AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Device Integration: F5 FirePass

CONTENTS

1. INTRODUCTION

The objective of this document is to explain how to configure an F5 FirePass 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. F5 FIREPASS INFORMATION

Device Name	Firepass
Device Vendor	F5
Device Type	VPN Concentrator
Data Source Name	f5-firepass
Connection Type	Syslog
Data Source ID	1674

3. CONFIGURING F5 FIREPASS TO SEND LOG DATA TO ALIENVAULT

F5 FirePass must be configured to send log data to an AlienVault Sensor over the syslog protocol.

1. Log into the F5 Web Interface.
2. Navigate to **Maintenance**.
3. In the System Logs section. Select Enable Remote Logging.
4. Select Enabled Extended System Logs.
5. Enter the IP Address of an Alienvault Sensor in the **Remote Host** text box.
6. Select Apply System Log Changes.

4. CONFIGURING ALIENVAULT TO RECEIVE LOGS FROM F5 FIREPASS

Devices that send log data via Syslog require configuration of the Syslog service to process those incoming logs into a unique file destination.

1. Open the AlienVault OSSIM/USM Console.
2. Select and accept the 'Jailbreak this appliance' option to gain command line access.
3. Create a new configuration file to save incoming FirePass logs:

```
nano –w /etc/rsyslog.d/f5-firepass.conf
```

4. Add the following line to the file, one for each F5 FirePass device you are sending logs from:

```
if ($fromhost-ip == '<IP_Address_FirePass>') then -/var/log/f5-
firepass.log
```

5. Press **Crtl+W** to save the file and **Ctrl+X** to exit the editor.
6. Restart the Syslog Collector:

```
/etc/init.d/rsyslog restart
```

5. CONFIGURING LOG FILE EXPIRATION

Incoming logs will be processed by the Sensor and passed on to the SIEM Service. Keeping the raw log files on the sensor for more than a few days is unnecessary and they should be purged to maintain adequate free filesystem capacity.

1. Create a new log rotation configuration file.

```
nano –w /etc/rsyslog.d/f5-firepass
```

2. Add the follows content to the file:

```
/var/log/f5-firepass.log
{
 rotate 4 # save 4 days of logs
 daily # rotate files daily
 missingok
 notifempty
 compress
```

```
 delaycompress
 sharedscripts
 postrotate
 invoke-rc.d rsyslog reload > /dev/null
 endscript
}
```

6. 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. The instructions about how to enable this plugin can be found in the AlienVault document "Data Source Plugin Management".