Zscaler Proxy

Deployment Guide

Published on November 02, 2021

SECURONIX
Security Analytics. Delivered.

Securonix proprietary statement

This material constitutes proprietary and trade secret information of Securonix, and shall not be disclosed to any third party, nor used by the recipient except under the terms and conditions prescribed by Securonix. The trademarks, service marks, and logos of Securonix and others used herein are the property of Securonix or their respective owners.

Securonix copyright statement

Contact information

Securonix

5080 Spectrum Drive Suite 950W

Addison, TX 75001

(855) 732-6649

Table of Contents

Introduction

A connector is used to establish communication between the SNYPR application and a datasource. Following a successful deployment, the connector makes data from a datasource available to query and view in the SNYPR application.

The instructions in this deployment guide describe how to deploy Zscaler Proxy security log data in the SNYPR application.

> **Note:** The images in this guide are for illustrative purposes only. Images may differ from the actual product due to product enhancements.

About Zscaler Proxy

Zscaler Proxy is a cloud security platform that delivers a complete security stack as a cloud service, eliminating the cost and complexity of traditional secure web gateway appliances. By moving security to a globally distributed cloud, Zscaler brings the Internet and web gateway closer to the user for a faster experience. Organizations can easily scale protection to all mobile users or offices through local Internet breakouts and minimize the network and appliance infrastructure.

The following properties are specific to the Zscaler Proxy connector:

- **Collection Method**: Syslog
- **Format**: CEF
- **Functionality**: Web Proxy
- **Parser**: SCNX_ZSCALER_ZSCALERPROXY_PXY_SYS_CEF
- **Vendor Version**:

- **Windows**: 3.1.0.96
- **Mac**: 3.2.0.62

Prerequisites

Before you connect Zscaler Proxy, ensure you have the Remote Ingestion Node (RIN) details to send data.

Configure Zscaler Proxy

Complete the following steps to configure the Zscaler Proxy connection:

1. Log in to the administration portal for Zscaler NSS.
2. In the navigation pane, select **Administration > Settings > Nanolog Streaming Service**.
3. From the **NSS Feeds** tab, click **Add NSS Feed**.
4. Complete the following information:
    - **Feed Name**: Type the name of the NSS feed.
    - **NSS Type**: Keep the default, **NSS for Web**.
    - **NSS Server**: Select the ZScaler NSS system.
    - **Status**: Select **Enabled**.
    - **SIEM IP Address**: Enter the IP address of the RIN.
    - **SIEM TCP Port**: Enter **514**.
    - **Log Type**: Select **Alerts**, and then choose which alert levels you want to send.
5. Click **Save** and then activate your changes.
6. Verify logs are being received on the RIN using the following command:

    ```
    tcpdump -i eth0 udp port 514 -v -A
    ```

    The logs will look similar to the following example:

    ```
    Nov 2 08:00:00 zscaler-nss
    CEF:0|Zscaler|NSSWeblog|5.0|Allowed|Allowed|3|act=Allowed
    app=HTTPS cat=Bypass Salesforce
    dhost=securonix.lightning.force.com dst=101.53.162.79
    src=114.124.131.105 in=722 outcome=200 out=1784
    ```

```
request=securonix.lightning.force.com/cometd/45.0/ rt=Nov
02 2021 08:00:00 sourceTranslatedAddress=114.124.131.105
requestClientApplication=Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.69 Safari/537.36 requestMethod=POST
suser=dewi.sawitri@aux.securonix.com spriv=Road Warrior
externalId=7025755607084892167 fileType=GZIP reason=Allowed
destinationServiceName=Salesforce cn1=10 cn1Label=riskscore
cs1=MERCHANT KYC QUALITY CONTROL cs1Label=dept cs2=User-
defined cs2Label=urlsupercat cs3=Business cs3Label=appclass
cs4=None cs4Label=malwarecat cs5=None cs5Label=threatname
cs6=None cs6Label=dlpeng ZscalerNSSWeblogURLClass=Bandwidth
Loss ZscalerNSSWeblogDLPDictionaries=None
requestContext=securonix.lightning.force.com/lightning/r/ac
count/0012s00000aobrzaan/view?ws=/lightning/r/Outlet__
c/a0L2s000000MAQ8EAO/view contenttype=application/json
unscannabletype=None deviceowner=dewi.sawitri
devicehostname=GF030000427145
```

