Palo Alto

Integration of Palo Alto's System, Configuration, Traffic and Threat logs into XpoLog.

Prerequisites:

A. Open the relevant ports (TCP\UDP) on the XpoLog machine.
B. Create a syslog listener on the listeners tab in XpoLog that will listen and collect the log from the Palo Alto machine.

Palo Alto Configurations:

1. Open the relevant port on the Palo Alto Machine:
I. Login to the GUI of the Palo Alto machine, and then enter to Objects->Services->Add.

II. During the creation of the service, you have to determine the name for the service, the format\protocol in which the service will send the data (ie TCP or UDP), source port and the destination port (which you have already configured in XpoLog's listener).

2. Create new syslog device which will send the system and configuration logs into XpoLog:

I. From the GUI of the Palo Alto, enter to Devices->Server Profiles->Syslog->Add.
II. During the creation of the device, you have to determine the name for the syslog server profile, and also to configure the values for the following fields.

- **Name**—Unique name for the server profile.
- **Syslog Server**—IP address or fully qualified domain name (FQDN) of the syslog server (in case that DNS server was configured)
- **Transport**—Select **TCP**, **UDP**, or **SSL** (TLS) as the protocol for communicating with the syslog server. For **SSL**, the firewall supports only TLSv1.2.
- **Port**—The port number on which to send syslog messages (default is UDP on port 514); you must use the same port number on the firewall and the syslog server.
- **Format**—Select the syslog message format to use: **BSD** (the default) or **IETF**. Traditionally, **BSD** format is over UDP and **IETF** format is over TCP or SSL/TLS.
- **Facility**—Select a syslog standard value (default is **LOG_USER**) to calculate the priority (PRI) field in your syslog server implementation. Select the value that maps to how you use the PRI field to manage your syslog messages.

3. Configure the 'Log Settings' for your System and Configuration logs:

I. From the GUI of your Palo Alto, enter to Devices->Log Settings, and add new log setting under the relevant tab (system\configuration\traffic'threat).

II. Please grant a name for the log setting and under the 'syslog\ tab, choose the syslog devices that you have already configured in section 2 and add them.

4. Create a 'Log Forwarder' for your logs.

I. From the GUI of the Palo Alto, enter to Objects - > Log Forwarding - > Add.

II. Name the log forwarder. Then from the syslog tab, choose the devices that you have already configured in section 2 and add them.

5. Commit all these configuration changes - from the top left part of the GUI, press on the 'commit' button in order that the configuration changes will take effect.

XpoLog Configurations (edit the syslog logs that were generated for the Palo Alto machine):

System Log -

I. For the syslog of the system log, set the logTypes of the syslog to 'syslog,paloalto,system,audit'.

II. Apply the following pattern on the log (default pattern)

XPLG:[{timestamp:Timestamp,MM/dd/yyyy HH:mm:ss.SSS}] [{text:Facility}] [{priority:Level,DEBUG;INFO;WARN;ERROR;FATAL}] [{text:Source Device}] {block,start,emptiness=true}{text:Application Name}[{text:Process Id}]: {block,end,emptiness=true}{text:Device,ftype=device} {text:Domain,ftype=domain},{date:Receive Time,yyyy/MM/dd HH:mm:ss},{text:Serial#,ftype=serial},{text:Type,ftype=eventSource},{text:Subtype,ftype=subtype},{text:Config Version,ftype=configversion},{date:Time Generated,yyyy/MM/dd HH:mm:ss},{block,start,emptiness=true}{text:Virtual System,ftype=virtualsystem}{block,end,emptiness=true},{text:Event ID,ftype=eventName},{block,start,emptiness=true}{text:Object,ftype=object}{block,end,emptiness=true},{text:fmt,ftype=fmt},{text:ID,ftype=id},{text:Module,ftype=module},{priority:Severity,ftype=status;High;Medium;Low;Informational},"{text:Description,ftype=message;,}"{regexp:Username,ftype=username;refName=Description,(Failed password for |User |for user \u0027|Password changed for user |failed authentication for user \u0027 |authenticated for user \u0027)[XPLG_PARAM([^\u0027\s]+)].*}{regexp:SourceIP,ftype=sourceip;refName=Description,(From: |from)[XPLG_PARAM([^\s]\d+\.\d+\.\d+.\d+)].*}{regexp:logout,ftype=logout;refName=Description,logged out},{text:Sequence Number,ftype=sequencenumber},{text:Action Flags,ftype=actionflags},{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=dghierlevel3},{text:dg_hier_level_4,ftype=dghierlevel4},{text:Virtual System Name,ftype=vsysname},{text:Device Name,ftype=devicename}{eoe}

