Integrate Cisco PIX 500 and ASA 5500 series Firewall

EventTracker Enterprise

Publication Date: May 9, 2016
Abstract

This guide helps you in configuring Cisco PIX 500 and ASA 5500 series Firewall to send logs to EventTracker Enterprise.

Audience

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

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.x and later, and Cisco PIX 500 and ASA 5500 series firewall.
## Table of Contents

Abstract .................................................................................................................................................. 1  
Audience .............................................................................................................................................. 1  
Scope ................................................................................................................................................... 1  
Overview ............................................................................................................................................. 3  
Prerequisites ........................................................................................................................................... 3  
Configure Cisco PIX 500 and ASA 5500 series firewall to send logs to EventTracker .................. 3  
  Cisco PIX and ASA Trap Levels ........................................................................................................... 4  
EventTracker Knowledge Pack ............................................................................................................. 4  
Import Cisco ASA knowledge pack into EventTracker ....................................................................... 7  
  Import Alerts ...................................................................................................................................... 8  
  Import Flex Reports ........................................................................................................................... 11  
  Import Parsing Rule .......................................................................................................................... 12  
  Import Template ............................................................................................................................... 13  
Verify Cisco ASA Knowledge Pack in EventTracker ....................................................................... 15  
  Verify Cisco ASA Alerts ................................................................................................................... 16  
  Verify Cisco ASA Flex Reports ........................................................................................................ 18  
  Verify Cisco ASA Parsing Rule ........................................................................................................ 18  
  Verifying Cisco ASA Template ......................................................................................................... 19  
Create Dashboards in EventTracker ................................................................................................... 20  
  Schedule Reports ............................................................................................................................. 20  
  Create Dashlets ............................................................................................................................... 22  
Sample Dashboards ............................................................................................................................. 26  
Sample Reports ...................................................................................................................................... 27
Overview

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

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

Cisco PIX supports both TCP and UDP. PIX can be configured using either a command line interface (CLI) or using PIX Device Manager (PDM), an HTML configuration application that comes with the PIX.

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 v7.x should be installed.
- Cisco PIX 500 and ASA 5500 series firewall should be installed.

Configure Cisco PIX 500 and ASA 5500 series firewall to send logs to EventTracker

1. Connect to your firewall using an SSH or Telnet client.
2. Login using administrative credentials for the firewall.
3. Enter `Enable` command.
4. Reenter the administrative password for the firewall.
5. Enter `configure terminal` command.
6. Enter `logging host` interface name EVENTTRACKER_IP_address.
   
   **NOTE:** EVENTTRACKER_IP_address is the IP address of your EVENTTRACKER Manager and interface name which the users have in their environment.

7. Enter `logging facility 2`. 
This defines where the EVENTTRACKER Manager will look for the firewall logs.

**NOTE:** The "logging facility" in Cisco products is equivalent to the local facility on the logging destination **plus 16**. For example, Cisco's logging facility 18 is the same as local facility 2 on your EVENTTRACKER Manager.

8. Enter **logging trap** level.

**Note:** Choose one of the logging levels listed below for the level value above. You can use either the Trap Level or Code for this value. We recommend using the **debug** logging level.

9. Enter **logging enable** command to enable logging with these settings.

10. Enter **exit** command to return to the previous prompt.

11. Run **copy running-config startup-config** or **write** command to save the configuration.

12. Now, verify the syslog messages in EventTracker manager.

### Cisco PIX and ASA Trap Levels

<table>
<thead>
<tr>
<th>Trap Level</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>0</td>
<td>Forwards only the highest priority messages, usually indicating failure or panic scenarios that must be addressed immediately.</td>
</tr>
<tr>
<td>Alert</td>
<td>1</td>
<td>Forwards messages that require immediate attention.</td>
</tr>
<tr>
<td>Critical</td>
<td>2</td>
<td>Forwards messages that should be reviewed as soon as possible and might be early warning signs of further problem.</td>
</tr>
<tr>
<td>Error</td>
<td>3</td>
<td>Forwards messages that might indicate a problem.</td>
</tr>
<tr>
<td>Warning</td>
<td>4</td>
<td>Forwards messages that should receive attention and might be errors.</td>
</tr>
<tr>
<td>Notification</td>
<td>5</td>
<td>Forwards messages that are considered to be important information, but that are not error conditions.</td>
</tr>
<tr>
<td>Information</td>
<td>6</td>
<td>Forwards most messages.</td>
</tr>
<tr>
<td>Debug</td>
<td>7</td>
<td>Forwards all messages, including IDS messages.</td>
</tr>
</tbody>
</table>

**Figure 1**

### EventTracker Knowledge Pack

Once Cisco ASA events are enabled and received in EventTracker then Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Cisco ASA monitoring.
Categories

