Common Event Format Configuration Guide

Zscaler, Inc.

Nanolog Streaming Service 4.1

Date: Wednesday, October 09, 2013

CEF Connector Configuration Guide

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to HP. HP does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Certified CEF:

The event format complies with the requirements of the HP ArcSight Common Event Format. The HP ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HP's ArcSight product. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. The events will be sufficiently categorized to be used in correlation rules, reports and dashboards as a proof-of-concept (POC) of the joint solution

Zscaler Nanolog Streaming Service v. 4.1

Oct 7, 2013

Revision History

Date	Description
10/07/2013	First edition of this Configuration Guide.
10/09/2013	Version 4.1 Certified by HP Enterprise Security

CEF Connector Support Information when an issue is outside of the ArcSight team's ability

In some cases the ArcSight customer service team is unable to help with issues that lie within the configuration itself in which case, the certified vendor should be contacted for assistance:

Zscaler Customer Support

Phone -1-800-953-3897

Email –support@zscaler.com

Instructions – Arcsight or end customer can call into our support directly when there are NSS issues integrating with Arcsight.

They would be required to provide the customer name/contact, their Arcsight Sales & SE contact as well. If additional support is required, SOC will engage Zscaler PM and Business Development team.

Nanolog Streaming Service Configuration Guide

This guide provides information for configuring the Zscaler Nanolog Streaming Service for syslog event collection. This Connector is supported on VMware ESX/ESXi Hypervisor platforms. Version 4.1 is supported.

Overview

Zscaler Nanolog Streaming Service (NSS) enables organizations to seamlessly integrate their Zscaler weblogs with their preferred SIEM platform, Arcsight in real time. NSS provides users the flexibility of sending only a subset of the logs to their SIEM using multiple event filters.

Configuration

- Login to the UI. Go to Policy > Adminstration > Configure Nanolog streaming Service
- It is assumed that you've already registered the NSS VM.

