Configure Threat Scanner Per-Policy Scanning for SEG

Contents

Introduction

Prerequisites

Components Used

Overview

Configure

Web Interface Setup

Command Line Interface Setup

Verify

Related Information

Introduction

This document describes the service and configuration of Threat Scanner (TS) Per Policy Integration for the Cisco Secure Email Gateway (SEG).

Prerequisites

Knowledge of the SEG general settings and configuration is desired.

Components Used

The information in this document is based on these software versions:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 and newer.
- Graymail Service.
- Antispam Service.
- Incoming Mail Policies.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Threat Scanner (TS) a newly activated sub-component of the Graymail service, has been integrated with Antispam CASE providing more effective of AntiSpam detection.

Once the Graymail service has been activated, options to enable Threat Scanner become active within each Incoming Mail Policy AntiSpam setting. Once enabled TS improves overall Antispam detection with an emphasis on HTML Smuggling detection:

- HTML parsing and malicious script detection

- URL parsing and redirection detection

The Antispam CASE engine governs the two services, managing updates and spam convictions.

TS has visible enable/disable settings within each Incoming Mail Policy Antispam setting.

TS influences verdicts, increasing the weight of the final Antispam CASE verdict.

Configure

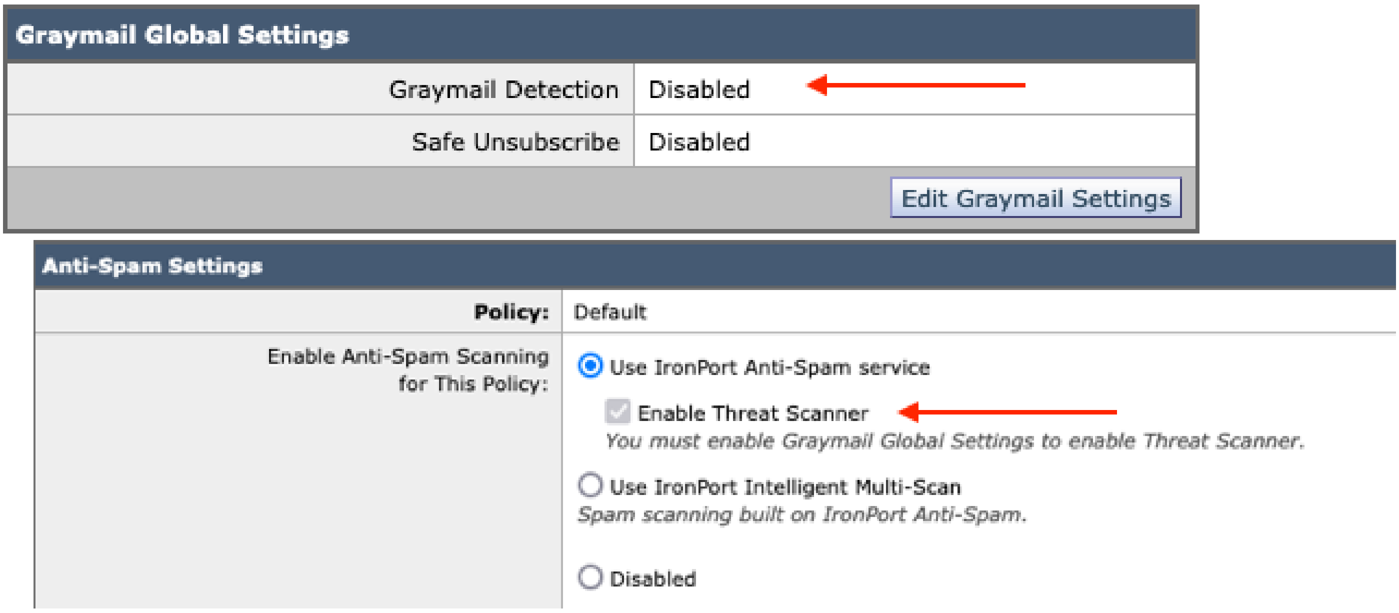
Configuration consists of two actions; Enable Graymail Detection and Enabling TS within the Incoming Mail Poilces.

