AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Device Integration: Fortinet FortiGate

CONTENTS

1. INTRODUCTION

The objective of this document is to explain how to configure a Fortinet FortiGate 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. FORTINET FORTIGATE INFORMATION

Device Name	Fortigate
Device Vendor	Fortinet
Device Type	UTM
Data Source Name	fortigate
Connection Type	Syslog
Data Source ID	1554

3. CONFIGURING FORTINET FORTIGATE TO SEND LOG DATA TO ALIENVAULT

Fortinet FortiGate must be configured to send log data to an AlienVault Sensor over the syslog protocol

1. Configure your policies for logging:

```
Firewall -> Policy
```

2. Edit each policy and enable:

```
Log Allowed Traffic
```

3. Select **OK**.
4. Configure Log Settings.

```
Log & Report -> Log Config -> Log Settings
Remote Logging and Archiving
```

```
Select 'Syslog'
```

5. Enter the following settings:

```
IP: <IP_address_AlienvaultSensor>

Port: 514

Severity: Information

Facility: Local0
```

6. Select APPLY.

4. CONFIGURING ALIENVAULT TO RECEIVE LOGS FROM FORTINET FORTIGATE

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/fortigate.conf
```

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

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

   IP_Address refers to the Fortinet FortiGate 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/fortigate
```

2. Add the follows content to the file:

```
/var/log/fortigate.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".