AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Device Integration: Cisco ASA

CONTENTS

1. INTRODUCTION

The objective of this document is to explain how to configure a Cisco ASA 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 ASA DATA INFORMATION

Device Name	ASA
Device Vendor	Cisco
Device Type	UTM
Data Source Name	cisco-asa
Connection Type	Syslog
Data Source ID	1636

3. CONFIGURING CISCO ASA TO SEND LOG DATA TO ALIENVAULT

Cisco ASA must be configured to send log data to an AlienVault Sensor over the syslog protocol.

Pre-Requisites:

- IP Address of the AlienVault Sensor or All-in-One

1. Connect to the ASA box with telnet or SSH, enter enable mode to begin configuration.

```
enable
```

2. Enter the configure mode by typing the following command:

```
config terminal
```

3. Type the following lines:

```
no logging timestamp
```

```
logging trap notification

logging host inside <IP_Address_AlienVault_Sensor>
```

4. Press **Ctrl+Z** to exit config mode.

5. Save the configuration changes:

```
copy running-config startup-config
```

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