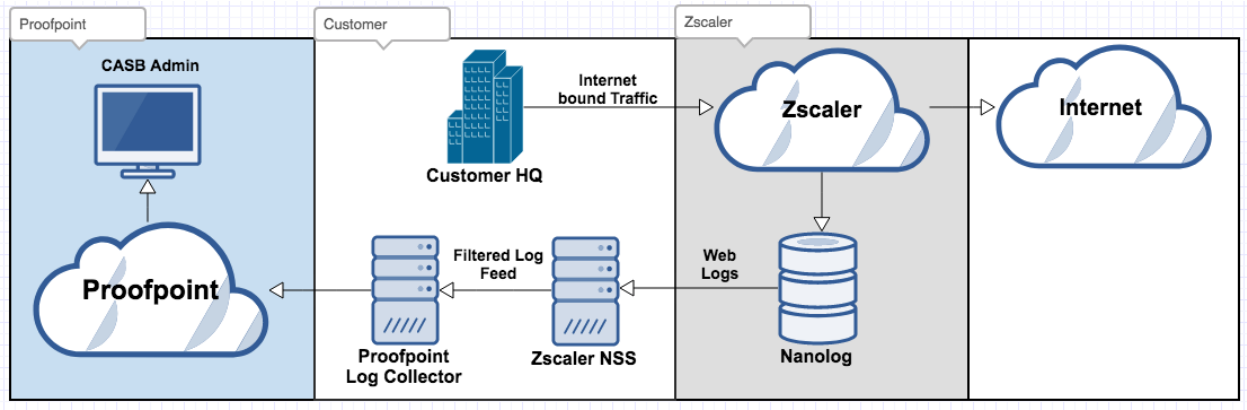
proofpoint®

Proofpoint CASB Zscaler Integration Guide for Application Governance

1.1 revision 1

Overview

The Proofpoint CASB Application Governance module provides Shadow IT functionalities in Proofpoint CASB (PCASB), enabling discovery of cloud applications from traffic logs. The Proofpoint log collector (PLC) consumes traffic logs from a firewall or secure gateway and then sends them securely to PCASB. The PCASB product identifies which traffic represents cloud applications and calculates application severity. Discovered applications are managed in the PCASB web interface, providing visibility of the application landscape.



Support

Version	NSS Deployment	PLC Deployment
Zscaler Internet Access v5.7	vSphere, AWS, Azure	On-premises, AWS *Server must be able to run Docker.*

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.

Deployment Workflow

To deploy the Application Governance module, complete the following workflow.

1. Allocate a machine for the PLC.
2. Install the PLC.
3. Configure the NSS traffic log feed.
   After completing this step, contact Proofpoint to enable the Cloud Discovery screen in the PCASB web interface.
4. (Optional) Enforce application governance policies in Zscaler.

As a data processor, Proofpoint is committed to maintaining the privacy and confidentiality of the personal data entrusted to us, as well as conforming to standards such as GDPR. We have a documented Information Security Program describing how technical and administrative security controls are implemented to protect personal data and the physical locations in which it is hosted – for more information on this please see: https://www.proofpoint.com/us/legal/trust

If you have further queries around data residency or compliance, please contact your account manager.

Allocate a machine for the PLC

Hardware Requirements

Users	AWS	On-prem	Storage	OS
10K	M5.large	2 CPU, 8GB ram	500GB	Linux - CentOS 7.6.1810
>10K	C5.xlarge	2 4PU, 8GB ram	500GB	Linux - CentOS 7.6.1810

Network Requirements

- Network Bandwidth up to 10 Gbps
- NSS server needs access to the PLC port (9514 by default)

Install the PLC

The PLC is provided as a Docker image. The image is configured to forward data to the Proofpoint S3 location.

To install and configure the PLC

1. Install Docker on the selected VM (or local server).
   See Docker documentation for details.
2. Create a new Linux user with the username “proofpoint” and a strong password. Give the user sudo rights.
3. Login as the proofpoint user.
4. Download the PLC configuration files and scripts from the location provided to you by your Proofpoint representative.
5. Create a directory on the VM.
6. Change the owner of the new directory and all its children to the proofpoint user by running the following command from the parent of the new directory:
   chown -R proofpoint *<directory name>*
   where *<directory name>* is the name of the directory you just created.
7. Place the scripts and configuration files you downloaded in the new directory.
   Change the permission on the configuration file by running the following command: `chmod 700` *<directory name>/.*`proofpointConfig`
   where *<directory name>* is the name of the directory you just created.
8. Execute the `plc` script.
   - If successful, the following message appears: “Proofpoint Log Collector successfully started”.
   - If failed, please see: PLC Installation Troubleshooting.
   - The PLC Docker image downloads and the PLC starts. The PLC size is 820MB.

