Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring SonicWALL UTM to Forward Logs to EventTracker

Publication Date:

March 20, 2022

Abstract

This guide provides instructions to configure SonicWALL UTM (Unified Threat Management) to send the syslog events to EventTracker.

Audience

The SonicWALL UTM users, who wish to forward the syslog events to the EventTracker Manager.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.X and later, and SonicOS 5.8 and later for SonicWALL NSA and TZ Series.

Table of Contents

Table of Contents 3
1. Overview 4
2. Prerequisites 4
3. Integrating SonicWALL UTM with EventTracker 4
3.1 Configuring the Syslog Settings 4
3.2 Configuring the Syslog Server 7
4. Syslog Send Receive Verification 8
4.1 Verifying the Ping from SonicWALL UTM to EventTracker 8
4.2 Verifying the Syslog messages forwarding on SonicWALL UTM 9
4.3 Verifying the Syslog messages in EventTracker 11
About Netsurion 12
Contact Us 12

1. Overview

SonicWALL's approach to the Unified Threat Management (UTM) is the best security approach for Small- to Medium-sized Businesses (SMBs) bringing a new level of efficiency to the security field. EventTracker gathers and examines acquired logs to identify malicious traffic, fatal threats, configuration changes, VPN activity, and user behavior.

2. Prerequisites

- EventTracker Agent 9.x and later should be installed.
- SonicOS 5.8 and later should be installed.
- Port 514 must be allowed on SonicWALL UTM.
- An exception should be added to the Windows Firewall on the EventTracker Manager system for Syslog port 514.

3. Integrating SonicWALL UTM with EventTracker

To forward the logs from SonicWALL UTM to EventTracker follow the below steps:

