proofpoint.
CASB

Onboarding Zscaler ZIA Server

V1

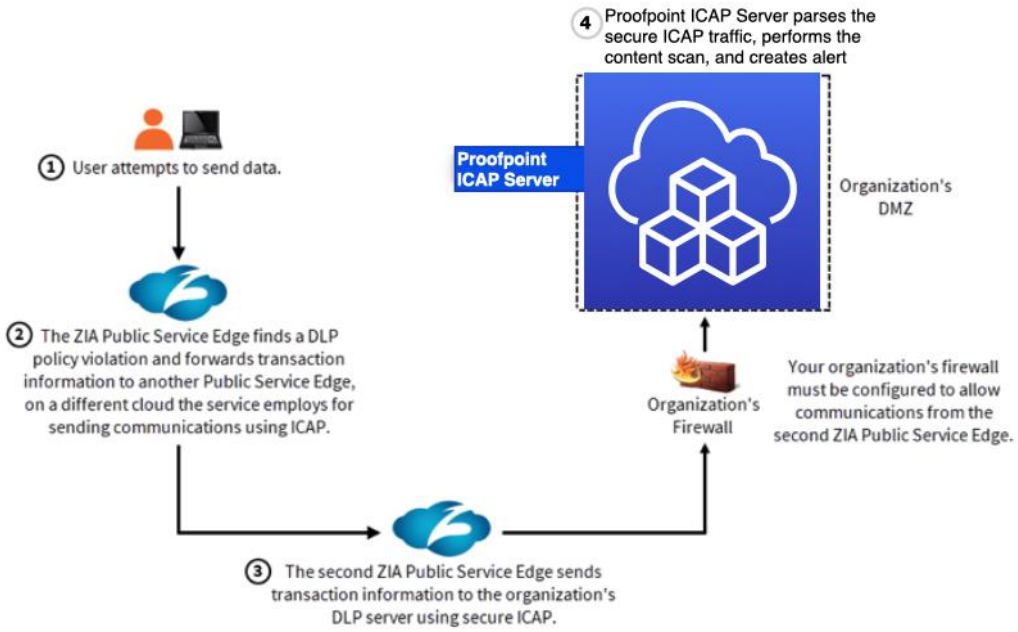
How to configure a Zscaler ZIA server to forward traffic to Proofpoint's public ICAP server

Overview

This document describes how to configure the Zscaler ZIA server to forward traffic to Proofpoint public ICAP server.

To begin protecting your Workplace, you will enable connectivity between your Workplace environment and the Proofpoint Cloud service. After configuration is complete, Proofpoint will initiate the on-boarding process which will help protect your environment against data loss, various threats, data risks, malicious outsider, insider threat, etc. Configuration is simple and is easily accomplished in just a few minutes by following these simple steps to enable the Proofpoint public ICAP service.
The diagram below shows the traffic flow:

1. Starting from the customer's end user when he uploads the file.
2. Zscaler system performs the preliminary processing.
3. Zscaler Zia Server relays the traffic to Proofpoint ICAP Server.
4. Proofpoint ICAP Server performs the DLP scan and reports the violations.



So, the general key configuration steps for this deployment will have three parts:

1. End user configuration. End user configuration will be required to install Zscaler client connector software. See Zscaler link for details: https://help.zscaler.com/client-connector . This document will not cover it.

2. Zscaler server configuration. See Zscaler document for details: https://help.zscaler.com/zia/step-step-configuration-guide-zia#policy This document will not cover it.

3. Proofpoint public ICAP configuration. This document will cover the sections below:
   - Quick Start: Configuration Steps
   - Onboarding to ZScaler and Proofpoint: Configuration Steps
   - Resources

The audience of this document are:

- Administrators who configure the DLP policy for customer
- ZScaler support engineers
- Proofpoint developers, support engineers, product/project managers

Prerequisites

The following is required to enable the connection:

- Proofpoint account to access platform console with admin role.

  https://oit-test1.explore.proofpoint.com

- Zscaler account to access Zscaler portal with admin role.
  https://admin.zscalerbeta.net/#dashboard/1

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.

