排除與"；由IP信譽過濾"；停止的相關問題

目錄

簡介

本文檔介紹對指示通過「IP信譽過濾」停止的電子郵件的報告的常見查詢。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全電子郵件裝置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全電子郵件裝置

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

IP信譽過濾是垃圾郵件防護的第一層，它允許根據發件人的可信度（由發件人IP信譽服務確定）來控制通過郵件網關的郵件。本文討論如何解決與IP信譽過濾有關的問題。

問題

導航到Monitor > Incoming Mail訪問ESA/CES裝置中的報告時，某些電子郵件似乎被「IP信譽過濾」阻止。 在某些情況下，嘗試傳送的電子郵件總數與通過IP信譽過濾阻止的電子郵件總數相符，這令人擔心其準確性。此外，可能難以找到被阻止的特定電子郵件。

一個常見問題是無法生成受IP信譽過濾阻止的電子郵件清單，從而導致合法電子郵件是否被錯誤過濾的困惑。

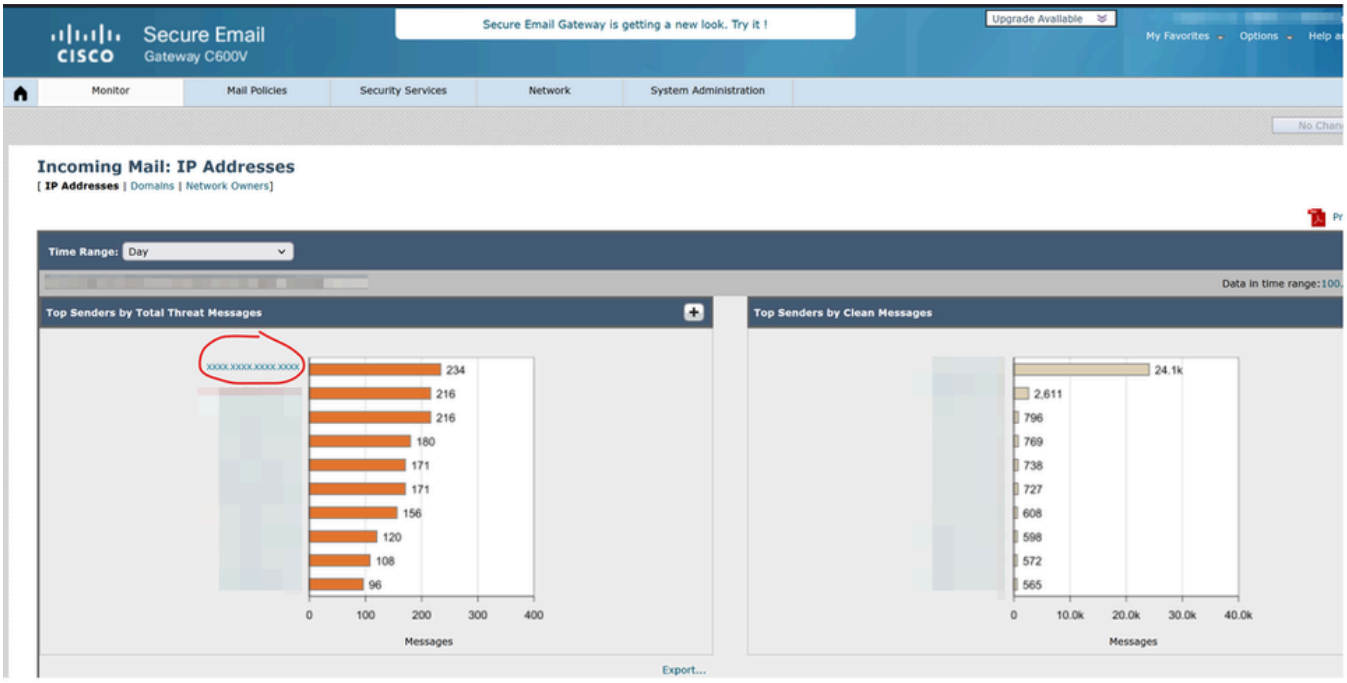
解決方案

IP信譽過濾功能與ESA裝置中的發件人基本信譽得分(SBRS)類似，使用可比計算方法。

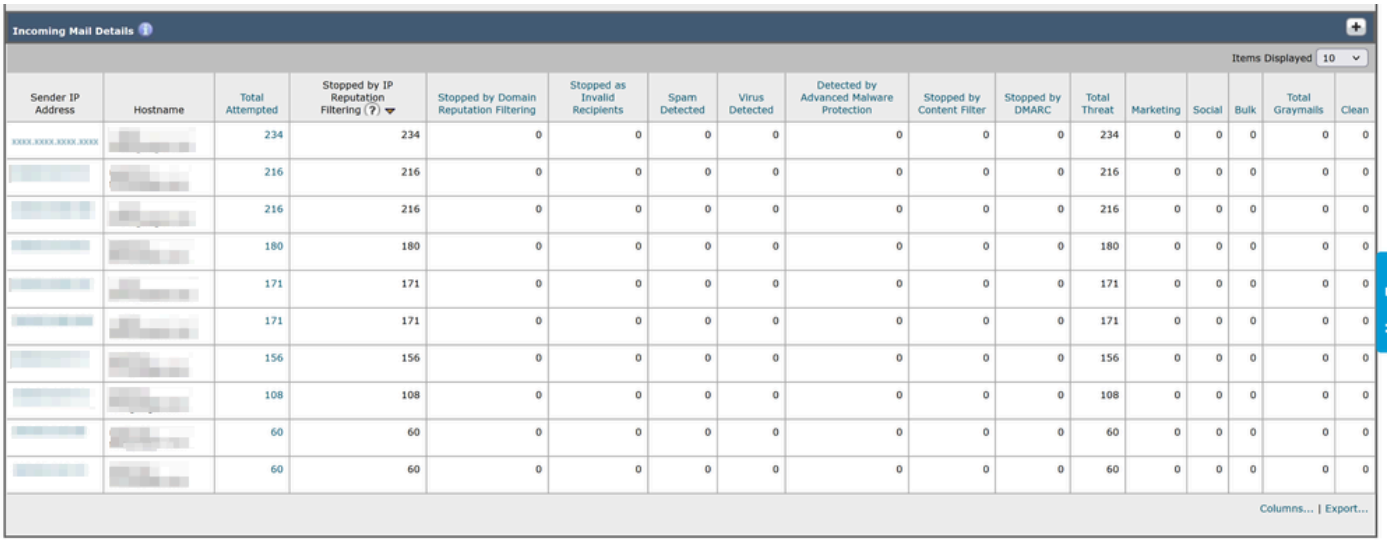
瞭解IP信譽過濾

發件人IP信譽過濾是垃圾郵件防護的第一層，它允許根據發件人IP信譽服務確定的發件人可信度來控制通過郵件網關的郵件。IP信譽服務使用來自Talos關聯網路的全域性資料，根據投訴率、郵件量統計資訊以及來自公開阻止清單和開放代理清單的資料，向電子郵件發件人分配IP信譽得分(IPRS)。IP信譽得分有助於區分合法發件人和垃圾郵件來源。您可以確定阻止來自信譽得分低的發件人的郵件的閾值。Talos Intelligence(Talos Intelligence)提供最新電子郵件和基於Web的威脅的全域性概述，按國家/地區顯示當前電子郵件流量，並允許您根據IP地址、URI或域查詢信譽得分。