3.1 Configuring the Syslog Settings

1. Login to **SonicWALL UTM** using the Web browser**.**

2. Click the **Log** option at the bottom left of the **SonicWALL UTM** screen.

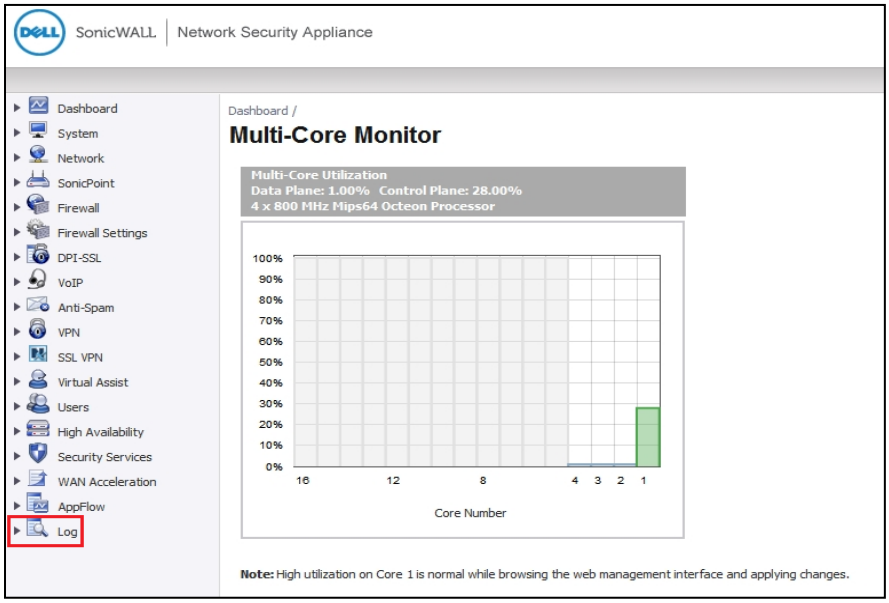

Figure 1

3. Select the **Syslog** option.

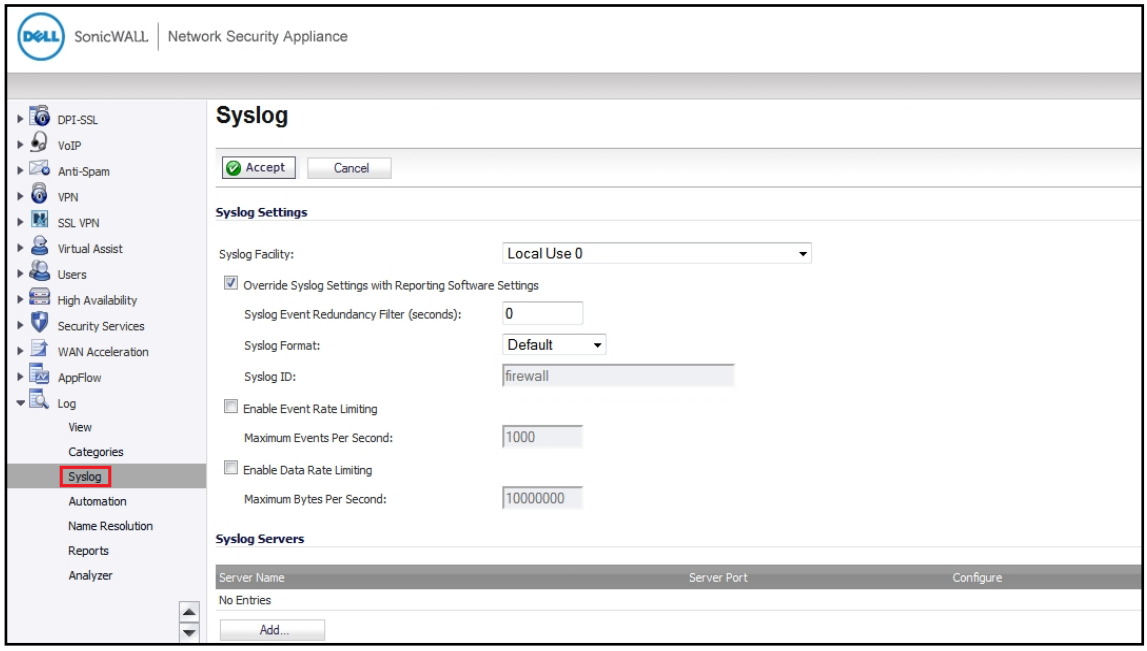

Figure 2

4. Under the **Syslog Setting** configure the following.

- **Syslog Facility-** Select the Syslog Facility you want or keep it as default.
- **Override Syslog Settings with Reporting Software Settings** - Uncheck this box to override the Syslog settings.