Configure the NSS traffic log feed

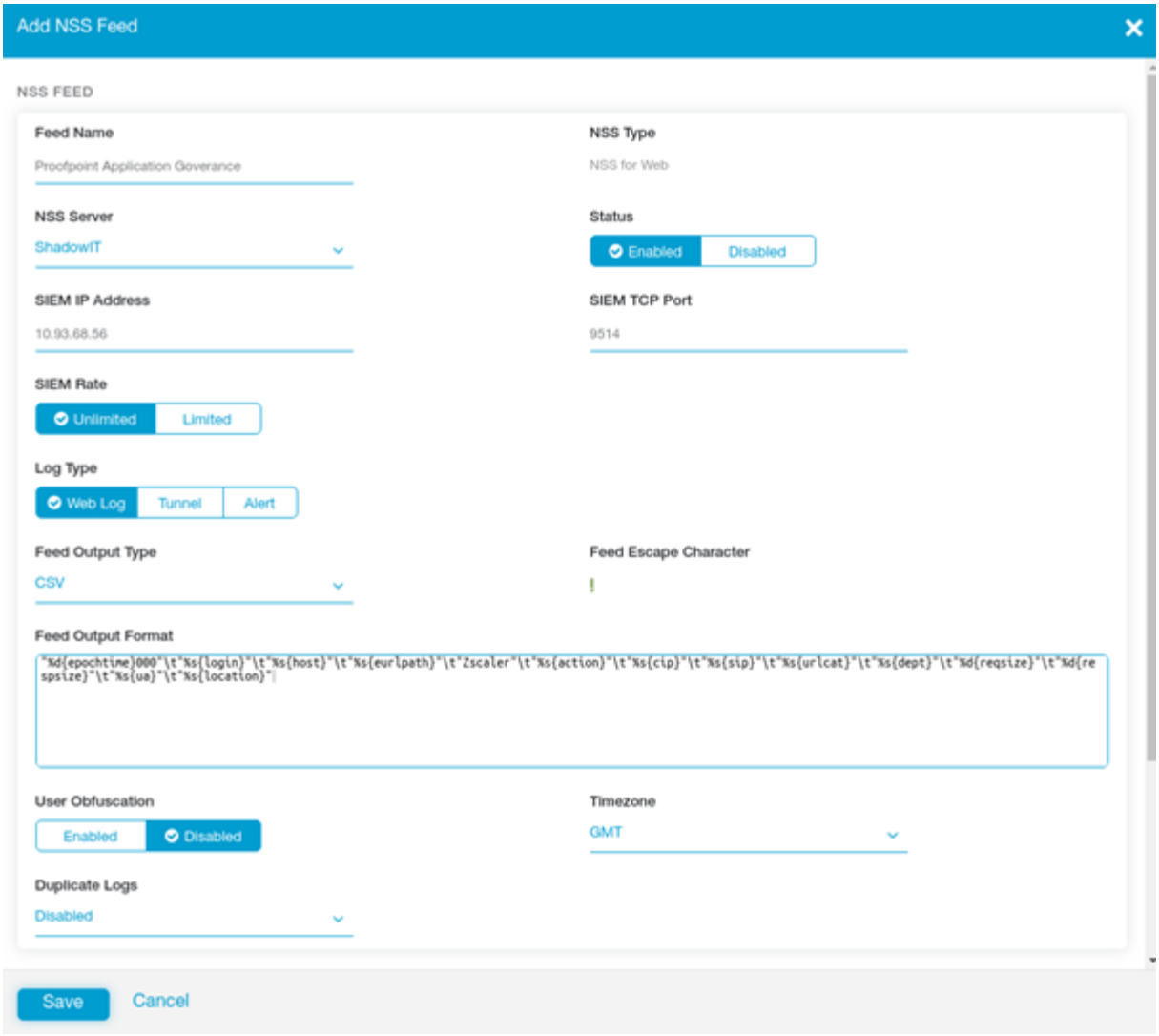
Configuring the NSS traffic log feed requires deploying the NSS server and then configuring it to send traffic logs to the PLC.

To deploy the NSS server

You must deploy a Zscaler NSS server or utilize an existing one. See Zscaler documentation for details.

To configure the NSS feed

1. Open the Zscaler Admin console.
2. Navigate to **Administration** > **Nanolog Streaming Service**, and select the **NSS FEEDS** tab.
3. Click **Add NSS Feed**.
   The **Add NSS Feed Dialog** box appears.