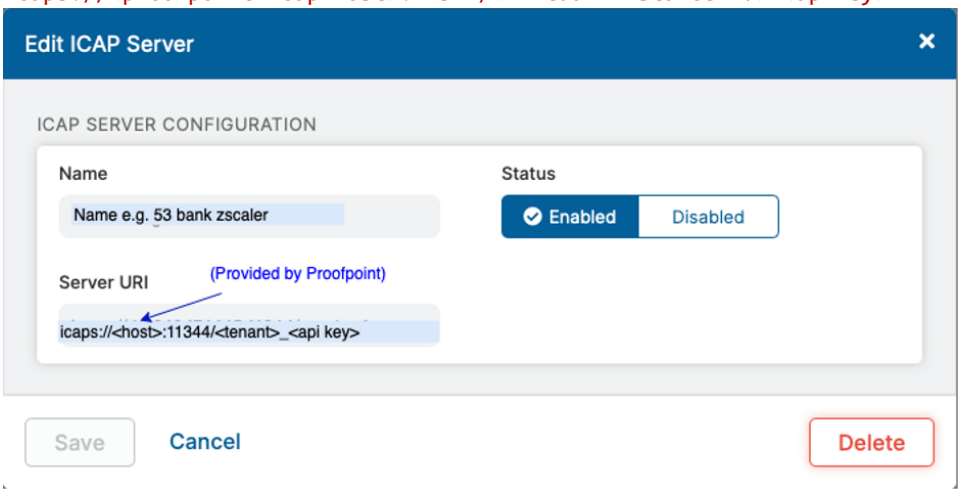
Quick Start

Enable to access Proofpoint public ICAP server

1. Sign in as admin (use Zscaler account) to Zscaler cloud portal https://admin.zscalerbeta.net/

2. Click to Administration → Cloud Configuration → DLP Incident Receiver → ICAP Settings → Add ICAP Receiver

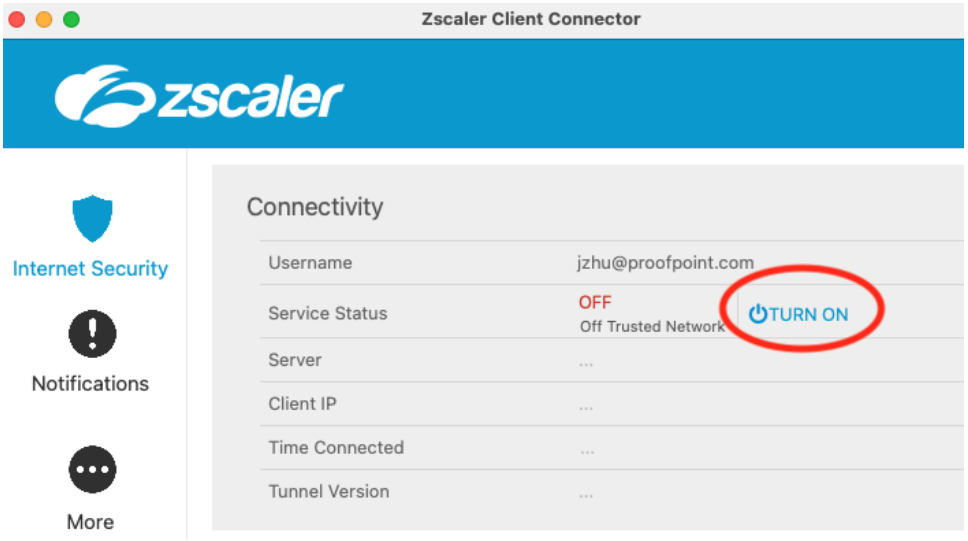
3. Input a name, Input the Server URI (Server URI will be provided by Proofpoint), Click Enabled button, and save it.
   `icaps://<proofpoint-icap-host>:11344/<virtual-instance-id>-<apikey>`



4. The configuration is complete.

Verify the Configuration

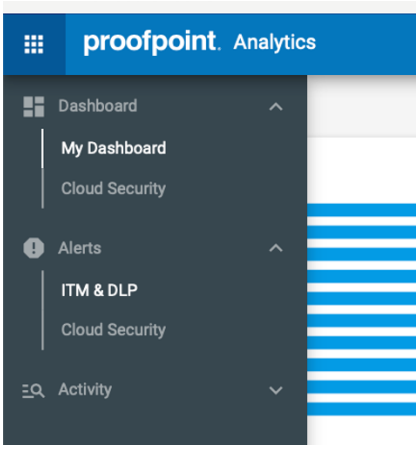
1. Turn on Zscaler client connector.