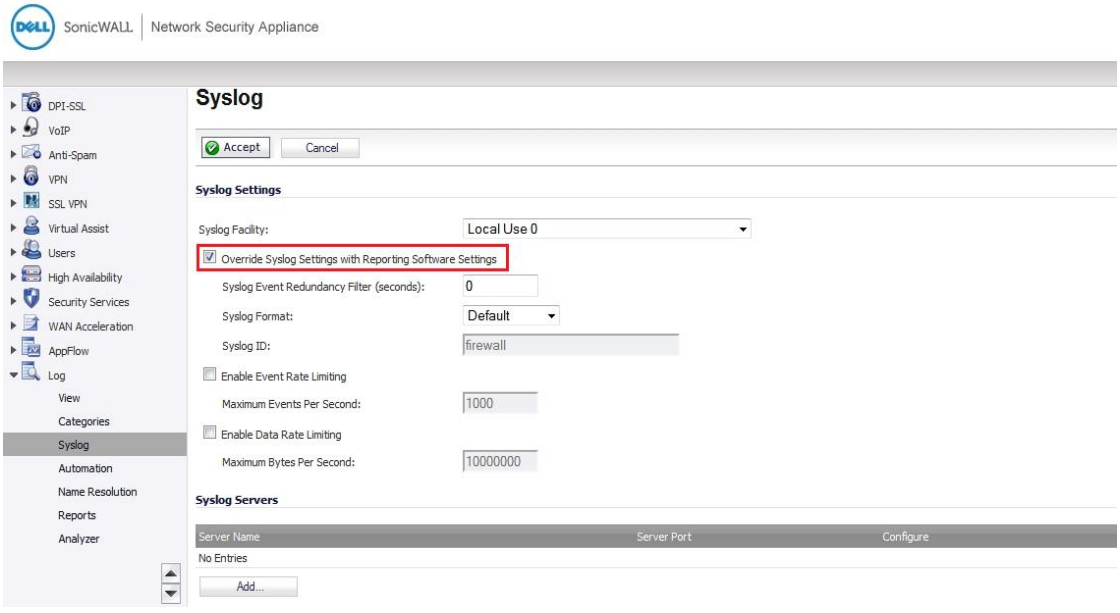

Figure 3

5. From the **Syslog Format** menu list, select the **Enhanced Syslog format**.

6. Click the Configure icon . The **Enhanced Syslog Settings** configuration window appears.

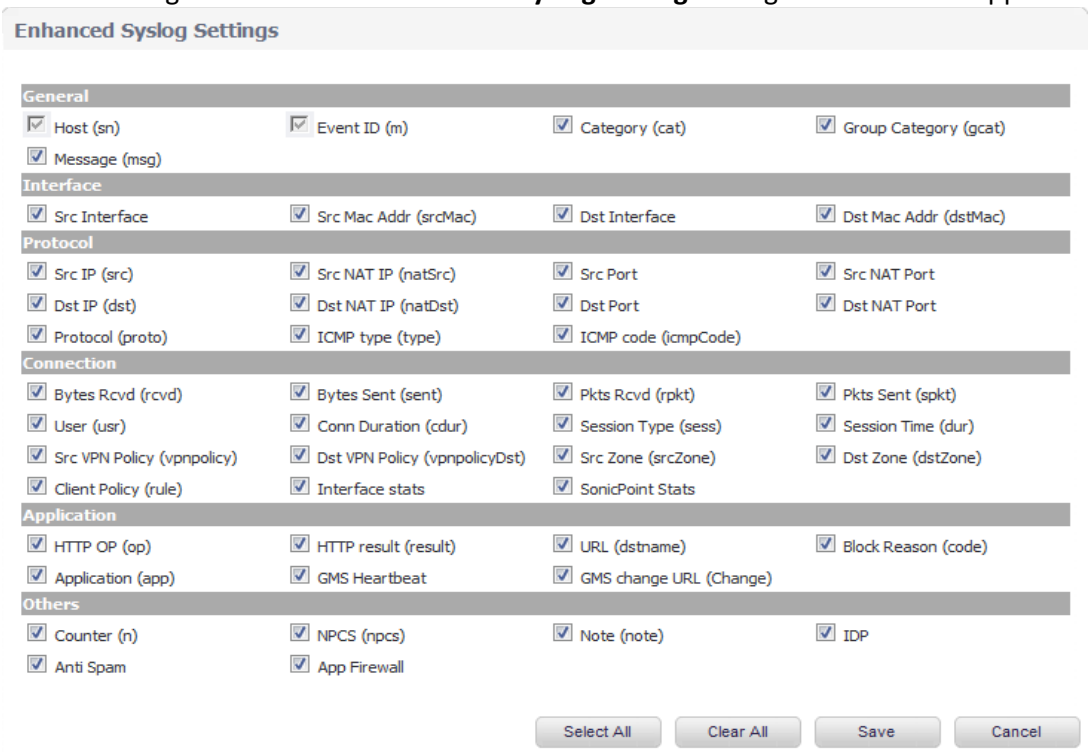

Figure 4

7. Select the **Enhanced Syslog** options you want to log into. To select all options, click **Select All**. To deselect all the options, click **Clear All**.

8. Click the **Save** button.

9. In the **Syslog ID** box, enter the Syslog ID that you want.

   A **Syslog ID** field is included in all the generated Syslog messages, prefixed by “id= ". Thus, for the default value, firewall, all Syslog messages include "id=firewall." The ID can be set to a string consisting of 0 to 32 alphanumeric and underscore characters.

10. **(Optional)** Select **Enable Event Rate Limiting** if required. This control allows you to enable the rate limiting of the events to prevent the internal or external logging mechanism from being overwhelmed by the log events. Specify the maximum number of events in the Maximum Events per Second field; the minimum number is 0, the maximum is 1000, and the default is 1000 per second.