Configuration Log -

I. For the syslog of the configuration log, set the logTypes of this log to 'syslog,paloalto,configuration.audit'.

II. Apply the following pattern on the log:

XPLG:[{timestamp:Timestamp,MM/dd/yyyy HH:mm:ss.SSS}] [{text:Facility,ftype=facility}] [{priority:Level,ftype=level,DEBUG;INFO;WARN;ERROR;FATAL}] [{text:Source Device,ftype=source-device}] {block,start,emptiness=true}{text:Application Name,ftype=app-name}[{text:Process Id,ftype=pid}]: {block,end,emptiness=true}{text:Device} {text:Domain,ftype=domain;,},{date:Receive Time,yyyy/MM/dd HH:mm:ss},{text:Serial#,ftype=serial},{text:Type,ftype=eventSource},{text:Subtype,ftype=subtype},{text:Config Version,ftype=configversion},{date:Time Generated,yyyy/MM/dd HH:mm:ss},{geoip:Host,ftype=sourceip;type=country:region:city;,},{text:Virtual System,ftype=virtualsystem},{choice:CMD,ftype=command,add,clone.commit,delete,edit,move,rename,set},{text:Admin,ftype=username},{choice:Client,ftype=client,Web,CLI},{choice:Result,ftype=status,Submitted,Succeeded,Failed,Unauthorized},{text:Configuration-path,ftype=path}{regexp:Event Name,ftype=eventName;refName=configuration-path,config mgt-config users|config shared local-user-database user |config shared local-user-database user-group|config shared admin-role|config shared authentication-profile|config mgt-config password-profile}{regexp:Audited_Object,ftype=auditedobject;refName=configuration-path,(config mgt-config users|config shared local-user-database user |config shared local-user-database user-group |config shared admin-role |config shared authentication-profile |config mgt-config password-profile)[XPLG_PARAM([^,]+)]},{text:Sequence Number,ftype=sequencenumber},{text:Action Flags,ftype=actionflags},{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=dghierlevel3},{text:dg_hier_level_4,ftype=dghierlevel4},{text:Virtual System Name,ftype=vsysname},{text:Device Name,ftype=devicename}{eoe}

Threat Log -

I. For the syslog of the threat log, set the logTypes of this log to 'syslog,paloalto,threat'.

II. Apply the following pattern on the log:

XPLG:[{timestamp:Timestamp,MM/dd/yyyy HH:mm:ss.SSS}] [{text:Facility,ftype=facility}] [{priority:Level,ftype=level,DEBUG;INFO;WARN;ERROR;FATAL}] [{text:Source Device,ftype=source-device}] {block,start,emptiness=true}{text:Application Name,ftype=app-name}[{text:Process Id,ftype=pid}]: {block,end,emptiness=true}{text:Device,ftype=device} {text:Domain,ftype=domain},{date:Receive Time,yyyy/MM/dd HH:mm:ss},{text:Serial#,ftype=serial},{text:Type,ftype=eventSource},{text:Subtype,ftype=subtype},{text:Config Version,ftype=configversion},{date:CEF-Formatted-Time-Generated,yyyy/MM/dd HH:mm:ss},{ip:SourceIP,ftype=sourceip},{ip:Destination IP,ftype=targetip},{ip:Nat SourceIP,ftype=natsourceip},{ip:Nat Destination IP,ftype=nattargetip},{text:Rule Name,ftype=rulename},{text:Source User,ftype=username},{text:Destination User,ftype=dstusername},{text:Application,ftype=application},{block,start,emptiness=true}{text:Virtual System,ftype=virtualsystem}{block,end,emptiness=true},{text:Source Zone,ftype=srczone},{text:Destination Zone,ftype=dstzone},{text:Inbound Interface,ftype=srcintf},{text:Outbound Interface,ftype=dstintf},{text:Log Action,ftype=logaction},{date:Time Logged,yyyy/MM/dd HH:mm:ss},{text:SessionID,ftype=sessionid},{text:Repeat Count,ftype=repeatcount},{number:Source Port,ftype=sourceport},{number:Destination Port,ftype=dstport},{number:Nat Source Port,ftype=natsrcport},{number:Nat Destination Port,ftype=natdstport},{text:Flags,ftype=flags},{text:IP Protocol,ftype=ipprotocol},{text:Action,ftype=eventName},{url:URL,paramsFtype=querystring;ftype=requrl;paramsName=Query;,},{text:Threat/Content Name,ftype=threatcontentname},{text:Category,ftype=category},{priority:Severity,ftype=status;Critical;High;Medium;Low;Informational},{text:Direction,ftype=direction},{text:Sequence Number,ftype=sequencenumber},{text:Action Flags,ftype=actionflags},{text:Source Country,ftype=srccountry},{text:Destination Country,ftype=dstcountry},{text:cpadding,ftype=cpadding},{text:Content Type,ftype=contenttype},{text:PCAP ID,ftype=pcapap},{text:File Digest,ftype=filedigest},{text:Cloud,ftype=cloud},{text:URL Index,ftype=urlindex},{text:User Agent,ftype=useragent},{text:File Type,ftype=filetype},{text:X-Forwarded-For,ftype=forwardedforip},{text:RefererQuery,ftype=refererquery;,}{regexp:Referer,ftype=referer;refName=RefererQuery,^([w-]+://[^?]+|/[^?]+)},{text:Sender,ftype=sender},{text:Subject,ftype=subject},{text:Recipient,ftype=recipient},{text:Report ID,ftype=reportid},{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=dghierlevel3},{text:dg_hier_level_4,ftype=dghierlevel4},{text:Virtual System Name,ftype=vsysname},{text:Device Name,ftype=devicename},{url:URL,paramsFtype=querystring;ftype=requrl;paramsName=Query;,},{text:Source VM UUID,ftype=sourcevmuuid},{text:Destination VM UUID,ftype=targetvmuuid},{choice:Method,ftype=reqmethod;,Connect;Delete;Get;Head;Options;Post;Put},{text:Tunnel ID/IMSI,ftype=tunnelid},{text:Monitor Tag/IMEI,ftype=monitortag},{text:Parent Session ID,ftype=parentsessionid},{text:Parent Start Time,ftype=parentstarttime},{text:Tunnel Type,ftype=tunneltype},{text:Threat Category,ftype=threatcategory},{text:Content Version,ftype=contentversion},{text:SIG_Flags,ftype=sigflafs},{text:SCTP Assoication ID,ftype=sctpassociationid},{text:Payload Protocol ID,ftype=payloadprotocolid},{text:HTTP Headers,ftype=httpheaders}{eoe}

