Risoluzione dei problemi relativi a "Stopped by IP Reputation Filtering"

Sommario

Introduzione

Questo documento descrive una richiesta comune sui rapporti che indicano email interrotte da "IP reputation filtering" (filtro reputazione IP).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Email Appliance

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Email Appliance

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il filtro della reputazione IP è il primo livello di protezione dalla posta indesiderata che consente il controllo dei messaggi che passano attraverso il gateway di posta elettronica in base all'affidabilità del mittente, come determinata dal servizio di reputazione IP del mittente. In questo articolo viene descritto come risolvere i problemi relativi al filtro della reputazione IP.

Problema

Quando si accede ai report nell'appliance ESA/CES selezionando Monitor > Incoming Mail (Monitoraggio posta in arrivo), alcune e-mail sembrano essere bloccate da "Filtro reputazione IP". In alcuni casi, il numero totale di messaggi di posta elettronica tentati corrisponde a quelli bloccati dal filtro della reputazione IP, il che solleva preoccupazioni sulla sua accuratezza. Inoltre, può essere difficile individuare e-mail specifiche che sono state bloccate.

Una preoccupazione comune è l'incapacità di generare un elenco di e-mail bloccate dal filtro della reputazione IP, che porta alla confusione circa il fatto che le e-mail legittime siano state filtrate per errore.

