为SEG配置按策略扫描的威胁扫描程序

目录

简介

本文档介绍思科安全邮件网关(SEG)的按策略集成的威胁扫描程序(TS)的服务和配置。

先决条件

需要了解SEG常规设置和配置。

使用的组件

本文档中的信息基于以下软件版本：

- 思科安全邮件网关(SEG) AsyncOS 15.5.1及更高版本。
- 灰色邮件服务。
- 反垃圾邮件服务。
- 传入邮件策略。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

威胁扫描(TS)是灰色邮件服务新激活的子组件，已与AntiSpam CASE集成，可提供更有效的反垃圾邮件检测。

激活灰色邮件服务后，在每个传入邮件策略AntiSpam设置内，启用威胁扫描器的选项会变为活动状态。启用TS后，TS将改善整体反垃圾邮件检测，重点关注HTML走私检测：

- HTML解析和恶意脚本检测
- URL解析和重定向检测

反垃圾邮件CASE引擎控制这两种服务，即管理更新和垃圾邮件判定。

TS在每个传入邮件策略反垃圾邮件设置中有可见的启用/禁用设置。

TS影响判定，增加最终反垃圾邮件案例判定的权重。

配置

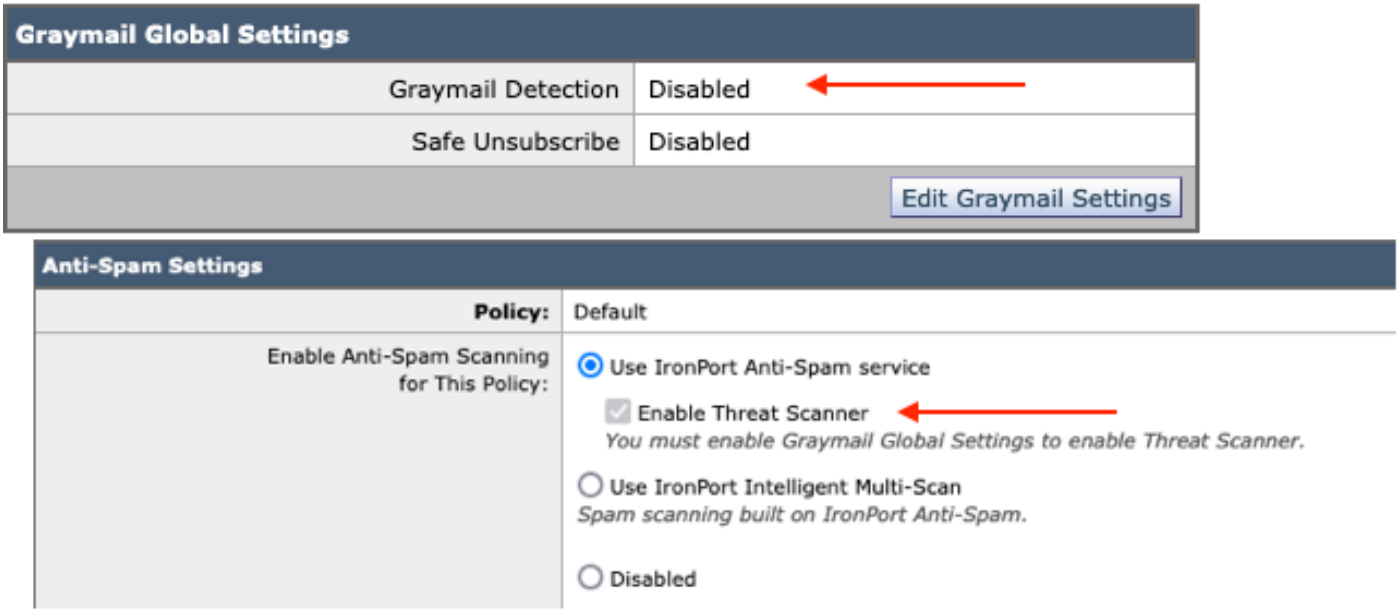
配置包括两个操作：启用灰色邮件检测和启用传入邮件策略中的TS。

- 必须启用灰色邮件全局服务才能激活TS。
- 全局启用灰色邮件后，入站邮件策略“反垃圾邮件”(Anti-spam)选项“启用威胁扫描程序”(Enable Threat Scanner)将变为可用。

Web界面设置

要在WebUII中启用灰色邮件，请执行以下操作：

- 导航到安全服务
  - IMS和灰色邮件
    - 灰色邮件全局设置
      - 编辑灰色邮件设置。
        - 选择选项以启用灰色邮件检测。
- 提交并确认更改，以完成操作。