Traffic Log -

I. For the syslog of the traggic log, set the logTypes of this log to 'syslog,paloalto,traffic'.

II. Apply the following pattern on the log:

XPLG:[{timestamp:Timestamp,MM/dd/yyyy HH:mm:ss.SSS}] [{text:Facility,ftype=facility}] [{priority:Level,ftype=level,DEBUG;INFO;WARN;ERROR;FATAL}] [{text:Source Device,ftype=source-device}] {block,start,emptiness=true}{text:Application Name,ftype=app-name}[{text:Process Id,ftype=pid}]: {block,end,emptiness=true}{text:Device,ftype=device} {text:Domain,ftype=domain},{date:Receive Time,yyyy/MM/dd HH:mm:ss},{text:Serial#,ftype=serial},{text:Type,ftype=eventSource},{text:Subtype,ftype=subtype},{text:Config Version,ftype=configversion},{date:CEF-Formatted-Time-Generated,yyyy/MM/dd HH:mm:ss},{ip:SourceIP,ftype=sourceip},{ip:Destination IP,ftype=targetip},{ip:Nat SourceIP,ftype=natsourceip},{ip:Nat Destination IP,ftype=nattargetip},{text:Rule Name,ftype=rulename},{text:Source User,ftype=username},{text:Destination User,ftype=dstusername},{text:Application,ftype=application},{block,start,emptiness=true}{text:Virtual System,ftype=virtualsystem}{block,end,emptiness=true},{text:Source Zone,ftype=srczone},{text:Destination Zone,ftype=dstzone},{text:Inbound Interface,ftype=srcintf},{text:Outbound Interface,ftype=dstintf},{text:Log Action,ftype=logaction},{date:Time Logged,yyyy/MM/dd HH:mm:ss},{text:SessionID,ftype=sessionid},{text:Repeat Count,ftype=repeatcount},{number:Source Port,ftype=sourceport},{number:Destination Port,ftype=dstport},{number:Nat Source Port,ftype=natsourceport},{number:Nat Destination Port,ftype=natdstport},{text:Flags,ftype=flags},{text:IP Protocol,ftype=ipprotocol},{text:Action,ftype=eventName},{number:Bytes,ftype=bytes},{text:Bytes Sent,ftype=bytesent},{text:Bytes Received,ftype=bytesreceived},{number:Packets,ftype=packets},{text:Start,ftype=start},{number:Elapsed Time(sec),ftype=elapsedtime},{text:Category,ftype=category},{text:tpadding,ftype=tpadding},{text:Sequence Number,ftype=sequencenumber},{text:Action Flags,ftype=actionflags},{text:Source Country,ftype=srccountry},{text:Destination Country,ftype=dstcountry},{text:cpadding,ftype=cpadding},{number:Sent Packets,ftype=sentpkt},{number:Received Packets,ftype=rcvdpkt},{text:Session End Reason,ftype=sessionendreason},{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=dghierlevel3},{text:dg_hier_level_4,ftype=dghierlevel4},{text:Virtual System Name,ftype=vsysname},{text:Device Name,ftype=devicename},{text:Action Source,ftype=actionsource},{text:Source VM UUID,ftype=sourcevmuuid},{text:Destination VM UUID,ftype=targetvmuuid},{text:Tunnel ID,ftype=tunnelid},{text:Monitor Tag,ftype=monitortag},{text:Parent Session ID,ftype=parentsessionid},{text:Parent Start Time,ftype=parentstarttime},{text:Tunnel Type,ftype=tunneltype},{text:SCTP Assoication ID,ftype=sctpassociationid},{number:SCTP Chunks,ftype=chunks},{number:SCTP Chunks Sent,ftype=chunkssent},{number:SCTP Chunks Received,ftype=chunksreceived}{eoe}

For more information about the system log fields, see below the format Conversion Table:

Field Name	Description	XpoLog Pattern
$domain	The domain which the messages were sent from.	{text:Domain,ftype=domain}
$dev	The device which the messages were sent from.	{text:Device,ftype=device}
$receive_time	Time the log was received at the management plane	{date:Receive Time,yyyy/MM/dd HH:mm:ss}
$serial	Serial number of the firewall that generated the log	{text:Serial#,ftype=serial}
$type	Type of log; values are traffic, threat, config, system and hip-match	{text:Type,ftype=eventSource}