Configure Zscaler Proxy in SNYPR

Complete the following steps to configure Zscaler Proxy in the SNYPR application:

Step 1. Resource group information

Follow the following steps if you are using SNYPR 6.3.1:

1. Navigate to **Menu > Add Data > Activity** in the SNYPR application.
2. Click **Add Data > Add Data for Supported Device Type** to setup the ingestion process.
3. Click **Vendor** in the **Resource Type Information** section and select the following information:
    - **Vendors**: Zscaler
    - **Device Types**: Zscaler Proxy
    - **Collection Method**: CEF[SYSLOG]
4. Perform the following steps in the **Ingesters** section:
    a. Select an ingester from the list.
    b. Click **+** to add a filter for the ingester, and then provide the following information:

i. Provide a name for the filter.

ii. Add the following syslog expression to identify events that are associated with the device:

```
{host("10.0.0.1");};
```

> **Note:** The IP address is the address of the host initiating the traffic.

iii. Click **Add** to add the filter.

5. Complete the following information in the **Device Information** section:
   - **Datasource Name**: Zscaler Proxy
   - **Specify timezone for activity logs**: Select a time zone from the list.
6. Click **Get Preview** in the upper right corner of the page to preview the ingested data from the datasource.
7. Click **Save & Next**.

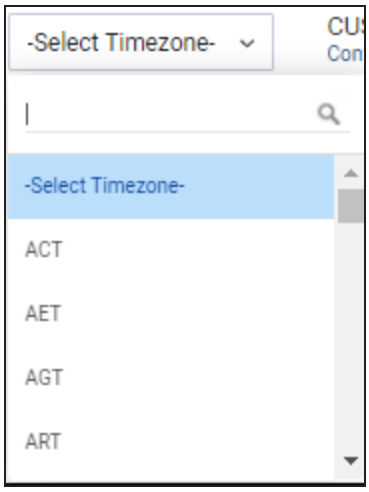
Follow the following steps if you are using SNYPR 6.4:

1. Navigate to **Menu > Add Data > Activity** in the SNYPR application.
2. Click **Discovered**. The section displays a list of discovered devices by recommended parsers.

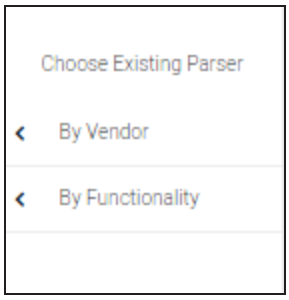
   > **Note:** Note: You can locate a datasource/device by specifying CIDR or keyword in the Search field.

3. Review discovered devices to locate devices that you want to onboard.
4. Select a resource or any number of resources to view details on the right-section of the screen.

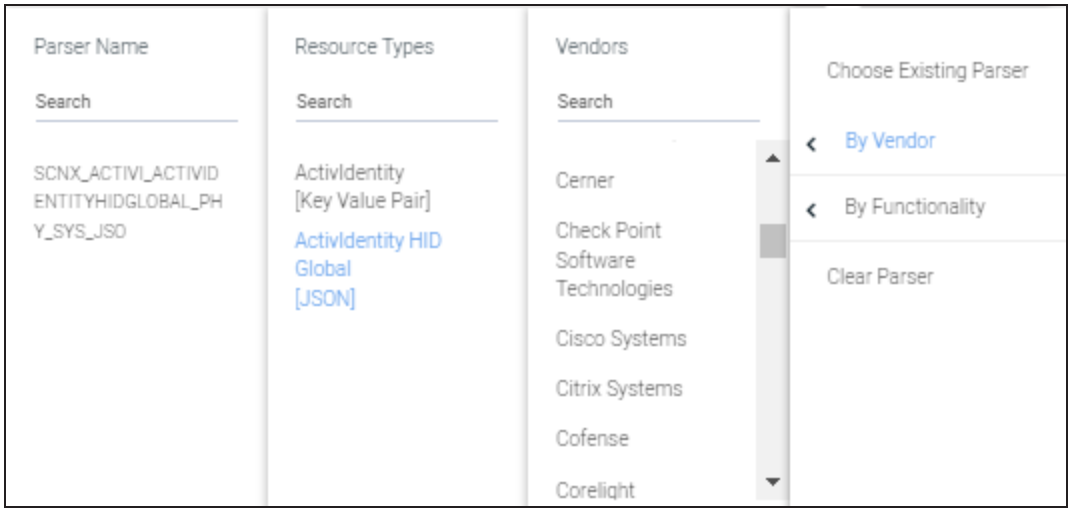
5. In the right section of the screen, select a resource and click **Select Timezone**. The **Select Timezone** drop-down list is displayed.