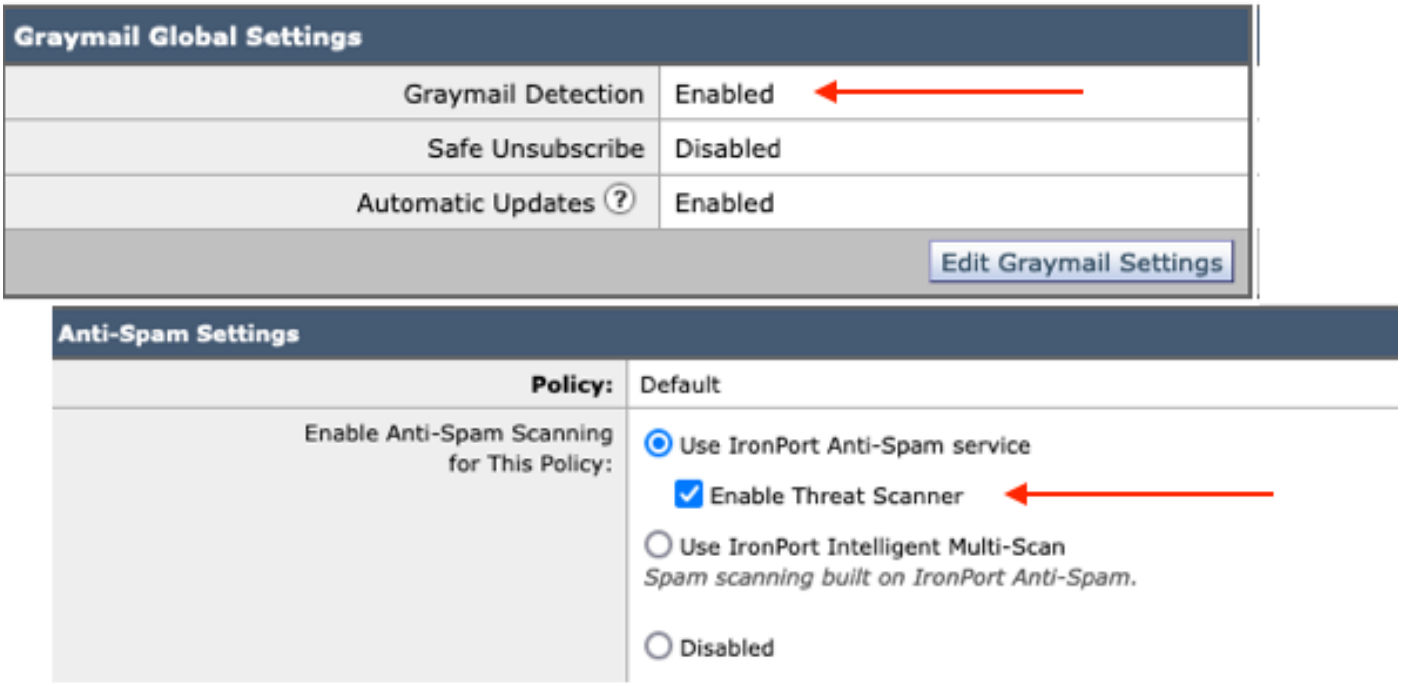
设置前的视图

启用灰色邮件后，威胁扫描程序选择框可用于每个传入邮件策略。

要在WebUI中启用威胁扫描程序，请执行以下操作：

- 导航至“邮件策略”(Mail Policies)
  - 传入邮件策略

- 选择所需的邮件策略
  - 选择Anti-Spam。
    - 配置页面顶部显示了用于启用威胁扫描程序的复选框选项。
- 提交并确认更改，以完成配置



反垃圾邮件中的威胁扫描程序选项

命令行界面设置

使用CLI命令启用灰色邮件服务。

- imsandgraymailconfig
  - 灰色邮件
    - 设置
      - 是否要使用灰色邮件检测？[Y] >
        - 是否要启用灰色邮件引擎的自动更新？[Y]>
  - 完成其余提示以返回主机提示符。

- 提交+添加所需的注释>按“Return”键完成操作。

从CLI启用或禁用策略中的威胁扫描程序。

- CLI> policyconfig

是否要配置传入邮件策略、传出邮件策略或匹配信头优先级？

1. 传入邮件策略
2. 外发邮件策略
3. 匹配报头优先级

[1]> 1

传入邮件策略配置

1. 北1
2. BLOCKED_LIST
3. ALLOW_LIST
4. 允许_欺骗
5. 默认

输入要编辑的条目的名称或编号：
[]> 1

选择要执行的操作：
- NAME -更改策略名称
- 新建-添加新策略成员行
- 删除-删除策略成员行
- PRINT -打印策略成员行
- 反垃圾邮件-修改反垃圾邮件策略
- 防病毒-修改防病毒策略
- 病毒爆发-修改病毒爆发过滤器策略
- 高级恶意软件-修改高级恶意软件防护策略
- 灰色邮件-修改灰色邮件策略
- THREATDEFENSECONNECTOR -修改威胁防御连接器
- 过滤器-修改过滤器
[]>反垃圾邮件

选择要执行的操作：
- DISABLE -禁用反垃圾邮件策略（禁用所有策略相关操作）
- 启用-启用反垃圾邮件策略
[]>启用

开始反垃圾邮件配置

是否要对此策略使用智能多重扫描？[N]>

是否要在此策略中使用IronPort反垃圾邮件？[Y]>

某些邮件被明确标识为垃圾邮件。某些消息是
识别为可疑垃圾邮件。您可以设置IronPort反垃圾邮件疑似垃圾邮件
低于阈值。
配置选项适用于POSITIVELY IDENTIFIED AS消息
垃圾邮件：
是否要启用对威胁扫描程序裁决的特殊处理？[N]>是