- **Cisco ASA: Alert messages** – All alert messages logged by Cisco ASA. Severity 1.
- **Cisco ASA: All events** – All Syslog messages logged by Cisco ASA device.
- **Cisco ASA: Connection denied** – All Syslog messages logged by Cisco ASA when connection denied.
- **Cisco ASA: Critical alert** – All critical alert messages logged by Cisco ASA. Severity 1.
- **Cisco ASA: Critical messages** – All critical messages logged by Cisco ASA. Severity 2.
- **Cisco ASA: Debugging messages** – All debugging messages logged by Cisco ASA. Severity 7
- **Cisco ASA: Error messages** – All error messages logged by Cisco ASA. Severity 3.
- **Cisco ASA: IDS intrusion detection** – All Syslog messages logged by Cisco ASA related to Cisco Secure Intrusion Detection System.
- **Cisco ASA: Informational messages** – All informational messages logged by Cisco ASA. Severity 6.
- **Cisco ASA: Notification messages** – All notification messages logged by Cisco ASA. Severity 5.
- **Cisco ASA: Priv level changed** – All Syslog messages logged when privilege changes made in Cisco ASA device.
- **Cisco ASA: Security incidents detection** – All events logged by Cisco ASA when any security incidents detected.
- **Cisco ASA: User account locked out** – All Syslog messages logged by Cisco ASA when a user locked out on exceeding number successive failed authentication attempts
- **Cisco ASA: User account unlocked** – All Syslog messages logged by Cisco ASA when a user account unlocked by administrator.
- **Cisco ASA: User authentication failure** – All Syslog messages logged by Cisco ASA when authentication failed.
- **Cisco ASA: User authentication success** – All Syslog messages logged by Cisco ASA when authentication permitted for user.
- **Cisco ASA: User login failed** – All Syslog messages logged by Cisco ASA when User username did NOT have appropriate Admin Rights.
- **Cisco ASA: User password changed** – All Syslog messages logged by Cisco ASA when the user authenticated successfully after changing the password.

Alerts

- **Cisco ASA: Access denied** – This alert is generated when access denied event occurs.
- **Cisco ASA: Authentication failed** – This alert is generated when authentication failed event occurs.
- **Cisco ASA: Failover messages** – This alert is generated when failover event occurs.
• **Cisco ASA: IDS intrusion detection** - This alert is generated when IDS intrusion detection event occurs.

• **Cisco ASA: Security incidents detected** - This alert is generated when security incidents detected event occurs.

**Reports**

• **Cisco ASA: User account locked out**
  This flex report provides information related to user account locked out. It gives the user account name and reason why it is locked out.

• **Cisco ASA: User account unlocked**
  This flex report provides information related to user account unlocked. It gives the user account name and who has unlocked the user account.

• **Cisco ASA: Privilege level changed**
  This flex report provides information related to user privilege level changed. It shows from which level to which level user privilege changed by whom.

• **Cisco ASA: Attack detected**
  This flex report provides information related to failure attacks that have occurred from which source address to which targeted address.

• **Cisco ASA: Security incident**
  This flex report provides information related to security incident detection.

• **Cisco ASA: Traffic details**
  This flex report provides information related to access and denied traffic. It gives information about traffic direction, source and destination address and port, bytes transfer, duration for connection and its status.

• **Cisco ASA: User authentication failed**
  This flex report provides information related to user authentication failed. It gives the information about authentication failed for username, Source IP, Source port no. and Target IP, Target port no.

• **Cisco ASA: User authentication success**
  This flex report provides information related to user authentication success. It gives the information about authentication success for username, Source IP, Source port no. and Target IP, Target port no.

• **Cisco ASA: User login failed**
  This flex report provides information related to user login failed. It gives information which user, from source IP and port no. login failed and what was the logon type.
• **Cisco ASA: User password changed**
  This flex report provides information related to user password changed. It gives information about for which user password has been changed.

• **Cisco ASA: Connection denied**
  This flex report provides information related to traffic denied by firewall. It gives information about traffic direction, source and destination address and port, protocol details.

**Import Cisco ASA knowledge pack into EventTracker**

Following are the steps for importing KP items in EventTracker Manager.

1. Open EventTracker Control Panel
2. Click on Export Import Utility
Figure 2

Note: please follow the following sequence for uploading the KP items:

Categories > alerts > parsing rules and template > flex reports

Import Category

1. Click Category option, and then click the browse button.
2. Locate All Cisco ASA group of Categories.iscat file, and then click the Open button.

3. To import the categories, click the Import button.

   EventTracker displays success message.

   ![Export Import Utility](image)

   Figure 4

4. Click OK, and then click the Close button.
Import Alerts

1. Click the Alert option and then click the browse button.

![Image of Import Utility dialog box]

Figure 5

2. Locate All Cisco ASA group of Alerts.isalt file, and then click the Open button.

3. To import alerts, click the Import button.

   EventTracker displays success message.
4. Click OK, and then click the Close button.