4. Complete the following fields:

In this field…	Do This…
Feed Name	Type a name for the feed, such as “Proofpoint Application Governance”.
SIEM IP Address	Type the IP address of the host where the PLC is running.
SIEM TCP Port	Type the PLC port (9514 by default).
Feed Output Type	Select **CSV**.
Feed Output Format	Copy and paste the following: **“%d{epochtime}000"\t"%s{login}"\t"%s{host}"\t"%s{eurlpath}"\t"Zscaler"\t"%s{action}"\t"%s{cip}"\t"%s{sip}"\t"%s{urlcat}"\t"%s{dept}"\t"%d{reqsize}"\t"%d{respsize}"\t"%s{ua}"\t"%s{location}"** **IMPORTANT: Make sure this field does not contain any line breaks or empty lines.** See Zscaler documentation for more details.
User Obfuscation	Disable this option. **Note: Disabling user obfuscation enables Proofpoint CASB to provide insights on user usage.**
Timezone	Select **GMT**.

5. Click **Save**.
6. Navigate to **Administration** > **Activation**, and click **Activate**.

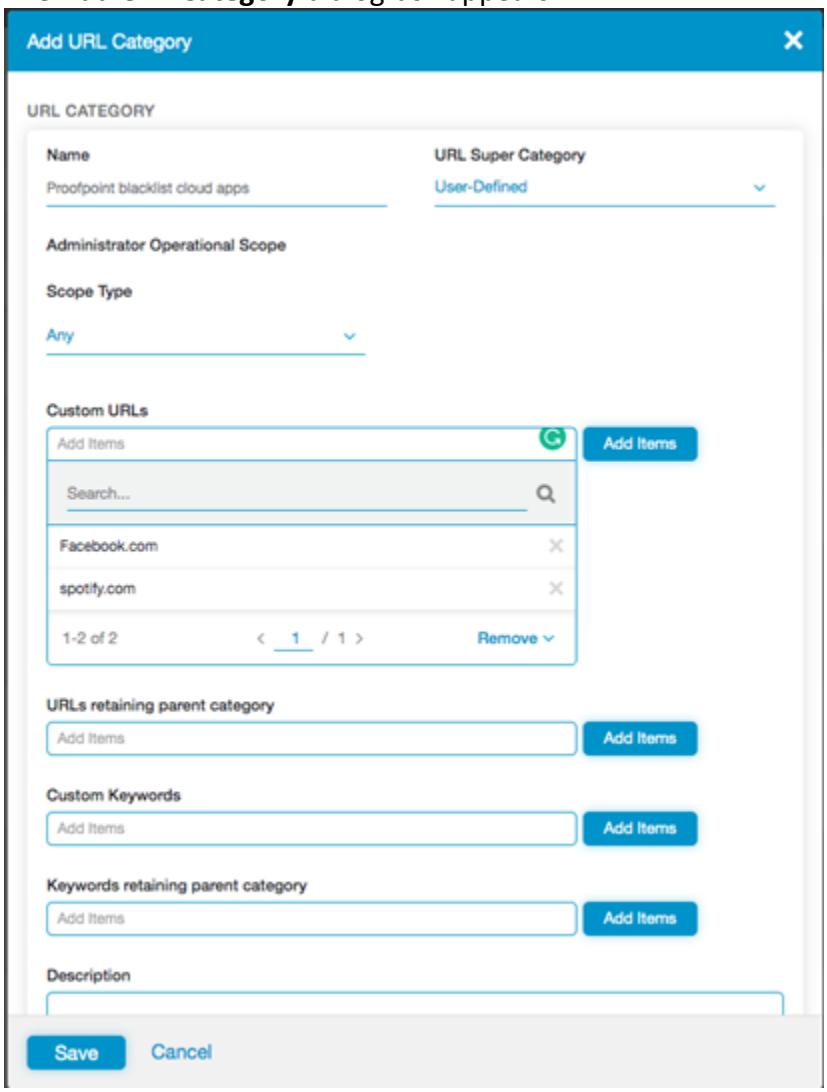
Enforce application governance policies in Zscaler

Zscaler policies enable IT or security administrators to manage access to risky cloud applications and enforce governance policies on employees' cloud usage. Zscaler requires defining a *Custom URL* category, and you can then build a policy of rules to control access to all URLs in the category.

Apply a blocking policy in Zscaler

This procedure describes how to create a policy that blocks applications discovered by Proofpoint. This involves creating a custom category with the Proofpoint provided URLs and adding a rule that blocks the category.