继续选择菜单以完成邮件策略选择，然后按“返回键”接受每个选择的默认操作。

使用命令完成保存。

- 提交+添加所需的注释>按“Return”键完成操作。

验证

如何阅读和解释日志。

Threat Scanner的邮件日志记录仅提供临时裁决，而CASE提供最终裁决。

邮件日志显示了两种不同的正常与已判定威胁扫描程序判定的判定

- 如果威胁扫描程序临时判定是正常的，则日志的显示方式与这些示例类似。
  - 信息：临时灰色邮件裁决- LEGIT (0) <正常邮件>
  - 信息：临时灰色邮件裁决- MCE (11) <其他电子邮件活动>
- 如果威胁扫描程序临时判定有罪，则日志的显示方式与这些示例类似。
  - 信息：临时ThreatScanner裁决-网络钓鱼(101)
  - 信息：临时ThreatScanner裁决-病毒(2)

邮件日志示例：威胁扫描程序清除裁决使用不同的措辞：灰色邮件裁决。

<#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
```

邮件跟踪不显示威胁扫描程序日志条目，仅显示CASE：最终裁决。

这些威胁扫描程序(TS)样本提供了4种判定方案。

注意：“网络钓鱼”和“病毒”的TS类别是唯一能够增加案例判定权重的检测

邮件日志示例：存在网络钓鱼TS定罪和反垃圾邮件定罪

<#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

跟踪示例：不存在网络钓鱼TS定罪且存在CASE定罪。

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

网络钓鱼TS被定罪和反垃圾邮件被定罪的跟踪

邮件日志示例：存在网络钓鱼TS定罪和AntiSpam否定。

<#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

跟踪示例：存在网络钓鱼TS判定和AntiSpam阴性。

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

邮件日志示例：邮件日志的VIRUS TS Conviction和AntiSpam Conviction示例。

<#root>

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

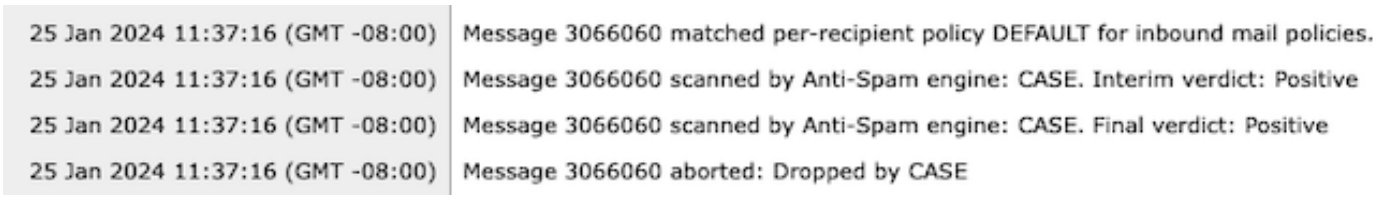
ThreatScanner verdict - VIRUS (2)

<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

跟踪示例：未发现病毒TS判定，且存在反垃圾邮件判定。



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

邮件日志示例：病毒TS判定和AntiSpam Negative均存在。

<#root>

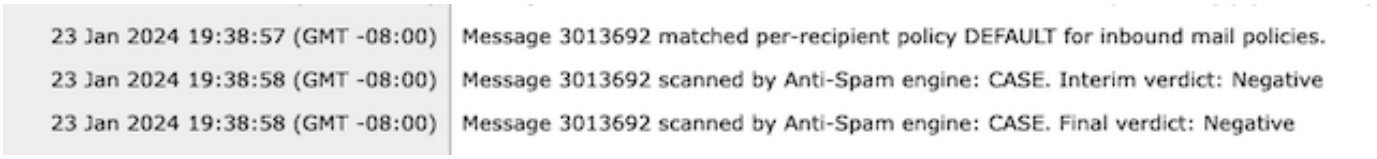
```
Jan 23 21:38:57 2024 Info: MID 3013692
```

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

跟踪示例：未发现病毒TS判定，且存在反垃圾邮件阴性。



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

灰色邮件日志包含威胁扫描程序判定以及用于TALOS分析的支持内容（如果出现误报质询）。

威胁扫描程序原始结果的存在导致Graymail日志记录更快速地回滚。为了解决此行为，已对灰色邮件日志进行了SEG修改。

- AsyncOS 15.5将灰色邮件日志文件的默认日志订阅设置为20，以提高日志保留率。
  - 如果在升级时设置大于20，则日志文件设置不会更改。
- 入站灰色邮件临时判定邮件在“信息级别”显示完整扫描原始结果。
- 所有其他邮件的灰色邮件扫描结果显示在调试级别。

相关信息

- 邮件安全设置指南
- 支持指南的思科安全电邮网关发布页面

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。