Integrating Juniper NetScreen (ScreenOS)
Abstract

This guide provides instructions to configure Juniper NetScreen (ScreenOS) to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.X and later, and Juniper NetScreen (ScreenOS) 5.2.0 and later.

Audience

Administrators who are assigned the task to monitor and manage Juniper NetScreen events using EventTracker.
# Table of Contents

Abstract .................................................................................................................................................. 1
Overview................................................................................................................................................ 3
Prerequisites.......................................................................................................................................... 3
Configuration......................................................................................................................................... 3
  Configure Syslog logging..................................................................................................................... 3
EventTracker Knowledge Pack ............................................................................................................ 4
  Categories.......................................................................................................................................... 4
  Alerts.................................................................................................................................................. 5
  Reports.............................................................................................................................................. 5
Import Juniper NetScreen knowledge pack into EventTracker............................................................ 7
  Import Category ................................................................................................................................. 7
  Import Alerts .................................................................................................................................... 8
  Import Flex Reports .......................................................................................................................... 9
  Import Template ............................................................................................................................... 10
Verify Juniper NetScreen knowledge pack in EventTracker............................................................... 13
  Verify Juniper NetScreen Categories.............................................................................................. 13
  Verify Juniper NetScreen Alerts ...................................................................................................... 13
  Verify Juniper NetScreen Reports .................................................................................................. 15
Verifying Template .................................................................................................................................. 16
Sample Reports ...................................................................................................................................... 17
Overview

The Juniper Networks NetScreen Series Security Systems are ideally suited for large enterprise network backbones, including departmental or campus segmentation, Enterprise data centers for securing high-density server environments and carrier-based managed services or core infrastructure.

Prerequisites

- EventTracker 7.x and later should be installed.
- Juniper ScreenOS 5.2.x and later should be installed on Juniper NetScreen.
- Administrative access on the EventTracker Enterprise and Juniper NetScreen.
- An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.
- Port 514 should be opened on Juniper NetScreen (ScreenOS).

Configuration

To monitor Juniper NetScreen in EventTracker, configure Juniper NetScreen to send all events as Syslog to the EventTracker system.

Configure Syslog logging

1. Login into WebUI of Juniper NetScreen.
2. Expand Configuration and select Report Settings, and then click Syslog.
3. Check ‘Enable Syslog Messages’ to enable Syslog.

Figure 1
4. In the **Syslog Host Name/Port** field, type the IP address of the EventTracker Manager.
5. Click **Apply**.

**EventTracker Knowledge Pack**

Once Juniper NetScreen events are enabled and Juniper NetScreen events are received in EventTracker, the Categories, Alerts and Flex based Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Juniper NetScreen monitoring.

**Categories**

- **NetScreen: Account management** - This category based report provides information related to account management.
- **NetScreen: Administration** - This category based report provides information related to administration.
- **NetScreen: All events** - This category based report provides information related to all events of NetScreen.
- **NetScreen: Antivirus** - This category based report provides information related to antivirus.
- **NetScreen: Firewall policy** - This category based report provides information related to firewall policy.
- **NetScreen: Firewall traffic allowed** - This category based report provides information related to firewall traffic allowed.
- **NetScreen: Firewall traffic denied** - This category based report provides information related to firewall traffic denied.
- **NetScreen: Intrusion detection** - This category based report provides information related to Intrusion detection.
- **NetScreen: Network services** - This category based report provides information related to network services.
- **NetScreen: Security device events** - This category based report provides information related to security device events.
- **NetScreen: System authentication** - This category based report provides information related to system authentication.
- **NetScreen: System services** - This category based report provides information related to system services.
- **NetScreen: URL allowed** - This category based report provides information related to URL allowed.
- **NetScreen: URL blocked** - This category based report provides information related to URL blocked.
- **NetScreen: User authentication** - This category based report provides information related to user authentication.
Integrating Juniper NetScreen

- **NetScreen: Virtual router** - This category based report provides information related to virtual router.
- **NetScreen: Virtual systems** - This category based report provides information related to virtual systems.
- **NetScreen: VPN** - This category based report provides information related to VPN.
- **NetScreen: Web filtering** - This category based report provides information related to Web filtering.

