Zscaler Deployment Guide

Jan 2022

For the latest documentation, please go to
https://docs.arcticwolf.com/syslog/zscaler_syslog.html

ARCTIC WOLF

Syslog Configuration for ZScaler

Configuration Guide

PRODUCT DOCUMENTATION

Syslog Configuration for ZScaler

Overview

This document describes how to configure the Nanolog Streaming Service (NSS) to send syslog-formatted messages from ZScaler device(s) to your Arctic Wolf® sensor. Arctic Wolf supports the `QRadar LEEF` feed output type.

Before you begin, you need to have the Nanolog Streaming Service virtual appliance installed and configured to stream web logs from your ZScaler device(s). For more information, see About Nanolog Streaming Service (NSS) and the NSS Configuration Guide on the Zscaler support website.

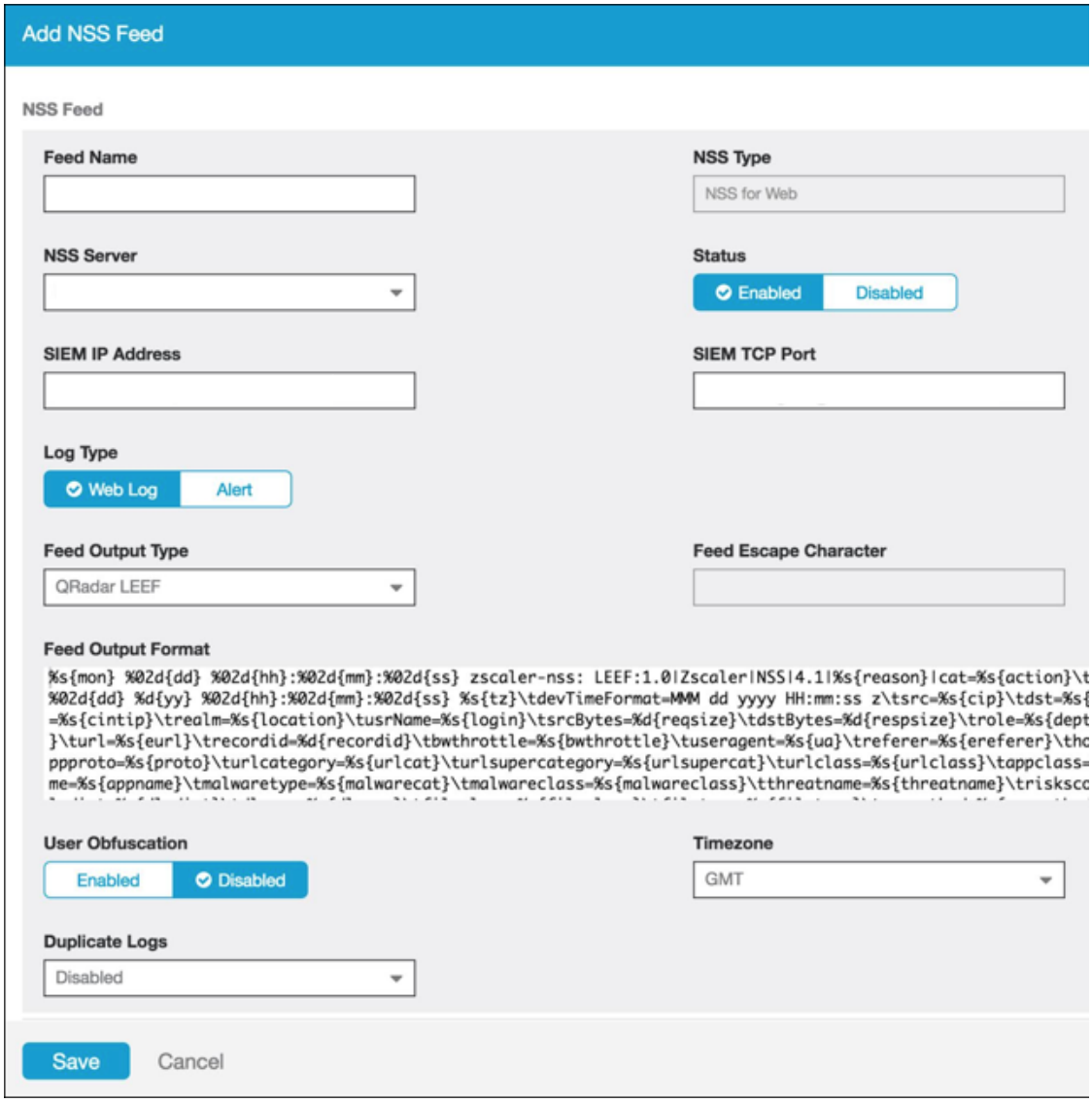
Configure ZScaler Nanolog Streaming Service

To configure your ZScaler NNS:

1. Access your ZScaler NSS web administration interface and log in with appropriate credentials.
2. Select **Administration** > **Settings** > **Nanolog Streaming Service** to access the Nanolog Streaming Service page.
3. Select the **NSSFeeds** tab and then click **Add**.
4. Complete the following steps to create a new NSS feed:
    a. In the **Feed Name** text box, enter a descriptive title for the feed, for example, `AWN Syslog`.
    b. Select the appropriate server from the **NSS Server** box.

    > **Tip:** If only one server is available, it is selected by default.

    c. Under **Status**, click **Enabled**.
    d. Set the **SIEM IP Address** to the management IP address of the Arctic Wolf sensor.
    e. Set the **SIEM TCP Port** to `514`.
    f. Verify that the **Log Type** is set to **Web Log**.
    g. Set the Feed Output Type to QRadar LEEF. The Feed Output Format box will be populated with the appropriate string.



Leave the remaining fields in this dialog box as their default values. We suggest leaving **User Obfuscation** set to **Disabled** to allow your Concierge Security® Team (CST) to correlate these events with additional user actions in your environment. Additionally, leave the **Timezone** at its default of **GMT**, and confirm that the **Duplicate Logs** setting is set to **Disabled**.

5. Click **Save**. You have successfully configured your ZScaler Nanolog Streaming Service to send syslog-formatted messages to your Arctic Wolf sensor.

6. Create a ticket for your CST advising that you have completed this configuration, as well as the IP address assigned to the NSS virtual machine. Your CST will confirm when Arctic Wolf is successfully processing logs from the ZScaler device(s).

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com