$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.	{text:Subtype,ftype=subtype}
$configversion	Config Version associated with the system log.	{text:Config Version,ftype=configversion}
$time_generated	Time the log was generated on the dataplane.	{date:Time Generated,yyyy/MM/dd HH:mm:ss}
$vsys	Virtual System associated with the system log.	{block,start,emptiness=true}{text:Virtual System,ftype=virtualsystem}{block,end,emptiness=true}
$eventid	String showing the name of the event.	{text:Event ID,ftype=eventName}
$object	Name of the object associated with the system event	{block,start,emptiness=true}{text:Object,ftype=object}{block,end,emptiness=true}
$fmt		{text:fmt,ftype=fmt}
$id		{text:ID,ftype=id}
$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.	{text:Module,ftype=module}

$severity	Severity associated with the event; values are informational, low, medium, high, critical	{priority:Severity,ftype=status;High;Medium;Low;Informational}
$opaque	Detailed description of the event, up to a maximum of 512 bytes	"{text:Description,ftype=message;,}"{regexp:Username,ftype=username;refName=Description,(Failed passwor user |failed authentication for user \u0027 |authenticated for user \u0027)[XPLG_PARAM([^\u0027\s]+)].*}{regexp:SourceIP,ftype=sourceip;refName=Description,(From: |from)[XPLG_PARAM([^\s]\d+\.\d+\.\d+.\d+)].*}{regexp:logout,ftype=logout;refName=Description,logged out}
$seqno	A 64-bit log entry identifier incremented sequentially; each log type has a unique number space.	{{text:Sequence Number,ftype=sequencenumber}
$actionflags	A bit field indicating if the log was forwarded to Panorama	{text:Action Flags,ftype=actionflags}
$dg_hier_level_1 $dg_hier_level_2 $dg_hier_level_3 $dg_hier_level_4	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.	{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=

$vsys_name	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.	{text:Virtual System Name,ftype=vsysname}
$device_name	The hostname of the firewall on which the session was logged.	{text:Device Name,ftype=devicename}
$cef-formatted-receive_time		{date:CEF-Formatted-Receive-Time,MMM dd yyyy HH:mm:ss z}
$cef-formatted-time_generated		{date:CEF-Formatted-Time-Generated,MMM dd yyyy HH:mm:ss z}
$cef-number-of-severity		{number:CEF-Number-Of-Severity,ftype=cefnumberofseverity}
$number-of-severity		{number:Number-Of-Severity,ftype=numberofseverity}
$sender_sw_version		{text:Sender_Sw_Version,ftype=senderswversion}
$vsys_id		{block,start,emptiness=true}{text:Virtual System ID,ftype=virtualsystemid}{block,end,emptiness=true}

For more information about the configuration log fields, see below the format Conversion Table:

Field Name	Description	XpoLog Pattern
$domain	The domain which the messages were sent from.	{text:Domain,ftype=domain}
$dev	The device which the messages were sent from.	{text:Device,ftype=device}
$receive_time	Time the log was received at the management plane	{date:Receive Time,yyyy/MM/dd HH:mm:ss}
$serial	Serial number of the firewall that generated the log	{text:Serial#,ftype=serial}
$type	Type of log; values are traffic, threat, config, system and hip-match	{text:Type,ftype=eventSource}

$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.	{text:Subtype,ftype=subtype}
$configversion	Config Version associated with the system log.	{text:Config Version,ftype=configversion}
$time_generated	Time the log was generated on the dataplane.	{date:Time Generated,yyyy/MM/dd HH:mm:ss}
$host	Hostname or IP address of the client machine	{geoip:Host,ftype=sourceip;type=country:region:city;,}
$vsys	Virtual System associated with the configuration log	{block,start,emptiness=true}{text:Virtual System,ftype=virtualsystem}{block,end,emptiness=true}
$cmd	Command performed by the Admin; values are add, clone, commit, delete, edit, move, rename, set.	{choice:CMD,ftype=command,add,clone.commit,delete,edit,move,rename,set}
$admin	Username of the Administrator performing the configuration	{text:Admin,ftype=username}
$client	Client used by the Administrator; values are Web and CLI	{choice:Client,ftype=client,Web,CLI}
$result	Result of the configuration action; values are Submitted, Succeeded, Failed, and Unauthorized	{choice:Result,ftype=status,Submitted,Succeeded,Failed,Unauthorized}

$path	The path of the configuration command issued; up to 512 bytes in length	{{text:Configuration-path,ftype=path}{regexp:Event Name,ftype=eventName;refName=configuration-path,config user |config shared local-user-database user-group|config shared admin-role|config shared authentication-profil password-profile}{regexp:Audited_Object,ftype=auditedobject;refName=configuration-path,(config mgt-config us shared local-user-database user-group |config shared admin-role |config shared authentication-profile |config m
$before-change-detail	This field is in custom logs only; it is not in the default format. It contains the full xpath before the configuration change.	{text:Before-Change-Detail,ftype=beforechangedetail}
$after-change-detail	This field is in custom logs only; it is not in the default format. It contains the full xpath after the configuration change.	{text:After-Change-Detail,ftype=afterchangedetail}
$seqno	A 64bit log entry identifier incremented sequentially; each log type has a unique number space.	{text:Sequence Number,ftype=sequencenumber}
$actionflags	A bit field indicating if the log was forwarded to Panorama.	{text:Action Flags,ftype=actionflags}