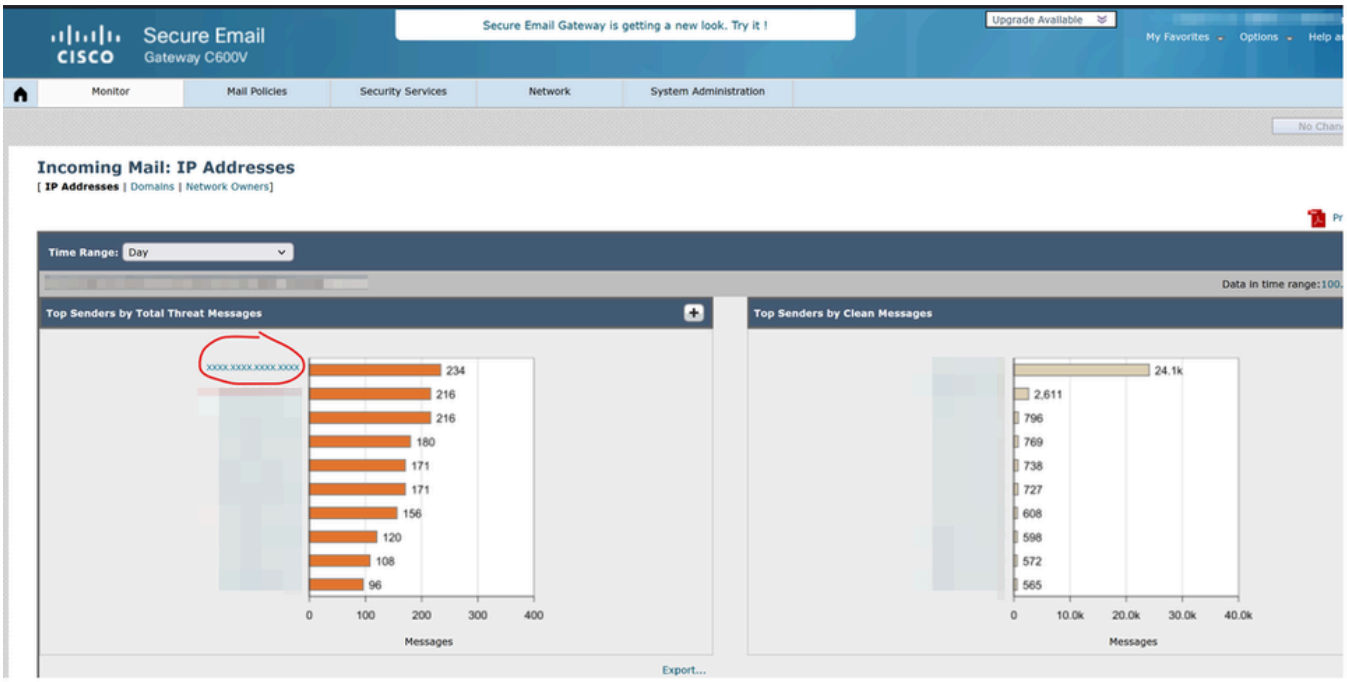
Soluzione

Il filtro della reputazione IP funziona in modo simile ai punteggi base della reputazione del mittente (SBRS, Sender Base Reputation Scores) nelle appliance ESA, usando un metodo di calcolo comparabile.

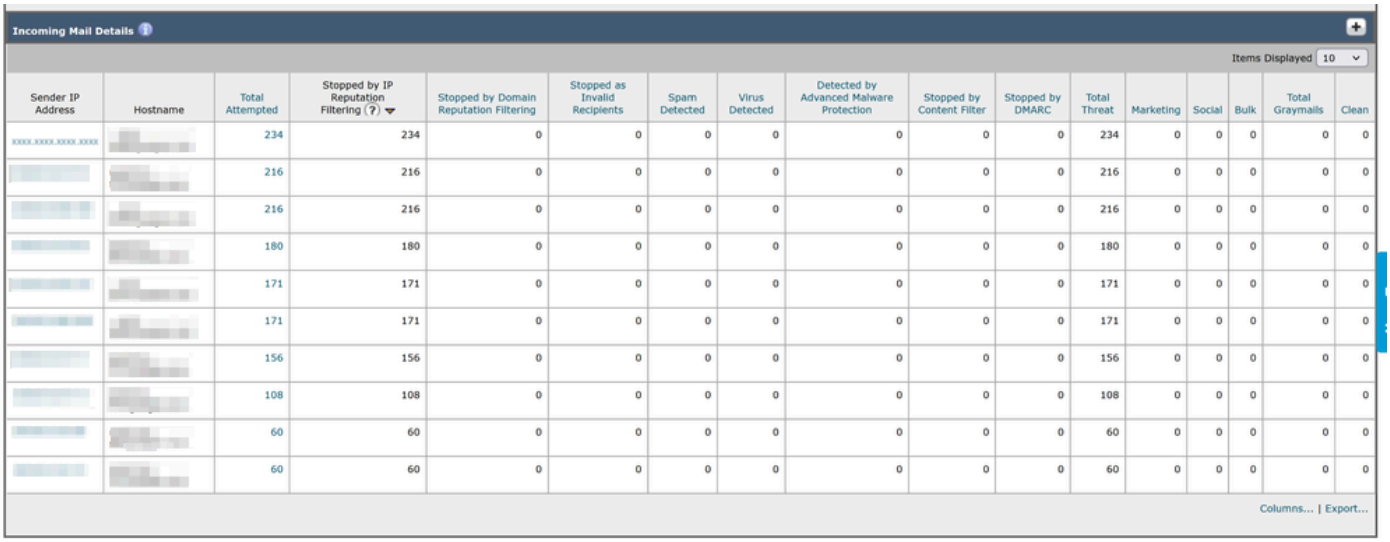
Informazioni sul filtro della reputazione IP

Il filtro della reputazione IP del mittente è il primo livello di protezione dalla posta indesiderata, che consente il controllo dei messaggi provenienti dal gateway di posta elettronica in base all'affidabilità dei mittenti, come determinata dal servizio di reputazione IP del mittente. Il Servizio di Reputazione IP, utilizzando i dati globali della rete di affiliazione Talos, assegna un punteggio di reputazione IP (IP Reputation Score, IPRS) ai mittenti di posta elettronica in base alla percentuale di reclami, alle statistiche del volume dei messaggi e ai dati degli elenchi di proxy aperti e bloccati pubblicamente. Il punteggio di reputazione IP consente di distinguere i mittenti legittimi dalle fonti di posta indesiderata. È possibile determinare la soglia per il blocco dei messaggi provenienti da mittenti con punteggi bassi. Talos Intelligence (Talos Intelligence) fornisce una panoramica globale delle più recenti minacce basate su Web e posta elettronica, visualizza il volume di traffico di posta elettronica corrente per paese e consente di cercare punteggi di reputazione in base a indirizzo IP, URI o Dominio.

