View Image Analysis Verdict Scores in mail_logs on ESA

Contents

Introduction

This document describes how to view the Image Analysis verdict score for a message on an ESA running AsyncOS for Email Security.

Overview

ESA stands for Cisco Email Security Appliance. Image Analysis requires a license to enable. Some messages contain images that an organization can scan for inappropriate content. Image Analysis is not designed to supplement or replace anti-virus and anti-spam scanning engines. Its purpose is to enforce acceptable use by identifying inappropriate content in email.

After configuring Cisco AsyncOS for Email Security for Image Analysis, use Image Analysis filter rules to perform actions on suspect or inappropriate email.

Supported File Types

Image Analysis can scan the attached image file types:

- BMP
- GIF
- ICO
- JPEG
- PCX
- PNG
- TGA
- TIFF

The image analyzer uses algorithms that measure skin color, body size, and curvature to determine the probability that a graphic contains inappropriate content. When scanning image attachments, Cisco

fingerprinting determines the file type and the image analyzer evaluates the image content. If an image is embedded in another file, the Stellent scanning engine extracts the image (for example, from Word, Excel, and PowerPoint documents). The Image Analysis verdict is computed for the message as a whole. If a message contains no images, Image Analysis assigns a score of 0 (Clean).

Note: Images cannot be extracted from PDF files.

Prerequisites

- Image Analysis license installed.
- Image Analysis enabled in Cisco AsyncOS for Email Security (AsyncOS).
- Access to **mail_logs** (CLI or GUI access) and the message ID (MID) for the message to investigate.

Limitations

- Verdict is computed for the message as a whole; mail logs report results per attachment (for example, a ZIP attachment shows the ZIP filename and the maximum score of images inside it).
- Images cannot be extracted from PDF files.

View the Verdict Score of a Particular Message

Procedure

1. Identify the message ID (MID) for the message.
2. Access **mail_logs** (from the GUI or CLI, depending on the deployment).
3. Search for log entries that include the MID and **Image Analysis**.
4. Record the attachment name, **score**, and whether the attachment is marked **unscannable**.
5. Review subsequent log lines for the action taken (for example, filter rule action, quarantine, or drop).

Expected Results

Log entries show the attachment name, the Image Analysis score, and whether the attachment was scannable or unscannable. The logs do not directly map scores to verdict labels.

This example shows Image Analysis-related entries in **mail_logs**:

```
Thu Apr 3 08:17:56 2009 Debug: MID 154 IronPort Image Analysis: image 'Unscannable.jpg'
 is unscannable.
Thu Apr 3 08:17:56 2009 Info: MID 154 IronPort Image Analysis: attachment
 'Unscannable.jpg' score 0 unscannable
Thu Apr 3 08:17:56 2009 Info: MID 6 rewritten to MID 7 by
 drop-attachments-where-image-verdict filter 'f-001'
Thu Apr 3 08:17:56 2009 Info: Message finished MID 6 done
```

Related Information

- AsyncOS Email User Guide

- GLO Support Contact Information
- Technical Support & Documentation - Cisco Systems