Device Group Hierarchy $dg_hier_level_1 $dg_hier_level_2 $dg_hier_level_3 $dg_hier_level_4	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.	{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=d
$vsys_name	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.	{text:Virtual System Name,ftype=vsysname}
$device_name	The hostname of the firewall on which the session was logged.	{text:Device Name,ftype=devicename}
$cef-formatted-receive_time		{date:CEF-Formatted-Receive-Time,MMM dd yyyy HH:mm:ss z}
$cef-formatted-time_generated		{date:CEF-Formatted-Time-Generated,MMM dd yyyy HH:mm:ss z}
$sender_sw_version		{text:Sender_Sw_Version,ftype=senderswversion}
$vsys_id		{block,start,emptiness=true}{text:Virtual System ID,ftype=virtualsystemid}{block,end,emptiness=true}

Field Name	Description	XpoLog Pattern

$domain	The domain which the messages were sent from.	{text:Domain,ftype=domain}
$dev	The device which the messages were sent from.	{text:Device,ftype=device}
$receive_time	Time the log was received at the management plane	{date:Receive Time,yyyy/MM/dd HH:mm:ss}
$serial	Serial number of the firewall that generated the log	{text:Serial#,ftype=serial}
$type	Type of log; values are traffic, threat, config, system and hip-match	{text:Type,ftype=eventSource}
$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.	{text:Subtype,ftype=subtype}
$configversion	Config Version associated with the system log.	{text:Config Version,ftype=configversion}
$time_generated	Time the log was generated on the dataplane.	{date:Time Generated,yyyy/MM/dd HH:mm:ss}
$vsys	Virtual System associated with the system log.	{block,start,emptiness=true}{text:Virtual System,ftype=virtualsystem}{block,end,emptiness=true}
$eventid	String showing the name of the event.	{text:Event ID,ftype=eventName}
$object	Name of the object associated with the system event	{block,start,emptiness=true}{text:Object,ftype=object}{block,end,emptiness=true}

$fmt		{text:fmt,ftype=fmt}
$id		{text:ID,ftype=id}
$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.	{text:Module,ftype=module}
$severity	Severity associated with the event; values are informational, low, medium, high, critical	{priority:Severity,ftype=status;High;Medium;Low;Informational}
$opaque	Detailed description of the event, up to a maximum of 512 bytes	"{text:Description,ftype=message;,}"{regexp:Username,ftype=username;refName=Description,(Failed passwor user |failed authentication for user \u0027 |authenticated for user \u0027)[XPLG_PARAM([^\u0027\s]+)].*}{regexp:SourceIP,ftype=sourceip;refName=Description,(From: |from)[XPLG_PARAM([^\s]\d+\.\d+\.\d+.\d+)].*}{regexp:logout,ftype=logout;refName=Description,logged out}
$seqno	A 64-bit log entry identifier incremented sequentially; each log type has a unique number space.	{{text:Sequence Number,ftype=sequencenumber}
$actionflags	A bit field indicating if the log was forwarded to Panorama	{text:Action Flags,ftype=actionflags}

$dg_hier_level_1 $dg_hier_level_2 $dg_hier_level_3 $dg_hier_level_4	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.	{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=d
$vsys_name	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.	{text:Virtual System Name,ftype=vsysname}
$device_name	The hostname of the firewall on which the session was logged.	{text:Device Name,ftype=devicename}
$cef-formatted-receive_time		{date:CEF-Formatted-Receive-Time,MMM dd yyyy HH:mm:ss z}
$cef-formatted-time_generated		{date:CEF-Formatted-Time-Generated,MMM dd yyyy HH:mm:ss z}
$cef-number-of-severity		{number:CEF-Number-Of-Severity,ftype=cefnumberofseverity}
$number-of-severity		{number:Number-Of-Severity,ftype=numberofseverity}
$sender_sw_version		{text:Sender_Sw_Version,ftype=senderswversion}
$vsys_id		{block,start,emptiness=true}{text:Virtual System ID,ftype=virtualsystemid}{block,end,emptiness=true}

For more information about the threat log fields, see below the format Conversion Table:

Field Name	Description	XpoLog Pattern
$domain	The domain which the messages were sent from.	{text:Domain,ftype=domain}
$dev	The device which the messages were sent from.	{text:Device,ftype=device}
$receive_time	Time the log was received at the management plane	{date:Receive Time,yyyy/MM/dd HH:mm:ss}
$serial	Serial number of the firewall that generated the log	{text:Serial#,ftype=serial}
$type	Type of log; values are traffic, threat, config, system and hip-match	{text:Type,ftype=eventSource}
$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.	{text:Subtype,ftype=subtype}
$configversion	Config Version associated with the system log.	{text:Config Version,ftype=configversion}
$time_generated	Time the log was generated on the dataplane.	{date:Time Generated,yyyy/MM/dd HH:mm:ss}
$src	Original session source IP address	{ip:SourceIP,ftype=sourceip}
$dst	Original session destination IP address.	{ip:DetinationIP,ftype=targetip}
$natsrc	If source NAT performed, the post-NAT source IP address.	{ip:Nat SourceIP,ftype=natsourceip}
$natdst	If destination NAT performed, the post-NAT destination IP address.	{ip:Nat DestinationIP,ftype=natdestinationip}
$rule	Name of the rule that the session matched.	{text:Rule Name,ftype=rulename}
$srcuser	Username of the user who initiated the session.	{text:Source User,ftype=username}
$dstuser	Username of the user to which the session was destined.	{text:Destination User,ftype=dstusername}
$app	Application associated with the session.	{text:Application,ftype=application}
$vsys	Virtual System associated with the session.	{block,start,emptiness=true}{text:Virtual System,ftype=virtualsystem}{block,end,emptiness=true}
$srczone	Zone the session was sourced from.	{text:Source Zone,ftype=srczone}

$dstzone	Zone the session was destined to.	{text:Destination Zone,ftype=dstzone}
$inbound_if	Interface that the session was sourced from.	{text:Inbound Interface,ftype=srcintf}
$outbound_if	Interface that the session was destined to.	{text:Outbound Interface,ftype=dstntf}
$logset	Log Forwarding Profile that was applied to the session.	{text:Log Action,ftype=logaction}
$time_logged		{date:Time Logged,yyyy/MM/dd HH:mm:ss}
$sessionid	An internal numerical identifier applied to each session.	{text:Session ID,ftype=sessionid}
$repeatcnt	Number of sessions with same Source IP, Destination IP, Application, and Content/Threat Type seen within 5 seconds.	{text:Repeat Count,ftype=repeatcount}
$sport	Source port utilized by the session.	{text:Source Port,ftype=srcport}
$dport	Destination port utilized by the session.	{text:Destination Port,ftype=dstport}
$natsport	Post-NAT source port.	{text:Nat Source Port,ftype=natsrcport}
$natdport	Post-NAT destination port.	{text:Nat Destinationport,ftype=natdstport}
$flags	32-bit field that provides details on session;	{text:Flags,ftype=flags}
$proto	IP protocol associated with the session.	{text:IP Protocol,ftype=ipprotocol}
$action	Action taken for the session; values are alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url.	{text:Action,ftype=eventName}
$file_url	Field with variable length. A Filename has a maximum of 63 characters. A URL has a maximum of 1023 characters	"{text:URL/Filename,ftype=requrl}"
$contentname	Palo Alto Networks identifier for the threat.	{text:Threat/Content Name,ftype=threatcontentname}
$category	For URL Subtype, it is the URL Category; For WildFire subtype, it is the verdict on the file and is either ‘malicious’, ‘phishing’, ‘grayware’, or ‘benign’; For other subtypes, the value is ‘any’.	{text:Category,ftype=category}
$severity	Severity associated with the threat; values are informational, low, medium, high, critical.	{priority:Severity,ftype=status;High;Medium;Low;Informational}

$direction	Indicates the direction of the attack, client-to-server or server-to-client: • 0—direction of the threat is client to server • 1—direction of the threat is server to client	{text:Direction,ftype=direction}
$seqno	A 64bit log entry identifier incremented sequentially; each log type has a unique number space.	{text:Sequence Number,ftype=sequencenumber}
$actionflags	A bit field indicating if the log was forwarded to Panorama.	{text:Action Flags,ftype=actionflags}
$srcloc	Source country or Internal region for private addresses. Maximum length is 32 bytes.	{text:Source Country,ftype=srcountry}
$dstloc	Destination country or Internal region for private addresses. Maximum length is 32 bytes.	{text:Destination Country,ftype=dstcountry}
$padding		{text:cpadding,ftype=cpadding}
$contenttype	Applicable only when Subtype is URL. Content type of the HTTP response data. Maximum length 32 bytes.	{text:Content Type,ftype=contenttype}
$pcap_id	The packet capture (pcap) ID is a 64 bit unsigned integral denoting an ID to correlate threat pcap files with extended pcaps taken as a part of that flow. All threat logs will contain either a pcap_id of 0 (no associated pcap), or an ID referencing the extended pcap file.	{text:PCAP ID,ftype=pcapid}
$filedigest	Only for WildFire subtype; all other types do not use this field The filedigest string shows the binary hash of the file sent to be analyzed by the WildFire service.	{text:File Digest,ftype=filedigest}

$cloud	Only for WildFire subtype; all other types do not use this field. The cloud string displays the FQDN of either the WildFire appliance (private) or the WildFire cloud (public) from where the file was uploaded for analysis.	{text:Cloud,ftype=cloud}
$url_idx	Used in URL Filtering and WildFire subtypes.	{text:URL Index,ftype=urlindex}
$user_agent	Only for the URL Filtering subtype; all other types do not use this field.	{text:User Agent,ftype=useragent}
$filetype	Only for WildFire subtype; all other types do not use this field. Specifies the type of file that the firewall forwarded for WildFire analysis.	{text:File Type,ftype=filetype}
$xff	Only for the URL Filtering subtype; all other types do not use this field. The X-Forwarded-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.	{text:X-Forwarded-For,ftype=forwardedforip}
$referer	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.	{text:RefererQuery,ftype=refererquery;,}{regexp:Referer,ftype=referer;refName=RefererQuery,^([\w-]+://[^?]+|/[^?]+
$sender	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.	{text:Sender,ftype=sender}