2. You can verify the configuration by using testing website like this: https://dataleaktest.com/uploader/upload-test3.aspx
    a. Click “Upload Test”
    b. Click “Choose File” to select your testing file (which contains the DLP file)
    c. Click “upload your File”

3. Login to Proofpoint DLP portal (use Proofpoint account) https://oit-test1.explore.proofpoint.com

4. Choose Analytics → Alerts → ITM&DLP to see the incident alert.



Onboarding customer

To enroll the customer, it takes two onboarding steps: Onboarding to Zscaler and onboarding to Proofpoint.

Two accounts are required to onboard the customer:

- Proofpoint account to access platform console with admin role. https://oit-test1.explore.proofpoint.com
- Zscaler account to access Zscaler portal with admin role. https://admin.zscalerbeta.net/#dashboard/1

Steps: Onboard to ZScaler

Here is the overview of the major steps to onboard Zscaler. For detailed configuration steps, please contact the Zscaler account manager and/or technical support team.

- End user client installation. This ensures that the end user traffic will be routed to the Zscaler ZIA server. See Zscaler link for details: https://help.zscaler.com/client-connector

- Zscaler cloud portal DLP configuration.

    a. Define DLP engines and dictionary
    b. Define DLP policy
    c. Define DLP incident receiver

Steps: Onboard to Proofpoint

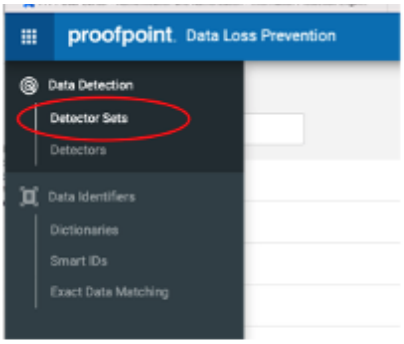
1. Create Proofpoint platform account. This account will allow customers (e.g., 5/3bank) to access Proofpoint Platform Console.

2. Get Configuration String and virtual instance ID. The configuration string format:

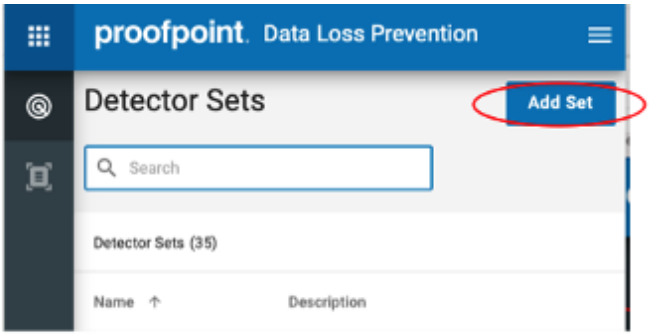
   icaps://<proofpoint domain>:11344/<virtual instance ID>-<Api-key>

   a. Login to the Proofpoint Platform Console https://oit-test1.explore.proofpoint.com

   b. Create DLP detector sets. Note: use zscaler-1 as detector sets name, do not use another name. If zscaler-1 already exists, modify it as needed