L'esempio spiega il funzionamento del filtro della reputazione IP:

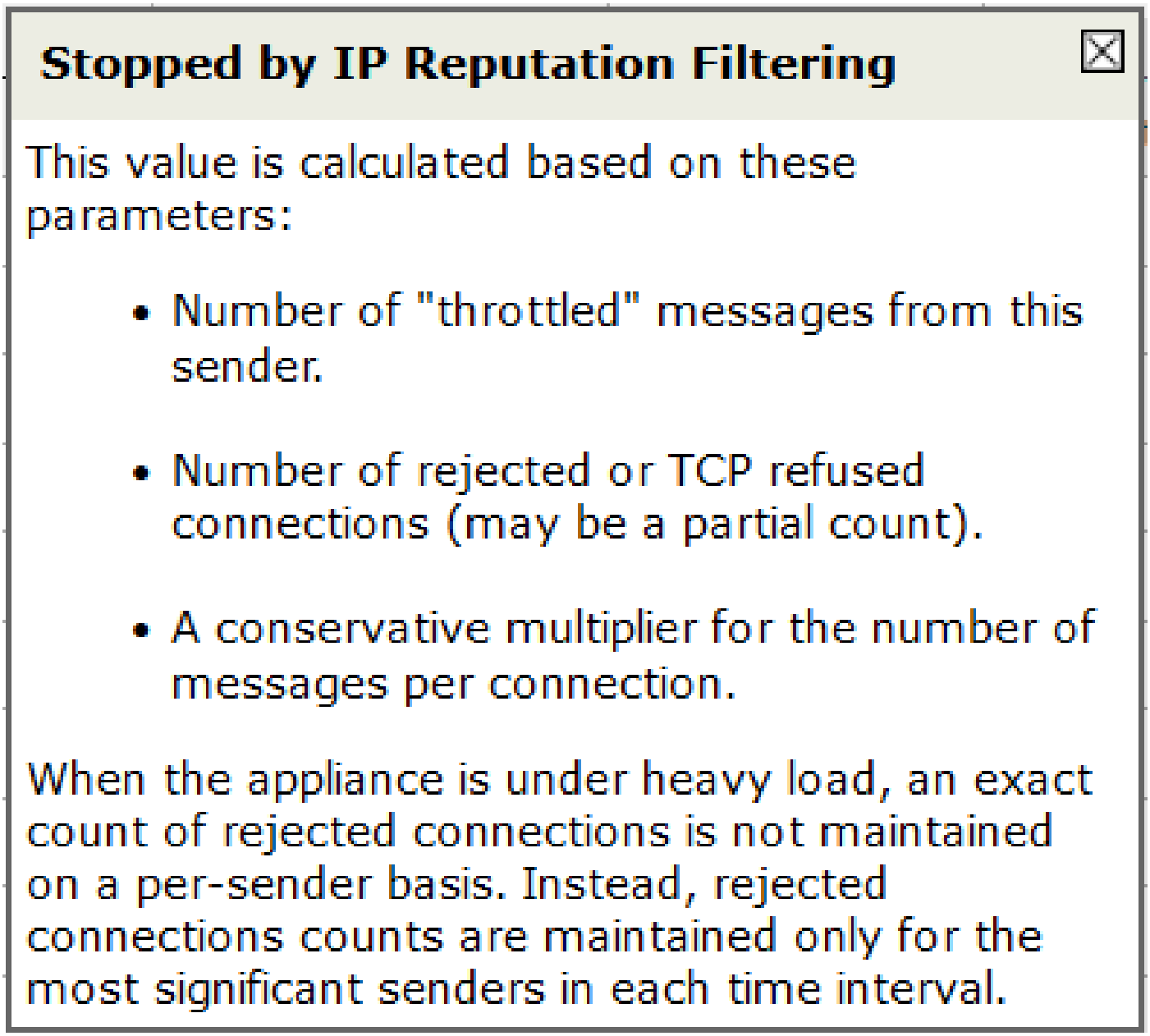


Mittenti principali



Dettagli posta in arrivo

IP XXXX.XXXX.XXXX.XXXX ha inviato 234 e-mail, tutte sembrano essere state bloccate dal filtro della reputazione IP. Tuttavia, analizzando i log di posta e di verifica dei messaggi contenuti nell'accessorio, è possibile verificare che le e-mail provenienti da questo indirizzo IP siano state recapitate correttamente e che non sia stato rilevato alcun blocco da parte del filtro della reputazione IP.



Condizioni applicabili al filtro reputazione IP

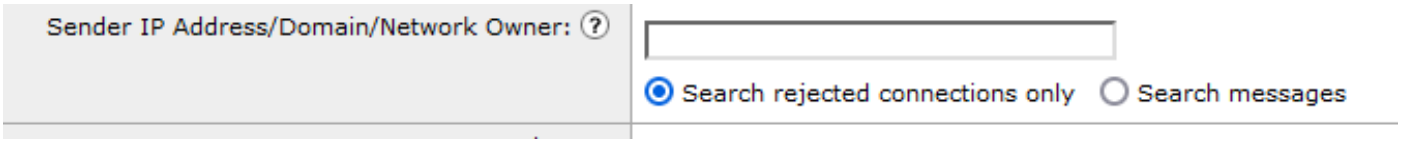
Il filtro della reputazione IP viene calcolato in base a parametri specifici, come mostrato nella schermata di riferimento. In alcuni casi, le e-mail possono essere allineate alla terza condizione, ovvero un moltiplicatore conservativo per il numero di messaggi per connessione. I registri di rifiuto sono visibili solo se i messaggi di posta elettronica soddisfano le prime due condizioni. In base a questo moltiplicatore, tuttavia, l'accessorio può visualizzare un numero stimato di messaggi.