    NOTE: Event rate and data rate limiting are applied regardless of the Log Priority of individual events.

11. **(Optional)** Select the Enable Data Rate Limiting if required. This control allows you to enable the rate limiting of the data to prevent the internal or external logging mechanism from being overwhelmed

by the log events. Specify the maximum number of bytes in the **Maximum Bytes per Second** field; the minimum is 0, the maximum is 1000000000, and the default is 10000000 bytes per second.

12. **(Optional)** Select **Enable NDPP Enforcement** for the Syslog Server if required.

3.2 Configuring the Syslog Server

1. Under the **Syslog Servers** heading, click the **Add** button.

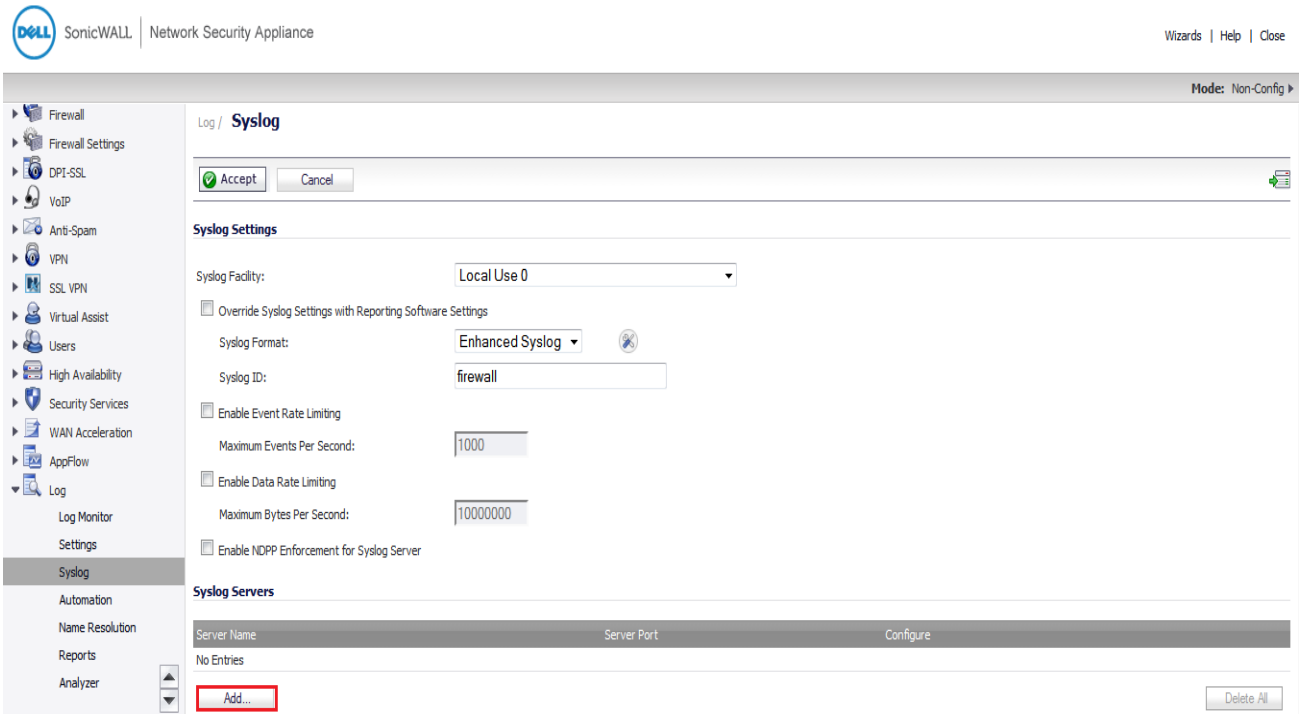

Figure 5

The Add Syslog Server window display.