Import Flex Reports

1. Click Reports option, and then click the browse button.
2. Locate All Cisco ASA group reports.issch file, and then click the Open button.

3. To import reports, click the Import button.
EventTracker displays success message.

![Success Message]

**Figure 8**

4. Click **OK**, and then click the **Close** button.

**Import Parsing Rule**

1. Click **Token value** option, and then click the **browse** button.

![Import Parsing Rule]

**Figure 9**

2. Locate the .istoken file, and then click the **Open** button.

3. To import tokens, click the **Import** button.
EventTracker displays success message.

![Export Import Utility]

**Figure 10**

4. Click OK, and then click the Close button.

**Import Template**

1. Logon to EventTracker Enterprise.
2. Click the Admin menu and then click the Parsing rule.
3. Click the Template tab.
4. Click the Import button, it will open new window. (Note: Make sure pop-up is enable for EventTracker)
5. Locate and Choose All Cisco ASA group of Token Templates.ETTD file and then click the Open button.

6. Select the template you want to upload.
7. Then click on Import configuration button.
8. Click OK it will automatically close the window

Verify Cisco ASA Knowledge Pack in EventTracker

Verify Cisco ASA Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. In the Category Tree, expand Cisco ASA group folder to view the imported categories.
Verify Cisco ASA Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In Search field, type ‘Cisco ASA’, and then click the Go button.

Alert Management page will display all the imported Cisco ASA alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

![Message from webpage](image)

**Figure 17**

5. Click **OK**, and then click the **Activate Now** button.

**NOTE:**

You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.
Verify Cisco ASA Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click Cisco ASA group folder.
5. Scheduled Reports are displayed in the Reports configuration pane.

![Image of Reports Configuration]

Figure 18

Verify Cisco ASA Parsing Rule

1. Click the Admin menu, and then click Parsing rule.
2. Scroll and find imported Parsing rule.
Verifying Cisco ASA Template

1. Logon to EventTracker Enterprise, Go to Parsing rule.
2. Click on Template tab.
3. Check the template you have uploaded in Cisco ASA group
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.
2. Navigate to Reports > Configuration.

![Figure 22](image)

3. Select Cisco ASA in report groups. Check defined dialog box.

4. Click on ‘schedule’ to plan a report for later execution.

![Figure 23](image)
5. Choose appropriate time for report execution and in Step 8 check Persist data in Eventvault explorer box.

6. Check column names to persist using PERSIST checkboxes beside them. Choose suitable Retention period.
7. Proceed to next step and click Schedule button.
8. Wait for scheduled time or generate report manually.

Create Dashlets

1. EventTracker Enterprise is required to configure flex dashboard.
2. Open EventTracker in browser and logon.
3. Navigate to Dashboard > Flex. Flex Dashboard pane is shown.

4. Click + to add a new dashboard. Flex Dashboard configuration pane is shown.

5. Fill fitting title and description and click Save button.
6. Click 🔄 to configure a new flex dashlet. Widget configuration pane is shown.
7. Locate earlier scheduled report in Data Source dropdown.
8. Select Chart Type from dropdown.
9. Select extent of data to be displayed in Duration dropdown.
10. Select computation type in Value Field Setting dropdown.
11. Select evaluation duration in As Of dropdown.
12. Select comparable values in X Axis with suitable label.
13. Select numeric values in Y Axis with suitable label.
14. Select comparable sequence in Legend.
15. Click Test button to evaluate.

Evaluated chart is shown
1. If satisfied, click **Configure** button.

2. Click ‘customize’ to locate and choose created dashlet.
3. Click + to add dashlet to earlier created dashboard.
Sample Dashboards


![Cisco ASA Security Incidents](image1)

*Figure 31*

2. Cisco ASA Failure Attacks

![Cisco ASA Failure Attacks](image2)

*Figure 32*
3. Top protocol used in traffic

![Top Protocols Used in Traffic](image)