- The Graymail global service must be enabled to activate TS.
- The Inbound Mail Policy “Antispam” option to “Enable Threat Scanner” becomes available once Graymail has been enabled globally.

Web Interface Setup

To enable Graymail within the WebUIl:

- Navigate to Security services
  - IMS and Graymail
    - Graymail Global Settings
      - Edit Graymail Settings.
        - Select the option to enable Graymail Detection.
- Submit and Commit the Changes to finalize the action.



Graymail Global Settings

Graymail Detection	Disabled
Safe Unsubscribe	Disabled

Anti-Spam Settings

Policy: Default

Enable Anti-Spam Scanning for This Policy:

● Use IronPort Anti-Spam service

☑ Enable Threat Scanner

You must enable Graymail Global Settings to enable Threat Scanner.

○ Use IronPort Intelligent Multi-Scan

Spam scanning built on IronPort Anti-Spam.

○ Disabled

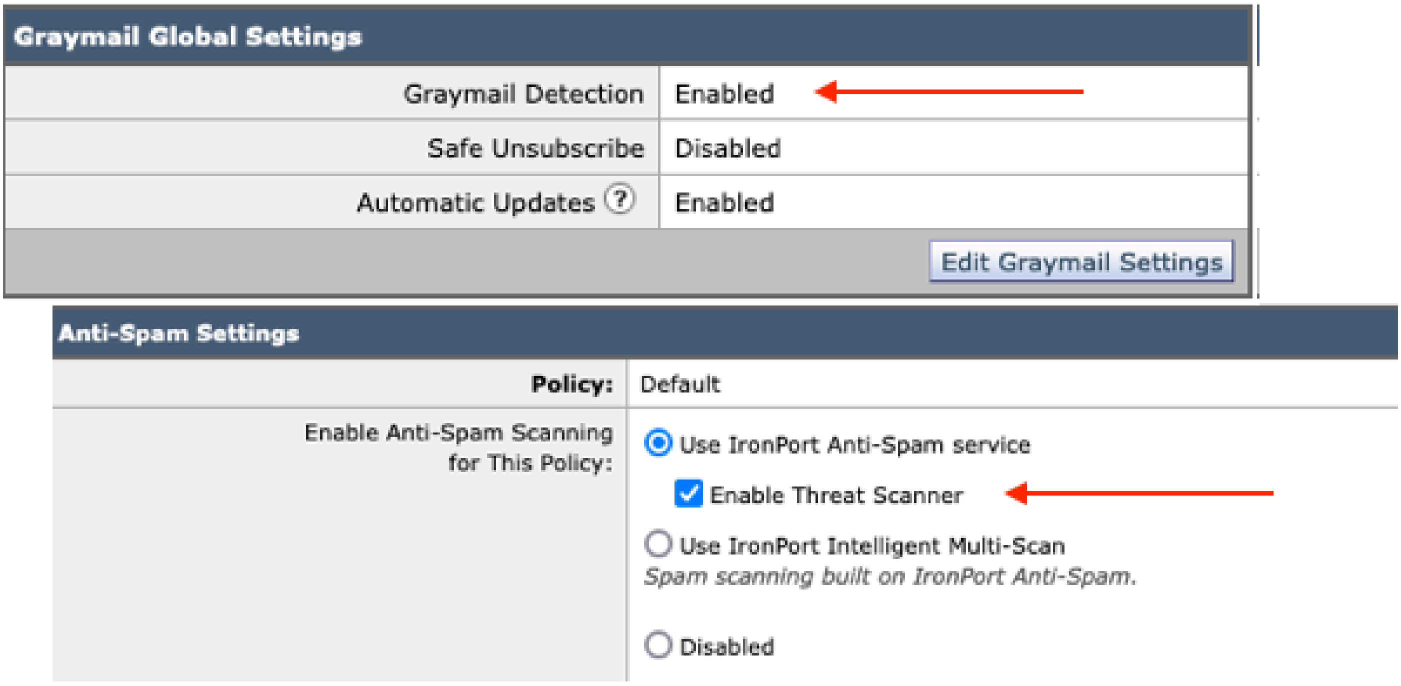
The view prior to setup

Once Graymail has been enabled, The Threat Scanner selection box becomes available for each Incoming Mail Policy.