Il report può indicare un numero approssimativo di connessioni, alcune delle quali non possono effettivamente raggiungere l'accessorio. Ad esempio, viene stabilita una connessione SMTP (Simple Mail Transfer Protocol) che viene successivamente eliminata a causa di un problema di rete. La terza condizione tiene conto di tali scenari, fornendo un'analisi stimata del fatto che la connessione abbia superato o meno il controllo della reputazione IP. Ciò non significa necessariamente che tutti i messaggi elencati siano stati bloccati dal filtro della reputazione IP.

Verifica messaggi di posta elettronica bloccati

Per determinare se i messaggi sono stati effettivamente bloccati:

- Gruppo di mittenti dell'elenco di controllo: I messaggi bloccati dal filtro della reputazione IP sono classificati nel gruppo di mittenti dell'elenco di blocco.
- Usa verifica messaggi: Passare a Opzioni avanzate, immettere l'indirizzo IP in cui eseguire la ricerca e selezionare Cerca solo connessioni rifiutate.



Cerca connessioni rifiutate in Verifica messaggi

- Rivedi log di posta: I messaggi di posta elettronica bloccati dal gruppo di mittenti dell'elenco di blocco possono essere identificati in mail_logs.
- Rifiuto HAT ritardato: Il filtro IP viene applicato a livello di connessione SMTP e la funzione di rifiuto HAT (Delayed Host Access Table) su ESA può essere utilizzata per capire la causa.

Informazioni correlate

- Domande frequenti sul rifiuto ritardato HAT
- Guida per l'utente Cisco ESA
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).