Figure 33

Sample Reports

### Cisco ASA Security Incidents Report

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Protocol Type</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Access type</th>
<th>Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/18/2015 02:14:30 PM</td>
<td>ASA-ASA</td>
<td>UDP</td>
<td>192.72.211.60/35465</td>
<td>192.168.2.34/467</td>
<td>interface</td>
<td>interface ramps</td>
</tr>
<tr>
<td>11/18/2015 02:14:30 PM</td>
<td>ASA-ASA</td>
<td>UDP</td>
<td>192.72.211.61/35465</td>
<td>192.168.1.256/233</td>
<td>interface</td>
<td>icmp</td>
</tr>
<tr>
<td>11/18/2015 02:14:30 PM</td>
<td>ASA-ASA</td>
<td>UDP</td>
<td>192.72.211.62/35465</td>
<td>192.168.2.35/467</td>
<td>interface</td>
<td>interface ramps</td>
</tr>
<tr>
<td>11/18/2015 02:14:30 PM</td>
<td>ASA-ASA</td>
<td>UDP</td>
<td>192.72.211.63/35465</td>
<td>192.168.1.262/233</td>
<td>interface</td>
<td>icmp</td>
</tr>
<tr>
<td>11/18/2015 02:14:30 PM</td>
<td>ASA-ASA</td>
<td>UDP</td>
<td>192.72.211.64/35465</td>
<td>192.168.1.263/233</td>
<td>interface</td>
<td>icmp</td>
</tr>
<tr>
<td>11/18/2015 02:14:31 PM</td>
<td>ASA-ASA</td>
<td>ICMP</td>
<td>10.4.4.2</td>
<td>10.2.1.1</td>
<td>interface</td>
<td>dnz</td>
</tr>
<tr>
<td>11/18/2015 02:14:31 PM</td>
<td>ASA-ASA</td>
<td>ICMP</td>
<td>10.1.1.1</td>
<td>192.168.1.1</td>
<td>interface</td>
<td>outside Snort attack</td>
</tr>
<tr>
<td>11/18/2015 02:14:31 PM</td>
<td>ASA-ASA</td>
<td>ICMP</td>
<td>10.4.4.2</td>
<td>10.2.1.1</td>
<td>interface</td>
<td>dnz</td>
</tr>
<tr>
<td>11/18/2015 02:14:31 PM</td>
<td>ASA-ASA</td>
<td>ICMP</td>
<td>10.4.4.2</td>
<td>10.2.1.1</td>
<td>interface</td>
<td>dnz</td>
</tr>
<tr>
<td>11/18/2015 02:14:31 PM</td>
<td>ASA-ASA</td>
<td>ICMP</td>
<td>10.4.4.2</td>
<td>10.2.1.1</td>
<td>interface</td>
<td>dnz</td>
</tr>
<tr>
<td>11/18/2015 02:14:31 PM</td>
<td>ASA-ASA</td>
<td>ICMP</td>
<td>10.4.4.2</td>
<td>10.2.1.1</td>
<td>interface</td>
<td>dnz</td>
</tr>
<tr>
<td>11/18/2015 02:14:31 PM</td>
<td>ASA-ASA</td>
<td>ICMP</td>
<td>10.4.4.2</td>
<td>10.2.1.1</td>
<td>interface</td>
<td>dnz</td>
</tr>
<tr>
<td>11/18/2015 02:14:31 PM</td>
<td>ASA-ASA</td>
<td>ICMP</td>
<td>10.4.4.2</td>
<td>10.2.1.1</td>
<td>interface</td>
<td>dnz</td>
</tr>
</tbody>
</table>

2. Cisco ASA Failure Attacks
### Cisco ASA Failure Attacks reports

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Source IP Address</th>
<th>Source Port</th>
<th>Target IP Address</th>
<th>Target Port Number</th>
</tr>
</thead>
</table>

### Cisco ASA – Connection denied

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Traffic Direction</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Access List</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/11/2016 06:07:28 PM</td>
<td>inbound</td>
<td>124.30.163.162</td>
<td>69500</td>
<td>69.163.162.12.22</td>
<td>12</td>
<td>TCP</td>
<td>denied</td>
<td></td>
</tr>
<tr>
<td>04/11/2016 06:07:28 PM</td>
<td>inbound</td>
<td>20.2.128.1</td>
<td>105.8.128.1</td>
<td>105.8.128.1</td>
<td>105.8.128.1</td>
<td>deny</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04/11/2016 06:07:28 PM</td>
<td>inbound</td>
<td>20.2.128.1</td>
<td>105.8.128.1</td>
<td>105.8.128.1</td>
<td>105.8.128.1</td>
<td>deny</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04/11/2016 06:07:28 PM</td>
<td>outbound</td>
<td>124.10.163.6</td>
<td>59000</td>
<td>124.10.163.6</td>
<td>59000</td>
<td>TCP</td>
<td>denied</td>
<td></td>
</tr>
<tr>
<td>04/11/2016 06:07:28 PM</td>
<td>outbound</td>
<td>124.10.163.6</td>
<td>59000</td>
<td>124.10.163.6</td>
<td>59000</td>
<td>TCP</td>
<td>denied</td>
<td></td>
</tr>
<tr>
<td>04/11/2016 06:07:28 PM</td>
<td>outbound</td>
<td>124.10.163.6</td>
<td>59000</td>
<td>124.10.163.6</td>
<td>59000</td>
<td>TCP</td>
<td>denied</td>
<td></td>
</tr>
</tbody>
</table>

---

**Figure 35**

**Figure 36**