

[TOOL] PLA – PIX Logging Architecture

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-11/msg00006.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 7 Nov 2006 19:06:24 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

PLA – PIX Logging Architecture

SUMMARY

DETAILS

The PIX Logging Architecture [PLA] is a free and open-source project allowing for correlation of Cisco PIX Firewall Traffic and IDS Logs.

PIX Log message parsing is performed through the use of the PLA parsing module or PLA Msyslogd module. Centralization of the logs is provided using a MySQL database, supported by a Web-based frontend for Log Viewing, Searching, and Event Management. PIX Logging Architecture is completely coded in the Perl programming language, and uses various Perl modules including Perl::DBI and Perl::CGI.

The PIX Logging Architecture parsing module, which is responsible for extracting the necessary fields from the PIX system log messages, gather information including, but not limited to, Translations (Xlate's), Informative Log Messages (i.e. PIX Failover, PIX VPN Establishment, PIX Interface Up/Down, PIX PPPoE VPDN establishment and the like). All the parsing information needed by the PLA Parsing Daemon (pla_parsed) in order

[TOOL] PLA – PIX Logging Architecture

to extract data from the logs is stored in the database, allowing for easy updates of the supported log messages without having to replace the parsing scripts.

The PLA Parsing Daemon runs as a daemonized Perl process in the background and reads straight and in quasi real-time from the system log files, so no more need to create crontab jobs like before and having to restart syslogd all the time.

Parse-Time Filtering:

With the PIX Logging Architecture v2.00 version comes the ability to perform parse-time filtering. Parse-time filtering allows you to use the PLA web interface to define traffic which you do not wish you log (i.e. between specific IP pairs and ports, on specific protocols, on specific firewalls). The PLA Parse Daemon (pla_parsed) then checks the incoming firewall logs and will exclude any traffic which matches the parse-time filters. Using these parse filters allows to keep tabs on the database size and prevents you from having to log all data.

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:kris@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>> Kris Philipsen.

The original article can be found at:
<<http://www.logging-architecture.net/pla2/>>
<http://www.logging-architecture.net/pla2/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.