AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Device Integration: Checkpoint Firewall-1

CONTENTS

1. INTRODUCTION 4
2. CHECKPOINT FIREWALL-1 DATA INFORMATION 4
3. CONFIGURING FW-1 TO SEND DATA TO ALIENVAULT THROUGH SYSLOG 4
4. HOW TO ENABLE THIS PLUGIN 6

1. INTRODUCTION

The objective of this document is to explain how to configure a Checkpoint Firewall-1 device to send log data to AlienVault USM.

This document is related to the AlienVault document "Data Source Plugin Management". The explanation about how to enable plugins can be found in that document.

2. CHECKPOINT FIREWALL-1 DATA INFORMATION

Device Name	Firewall-1
Device Vendor	Checkpoint
Device Type	Firewall
Data Source Name	fw1-alt
Connection Type	Syslog
Data Source ID	1504

3. CONFIGURING FW-1 TO SEND DATA TO ALIENVAULT THROUGH SYSLOG[1]

This procedure is not supported on Provider-1 / Multi-Domain Server.

The following instructions must be done on the Check Point appliance:

1. Backup the current */etc/syslog.conf* script:

[1] These instructions are being copied from Check Point Solution ID: sk33423

```
cp /etc/syslog.conf /etc/syslog.conf_ORIGINAL
```

2. Edit the current */etc/syslog.conf* script:

```
vi /etc/syslog.conf
```

3. Add the following line:

```
local4.info @IP_Address_of_External_Syslog_Server
```

It is necessary to enter a TAB after the *'local4.info'*.

4. Save the changes in the */etc/syslog.conf* file and exit from VI editor.
5. Backup the current */etc/rc.d/init.d/cpboot* script:

```
cp /etc/rc.d/init.d/cpboot  /etc/rc.d/init.d/cpboot_ORIGINAL
```

6. Edit the current */etc/rc.d/init.d/cpboot* script:

```
vi /etc/rc.d/init.d/cpboot
```

7. Add the following line at the very bottom:

```
fw log -f -t -n -l  2> /dev/null | awk 'NF' | logger -p local4.info -t
CP_FireWall &
```

The '&' character at the end of a command's syntax ensures that this command runs in the background. If the '&' character is not included in the command, the OS would stop at loading the syslogd service, and you never get a login prompt at the console.

For flags available for 'fw log', run:

	fw log --help **In our example:** **-f - Only in case of active log file - Upon reaching the end of file, wait for new records and print them as well.** **-n - No IP resolving. The default is to resolve all IPs.** **-l - Show date and time per log record. The default is to show the date above the relevant records, and then the time per log record.** **For flags available for 'logger', refer to logger manual page.**

8. Save the changes in the */etc/rc.d/init.d/cpboot* file and exit from VI editor.
9. Reboot the machine.

	**Restarting the Check Point services with *cpstop;cpstart* command is not enough to make this work.**

4. HOW TO ENABLE THIS PLUGIN

This plugin is already configured, but it is necessary to enable it, through command line console or through the web interface. It is needed to enable the **fw1-alt** plugin. The instructions about how to enable this plugin can be found in the AlienVault document "Data Source Plugin Management".