

**Zscaler Nano Logger - Boulder**

**Runbook**

April 07, 2019



© 2016 - 2018 IFF. All rights reserved.

No part of this technical document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, electronic, photocopying, recording, or otherwise, without prior written permission from IFF. The IFF logo is a trademark of IFF, registered in the U.S. and other countries.

|  |  |
| --- | --- |
| IFF Global Headquarters  521 West 57th Street  New York, NY 10019  United States  212-765-5500 | IFF Infrastructure Services  1515 State Highway #36  Union Beach, New Jersey 07735  732-264-4500 |

[www.iff.com](http://www.iff.com/)

|  |  |
| --- | --- |
| **Document Contributors and Approvers** | |
| The individuals listed below were involved in the creation, review and approval of this document. This section is for reference only. | |
| Name | Role |
| Maheshumanath Gopalakrishnan | Document Author |
| Venkatesa Perumal Pandian | Document Co-Author |
| Senthil Kumar | Reviewer and Approver |
| George Griesler | Approver |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Control** | | |  |
| Details regarding the version control of this document can be found below. | | |  |
| Date Created | Effective Date | Expiration / Review Date | Modified Date |
| April 07, 2019 |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Modified By: |  | Version: |  | Revision: |  |

Contents

[Purpose 4](#_Toc3821785)

[Zscaler Nano Logger Overview 4](#_Toc3821786)

[Configuration for Zscaler 4](#_Toc3821787)

# Purpose

This run book will guide Zscaler Nano Logger Configuration and Forwards Logs SIEM

Secure works & BT

# Zscaler Nano Logger Overview

This guide describes the tasks required to deploy a Nano log Streaming Service (NSS) to stream either web logs or firewall logs to a SIEM

# Configuration of Zscaler Nano Logger

1. NSS can be deployed on-premises on an ESX Virtual Machine, Azure, or Amazon Web Services (AWS). We are using ESX Virtual Machine Deployments

Valid Subscription Requires for NSS Web Logs

Deploying NSS Virtual Appliances

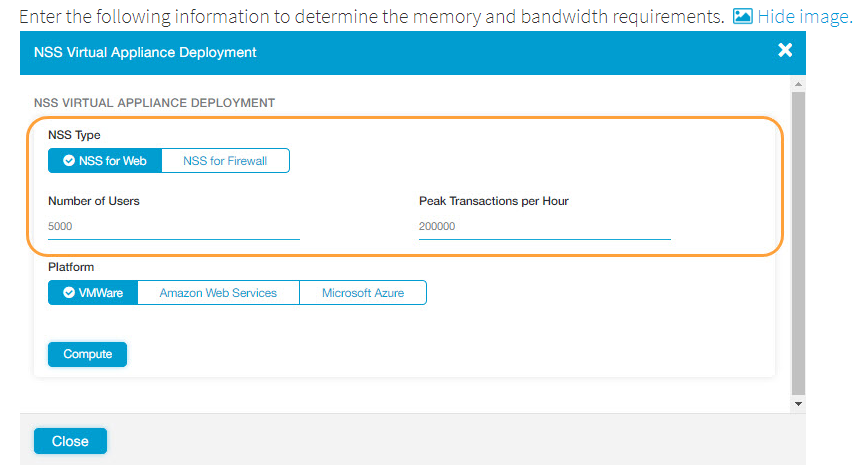
To deploy an NSS Virtual Appliance, follow the instructions below.

Go to Administration > Settings > Nano log Streaming Service.

Click Deploy NSS Virtual Appliance to enter data that the Zscaler service needs to compute the appropriate resources for your NSS.

Choose NSS configuration for either of the following:

NSS for Web



Specific Ova File needs to download and Share to IFF Engineering Team for VM Build

1. To configure the NSS virtual appliance on the ESX/ESXi server, log in to the vSphere client and do the following:

Import the NSS OVA file.

Go to File > Deploy OVF Template and use the Deploy OVF Template wizard to deploy the NSS virtual machine (VM).

Configure the network.

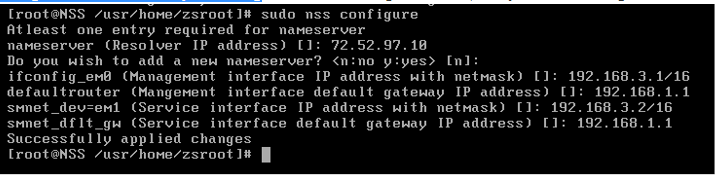
Select the NSS VM and click either the Power On button or Power On the virtual machine.

On the Console tab, log in at the FreeBSD command prompt with the following:

Username: XXXX

Password: XXXX

Configure the network by entering



Set the DNS server IP address.

For example: 10.13.140.10

Set the management interface IP with CIDR netmask. You will use the management IP address for SSH or FTP.

For example: 10.13.140.25

Set the default gateway for the management IP address.

For example: 10.13.140.1

Set the service IP address with CIDR netmask. NSS uses the service IP address to communicate with the Zscaler cloud and with the SIEM.

