解决与"；相关的问题，已被IP信誉过滤"；阻止

目录

简介

本文档介绍对指示“IP信誉过滤”停止的邮件的报告的常见查询。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全邮件设备

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全邮件设备

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。

背景信息

IP信誉过滤是垃圾邮件防护的第一层，它根据发件人IP信誉服务确定的发件人可信度来控制通过邮件网关的邮件。本文讨论如何解决与IP信誉过滤有关的问题。

问题

通过导航到Monitor > Incoming Mail访问ESA/CES设备中的报告时，某些邮件似乎被“IP信誉过滤”阻止。 在某些情况下，尝试的邮件总数与IP信誉过滤阻止的邮件总数相符，这令人担心其准确性。此外，可能很难找到被阻止的特定邮件。

一个常见问题是无法生成被IP信誉过滤阻止的电子邮件列表，从而导致合法电子邮件是否被错误过滤的混乱。

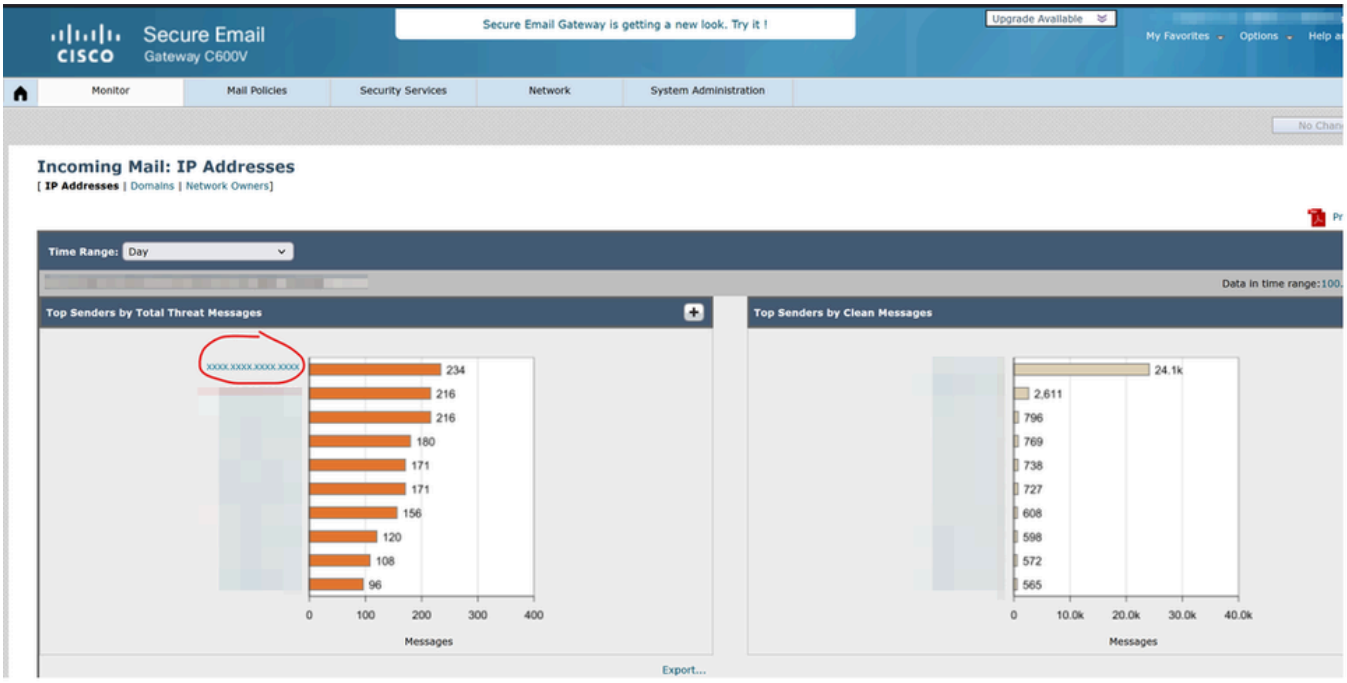
解决方案

IP信誉过滤功能类似于ESA设备中的发件人基本信誉得分(SBRS)，使用可比计算方法。

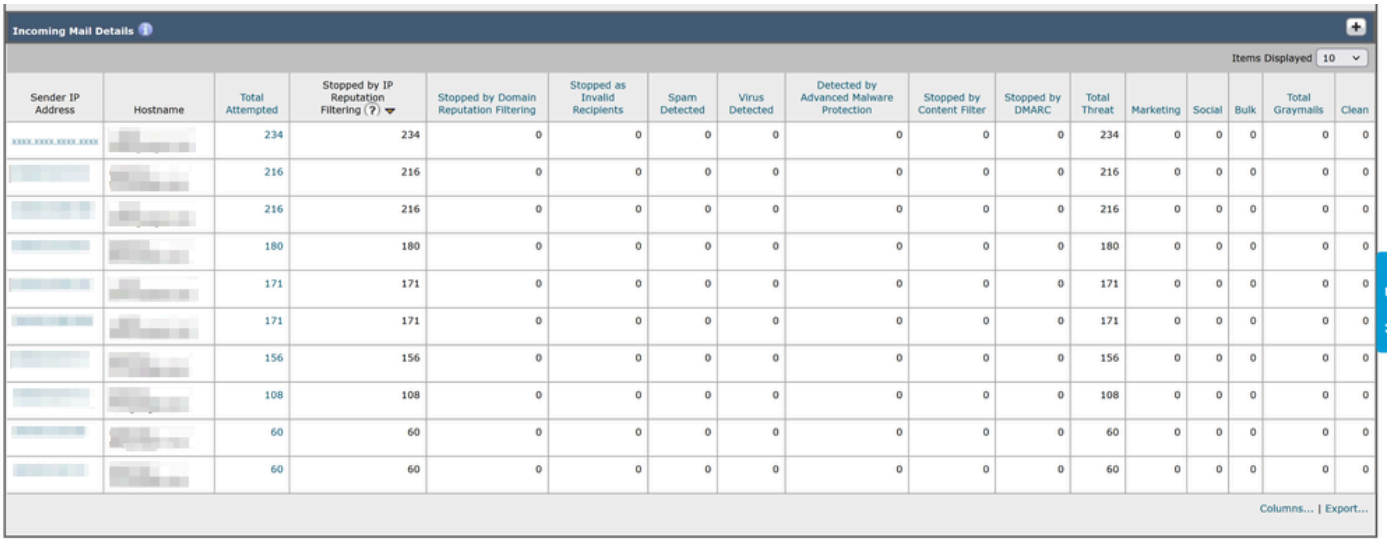
了解IP信誉过滤

发件人IP信誉过滤是垃圾邮件防护的第一层，它允许根据发件人IP信誉服务确定的发件人可信度来控制通过邮件网关的邮件。IP信誉服务使用来自Talos关联网络的全局数据，根据投诉率、邮件量统计信息以及来自公开阻止列表和开放代理列表的数据，向邮件发件人分配IP信誉得分(IPRS)。IP信誉得分有助于区分合法发件人和垃圾邮件来源。您可以确定阻止来自信誉得分低的发件人的邮件的阈值。Talos智能(Talos Intelligence)提供最新邮件和基于Web的威胁的全局概述，按国家/地区显示当前邮件流量，并允许您根据IP地址、URI或域查找信誉得分。