以下示例說明了IP信譽過濾的工作原理：



熱門發件人



Incoming Mail Details

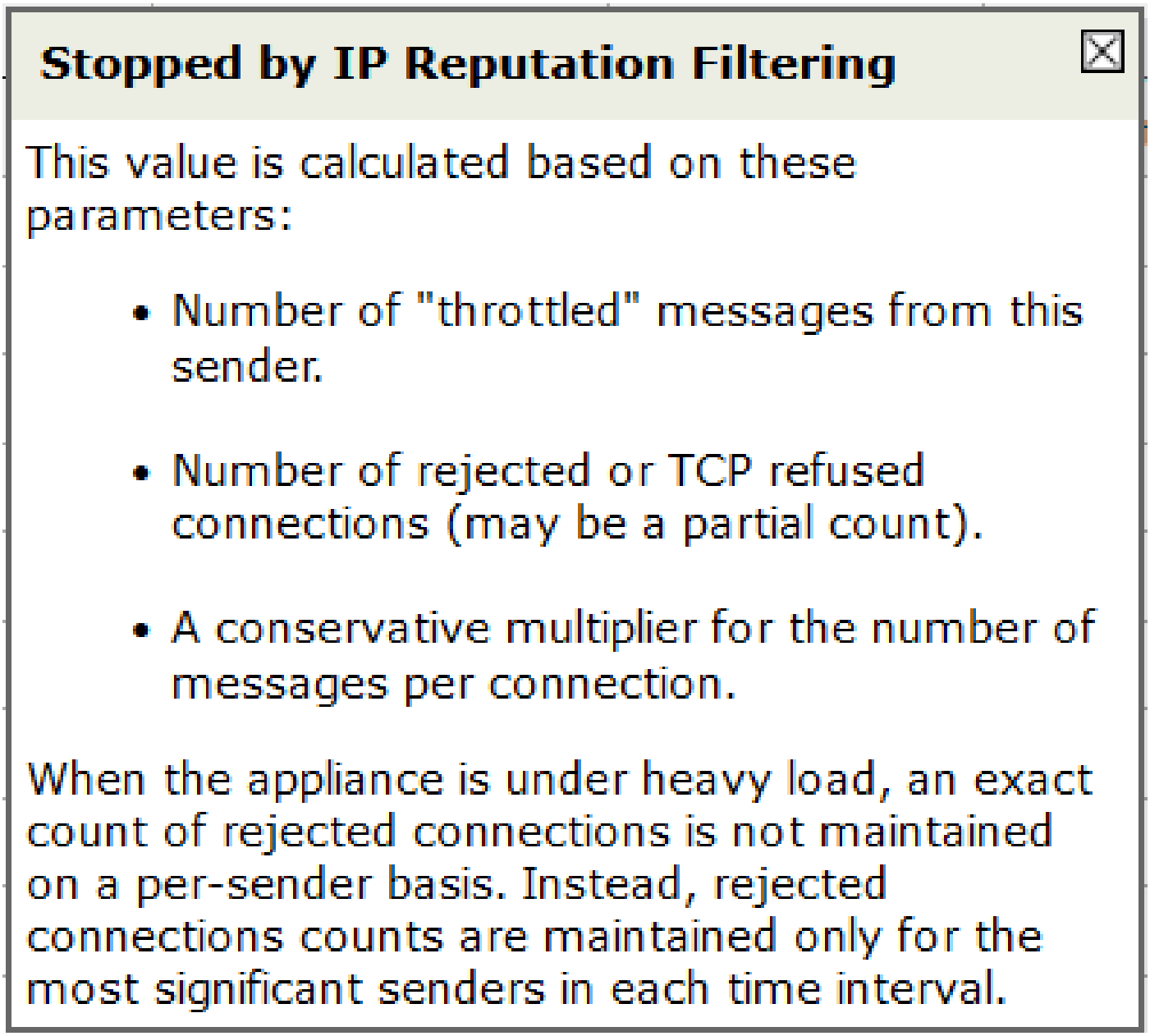
Items Displayed 10

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...

傳入郵件詳細資訊

IP XXXX.XXXX.XXXX.XXXX已傳送234封電子郵件，這些郵件似乎都被IP信譽過濾阻止。但是，對裝置內的郵件跟蹤和mail_logs的分析顯示，來自此IP的電子郵件已成功傳送，沒有證據顯示IP信譽過濾會阻止郵件。



適用於IP信譽過濾的條件

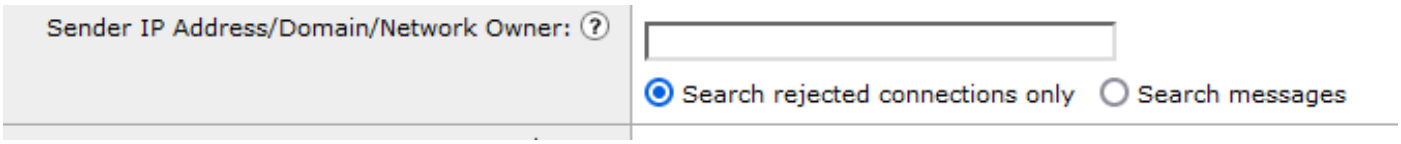
IP信譽過濾是根據特定引數計算的，如參考螢幕截圖所示。在某些情況下，電子郵件可能會與第三個條件保持一致，即每個連線的郵件數的保守乘數。拒絕日誌僅在電子郵件滿足前兩個條件時才可見。但是，裝置可以基於此乘數顯示預計的消息數。

報告可以反映大約數量的連線，其中一些連線實際上無法到達裝置。例如，已建立簡單郵件傳輸協定(SMTP)連線，但稍後由於網路問題而被丟棄。第三個條件考慮此類情況，提供連線通過還是未通過IP信譽檢查的估計分析。這並不一定表示所有列出的郵件都被IP信譽過濾阻止。

驗證被阻止的電子郵件

要確定郵件是否被實際阻止，請執行以下操作：

- 檢查阻止清單發件人組：被IP信譽過濾阻止的郵件被分類到阻止清單發件人組。
- 使用郵件跟蹤：導航到高級選項，輸入要搜尋的IP地址，然後選擇僅搜尋拒絕的連線。



在郵件跟蹤中搜尋拒絕的連線

- 檢視郵件日誌：可以在mail_logs中標識被阻止清單發件人組阻止的電子郵件。
- 延遲HAT拒絕：在SMTP連線級別實施IP過濾，ESA上的「延遲主機訪問表(HAT)拒絕」功能可用於瞭解原因。

相關資訊

- HAT延遲拒絕常見問題
- Cisco ESA使用手冊
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。