# Table of Contents

1 Document Overview ........................................................................................................... 5  
   1.1 Document Audience ....................................................................................................... 5  
   1.2 Software Revisions ......................................................................................................... 5  
   1.3 Request for Comments ................................................................................................... 5  
   1.4 Document Prerequisites ................................................................................................. 5  
   1.5 Document Revision Control ............................................................................................ 6  
   1.6 Flow of Events ................................................................................................................ 6  

2 Syslog, CEF and LEEF ..................................................................................................... 7  
   2.1 Log Format Overview ..................................................................................................... 7  
      2.1.1 Syslog ........................................................................................................................... 7  
      2.1.2 Common Event Format (CEF) ...................................................................................... 9  
      2.1.3 Log Event Extended Format (LEEF) ............................................................................. 9  
   2.2 Zscaler Logging Architecture ......................................................................................... 10  
      2.2.1 Zscaler Nanolog Streaming Service (NSS) ................................................................. 11  
      2.2.2 Zscaler Logging Streaming Service (LSS) ................................................................. 11  

3 Configuring ZIA for NSS ............................................................................................... 12  
   3.1 Logging into ZIA ........................................................................................................... 12  
   3.2 Configuring Nanolog Streaming Service (NSS) ............................................................ 13  
      3.2.1 Nanolog Streaming Service (NSS) ............................................................................. 13  
      3.2.2 Add new NSS Server ................................................................................................. 14  
      3.2.3 Download system generated SSL cert-key pair ......................................................... 15  
      3.2.4 Install this SSL cert on NSS ..................................................................................... 15  
      3.2.5 Verify NSS Server State ........................................................................................... 16  
      3.2.6 Add NSS Feed ............................................................................................................ 16  
      3.2.7 Configure NSS Feed Parameters ............................................................................. 17  

4 Configuring Phantom ...................................................................................................... 18  
   4.1 Create new Event Label in Phantom ............................................................................. 18  
   4.2 Create Automation user in Phantom ............................................................................. 19  
   4.3 Installing Zscaler App on Phantom ............................................................................. 20  
      4.3.1 Log into Phantom and navigate to Apps .................................................................... 20  
      4.3.2 Search for Zscaler App .............................................................................................. 21  
      4.3.3 Configure Zscaler App .............................................................................................. 22  
      4.3.4 Test connectivity between Phantom and Zscaler .................................................... 23  
   4.4 Installing Splunk App on Phantom .............................................................................. 24  
      4.4.1 Navigate to Apps ........................................................................................................ 24  
      4.4.2 Search for Splunk App ............................................................................................... 24  
      4.4.3 Configure Splunk App ............................................................................................... 25  
      4.4.4 Test connectivity between Phantom and Splunk ..................................................... 28  
   4.5 Playbooks .................................................................................................................... 29  
      4.5.1 Download Zscaler Playbook ..................................................................................... 29  
      4.5.2 Edit the playbook settings ....................................................................................... 30
# Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF</td>
<td>Common Event Format</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation <em>(RFC2890)</em></td>
</tr>
<tr>
<td>LEEF</td>
<td>Log Event Extended Format</td>
</tr>
<tr>
<td>LSS</td>
<td>Logging Streaming Service (For ZPA)</td>
</tr>
<tr>
<td>NSS</td>
<td>Nanolog Streaming Service (For ZIA)</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer <em>(RFC6101)</em></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security <em>(RFC5246)</em></td>
</tr>
<tr>
<td>ZAPP</td>
<td>Zscaler End-point Client Application</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
1 Document Overview

This Deployment Guide document will be to explain the feedback loop consisting of Zscaler, Splunk ES and Phantom playbooks. This guide is intended for standing up proof-on-concept topologies and demos, for evaluating interoperability, and joint integration. This guide should not be used to configure either vendor platform for production use. For production deployments, please contact Zscaler or Splunk for post-sale deployment assistance.

1.1 Document Audience

This document was designed for Network Security Engineers and Network Engineers. All examples in this guide presumes the reader has a basic comprehension of IP Networking and Syslog. For additional product and company resources, please refer to the Appendix section.

1.2 Software Revisions

This document was written using Zscaler Internet Access v5.7, Splunk Enterprise v7.2.6 and Phantom v4.5.15922

1.3 Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact partner-doc-support@zscaler.com.