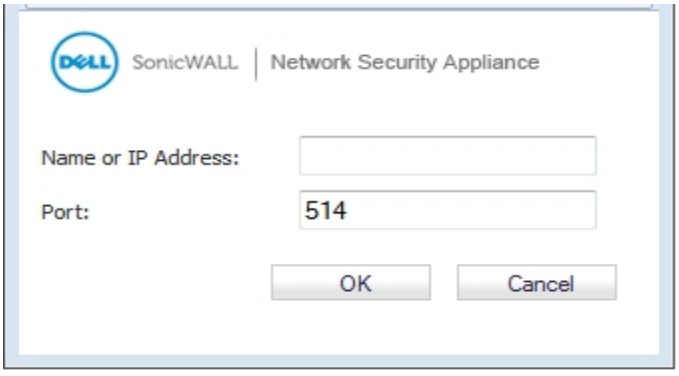

Figure 6

2. Type the **EventTracker Agent** machine name or IP address in the **Name or IP Address** field. Type the port number in the **Port Number** field. The Syslog default port is 514.

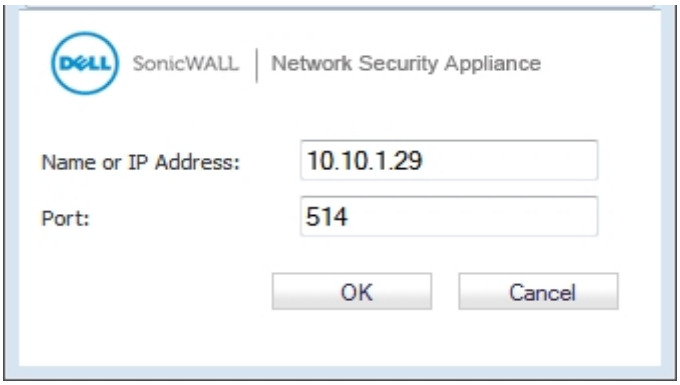

Figure 7

3. Click **OK**.

The Syslog server **EventTracker Agent** machine IP address would be added under the **Syslog Servers** section.

