EventTracker

Actionable Security Intelligence

How to – Configure ASA 5500-X Series Firewall to send logs to EventTracker

EventTracker

Publication Date: September 14, 2018

Abstract

This guide helps you in configuring **ASA 5500-X Series Firewall** to send logs to EventTracker.

Audience

Administrators, who are assigned the task to monitor and manage events using EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and **ASA 5500-X Series firewall**.

Table of Contents

Overview

Cisco hosts security firewall appliances like ASA (Adaptive Security Appliance). Initially PIX was widely used and later Cisco introduced ASA.

Cisco ASA can be widely used at home/small office/large enterprises.

Cisco ASA inherited many PIX features inculcating distinguished security interface levels. It is a combination of firewall, antivirus, intrusion prevention and virtual private network (VPN) defending against massive attacks in the network.

Prerequisites

- **EventTracker Agent v9.x** should be installed.
- **Cisco ASA 5500-X Series firewall** should be installed.

Configure ASA 5500-X Series firewall to send logs to EventTracker via CLI

1. Connect to your firewall using an SSH or Telnet client.
2. Login using administrative credentials for the firewall.
3. Type in the below commands in the CLI,

```
ASA> enable
ASA# configure terminal
ASA(config)# logging enable
ASA(config)# logging trap informational
ASA(config)# logging host <Interface_Name> <EventTracker_Agent_IP>
(e.g. ASA(config)# logging host inside 192.168.1.52)
ASA(config)# exit
ASA# write
```

Figure 1

4. Now, verify the syslog messages in **EventTracker**.

Configure ASA 5500-X Series firewall to send logs to EventTracker via ASDM.

1. Enable Logging

- Choose **Configuration** > **Device Management** > **Logging** > **Logging Setup** and check mark the **Enable logging** option as shown in the below image.

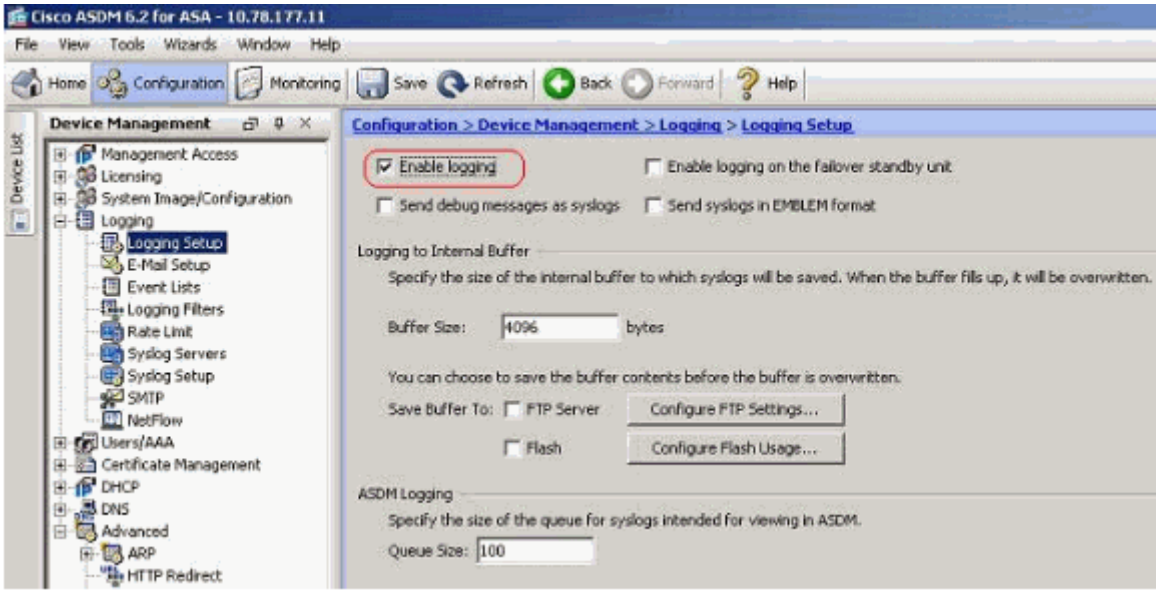

Figure 2

2. Logging to a Syslog Server

You can send all the syslog messages to a dedicated syslog server. Perform these steps by using ASDM:

- Choose **Configuration** > **Device Management** > **Logging** > **Syslog Servers** and click **Add** to add a syslog server. The Add Syslog Server window appears.

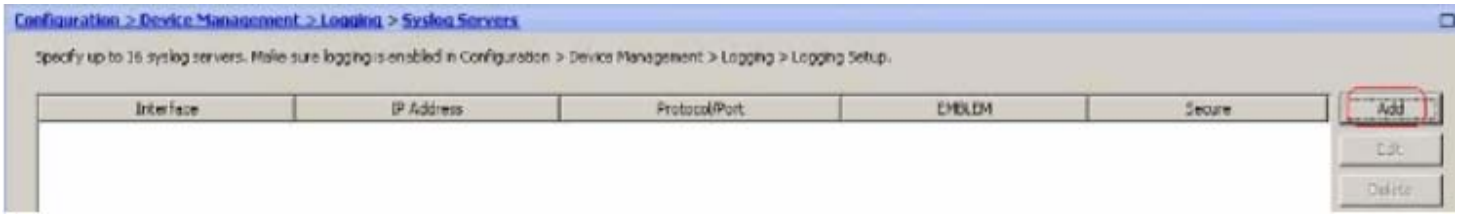

Figure 3

- Enter the following details as given below.
  - **Interface:** Specify an interface name from the dropdown.
  - **IP Address**: Enter the IP address of the **EventTracker Manager**.
  - **Protocol**: UDP
  - **Port**: 514
- Then, click **OK**.