To enable Threat Scanner within the WebUI:

- Navigate to Mail Policies

    - Incoming Mail Policies
        - Select the desired Mail Policy
            - Select Anti-Spam.
                - The top of the configuration page presents the check box option to Enable Threat Scanner.
- Submit and Commit the Changes to finalize the configuration



Graymail Global Settings

Graymail Detection	Enabled
Safe Unsubscribe	Disabled
Automatic Updates	Enabled

Anti-Spam Settings

Policy:	Default
Enable Anti-Spam Scanning for This Policy:	● Use IronPort Anti-Spam service ☑ Enable Threat Scanner ○ Use IronPort Intelligent Multi-Scan *Spam scanning built on IronPort Anti-Spam.* ○ Disabled

Threat Scanner Option within Antispam

Command Line Interface Setup

Enable the Graymail Service using the CLI commands.

- imsandgraymailconfig
    - graymail
        - setup
            - Would you like to use Graymail Detection? [Y] >
                - Would you like to enable automatic updates for Graymail engine? [Y]>
    - Complete the remaining prompts to return to the main machine prompt.

- Commit + add desired comments > Complete the action by pressing the “Return” key.

Enabling or disabling Threat Scanner within a Policy from the CLI.

- CLI> policyconfig

Would you like to configure Incoming Mail Policy or Outgoing Mail Policies or Match Headers Priority?

1. **Incoming Mail Policies**
2. Outgoing Mail Policies
3. Match Headers Priority

[1]> **1**

incoming Mail Policy Configuration

```
1. North1
2. BLOCKED_LIST
3. ALLOWED_LIST
4. ALLOW_SPOOF
5. DEFAULT


Enter the name or number of the entry you wish to edit:
[]> 1

Choose the operation you want to perform:
- NAME - Change name of policy
- NEW - Add a new policy member row
- DELETE - Remove a policy member row
- PRINT - Print policy member rows
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- OUTBREAK - Modify Outbreak Filters policy
- ADVANCEDMALWARE - Modify Advanced Malware Protection policy
- GRAYMAIL - Modify Graymail policy
- THREATDEFENSECONNECTOR - Modify Threat Defense Connector
- FILTERS - Modify filters
[]> antispam


Choose the operation you want to perform:
- DISABLE - Disable Anti-Spam policy (Disables all policy-related actions)
- ENABLE - Enable Anti-Spam policy
[]> enable

Begin Anti-Spam configuration

Would you like to use Intelligent Multi-Scan on this policy? [N]>

Would you like to use IronPort Anti-Spam on this policy? [Y]>

Some messages are positively identified as spam. Some messages are
identified as suspected spam. You can set the IronPort Anti-Spam Suspected Spam
Threshold below.
The configuration options apply to messages POSITIVELY identified as
spam:
Do you want to enable special treatment for Threat Scanner verdict? [N]> y
```

Continue through the menu selections to complete the Mail Policy choices, and press the "return key" to accept the default action for each choice.

Complete the save with the commands.

- Commit + add desired comments > Complete the action by pressing the “Return” key.

Verify

How to read and interpret the logs.

Mail Logging of Threat Scanner presents an interim verdict only, while CASE presents the final verdict.

The mail logs show two different verbiages for clean vs convicted Threat Scanner Verdicts

- If the Threat Scanner Interim verdict is clean, the log is presented similarly to these samples.
  - Info: **interim graymail verdict** - LEGIT (0) <Clean message>
  - Info: **interim graymail verdict** - MCE (11) <Miscellaneous email campaign>
- If the Threat Scanner Interim verdict is to convict, the log is presented similarly to these samples.
  - Info: **interim ThreatScanner verdict - PHISHING (101)**
  - Info: **interim ThreatScanner verdict - VIRUS (2)**

Mail Logs Sample: Threat Scanner Clean verdict uses different verbiage: graymail verdict.