Please refer to the NSS Guide to register, download and configure NSS VM

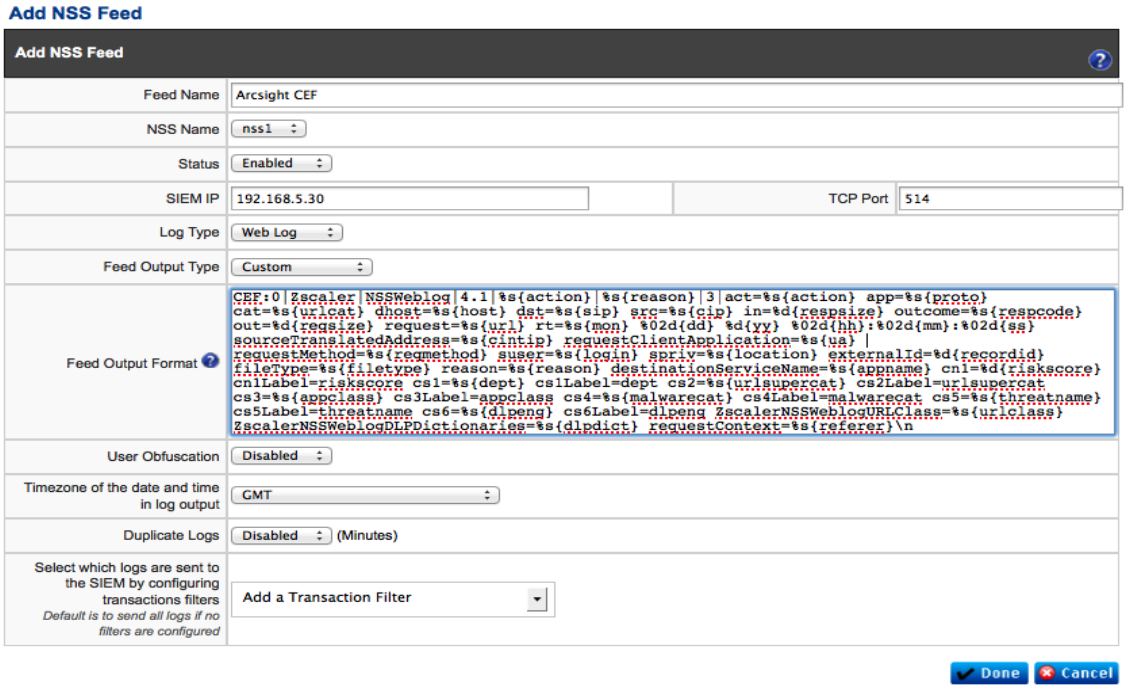
- Click on Edit > Add NSS Feed

Specify the name of the feed

Specify the IP Address of the Arcsight Collector (for ESM) or Logger. The TCP port should be 514 (syslog port)

Set the log output type to Custom and specify the output format given below:

- ```
  %s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss
  CEF:0|Zscaler|NSSWeblog|4.1|%s{action}|%s{reason}|3|act=%s{action} app=%s{proto}
  cat=%s{urlcat} dhost=%s{host} dst=%s{sip} src=%s{cip} in=%d{respsize}
  outcome=%s{respcode} out=%d{reqsize} request=%s{url} rt=%s{mon} %02d{dd} %d{yy}
  %02d{hh}:%02d{mm}:%02d{ss} sourceTranslatedAddress=%s{cintip}
  requestClientApplication=%s{ua} requestMethod=%s{reqmethod} suser=%s{login}
  spriv=%s{location} externalId=%d{recordid} fileType=%s{filetype} reason=%s{reason}
  destinationServiceName=%s{appname} cn1=%d{riskscore} cn1Label=riskscore cs1=%s{dept}
  cs1Label=dept cs2=%s{urlsupercat} cs2Label=urlsupercat cs3=%s{appclass} cs3Label=appclass
  cs4=%s{malwarecat} cs4Label=malwarecat cs5=%s{threatname} cs5Label=threatname
  cs6=%s{dlpeng} cs6Label=dlpeng ZscalerNSSWeblogURLClass=%s{urlclass}
  ZscalerNSSWeblogDLPDictionaries=%s{dlpdict} requestContext=%s{referer}\n
  ```
  ```



Events

The NSS sends Web Security logs to the Arcsight. There are two event types – allowed and blocked – logs.

Device Event Mapping to ArcSight Data Fields

Information contained within vendor-specific event definitions is sent to the ArcSight SmartConnector, then mapped to an ArcSight data field.

The following table lists the mappings from ArcSight data fields to the supported vendor-specific event definitions.

Zscaler NSS Connector Field Mappings

Vendor-Specific Event Definition	ArcSight Event Data Field
Zscaler	Device Vendor
NSSWeblog	Device Product
4.1	Device Version
action	Device Event Class ID

Vendor-Specific Event Definition	ArcSight Event Data Field
reason	Name
3	Device Severity
action	act
proto	app
urlcat	cat
host	dhost
sip	dst
cip	src
respsize	in
respcode	outcome
reqsize	out
url	request
cintip	sourceTranslatedAddress
ua	requestClientApplication
reqmethod	requestMethod
login	suser
location	spriv
recordid	externalId
filetype	fileType
reason	reason

Vendor-Specific Event Definition	ArcSight Event Data Field
appname	destinationServiceName
riskscore	cn1
dept	cs1
urlsupercat	cs2
appclass	cs3
malwarecat	cs4
threatname	cs5
dlpeng	cs6
referer	requestContext
urlclass	ZscalerNSSWeblogURLClass
malwareclass	ZscalerNSSWeblogMalwareClass
dlpdict	ZscalerNSSWeblogDLPDictionaries
fileclass	ZscalerNSSWeblogFileClass
bwthrottle	ZscalerNSSWeblogBWThrottle

Vendor-Specific Event Definition	ArcSight Event Data Field