$subject	Only for WildFire subtype; all other types do not use this field. Specifies the subject of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.	{text:Subject,ftype=subject}
$recipient	Only for WildFire subtype; all other 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.	{text:Recipient,ftype=recipient}
$reportid	Only for WildFire subtype; all other types do not use this field. Identifies the analysis request on the WildFire cloud or the WildFire appliance.	{text:Report ID,ftype=reportid}
Device Group Hierarchy $dg_hier_level_1 $dg_hier_level_2 $dg_hier_level_3 $dg_hier_level_4	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.	{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=dgl
$vsys_name	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.	{text:Virtual System Name,ftype=vsysname}
$device_name	The hostname of the firewall on which the session was logged.	{text:Device Name,ftype=devicename}
$file_url		{text:URL/Filename,ftype=requrl}

$src_uuid	Identifies the source universal unique identifier for a guest virtual machine in the VMware NSX environment.	{text:Source VM UUID,ftype=sourcevmuuid}
$dst_uuid	Identifies the destination universal unique identifier for a guest virtual machine in the VMware NSX environment.	{text:Destination VM UUID,ftype=targetvmuuid}
$http_method	Only in URL filtering logs. Describes the HTTP Method used in the web request. Only the following methods are logged: Connect, Delete, Get, Head, Options, Post, Put.	{choice:Method,ftype=reqmethod;,Connect;Delete;Get;Head;Options;Post;Put},
$tunnelid	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.	{text:Tunnel ID,ftype=tunnelid}
$imei	International Mobile Equipment Identity (IMEI) is a unique 15 or 16 digit number allocated to each mobile station equipment.	{text:Monitor Tag,ftype=monitortag}
$parent_session_id	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.	{text:Parent Session ID,ftype=parentsessionid}
$parent_start_time	Year/month/day hours:minutes:seconds that the parent tunnel session began.	{text:Parent Session Start Time,ftype=parentstarttime}
$tunnel	Type of tunnel, such as GRE or IPSec.	{text:Tunnel Type,ftype=tunneltype}
$thr_category	Describes threat categories used to classify different types of threat signatures.	{text:Threat Category,ftype=threatcategory}
$contentver	Applications and Threats version on your firewall when the log was generated.	{text:Content Version,ftype=contentversion}
$sig_flags		{text:SIG_Flags,ftype=sigflags}
$assoc_id	Number that identifies all connections for an association between two SCTP endpoints.	{text:SCTP Assoication ID,ftype=sctpassociationid}

$ppid	ID of the protocol for the payload in the data portion of the data chunk.	{text:Payload Protocol ID,ftype=payloadprotocoolid}
$http_headers	Indicates the inserted HTTP header in the URL log entries on the firewall.	{text:HTTP Headers,ftype=httpheaders}

For more information about the traffic log fields, see below the format Conversion Table:

Field Name	Description	XpoLog Pattern
$domain	The domain which the messages were sent from.	{text:Domain,ftype=domain}
$dev	The device which the messages were sent from.	{text:Device,ftype=device}
$receive_time	Time the log was received at the management plane	{date:Receive Time,yyyy/MM/dd HH:mm:ss}
$serial	Serial number of the firewall that generated the log	{text:Serial#,ftype=serial}
$type	Type of log; values are traffic, threat, config, system and hip-match	{text:Type,ftype=eventSource}
$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.	{text:Subtype,ftype=subtype}
$configversion	Config Version associated with the system log.	{text:Config Version,ftype=configversion}
$time_generated	Time the log was generated on the dataplane.	{date:Time Generated,yyyy/MM/dd HH:mm:ss}
$src	Original session source IP address	{ip:SourceIP,ftype=sourceip}
$dst	Original session destination IP address.	{ip:DetinationIP,ftype=targetip}
$natsrc	If source NAT performed, the post-NAT source IP address.	{ip:Nat SourceIP,ftype=natsourceip}
$natdst	If destination NAT performed, the post-NAT destination IP address.	{ip:Nat DestinationIP,ftype=natdestinationip}
$rule	Name of the rule that the session matched.	{text:Rule Name,ftype=rulename}
$srcuser	Username of the user who initiated the session.	{text:Source User,ftype=username}