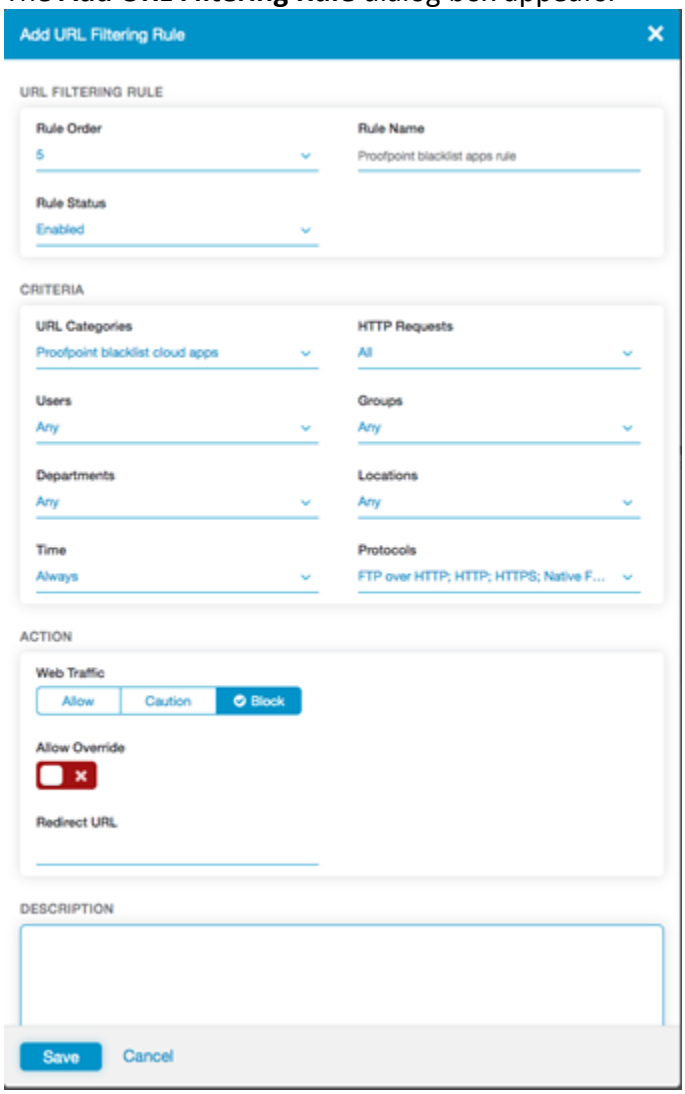
1. Create a new custom URL category by doing the following:
   a) Open the Zscaler Admin console.
   b) Navigate to **Administration** > **URL Categories**, and click **Add**.
   The **Add URL Category** dialog box appears.



   c) In the **Name** field, type **Proofpoint blacklist cloud apps category**.

d) In the **Custom URLs** field, type the Proofpoint CASB provided URLs you want to block. At least one URL is required to create the custom URL category.
e) Select **URLs retaining parent category**.

2. Create a new URL filtering rule for the Proofpoint category by doing the following:
   a) Navigate to **Policy** > **URL & Cloud App Control** [**URL FILTERING POLICY** tab], and click **Add URL Filtering Rule**.
   The **Add URL Filtering Rule** dialog box appears.



   b) In the **Rule Name** field, type **Proofpoint blacklist cloud apps rule**.
   c) In the URL Categories field, select **Proofpoint blacklist cloud apps category**.
   d) Navigate to **Action** > **Web Traffic**, and select **Block**.

The applications corresponding to the URLs defined in **Proofpoint blacklist cloud apps category** are blocked.

PLC Installation Troubleshooting

Problem	Description	Solution
Invalid PLC configuration	The error message which indicates this issue will be similar to the following: `2019-07-23T21:11:52,643][ERROR][logstash.agent ] Failed to execute action {:action=>LogStash::PipelineAction::Create/pipeline_id:metrics, :exception=>"LogStash::ConfigurationError", :message=>"Cannot evaluate `${AWS_SECRET_KEY}`. Replacement variable `AWS_SECRET_KEY` is not defined in a Logstash secret store or as an Environment entry and there is no default value given."`	Contact Proofpoint professional services. After resolving the configuration problem, restart the PLC.
PLC already running	An error message will appear, indicating this issue.	The PLC is already running, and only one PLC can run on a machine.
Port already in use	Implies that other services are running on the host. The error message which indicates this issue will be similar to the following: `listen "tcp 0.0.0.0:9600: bind: address already in use"`	Ideally, the PLC should be on its own machine. If that is not possible, the local host's port can be adjusted by modifying the port variables at the top of the PLC script.
PLC cannot send logs to S3	Implies a problem with the AWS keys specified in the `.proofpointConfig` file. Possible problems include: ▪ Wrong keys have been configured ▪ Keys do not have rights to the S3 location ▪ Wrong tenant Id is specified	View the logs by running "plc log" and look for errors.
Docker not running properly		See Docker troubleshooting tips and check the exit status codes.

No internet access	Upon starting the PLC, an error message similar to the following will appear:
	`Unable to find image 'docker.elastic.co/logstash/logstash-oss:7.0.1' locally`
	`docker: Error response from daemon: Get https://docker.elastic.co/v2/: dial tcp: lookup docker.elastic.co on 127.0.0.53:53: server misbehaving.`
	`Proofpoint Log Collector failed to start with error code 125`
		Resolve network issues and try again.