AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Device Integration: Cisco Wireless LAN Controller (WLC)

CONTENTS

1. INTRODUCTION

The objective of this document is to explain how to configure a Cisco WLC 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. CISCO WLC INFORMATION

Device Name	Wireless LAN Controller
Device Vendor	Cisco
Device Type	Wireless Access Point Manager
Data Source Name	cisco-wlc
Connection Type	syslog
Data Source ID	1663

3. CONFIGURING CISCO WLC TO SEND LOG DATA TO ALIENVAULT

Cisco WLC must be configured to send log data to an AlienVault Sensor over the Syslog protocol.

1. Connect to the WLC Console.
2. Enter Enable mode.
3. Enter the following commands:

```
config logging syslog host <IP_AlienVault_Sensor>
config logging syslog facility syslog
config logging syslog level informational
save config
Y
```

4. CONFIGURING ALIENVAULT TO RECEIVE LOGS FROM CISCO WLC

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 console on the AlienVault Appliance, or log in over Secure Shell (SSH) as the “root” user.
2. Select and accept the ‘Jailbreak this appliance’ option to gain command line access.
3. Create a new configuration file to save incoming logs:

```
nano -w /etc/rsyslog.d/cisco-wlc.conf
```

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

```
if ($fromhost-ip == ‘IP_Address_WLC’) then /var/log/cisco-wlc.log
```

5. End the file with this line:

```
& ~
```

6. Press **Crtl+W** to save the file and **Ctrl+X** to exit the editor.
7. 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/logrotate.d/cisco-wlc
```

2. Add the follows content to the file:

```
/var/log/cisco-wlc.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".