<#root>

```
Wed Jan 31 08:19:32 2024 Info: MID 3189755
```

`interim graymail verdict - LEGIT (0) <Clean message>`

```
Wed Jan 31 08:19:33 2024 Info: MID 3189755 interim verdict using engine: CASE negative
Wed Jan 31 08:19:33 2024 Info: MID 3189755 using engine: CASE spam negative
```

Message Tracking does not show the Threat Scanner log entry, only the CASE: Final Verdict.

These samples of Threat Scanner (TS) present the 4 verdict scenarios.

Note: TS categories of “PHISHING” and “VIRUS” are the only detection that increase the weight of the CASE Verdict

Mail Logs Sample: PHISHING TS Conviction and AntiSpam Conviction both are present

<#root>

```
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

`interim`

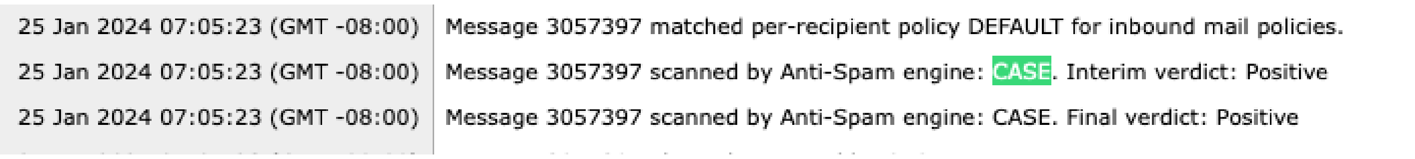
`ThreatScanner verdict - PHISHING (101)`

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:23 2024 Info: MID 3057397 interim verdict using engine: CASE spam positive
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

`using engine: CASE spam positive`

```
Thu Jan 25 09:05:23 2024 Info: Message aborted MID 3057397 Dropped by CASE
```

Tracking sample: PHISHING TS Conviction is absent and CASE Conviction is present.



```
25 Jan 2024 07:05:23 (GMT -08:00)   Message 3057397 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:23 (GMT -08:00)   Message 3057397 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 07:05:23 (GMT -08:00)   Message 3057397 scanned by Anti-Spam engine: CASE. Final verdict: Positive
```

PHISHING TS Convicted and AntiSpam Convicted Tracking

Mail Logs Sample: PHISHING TS Conviction and AntiSpam Negative both are present.

<#root>

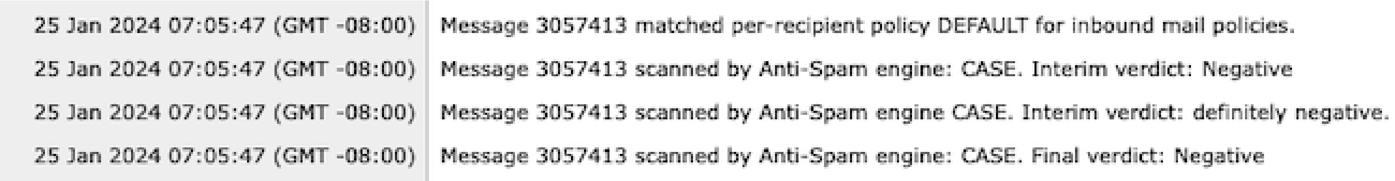
```
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

`interim ThreatScanner verdict - PHISHING (101)`

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:47 2024 Info: MID 3057413 interim verdict using engine: CASE spam negative
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

`using engine: CASE spam negative`

Tracking sample: PHISHING TS Convicted and AntiSpam Negative is present.



```
25 Jan 2024 07:05:47 (GMT -08:00)   Message 3057413 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:47 (GMT -08:00)   Message 3057413 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
25 Jan 2024 07:05:47 (GMT -08:00)   Message 3057413 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
25 Jan 2024 07:05:47 (GMT -08:00)   Message 3057413 scanned by Anti-Spam engine: CASE. Final verdict: Negative
```

Mail Logs Sample: VIRUS TS Conviction and AntiSpam Conviction sample of the mail logs.