4. Click the **Accept** button to **Save** the settings.

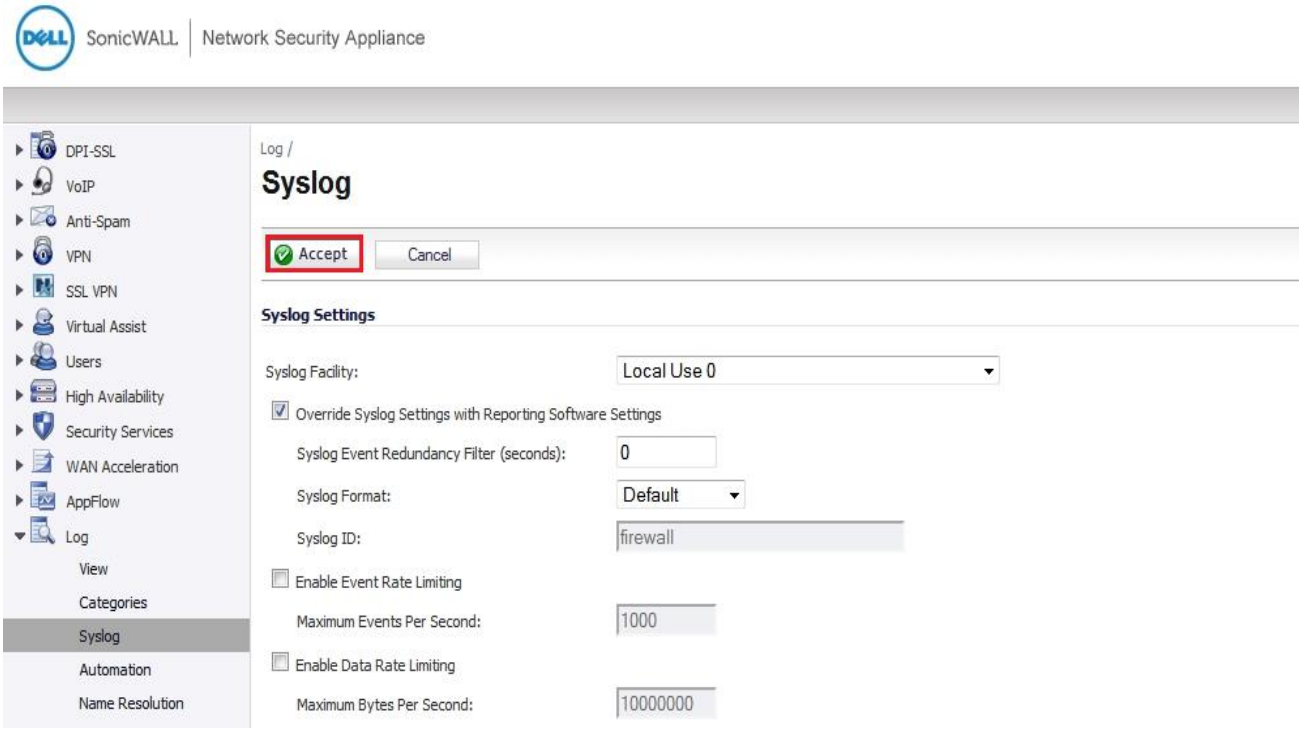

Figure 8

4. Syslog Send Receive Verification

4.1 Verifying the Ping from SonicWALL UTM to EventTracker

1. Login to SonicWALL UTM using the **Web** browser.

2. Click **System->Diagnostics.**

3. Select **Ping** from the **Diagnostic Tool** menu.

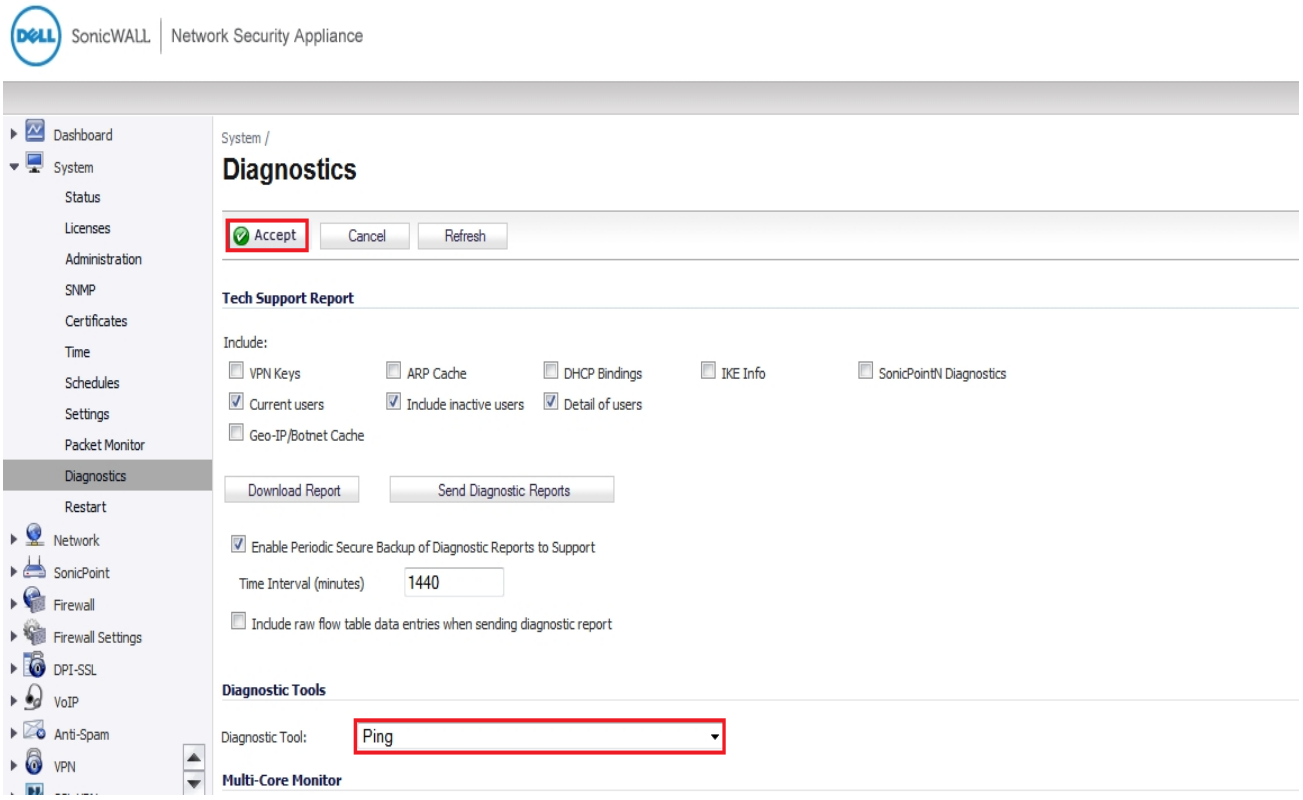

Figure 9

4. Enter the IP address or hostname of the EventTracker Manager system and click **Go**.

5. In the **Interface** pulldown menu, select the interface you want to test the ping from. Selecting the option **ANY** allows the appliance to choose among all the interfaces—including those that are not listed in the pulldown menu.