1.4 Document Prerequisites

Zscaler Internet Access (ZIA)

- A working instance of ZIA 5.7 (or newer)
- Zscaler API access (Needs to be requested by contacting Zscaler support)

Splunk ES

- Administrator access to Splunk instance
- Working log flow from Zcaler NSS into Splunk

Splunk Phantom

- Administrator access to Phantom instance
1.5 Document Revision Control

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Change Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>July 2019</td>
<td>Initial document created by Zscaler</td>
</tr>
</tbody>
</table>

1.6 Flow of Events

- **Zscaler**
  - Generates logs that get sent to Splunk

- **Splunk ES**
  - Splunk ES subscribes to various threat feeds
  - ES runs correlation searches against Zscaler logs and threat feeds
  - Based on correlation, if needed, ES creates notable events and feeds them to Phantom

- **Phantom**
  - Phantom playbooks get triggered based on these notable events
  - Playbook actions connect to Zscaler via REST API and add IP/Domain to blacklist, if required
2 Syslog, CEF and LEEF

2.1 Log Format Overview

2.1.1 Syslog

Syslog messages are seen in two major formats:

the “Original” (2001) BSD format (RFC 3164)

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8
```

Syslog message in RFC 3164 format

- `<34>` is a priority number. It represents the facility number multiplied by 8, to which severity is added. In this case, facility=4 (Auth) and severity=2 (Critical)
- Oct 11 22:14:15 is the timestamp. It misses the year, the time-zone and doesn’t have sub-second information
- mymachine is a host name where the message was written
- su: is a tag. Typically this is the process name – sometimes having a PID (e.g. su[1234]:)
- the message (MSG) is everything after the tag
The “New” (2009) format (RFC 5424)

RFC5424 compliant syslog message consists of three parts -
“Syslog Header”, “Structured Data” and the actual log “message”

- **Syslog Header** consists of priority, version, timestamp, hostname etc.

- **Structured Data** in key=value format. It provides a mechanism to express information in a defined, parsable and interpretable data format. (e.g. SD-ID, SD-PARAM)

- **Actual log message** follows these two fields above (Message field is free-form)

```
<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su -- - 'su root' failed for lon
vick on /dev/pts/8
```

Syslog message in RFC 5424 format

- The dashes seen above are places for PID, message ID and other structured data you may have

```
<100>2 1982-07-10T20:30:40.001Z myserver.com su 201 32001 - BOM 'su root' failed on /dev/pts/7
```

Another syslog message in RFC 5424 format
2.1.2 Common Event Format (CEF)

CEF is an open log management standard that improves the interoperability of security-related information from different security and network devices and applications.

Base CEF format:

CEF:Version|Device Vendor|Device Product|Device Version|Signature
IDINamelSeverity|Extension

2.1.3 Log Event Extended Format (LEEF)

Log Event Extended Format (LEEF) is a customized event format for IBM QRadar. It is designed to describe (network) security events and uses encoding and transport similar to those used by CEF. However, the two formats differ in the number and types of fields.

Base LEEF format:

LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension
2.2 Zscaler Logging Architecture

Every transaction that goes through Zscaler cloud generates a log entry. These logs are retained by Zscaler for 6 months. Customers can access these logs via Zscaler dashboard. These logs can also be sent over TCP to customer’s SIEM (on premises or in cloud).

To get logs from Zscaler cloud to customer SIEM, an intermediary is required. This intermediary is called Nanolog Streaming Service (NSS) and is a lightweight VM that acts as a relay between Nanolog cloud and the SIEM.

Note: Communication from NSS to customer’s SIEM is supported over TCP only and not UDP.

Zscaler has two primary products-
Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA)

All subsequent details in this document will be pertaining to ZIA and not ZPA.

ZIA logs generated by Zscaler are of two types - Web and Firewall
This is due to different fields that need to be looked into/logged with http vs. non-http traffic.

Depending on the type of logs of interest, we’ll need to deploy web and/or firewall NSS.
Flow of events for log messages:

- Customer deploys web or firewall NSS; either on premises or in any cloud
- Customer registers this NSS with Zscaler (Using SSL certificates obtained from Zscaler)
- Customer accesses internet while going through Zscaler (ZIA)
- Zscaler generates syslog and it is sent to Zscaler’s Nanolog service cloud
- Nanolog cloud now streams these logs in compressed and encrypted format to NSS
- NSS builds a separate TCP connection to SIEM & forwards these logs to it

### 2.2.1 Zscaler Nanolog Streaming Service (NSS)

NSS is the logging platform used by Zscaler Internet Access (ZIA)

For more information, please refer to the Appendix section for links to NSS documentation.

### 2.2.2 Zscaler Logging Streaming Service (LSS)

LSS is the logging platform used by Zscaler Private Access (ZPA). LSS is outside the scope of this document. This document will pertain to NSS (which is used with ZIA) only.

For more information, please refer to the Appendix section for links to LSS documentation.
3 Configuring ZIA for NSS

3.1 Logging into ZIA

First, we will setup the Zscaler side of this service. The required steps for this section are:

- Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, please contact support: [https://help.zscaler.com/submit-ticket](https://help.zscaler.com/submit-ticket).
3.2 Configuring Nanolog Streaming Service (NSS)

3.2.1 Nanolog Streaming Service (NSS)

After logging into ZIA, we first need to add an **NSS Server** and **NSS Feed**. First, we will create a new NSS Server. To navigate to the Nanolog Streaming area of ZIA, please follow: **Administration -> Cloud Configuration ->** and then click **Nanolog Streaming Service**.
3.2.2 Add new NSS Server

Provide a name for the new NSS server and click Save
3.2.3 Download system generated SSL cert-key pair

![Image of Zscaler Nanolog Streaming Service]

3.2.4 Install this SSL cert on NSS

Log into NSS via SSH and install the certificate using following command