6. Select a timezone.
7. Review and select the existing parser, or you can search for another parser by performing the following steps:
    i. Select **By Vendor** from **Choose Existing Parser**.



    ii. Click **Vendors** > **Resource Types** > **Parser Name**. The following image is just for reference:



For Zscaler Proxy, select the following information:

- **Vendors**: Zscaler
- **Resource Types**: Zscaler Proxy
- **Parser Name**: SCNX_ZSCALER_ZSCALERPROXY_PXY_SYS_CEF

8. Click **Get Preview** in the upper right corner of the page to preview the ingested data from the datasource.
9. Click **Save & Next**.

Step 2. Parser management

Click **Save & Next**.

Step 3. Identity attribution

1. Click **Add Condition > Add New Correlation Rule** to add a correlation rule.
2. Provide a descriptive name for the correlation rule in the **Correlation Rule** section.

> **Note:** For more information on Identity Attribution, refer to the SNYPR 6.4 Data Integration Guide.

3. Specify the **User Attribute**, **Operation**, **Parameter**, **Condition**, and **Separator** parameters in the **Correlate events to user using rule** section.
4. Click **Save** in the lower-right corner of the page to save the **Correlate events to user using rule** table.
5. Click **Save & Next** in the upper-right corner of the page.

Step 4. Detect policy violations

Click **Save & Next**.

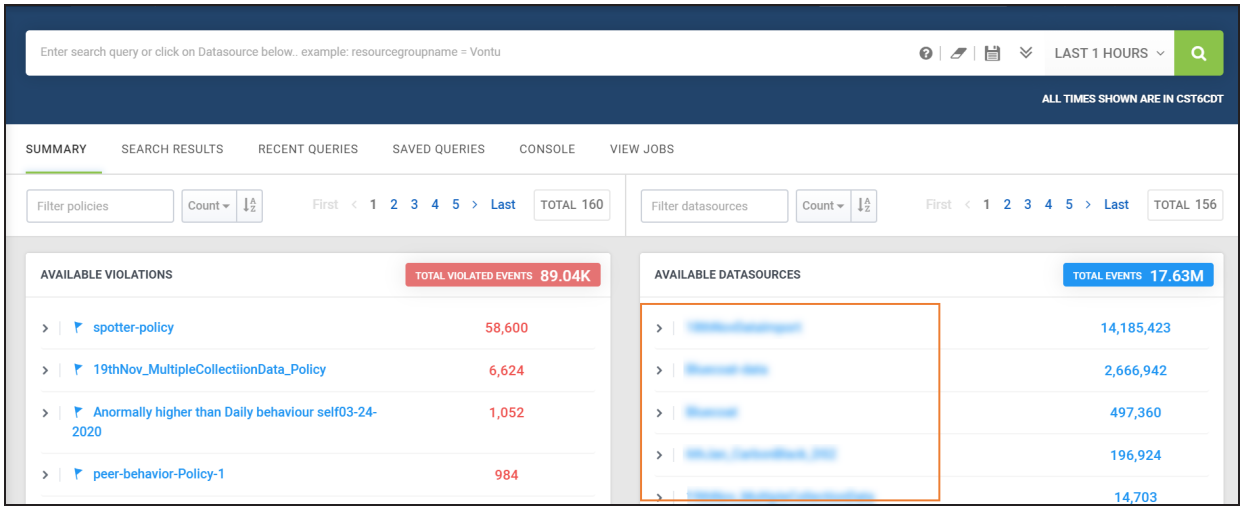
Step 5. Summary

1. Select **Do you want to schedule this job for future?** in the **Job Scheduling Information** section and select any of the following based on the collection method:
    - Run every 1 minutes for datasources with the collection method as syslog.
    - Run every 10 minutes for non-syslog based datasources.
2. Click **Save & Run**.

Verifying the job

Following a successful import, the security log data for the datasource is accessible in the **Available Datasources** section of Spotter. To access the imported security log data, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Enter the datasource name provided while creating the connection, and then click the magnifying glass icon in the search bar.



Note: Refer to the Spotter Query Reference Guide for information on how to write queries in Spotter.