Integrating Palo Alto Networks Next-Generation Security Platform with EndaceProbe

The Palo Alto Networks Security Platform can be integrated with EndaceProbe™ Network Recorders to provide a seamless connection to the recorded Network History residing on the EndaceProbes in your network.

Pivot-To-Vision lets security analysts pivot directly from Palo Alto Networks threat logs to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History. Using the IP address and time range of the trigger, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data.

EndaceVision lets analysts dissect and review terabytes of network history down to microsecond level with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

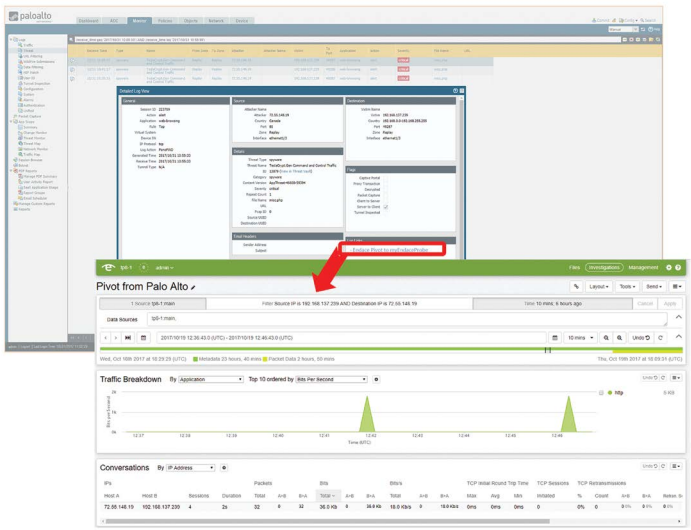
This document describes how to configure Palo Alto Networks Firewalls to integrate with EndaceProbe via Pivot-To-Vision APIs using log-links.

Palo Alto Networks VM-Series Firewalls can also be deployed on EndaceProbe hardware in the EndaceProbe's Application Dock hosting environment. This means Security Operations (SecOps) teams can dynamically deploy Intrusion Detection capability on the network anywhere that EndaceProbe Network Recorders are deployed, allowing them to increase detection footprint without truck rolls and additional hardware.

Refer to Endace's *Deployment Guide for Palo Alto Networks VM-Series Firewall for KVM* for step-by-step instructions on deploying Palo Alto Networks VM-Series on EndaceProbe in Application Dock.

Opening an EndaceVision Investigation using a Log-Link

Log-links encode all the information required to open an EndaceVision investigation browser window and automatically pre-configure EndaceVision filters to focus on the specific packets relating to the log event. Log-links must be configured by the Palo Alto Networks administrator. Once configured, log-links are accessed by regular users from the Palo Alto Networks Detailed Log View as shown below.



Creating a Log-Link

There are two methods of creating log-links:

- CLI – best for creating a single log-link to an EndaceProbe.
- XML API – best for creating many log-links to multiple EndaceProbes.

Pre-requisites to create Log-Links

- Endace OSm Software release 6.3.1 or greater,
- PAN-OS release 8.0.5 or greater,
- Admin privileges on PAN-OS CLI,
- An account with *vision_user* and *vision_download* user privileges on EndaceProbe,
- Download a copy of the supplied script "`palo_log_link.sh`" from the Endace Support Portal. This script helps create multiple log-links easily.

Using the CLI to Create a Log-Link

To configure a log-link using the CLI, log into PAN-OS CLI as admin and run the following. Copy the following and replace the highlighted text with details from your specific environment.

```
configure
set deviceconfig system log-link "Pivot to myEndaceProbe" url
"https://myEndaceProbe.mydomain.com/vision2/pivotintovision/?d
atasources=myEndaceProbe%3Amain&title=Palo_Alto_Networks_Log_
Alert&start={recvtime_YYYY}-{recvtime_MM}-{recvtime_DD}T{recvtime_
hh}%3A{recvtime_mm}%3A{recvtime_ss}-<time_zone_offset>&end=&tools=<i
nvestigation_tools>"
commit
exit
```

Note:
The set command must be entered as a continuous string – i.e. without line breaks etc. – when pasted into the PAN -OS CLI.

Option	Description
Pivot to myEndaceProbe	The name of the Log-link displayed in the Palo Alto Networks Detailed Log view.
myEndaceProbe. mydomain.com	The fully qualified address of the EndaceProbe. This can also be an IP Address.
myEndaceProbe	The host name of the EndaceProbe.
main	Name of the RotationFile on the EndaceProbe that contains the packet data
Palo_Alto_Networks_ Log_Alert	Name for the investigation. This name is displayed at the top of EndaceVision browser window.
<time_zone_offset>	Optional. Time zone offset. Sets the time zone offset e.g. "-05:00". This option enables you to define a time zone offset between the Palo Alto Networks Firewall and the EndaceProbe.
<investigation_tools>	The list of EndaceVision Investigation tools to display. If no tool is listed the Investigation is created without tools. You can then add the tools. Multiple tools can be listed, for example: `tools=trafficOverTime_by_sip&sip={src}&dip={dst}%2Cconversations_by_ipaddress` For details on the available Investigation tools, refer to the *EndaceVision v2 User Guide*.

Using Log-Links

- Test the log-link by opening the Palo Alto Networks Detailed Log View. The log-link you created should be listed. Click the log-link to open the EndaceVision Investigation.
- To view a list of all current log-links , run the following CLI command in the Palo Alto Networks CLI in config mode:
  `show deviceconfig system log-link`
- To remove a log-link, run the following CLI command in the Palo Alto Networks CLI in config mode:
  `delete deviceconfig system log-link [name]`

Using the XML API to Create a Log-Link

To configure a log-link using the XML API, complete the following two steps. Edit and run the BASH script in a separate Linux environment.