本示例解释了IP信誉过滤的工作原理：



排名靠前的发件人



Incoming Mail Details

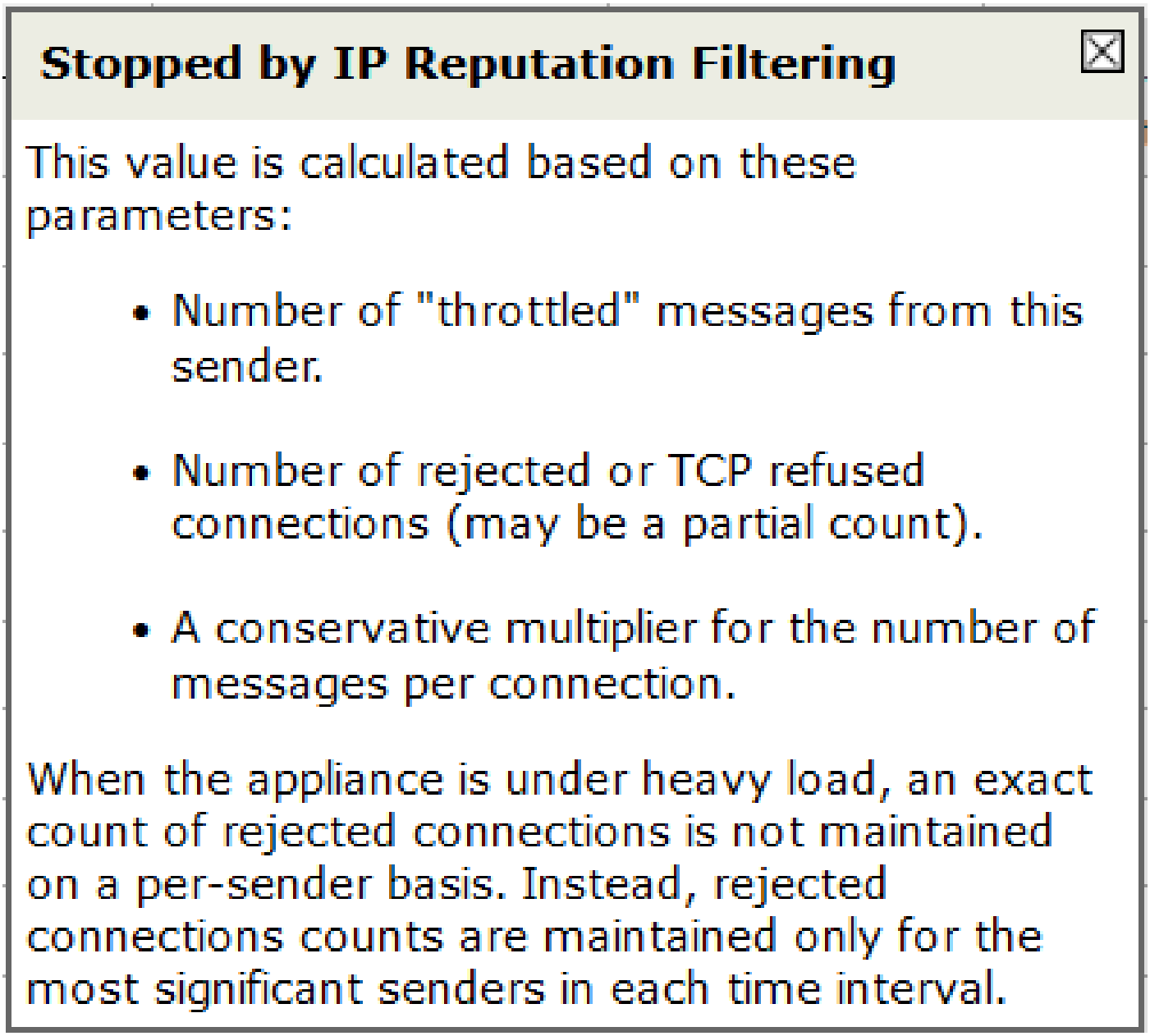
Items Displayed 10

Sender IP Address	Hostname	Total Attempted	Stopped by IP Reputation Filtering	Stopped by Domain Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Detected by Advanced Malware Protection	Stopped by Content Filter	Stopped by DMARC	Total Threat	Marketing	Social	Bulk	Total Graymails	Clean
XXXX.XXXX.XXXX.XXXX	[redacted]	234	234	0	0	0	0	0	0	0	234	0	0	0	0	0
[redacted]	[redacted]	216	216	0	0	0	0	0	0	0	216	0	0	0	0	0
[redacted]	[redacted]	216	216	0	0	0	0	0	0	0	216	0	0	0	0	0
[redacted]	[redacted]	180	180	0	0	0	0	0	0	0	180	0	0	0	0	0
[redacted]	[redacted]	171	171	0	0	0	0	0	0	0	171	0	0	0	0	0
[redacted]	[redacted]	171	171	0	0	0	0	0	0	0	171	0	0	0	0	0
[redacted]	[redacted]	156	156	0	0	0	0	0	0	0	156	0	0	0	0	0
[redacted]	[redacted]	108	108	0	0	0	0	0	0	0	108	0	0	0	0	0
