Troubleshoot Issues Related to "Stopped by IP Reputation Filtering"

Contents

Introduction

This document describes a common inquiry on reports indicating emails stopped by "IP reputation filtering".

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Email Appliance

Components Used

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

- Cisco Secure Email Appliance

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.

Background Information

IP Reputation filtering is the first layer of spam protection that allows control over messages passing through the email gateway based on the sender’s trustworthiness, as determined by the Sender IP Reputation Service. This article discusses how to address issues related to IP Reputation Filtering.

Problem

When accessing reports in the ESA/CES appliance by navigating to **Monitor** > **Incoming Mail**, certain emails appear to be blocked by "IP reputation filtering." In some cases, the total number of attempted emails matches those stopped by IP reputation filtering, raising concerns about its accuracy. Additionally, it can be difficult to locate specific emails that were blocked.

A common concern is the inability to generate a list of emails blocked by IP reputation filtering, leading to confusion about whether legitimate emails were mistakenly filtered.

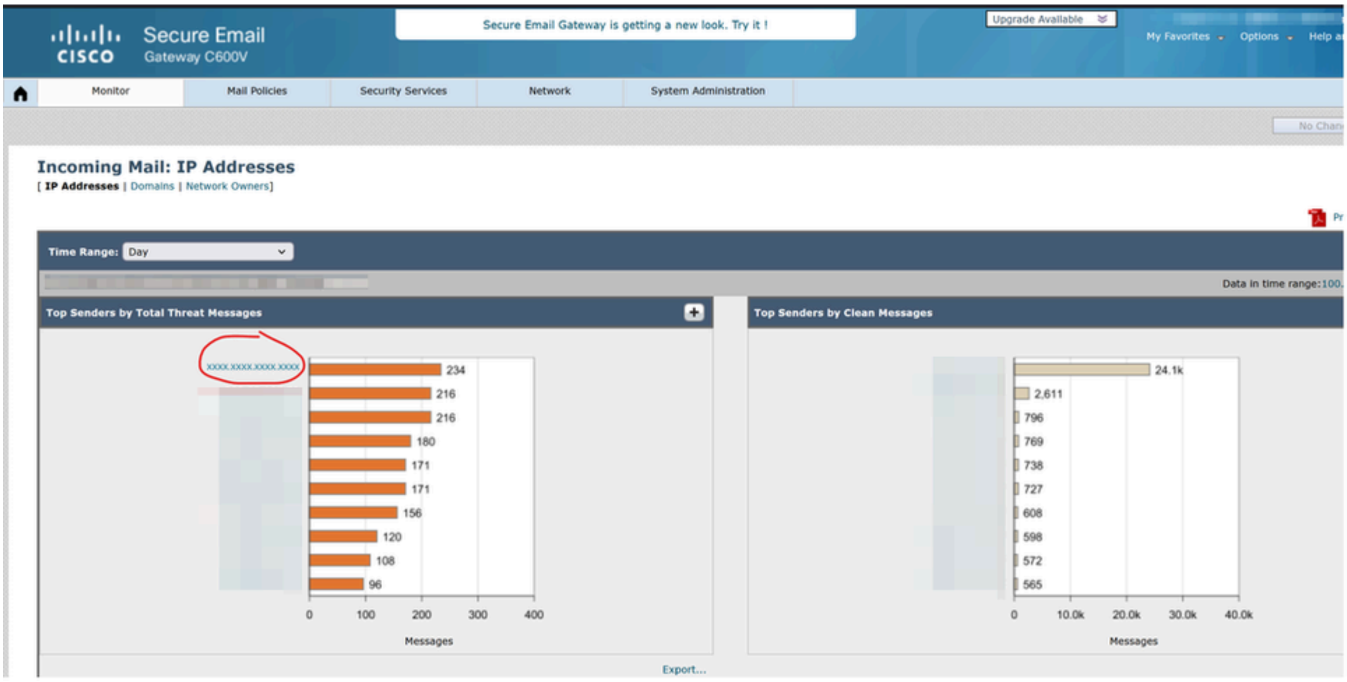
Solution

IP reputation filtering functions similar to the Sender Base Reputation Scores (SBRS) in ESA appliances, using a comparable calculation method.

Understand IP Reputation Filtering

Sender IP reputation filtering is the first layer of spam protection, allowing control over messages that come through the email gateway based on the senders' trustworthiness as determined by the Sender IP Reputation Service. The IP Reputation Service, using global data from the Talos Affiliate network, assigns an IP Reputation Score (IPRS) to email senders based on complaint rates, message volume statistics, and data from publically blocked lists and open proxy lists. The IP Reputation Score helps to differentiate legitimate senders from spam sources. You can determine the threshold for blocking messages from senders with low reputation scores. Talos intelligence ([Talos Intelligence]) provides a global overview of the latest email and web-based threats, displays current email traffic volume by country, and allows you to look up reputation scores based on IP address, URI, or Domain.

