This field can be decoded by ANDing the following values with the logged value:

Value	Meaning
0x8000	extra data captured (usually PCAP of threat or app)
0x0200	IPv6 session
0x0100	SSL session was decrypted
0x0080	session was denied via url filtering
0x0040	session was NAT'ed
0x0020	user information for the session was captured via the captive portal
0x0008	X-Forwarded-For value from a proxy is in the source user field

Value	Meaning
0x0004	log was for a proxy transaction within a session

Sending the Device Hostname in the Syslog Messages

There are two options for the syslog format when sent from the device. By default, the messages do not include the device hostname in the header. To include this, make sure it is configured on the *Setup* screen on the *Device* tab in the web interface.

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