6. If the test is successful, SonicWALL UTM returns a message saying that the IP address is alive, and the time taken to return in milliseconds (ms).

4.2 Verifying the Syslog messages forwarding on SonicWALL UTM

1. Login to the SonicWALL Network Security using the Web browser.

2. Navigate to the **System-> Packet Monitor** page in the GUI and click **Configure**.

Figure 10

3. In the **Monitor Filter** tab, specify the following information.

- **Ether Type(s): IP Address**
- **IP Type(s): UDP**
- **Destination Port(s): 514**
- **Enable** the check box **Enable Bidirectional Address and Port Matching.**

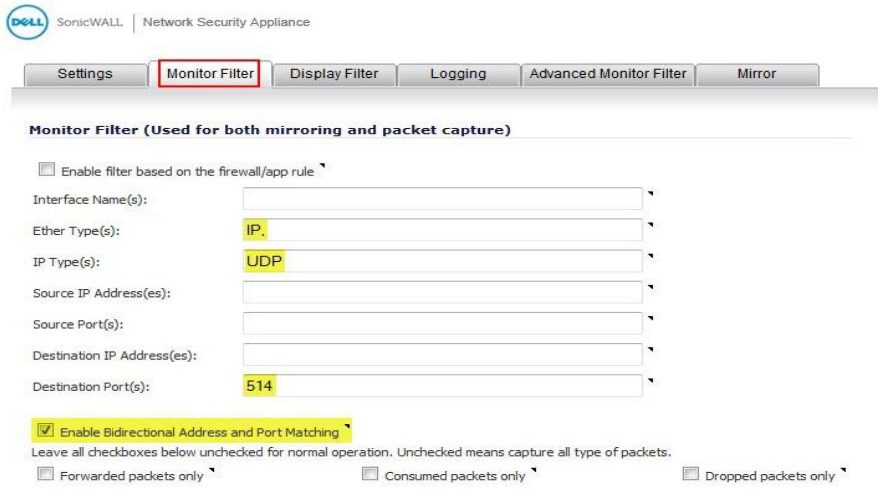

Figure 11

4. In the **Advanced Monitor Filter** tab, **enable** the check boxes.

- Monitor the Firewall Generated Packets. (This will bypass interface filter).
- Monitor the Intermediate Packets.