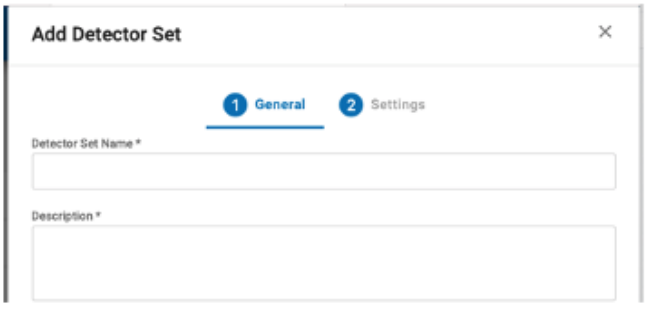


1

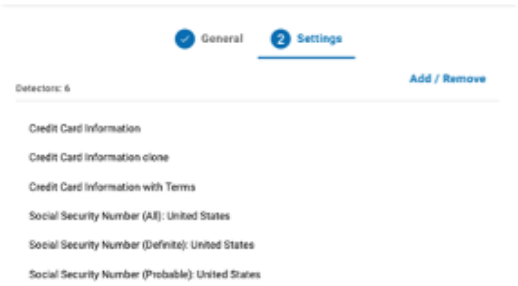


2

   c. Follow the wizard to add detectors and save it



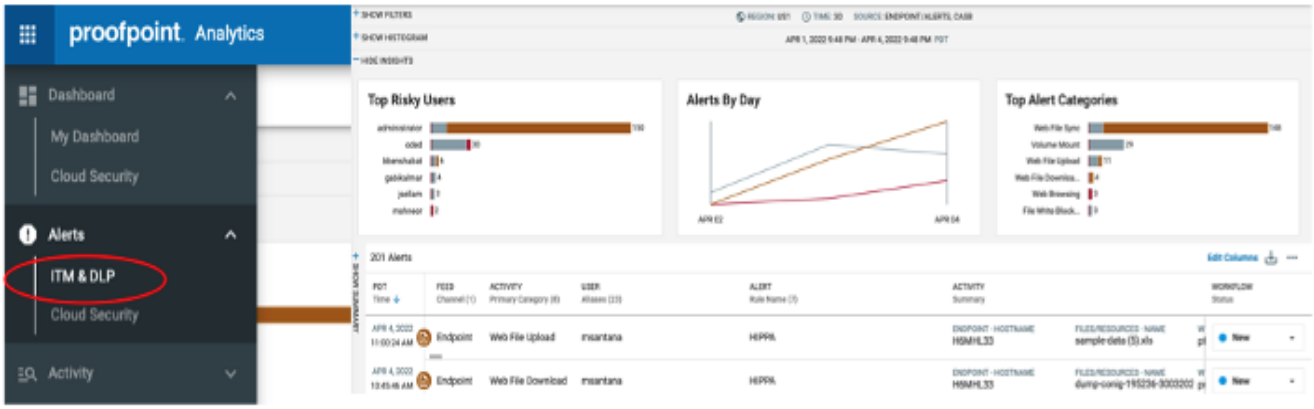
3



4

3. Check Alert.
    a. Login to the Proofpoint Platform Console https://oit-test1.explore.proofpoint.com

    b. Choose Analytics → Alerts → ITM&DLP to see the incident alert.



Resources

ZScaler Help Links

DLP Server Location
https://help.zscaler.com/zia/about-icap-communication-between-zscaler-and-dlp-servers

Server Configuration Portal
https://admin.zscalerbeta.net/

Documentation
https://help.zscaler.com/zia

Data Loss Prevention (DLP)
https://help.zscaler.com/zia/policies/data-loss-prevention

Create or Use a Predefined Dictionary and Engine
https://help.zscaler.com/zia/about-dlp-dictionaries

Configure DLP Policy
https://help.zscaler.com/zia/configuring-dlp-policy-rules-without-content-inspection

Sample ICAP Message

```
REQMOD icap://44.242.174.145:1344/entry-e9601cca-00c2-4a5c-8672-11eedfebbc98-
8fdc94d2-6a2c-4979-bd10-d8dcb75753e0 ICAP/1.0
User-Agent: ZICAP/1.0
Encapsulated: req-hdr=0, req-body=1067
Allow: 204
X-Client-IP: 172.79.197.231
X-Authenticated-User: TG9jYWw6Ly9jaHJpc3RvcGhlci5mYW50QDUzLmNvbQ==
X-DLP-Transaction-ID: 7021573009040202583
X-DLP-MD5: f3a296f63268da19df882439d1086e76

POST /origin-resource/form.pl HTTP/1.1
Host: www.origin-server.com
Accept: text/html, text/plain
Accept-Encoding: compress
Pragma: no-cache

1e
I am posting this information.
0
```