1. Edit the Endace-supplied BASH Script

Endace provides a BASH script to ease the deployment of log-links onto PAN-OS devices. This script is called `palo_log_link.sh` and available from the Endace Support Portal. The script can list, create and delete log-links from any PAN-OS device.

In order to simplify the parameters passed to the script each time it is run, a number of site-specific variables are included in the script and should be customized to your local environment before running the script for the first time.

The section in the script with the variables is as follows:

```
CURL="/usr/bin/curl -s -k -X GET"
DOMAIN="yourdomain.com"
DEFAULT_ROTFILE="main"
TARGET_TITLE="Pivot+from+Palo+Alto+Networks"
USER=[Palo Alto Networks API admin account]
PASS=[Palo Alto Networks API admin password]
```

Option	Description
DOMAIN	The domain address in which the EndaceProbe resides.
DEFAULT_ROTFILE	The name of the RotationFile. Each EndaceProbe must have the same RotationFile name.
TARGET_TITLE	The name of the generated EndaceVision Investigation. Use the "+" character to encode spaces.
USER	The user name used to login to the EndaceProbe. We recommend that the same User name and password is set on all EndaceProbe.
PASS	The password associated with the User name.

It is best practice to set up a separate Palo Alto Networks admin account for XML API access.

2. Run the BASH Script

Once customized for the local environment, the BASH script should be called from a separate Linux environment with the help argument to explore the command line arguments that it accepts:

```
palo_log_link.sh -a [get|set|del] -p <target probe name>
-f <target PA firewall name> [-t <offset>] [-l <log-link entry name>]
[-d] [-c] [-h]
```

The BASH script must be run in a linux environment in a BASH shell.

Option	Description
-a	The action to perform on PAN-OS Firewall. This can be GET, SET or DELETE.
-p	Sets the hostname of EndaceProbe on which the captured packets reside.
-f	Sets the hostname of the PAN-OS Firewall on which to create the log-link (can be a Firewall or Panorama).
-t	Optional. Time zone offset. Sets the time zone offset e.g. "-05:00". This option enables you to define a time zone offset between the Palo Alto Networks Firewall and the EndaceProbe.
-l	Optional. When used with SET, override the default log-link name constructed from the EndaceProbe's name. When used with DEL, specifies the log-link name to delete.
-d	Optional. Enables the debug functionality.
-c	Optional. Commit toggle. Use this option to commit the changes.
-h	Display the associated help file.

Note:

The hostnames supplied are not FQDNs (fully qualified domain names). The domain is specified in the site specific variables in the script which is used with the user supplied hostname to construct the FQDN.

Create a log-link:

Command

```
./palo_log_link.sh -a set -p myEndaceProbe -f myPalo-Alto-Networks-
Platform
 -t <offset>
```

Output

```
<response status="success" code="20"><msg>command succeeded</msg></
response>
```

Notes:

- *The EndaceProbe operates using UTC and automatically updates the time zone.*
- *The Palo Alto Networks log-link parameters have no time zone information.*
- *In the log-link, you can correct for the time zone difference between the Palo Alto Networks Firewall and the EndaceProbe by adding a time zone offset (`-t <offset>`). This offset must also be updated for Daylight savings.*

Validate success using the GET action:

Command

```
./palo_log_link.sh -a get -f myPalo-Alto-Networks-Platform
```

Output

```
<response status="success" code="19"><result total-count="1"
count="1"> <log-link admin="admin" dirtyId="9" time="2017/10/19
13:04:00"> <entry name="Pivot to myEndaceProbe" admin="admin"
dirtyId="9" time="2017/10/19 13:04:00"> <url admin="admin"
dirtyId="9" time="2017/10/19 13:04:00">https://myEndaceProbe.
mydomain.com/vision2/pivotintovision/?datasources=myEndaceProbe:m
ain&amp;title=Pivot_from_Palo_Alto_Networks&amp;incidenttime={rec
vtime_YYYY}-{recvtime_MM}-{recvtime_DD}T{recvtime_hh}:{recvtime_
mm}:{recvtime_ss}<time_offset>&amp;reltime=5m&amp;tools=trafficOverT
ime_by_app,conversations_by_ipaddress&amp;sip={src}&amp;dip={dst}</
url> </entry> </log-link> </result></response>
```

Delete log-links using the DEL action:

Command

```
./palo_log_link.sh -a del -p myEndaceProbe -f myPalo-Alto-Networks-
Platform
```

Output

```
<response status="success" code="20"><msg>command succeeded</msg></
response>
```

References

For further details on the following see the following references:

- the log-link feature, refer to the following web page: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-does-the-Log-Link-Feature-Work/ta-p/52298
- the PAN-OS XML API, refer to the following web page:https://www.paloaltonetworks.com/documentation/80/pan-os/xml-api
- the Pivot to Vision API, refer to the *Generating Investigations from Outside EndaceVision v2* section in your *EndaceVision v2 User Guide*.
- the required EndaceProbe user roles, refer to the *Setup* > *User* > *Role Based Access Control* section in your *EndaceProbe User Guide*.
- the `palo_log_link.sh script`, so to the Endace Support Portal, or contact Endace Support.
- on deploying a Palo Alto Networks VM-Series Firewall for KVM on an EndaceProbe, refer to the *Deployment Guide for Palo Alto Networks VM-Series* supplied by Endace.

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com