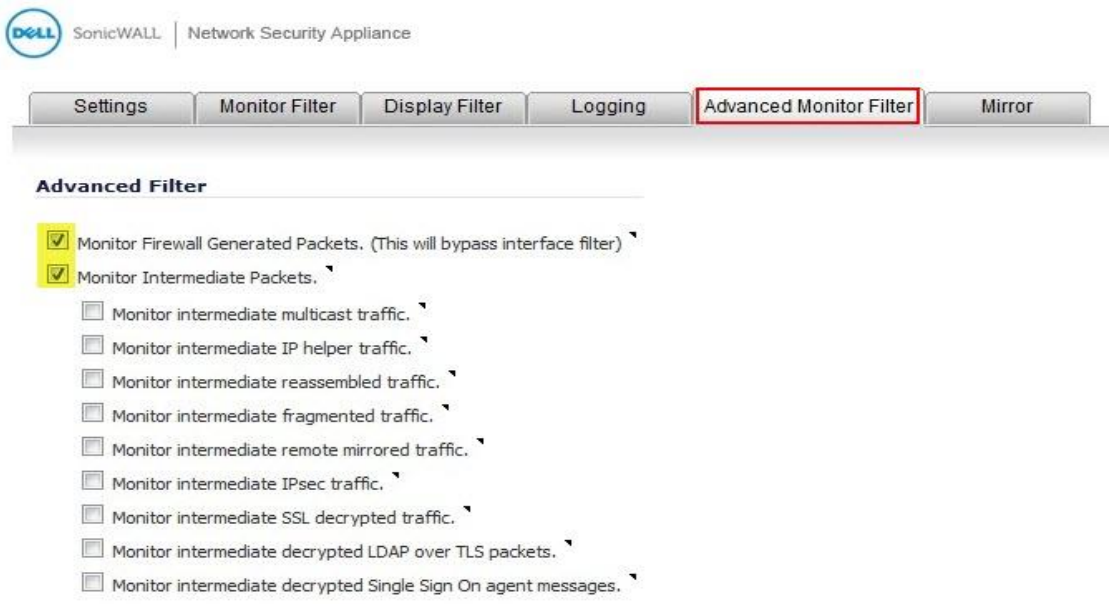

Figure 12

5. Click **OK** to save the packet capture setup.

6. Click **Start Capture** in the Packet Monitor page to see the **UDP 514** packets getting **generated** from SonicWALL destined for syslog server IP address as shown below.

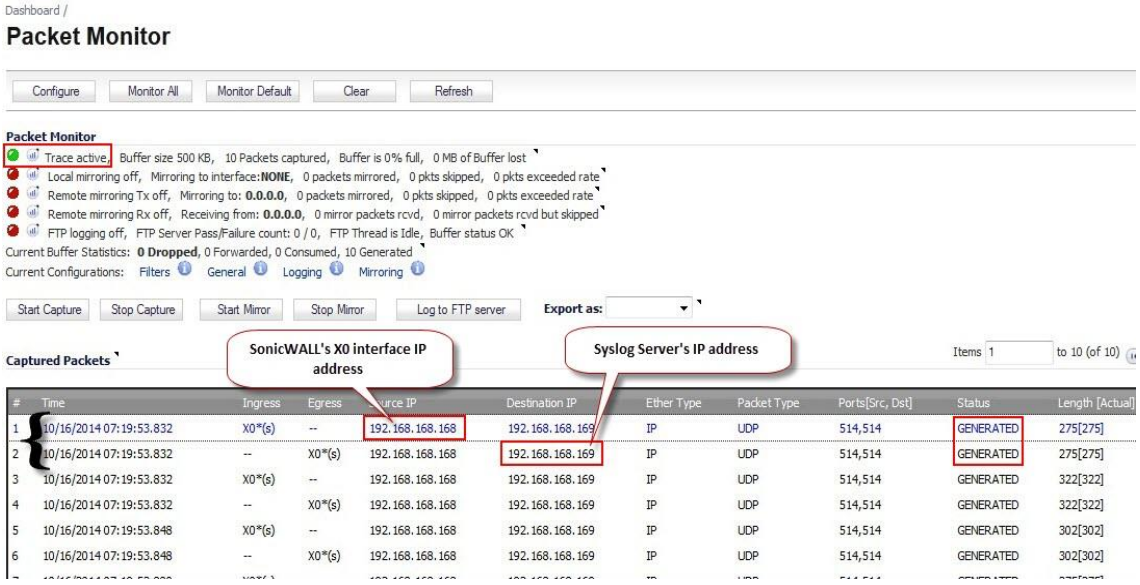

Figure 13

4.3 Verifying the Syslog messages in EventTracker

1. Login to the EventTracker Web Application.

2. Perform the Log Search for SonicWALL UTM device.

3. Log Search would display the syslog messages which EventTracker is receiving from SonicWALL UTM.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support