Figure 4

NOTE: Make sure that you have reachability to the syslog server from the Cisco ASA.

- The configured syslog server is seen as shown here. Modifications can be done when you select this server, then click Edit.

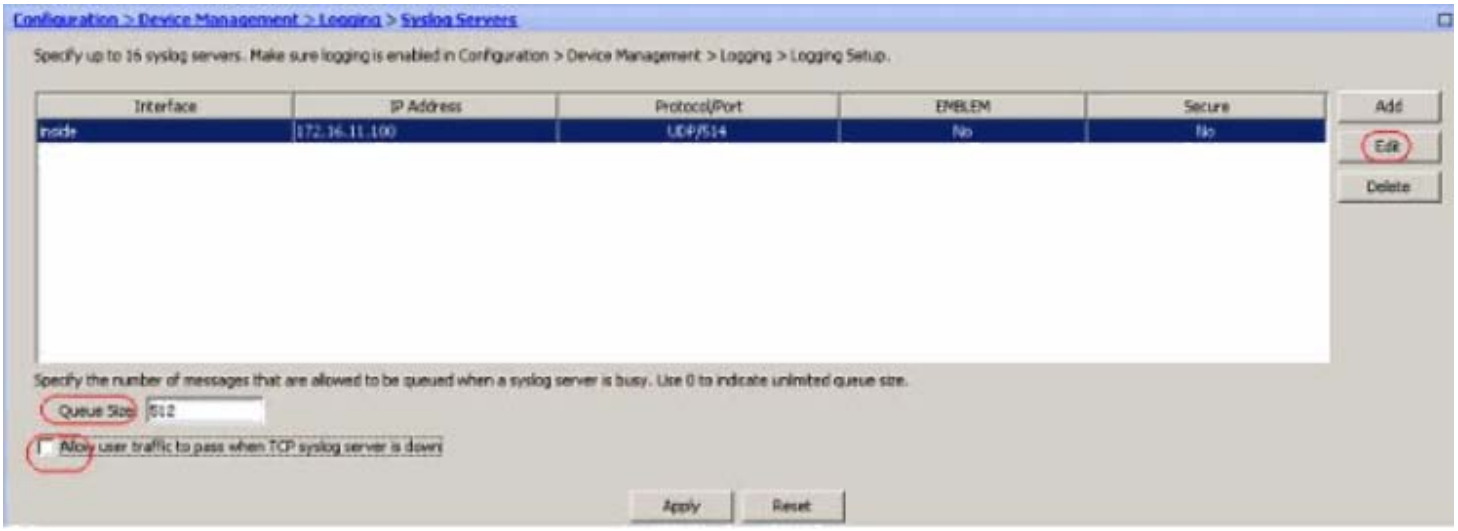

Figure 5

NOTE: Check the **Allow user traffic to pass when TCP syslog server is down** option. Otherwise, the new user sessions are denied through the ASA. This is applicable only when the transport protocol between the ASA and the syslog server is TCP. By default, new network access sessions are denied by the Cisco ASA when a syslog server is down for any reason.

3. Set Log Severity

- Choose **Configuration** > **Device Management** > **Logging** > **Logging Filters** and select the logging destination (**Syslog Server**). Then, click **Edit** to modify the settings.

Figure 6

- You can send the syslog messages based on the severity. Here, **Informational** must be selected as show in example.

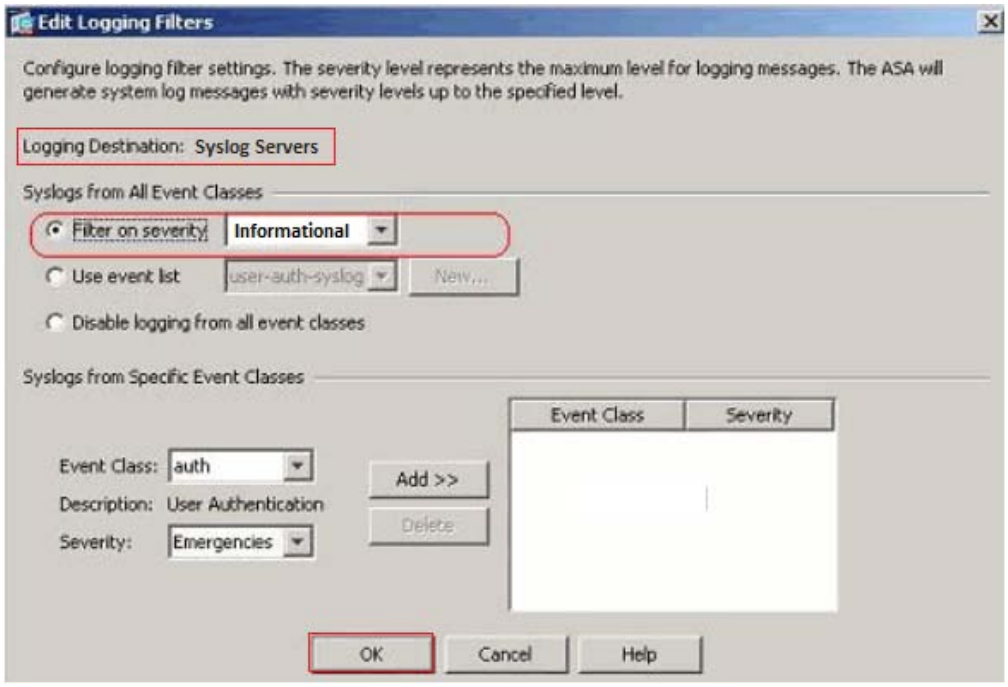

Figure 7

Then, click **OK**.