AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Device Integration: SonicWALL

CONTENTS

1. INTRODUCTION

The objective of this document is to explain how to configure a Dell SonicWALL 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. DELL SONICWALL INFORMATION

Device Name	SonicWALL
Device Vendor	Dell
Device Type	UTM
Data Source Name	sonicwall
Connection Type	syslog
Data Source ID	1573

3. CONFIGURING DELL SONICWALL TO SEND LOG DATA TO ALIENVAULT USM

1. Login to SonicWALL.
2. Select the Log entry on the left side of the menu.
3. Select the Log Settings tab located on the top of the menu.
4. Enter the IP Address of an AlienVault Sensor in the Syslog Host field.
5. Set the Syslog Server Port field to 514.
6. Select Default for the Syslog format.setting.
7. Choose Categories to log.
8. Click Update (at bottom of the menu).

4. CONFIGURING ALIENVAULT TO RECEIVE LOGS FROM DELL SONICWALL

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 "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/sonicwall.conf
```

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

```
if ($fromhost-ip == 'IP_Address') then /var/log/sonicwall.log
```

IP_Address refers to the Dell SonicWALL IP Address.

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/sonicwall
```

2. Add the follows content to the file:

```
/var/log/sonicwall.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".