```bash
sudo nss install-cert
```

- Specify the path to the uploaded certificate bundle. Check the configuration by running the command:

```bash
sudo nss dump-config
```
3.2.5 Verify NSS Server State

Before proceeding to further steps, ensure that NSS State is “Healthy”

![NSS Server State Image]

3.2.6 Add NSS Feed

![Add NSS Feed Image]
3.2.7 Configure NSS Feed Parameters

SIEM IP and TCP port should be filled in as per your network setup
Feed Output Type should be set to “Splunk CIM” from the dropdown
4 Configuring Phantom

Following steps assume that you have Admin access to Phantom instance

4.1 Create new Event Label in Phantom

Splunk will send events to Phantom with this label. Phantom playbook will be configured to be triggered only for events that contain this label. This is a way to limit a playbook to take action only on specific kind of events.

Navigate to Administration -> Event Settings -> Label Settings and then add a new label

We will name it “from_correlation_splunk_search”
4.2 Create Automation user in Phantom

This username will be used by splunk to be able to communicate with Phantom

Navigate to Administration -> Users and create a new automation user with following settings

Click on username we created and copy the section shown below for your record. This will be used later by Splunk to authenticate with Phantom
4.3 Installing Zscaler App on Phantom

4.3.1 Log into Phantom and navigate to Apps
4.3.2 Search for Zscaler App

Search for “zscaler”. Head over to “Unconfigured Apps” and click “Configure new Asset”
4.3.3 Configure Zscaler App

As shown below, “Asset Info” tab takes free form text input
Name your asset as per your organization’s naming conventions
“Asset Settings” need to be filled out with the your pertinent Zscaler details as shown below. After filling all the details, save and then click “Test Connectivity”

4.3.4 Test connectivity between Phantom and Zscaler
If all the information is filled in correctly, the connectivity test should pass, and you should get result similar to one shown below
4.4 Installing Splunk App on Phantom

4.4.1 Navigate to Apps

4.4.2 Search for Splunk App

Search for “splunk”
Head over to “Unconfigured Apps” and click “Configure new Asset”
4.4.3 Configure Splunk App

As shown below, “Asset Info” tab takes free form text input
Name your asset as per your organization’s naming conventions
“Asset Settings” need to be filled out with the your pertinent Splunk details as shown below. Communication from Phantom to Splunk on port 8089 needs to be permitted by the network.
Under “Ingest Settings” set polling interval as per your operational needs. In this document, we will set it to 1 minute.
4.4.4 Test connectivity between Phantom and Splunk

If all the information is filled in correctly, the connectivity test should pass, and you should get result similar to one shown below
4.5 Playbooks

4.5.1 Download Zscaler Playbook

Download Zscaler playbook using this link and import it into your Phantom instance.

![Import Playbook](import_playbook.png)

This playbook does a correlation search against known malicious IP/Domains and the customer’s Zscaler logs. If a malicious IP/Domain is found in these logs, the playbook checks if that IP/Domain is already on that customer’s Zscaler blacklist.

If it is, then no action is taken.
If it is not on blocklist, phantom checks how Zscaler classifies this IP/Domain and in case Zscaler classifies this as “Unknown”, phantom updates Zscaler blacklist via an API call.
4.5.2 Edit the playbook settings

Navigate to playbooks and open the one that we imported
Edit playbook properties and mark it as “Active”
Also change “Operates on” from dropdown to the label we created in step 6.1 and click save