$dstuser	Username of the user to which the session was destined.	{text:Destination User,ftype=dstusername}
$app	Application associated with the session.	{text:Application,ftype=application}
$vsys	Virtual System associated with the session.	{block,start,emptiness=true}{text:Virtual System,ftype=virtualsystem}{block,end,emptiness=true}
$srczone	Zone the session was sourced from.	{text:Source Zone,ftype=srczone}
$dstzone	Zone the session was destined to.	{text:Destination Zone,ftype=dstzone}
$inbound_if	Interface that the session was sourced from.	{text:Inbound Interface,ftype=srcintf}
$outbound_if	Interface that the session was destined to.	{text:Outbound Interface,ftype=dstntf}
$logset	Log Forwarding Profile that was applied to the session.	{text:Log Action,ftype=logaction}
$time_logged		{date:Time Logged,yyyy/MM/dd HH:mm:ss}
$sessionid	An internal numerical identifier applied to each session.	{text:Session ID,ftype=sessionid}
$repeatcnt	Number of sessions with same Source IP, Destination IP, Application, and Content/Threat Type seen within 5 seconds.	{text:Repeat Count,ftype=repeatcount}
$sport	Source port utilized by the session.	{text:Source Port,ftype=srcport}
$dport	Destination port utilized by the session.	{text:Destination Port,ftype=dstport}
$natsport	Post-NAT source port.	{text:Nat Source Port,ftype=natsrcport}
$natdport	Post-NAT destination port.	{text:Nat Destinationport,ftype=natdstport}
$flags	32-bit field that provides details on session;	{text:Flags,ftype=flags}
$proto	IP protocol associated with the session.	{text:IP Protocol,ftype=ipprotocol}
$action	Action taken for the session; values are alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url.	{text:Action,ftype=eventName}
$bytes	Number of total bytes (transmit and receive) for the session.	{number:Bytes,ftype=bytes}
$bytes_sent	Number of bytes in the client-to-server direction of the session. Available on all models except the PA-4000 Series.	{number:Bytes Sent,ftype=bytesent}

$bytes_received	Number of bytes in the server-to-client direction of the session. Available on all models except the PA-4000 Series.	{number:Bytes Received,ftype=bytesreceived}
$packets	Number of total packets (transmit and receive) for the session.	{number:Packets,ftype=packets}
$start	Time of session start.	{date:Start Time,yyyy/MM/dd HH:mm:ss}
$elapsed	Elapsed time of the session.	{number:Elapsed Time(sec),ftype=elapsedtime}
$category	URL category associated with the session (if applicable).	{text:Category,ftype=category}
$seqno	A 64bit log entry identifier incremented sequentially; each log type has a unique number space.	{text:Sequence Number,ftype=sequencenumber}
$actionflags	A bit field indicating if the log was forwarded to Panorama.	{text:Action Flags,ftype=actionflags}
$srcloc	Source country or Internal region for private addresses. Maximum length is 32 bytes.	{text:Source Country,ftype=srcountry}
$dstloc	Destination country or Internal region for private addresses. Maximum length is 32 bytes.	{text:Destination Country,ftype=dstcountry}
$padding		{text:cpadding,ftype=cpadding}
$pkts_sent	Number of client-to-server packets for the session. Available on all models except the PA-4000 Series.	{number:Sent Packets,ftype=sentpkt}
$pkts_received	Number of server-to-client packets for the session. Available on all models except the PA-4000 Series.	{numberReceived Packets,ftype=rcvdpkt}
$session_end_reason	The reason a session terminated. If the termination had multiple causes, this field displays only the highest priority reason.	{text:Session End Reason,ftype=sessionendreason}

Device Group Hierarchy $dg_hier_level_1 $dg_hier_level_2 $dg_hier_level_3 $dg_hier_level_4	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.	{text:dg_hier_level_1,ftype=dghierlevel1},{text:dg_hier_level_2,ftype=dghierlevel2},{text:dg_hier_level_3,ftype=d
$vsys_name	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.	{text:Virtual System Name,ftype=vsysname}
$device_name	The hostname of the firewall on which the session was logged.	{text:Device Name,ftype=devicename}
$action_source	Specifies whether the action taken to allow or block an application was defined in the application or in policy. The actions can be allow, deny, drop, reset- server, reset-client or reset-both for the session.	{text:Action Source,ftype=actionsource}
$src_uuid	Identifies the source universal unique identifier for a guest virtual machine in the VMware NSX environment.	{text:Source VM UUID,ftype=sourcevmuuid}
$dst_uuid	Identifies the destination universal unique identifier for a guest virtual machine in the VMware NSX environment.	{text:Destination VM UUID,ftype=targetvmuuid}
$tunnelid	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.	{text:Tunnel ID,ftype=tunnelid}

$imei	International Mobile Equipment Identity (IMEI) is a unique 15 or 16 digit number allocated to each mobile station equipment.	{text:Monitor Tag,ftype=monitortag}
$parent_session_id	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.	{text:Parent Session ID,ftype=parentsessionid}
$parent_start_time	Year/month/day hours:minutes:seconds that the parent tunnel session began.	{text:Parent Session Start Time,ftype=parentstarttime}
$tunnel	Type of tunnel, such as GRE or IPSec.	{text:Tunnel Type,ftype=tunneltype}
$thr_category	Describes threat categories used to classify different types of threat signatures.	{text:Threat Category,ftype=threatcategory}
$assoc_id	Number that identifies all connections for an association between two SCTP endpoints.	{text:SCTP Assoication ID,ftype=sctpassociationid}
$chunks	Sum of SCTP chunks sent and received for an association.	{text:SCTP Chunks,ftype=chunks}
$chunks_received	Number of SCTP chunks sent for an association.	{text:SCTP Chunks Sent,ftype=chunkssent}
$chunks_sent	Number of SCTP chunks received for an association.	{text:SCTP Chunks Received,ftype=chunksreceived}

.