[redacted]	[redacted]	60	60	0	0	0	0	0	0	0	60	0	0	0	0	0
[redacted]	[redacted]	60	60	0	0	0	0	0	0	0	60	0	0	0	0	0

Columns... | Export...

传入邮件详细信息

IP XXXX.XXXX.XXXX.XXXX已发送234封电子邮件，所有这些邮件似乎都被IP信誉过滤阻止。但是，对设备中的邮件跟踪和mail_logs的分析显示，来自此IP的邮件已成功传送，没有证据显示IP信誉过滤会阻止邮件。



适用于IP信誉过滤的条件

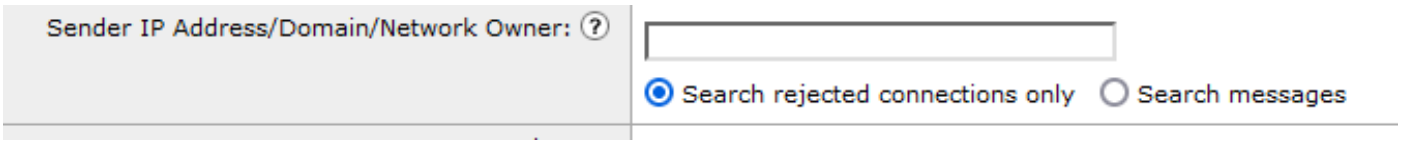
IP信誉过滤根据特定参数计算，如参考屏幕截图所示。在某些情况下，电子邮件可以与第三个条件保持一致，即每个连接的邮件数量的保守乘数。拒绝日志仅在电子邮件满足前两个条件时才可见。但是，设备可以基于此乘数显示预计数量的邮件。

报告可以反映大约数量的连接，其中一些连接实际上无法到达设备。例如，已建立简单邮件传输协议(SMTP)连接，但稍后由于网络问题而被丢弃。第三个条件考虑此类情况，提供连接通过还是未通过IP信誉检查的估计分析。这并不一定表示列出的所有邮件都被IP信誉过滤阻止。

验证阻止的电子邮件

要确定邮件是否被实际阻止，请执行以下操作：

- 检查阻止列表发件人组：被IP信誉过滤阻止的邮件归入阻止列表发件人组。
- 使用邮件跟踪：导航到高级选项，输入要搜索的IP地址，然后选择仅搜索拒绝的连接。



在邮件跟踪中搜索拒绝的连接

- 查看邮件日志：可以在mail_logs中标识被阻止列表发件人组阻止的邮件。
- 延迟的HAT拒绝：IP过滤在SMTP连接级别实施，ESA上的Delayed Host Access Table(HAT)Reject功能可用于了解原因。

相关信息

- HAT延迟拒绝常见问题
- Cisco ESA用户指南
- 思科技术支持和下载

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）。