<#root>

```
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim
```

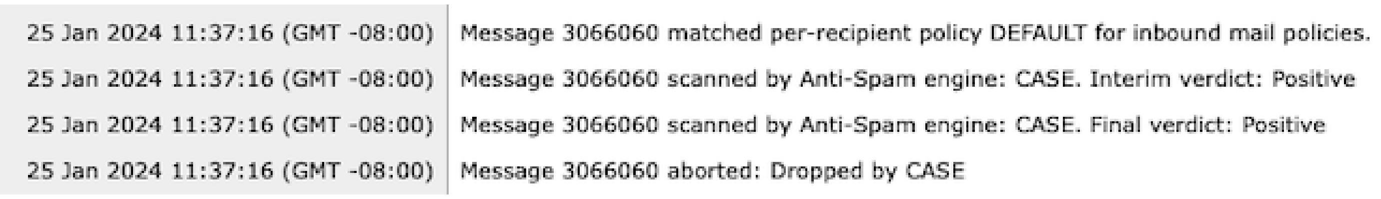
`ThreatScanner verdict - VIRUS (2)`

```
 <Virus detected by ThreatScanner engine>
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim verdict using engine: CASE spam positive
Thu Jan 25 13:37:16 2024 Info: MID 3066060
```

`using engine: CASE spam positive`

```
Thu Jan 25 13:37:16 2024 Info: Message aborted MID 3066060 Dropped by CASE
```

Tracking sample: VIRUS TS Conviction absent and AntiSpam Conviction is present.



```
25 Jan 2024 11:37:16 (GMT -08:00)   Message 3066060 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 11:37:16 (GMT -08:00)   Message 3066060 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)   Message 3066060 scanned by Anti-Spam engine: CASE. Final verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)   Message 3066060 aborted: Dropped by CASE
```

Mail Logs Sample: VIRUS TS Conviction and AntiSpam Negative are both present.

<#root>

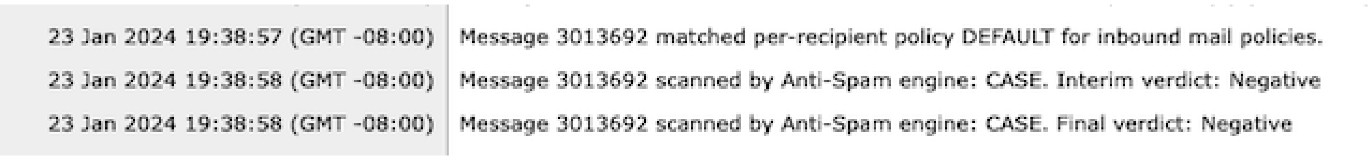
```
Jan 23 21:38:57 2024 Info: MID 3013692
```

```
interim ThreatScanner verdict - VIRUS (2)
```

```
 <Virus detected by ThreatScanner engine>
Jan 23 21:38:58 2024 Info: MID 3013692 interim verdict using engine: CASE spam negative
Jan 23 21:38:58 2024 Info: MID 3013692
```

```
using engine: CASE spam negative
```

Tracking sample: VIRUS TS Conviction absent and AntiSpam Negative is present.



23 Jan 2024 19:38:57 (GMT -08:00)	Message 3013692 matched per-recipient policy DEFAULT for inbound mail policies.
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Final verdict: Negative

Graymail Logs contain Threat Scanner verdict and supporting content for TALOS analysis if a false positive challenge is made.

The presence of the Threat Scanner raw results caused the Graymail logging to rollover more rapidly. To address this behavior the SEG modifications have been made to the Graymail Logs.

- AsyncOS 15.5 sets the Default Log Subscription for Graymail log files to 20 for increased log retention.
  - No log File settings change if the setting is set higher than 20 upon upgrade.
- Inbound Graymail Interim convicted messages display full scan raw results, at the Information Level.
- Graymail scan results for all other messages display at the Debug Level.

Related Information

- Email Security Setup Guide
- Cisco Secure Email Gateway Launch Page to Support Guides