5 Configuring Splunk

5.1 Configure Splunk ES

5.1.1 Install Splunk ES App

After logging into your Splunk instance, click on “Splunk Apps” and search for “enterprise security”

Install the Splunk ES app
5.1.2 Manage Threat Intelligence within ES App

Navigate to the newly installed “Enterprise Security” Splunk App and then click “App Configuration” section as shown below.
Click on “Content Management”

Type “Threat” in the search box and select type as “Correlation Search”
Enable the “Threat Activity Detected” correlation search as shown below
After enabling, click on “Threat Activity Detected” correlation search

This brings you to following page
5.1.3 Notable Events and Forwarding to Phantom

Once you scroll down to the bottom of this page, you will see “Notable” and “Risk Analysis” option checked by default. We will add “Send to Phantom” as a new response action in this section.
Notable events are automatically created by Splunk ES based on correlation searches. Below, we add action to forward artifacts related to such events to your Phantom setup.
5.2 Configure Phantom

5.2.1 Install Phantom App

We need to install Phantom App on Splunk. Phantom IP will be defined here and Splunk will forward artifacts to this Phantom instance. Install the “Phantom App for Splunk”
5.2.2 Configure Automation user

We will now configure username/authentication settings to establish communication between Splunk and Phantom.

Navigate to the newly installed “Phantom” Splunk App and then click “Create Server” section as shown below.
Populate the “Authorization Configuration” by pasting the content we copied in step 4.2 and click save.

You should receive confirmation as one shown below:

- Image of the New Server Configuration window with the message: "Splunk has added the server configuration."
5.2.3 Verify Logs in Phantom

Log back into Phantom. You should start seeing events getting populated as shown below. By default, it may take up to 30 min for events to show up
6 Configuring Zscaler API key

6.1 Obtaining Zscaler API key

Customers will need to contact Zscaler support to request a Zscaler API key. Please refer to Section 7 regarding contacting Zscaler support.

This API key along with Zscaler admin password will allow Phantom to make REST API calls to Zscaler and modify black/white list.

Once obtained from Zscaler support, the API key will need to be configured in Zscaler portal in the section shown below.

![API Key Management in Zscaler Portal](image-url)
7 Requesting Zscaler Support

7.1 Gather Support Information

7.1.1 Obtain Company ID

The navigation is: Administration -> Settings -> and then click Company profile
7.1.2 Save Company ID
7.1.3 Enter Support Section

Now that we have our company ID, we are ready to open a support ticket. The navigation is: “?” and then click Submit a Ticket.
8 Appendix A: Zscaler Resources

NSS

NSS Deployment Guide
https://help.zscaler.com/zia/documentation-knowledgebase/analytics/nss/nss-deployment

NSS Troubleshooting Guide
https://help.zscaler.com/zia/troubleshooting-nss

General

Zscaler: Getting Started
https://help.zscaler.com/zia/getting-started

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket

ZIA Test Page
http://ip.zscaler.com/
9  Appendix B: Splunk ES Resources

ES use cases:
https://docs.splunk.com/Documentation/ES/5.3.1/Usecases/Overview

ES Admin guide:
https://docs.splunk.com/Documentation/ES/5.3.1/Admin/Introduction

ES User guide:
https://docs.splunk.com/Documentation/ES/5.3.1/User/Overview

10  Appendix C: Phantom Resources

Introduction to Phantom:
https://my.phantom.us/4.5/docs/introduction/overview

Phantom Admin guide:
https://my.phantom.us/4.5/docs/admin/overview

Phantom Knowledgebase:
https://my.phantom.us/kb/