For example: 10.13.140.26

Set the default gateway for the service IP address.

For example: 10.13.140.1

Note that the management IP address and service IP address can be on different subnets, as long as the DNS server can be reached on both subnets.

1. Install the SSL certificate.

NSS uses this certificate to authenticate itself to the Zscaler service. Ensure that the SSL certificate is installed on only one active NSS VM at a time. Having multiple NSS VMs that use only one certificate causes cloud connection flapping, which disrupts the streaming of logs to the NSS.

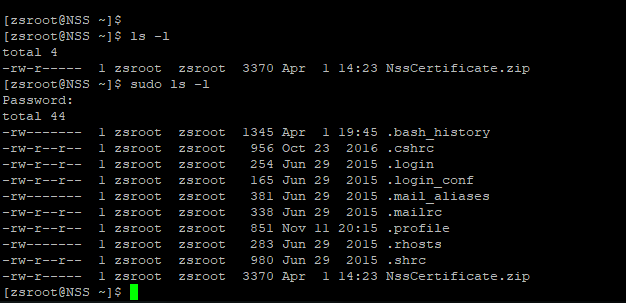
Navigate to the SSL certificate that you saved.

Use FTP, SCP or SFTP to upload it to the management IP address of NSS.

On the vSphere client, click the Console tab, and log in with the following credentials:

Username: xxxx

Password: xxxx



NSS Certificate will created By BT and we may need download and Transfer to NSS through WinSCP.

Above Diagram Shows NSSCeritficate

Go to the Console tab or use SSH to connect to the management IP address.

Run the command sudo nss install-cert

Specify the path to the uploaded certificate bundle.

Check the configuration by running the command sudo nss dump-config



1. Download the NSS Binaries.

You will need to download the NSS binaries once, before starting the NSS.

On the vSphere client, click the Console tab or use SSH to connect to the management IP address.

Run the command sudo nss update-now to download and install the NSS binaries.

After the NSS starts, it will automatically download and install new binaries when they’re available.

1. Start NSS.

On the vSphere client, click the Console tab or use SSH to connect to the management IP address.

Run the command sudo nss start

Ensure that the command shows that the NSS virtual appliance started successfully.

It may take a few minutes for the NSS to start streaming logs to the SIEM

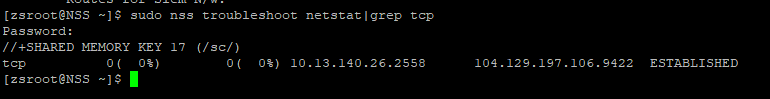
To enable the NSS to start automatically after a restart, run the command sudo nss enable-autostart

You can also explore other options by running: sudo nss help

1. Verify the configuration.

To verify the configuration, run the following command:

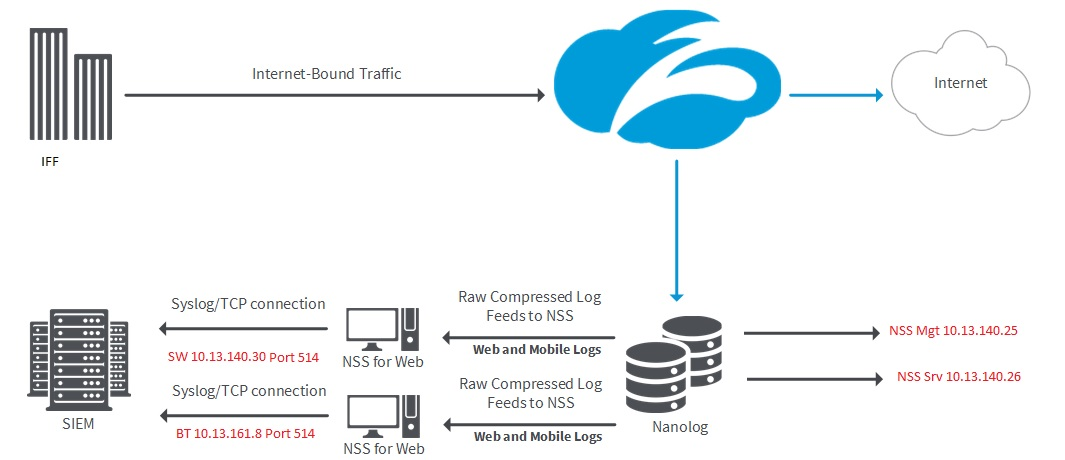
sudo nss troubleshoot netstat|grep tcp



Connection to the Zscaler cloud on port 9422: This is the control connection that is used to authenticate NSS to the Zscaler Central Authority and to download the configuration.

Connection to the SIEM: This is the long-lived TCP connection to the SIEM on the specified log data port. If there are multiple feeds configured, multiple connections must be listed.

1. Network Architecture –Zscaler Nano Logger



1. ASA Firewall Rule Object update with Following

Replace the Boulder Firewall object IP as below:

object network NSS\_MANAGEMENT

10.11.924.24 to 10.13.140.25

object network NSS\_SERVICE

10.19.65.172 to 10.13.140.26