Alerts

- **NetScreen: Authentication failure** - This alert is generated when system or user related authentication fails.
- **NetScreen: IDS intrusion detection** - This alert is generated when attacks are detected through NetScreen.
- **NetScreen: Security device error** - This alert is generated when response to problems or processes that occur at the hardware or Screen OS level.
- **NetScreen: Spam found** - This alert is generated when spam found.
- **NetScreen: System configuration erased** - This alert is generated when system configuration gets erased.
- **NetScreen: USB storage device attached/detached** - This alert is generated when USB storage device is attached/detached.
- **Juniper NetScreen-IP address conflict** - This alert is generated when IP address conflict occurs.
- **Juniper NetScreen-VPN service down** - This alert is generated when VPN service is down.

Reports

- **Juniper NetScreen: User Logon Success Report**: This report provides information related to user logon success for different logon types like SSH, Console, Telnet etc.
- **Juniper NetScreen: User Logoff Report**: This report provides information related to user logoff from different terminals.
- **Juniper NetScreen: User Authentication Success Report**: This report provides information related to authentication success done for different users from different source addresses.
- **Juniper NetScreen: User Authentication Failed Report**: This report provides information related to authentication failure for different users with what reasons.
- **Juniper NetScreen: Intrusion Detection Report**: This report provides information related with source IP and ports, destination IP and ports (victim details) and intrusion occurs in NetScreen firewall.
- **Juniper NetScreen: Account Management Report**: This report provides information related with creation, deletion and modification of user, group and account of NetScreen and by whom it is done.
- **Juniper NetScreen: System Authentication Report**: This report provides information related with MAC address of systems authenticated with NetScreen firewall.
- **Juniper NetScreen: URL Allowed or Blocked Report**: This report provides information related with URL blocked and allowed with source IP of system trying to access it.
- **Juniper NetScreen: Firewall Policy Change Report**: This report provides information related with changes in firewall policy component and by whom it is done.
- **Juniper NetScreen: USB Storage Device Attached and Detached Report**: This report provides information related with attached and detached of USB devices with NetScreen.
- **Juniper NetScreen: Web Filtering Report**: This report provides information about the changes in category and profiles of web filtering in NetScreen and by whom.
- **Juniper NetScreen: Traffic allowed and blocked report**: This report provides information related with what kind of traffic are allowed and blocked in NetScreen firewall.
- **Juniper NetScreen: Administration**: This report provides information related with the configuration changes happen and by whom it is done in NetScreen firewall.
- **Juniper NetScreen-DHCP server operations** - This report provides information related to DHCP server operations which include IP address, MAC address, status and reason from fields.
- **Juniper NetScreen-VPN service status** - This report provides information related to VPN service status which includes VPN name, source address and status from fields.
Import Juniper NetScreen knowledge pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility, and then click Import tab.
   Import Category/Alert/Flex Reports/Template as given below.

Import Category

1. Click Category option, and then click the browse button.

![Export Import Utility](image)

2. Locate All Juniper NetScreen group of Categories.iscat file, and then click the Open button.
3. To import categories, click the Import button.
   EventTracker displays success message.
4. Click **OK**, and then click the **Close** button.

### Import Alerts

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

2. Locate **All Juniper NetScreen group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
EventTracker displays success message.

![Selected alert configurations are imported successfully.](image)

**Figure 4**

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

**Import Flex Reports**

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

![Export Import Utility](image)

**Figure 6**
2. Locate **All Juniper NetScreen group of Report .issch** file, and then click the **Open** button.
3. To import flex report, click the **Import** button.
   EventTracker displays success message

![Export Import Utility](image)

*Figure 7*

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 and it will open a new window.
   *(Note: Make sure pop-up is enabled for EventTracker)*
5. Locate and select the .ETTD file and then click the **Open** button.