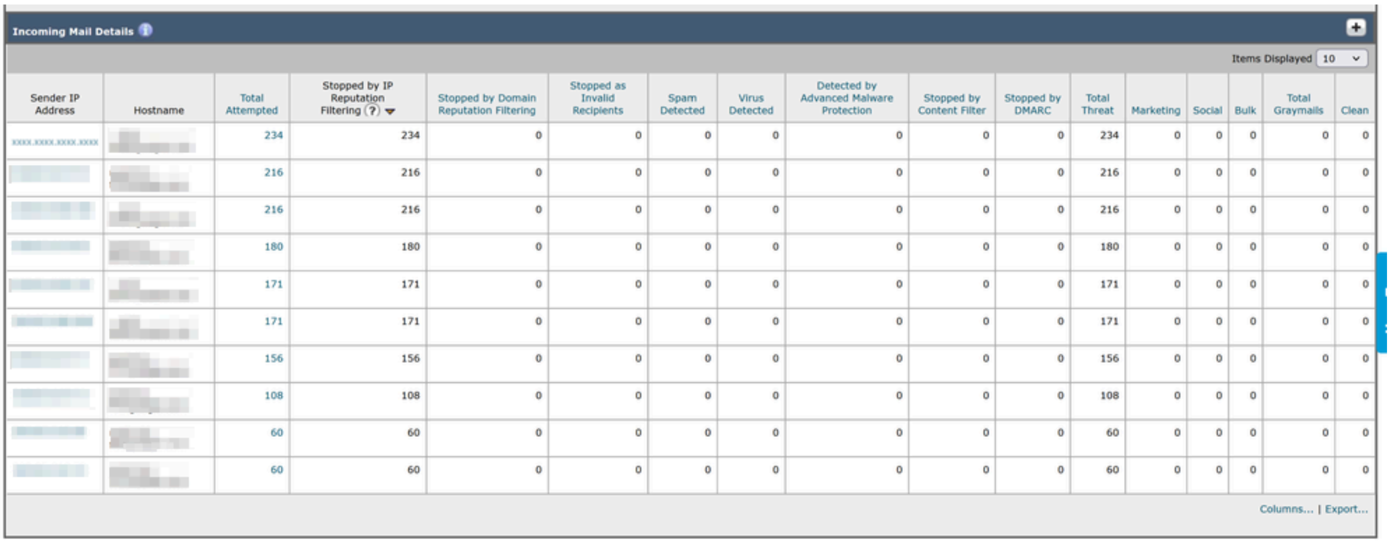
The example explains the working of IP reputation filtering:



Incoming Mail: IP Addresses

Time Range: Day

Top Senders



Incoming Mail Details

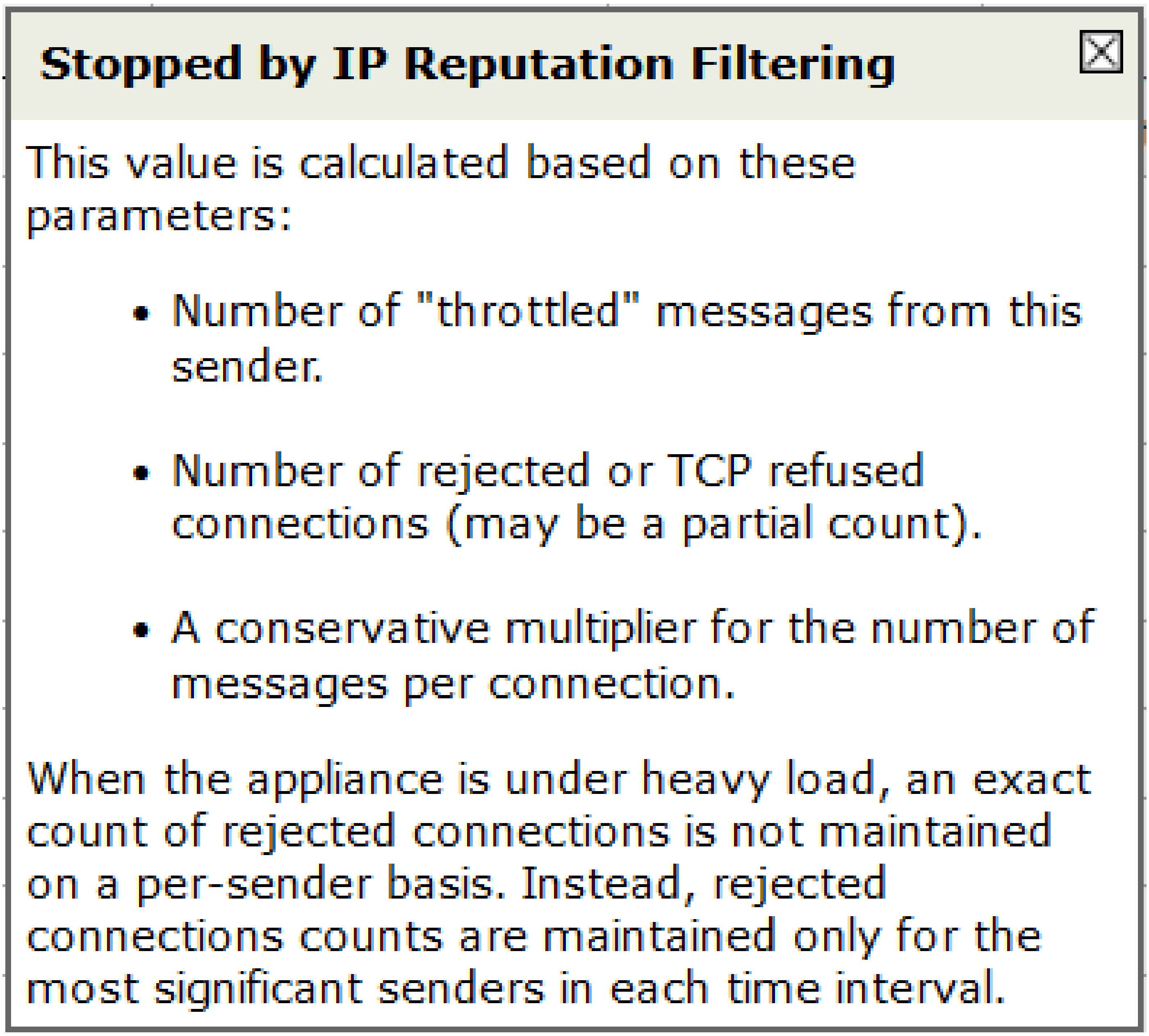
Items Displayed 10

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...

Incoming Mail Details

IP XXXX.XXXX.XXXX.XXXX has sent 234 emails, all of which seem to have been blocked by IP reputation filtering. However, an analysis of the message tracking and mail_logs within the appliance shows that emails from this IP were successfully delivered, with no evidence of blocking by IP reputation filtering.



Stopped by IP Reputation Filtering

This value is calculated based on these parameters:

- Number of "throttled" messages from this sender.
- Number of rejected or TCP refused connections (may be a partial count).
- A conservative multiplier for the number of messages per connection.

When the appliance is under heavy load, an exact count of rejected connections is not maintained on a per-sender basis. Instead, rejected connections counts are maintained only for the most significant senders in each time interval.

Conditions Applicable for IP Reputation Filtering

IP reputation filtering is calculated based on specific parameters, as shown in the referenced screenshot. In certain cases, emails can align with the third condition- a conservative multiplier for the number of messages per connection. Rejection logs are only visible if emails meet the first two conditions. However, the appliance can display an estimated number of messages based on this multiplier.

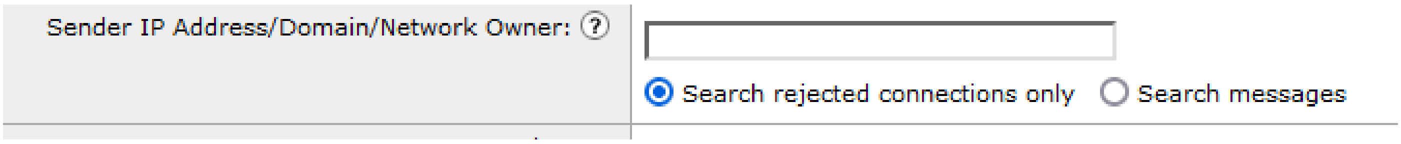
The report can reflect an approximate number of connections, some of which cannot actually reach the appliance. For instance, an Simple Mail Transfer Protocol (SMTP) connection is established but is later dropped due to a network issue. The third condition accounts for such scenarios, providing an estimated analysis of whether the connection passed or failed the IP reputation check. This does not necessarily indicate that all listed messages were blocked by IP reputation filtering.

Verify Blocked Emails

To determine whether messages were actually blocked:

- Check Blocklist Sender Group: Messages blocked by IP reputation filtering are categorized under the blocklist sender group.

- Use Message Tracking: Navigate to **Advanced Options**, enter the **IP address** to search, and select **Search rejected connections only**.



Sender IP Address/Domain/Network Owner: ?

● Search rejected connections only ○ Search messages

Search Rejected Connections in Message Tracking

- Review Mail Logs: Emails blocked by the blocklist sender group can be identified in mail_logs.
- Delayed HAT Reject: IP Filtering is enforced at the SMTP connection level and Delayed Host Access Table (HAT) Reject feature on ESA can be used to understand the cause.

Related Information

- HAT Delayed Rejection FAQ
- Cisco ESA User Guide
- Cisco Technical Support & Downloads