6. Select the template that you want to upload.
7. Click on the **Import configuration** button.

![Figure 10](image1.jpg)

**Figure 10**

EventTracker displays success message.

![Figure 11](image2.jpg)

**Figure 11**

8. Click **OK** and it will automatically close the window.
Verify Juniper NetScreen knowledge pack in EventTracker

Verify Juniper NetScreen Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand Juniper NetScreen group folder to view the imported categories.

![Category Management](image)

Figure 12

Verify Juniper NetScreen Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In Search field, type 'Juniper NetScreen', and then click the Go button.
   Alert Management page will display all the imported Juniper NetScreen alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Message from webpage](image)

**Figure 13**

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

**NOTE:** You can select alert notifications 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 Juniper NetScreen Reports

1. Logon to EventTracker Enterprise.
2. Click the Report Option and select Defined.
3. In Report Group Tree, to view imported reports, scroll down and expand Juniper NetScreen report group folder for the imported reports.

![Figure 15](image-url)
Verifying Template

1. Logon to EventTracker Enterprise and go to Parsing rule.
2. Click on Template tab.
3. Check the template you have uploaded.

Figure 16
Sample Reports


![Figure 17](image-url)

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User or Group</th>
<th>Changes</th>
<th>By Whom</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/01/2015 04:21:37 PM</td>
<td>NETSCREEN</td>
<td>user john</td>
<td>enabled</td>
<td>admin</td>
</tr>
<tr>
<td>07/01/2015 04:21:37 PM</td>
<td>NETSCREEN</td>
<td>user john</td>
<td>enabled</td>
<td>admin</td>
</tr>
<tr>
<td>07/01/2015 04:21:37 PM</td>
<td>NETSCREEN</td>
<td>group Marketing</td>
<td>modified</td>
<td>admin</td>
</tr>
<tr>
<td>07/01/2015 04:21:37 PM</td>
<td>NETSCREEN</td>
<td>group HR</td>
<td>deleted</td>
<td>admin</td>
</tr>
<tr>
<td>07/01/2015 04:21:37 PM</td>
<td>NETSCREEN</td>
<td>group Finance</td>
<td>created</td>
<td>admin</td>
</tr>
<tr>
<td>07/01/2015 04:21:37 PM</td>
<td>NETSCREEN</td>
<td>user john</td>
<td>enabled</td>
<td>admin</td>
</tr>
</tbody>
</table>
2. Juniper NetScreen: Intrusion Detection Report

### Juniper NetScreen: Intrusion Detection Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Source IP and Port</th>
<th>Destination IP and Port</th>
<th>Attack Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/01/2015 07:12:23 PM</td>
<td>NETSCREEN</td>
<td>192.168.1.1</td>
<td>192.168.2.1</td>
<td>ActiveX control blocked</td>
</tr>
<tr>
<td>07/01/2015 07:12:23 PM</td>
<td>NETSCREEN</td>
<td>192.168.1.1</td>
<td>224.0.0.22</td>
<td>IP spoofing</td>
</tr>
<tr>
<td>07/01/2015 07:12:23 PM</td>
<td>NETSCREEN</td>
<td>192.168.1.1:35834</td>
<td>192.168.2.1:1514</td>
<td>UDP flood</td>
</tr>
<tr>
<td>07/01/2015 07:12:23 PM</td>
<td>NETSCREEN</td>
<td>192.168.1.1</td>
<td>192.168.2.1</td>
<td>Java applet blocked</td>
</tr>
<tr>
<td>07/01/2015 07:12:23 PM</td>
<td>NETSCREEN</td>
<td>192.168.1.1</td>
<td>192.168.2.1</td>
<td>Java applet blocked</td>
</tr>
</tbody>
</table>

Figure 18