Probleme in Zusammenhang mit "Stopped by IP Reputation Filtering" beheben

Inhalt

Einleitung

In diesem Dokument wird eine häufige Abfrage von Berichten beschrieben, die angeben, dass E-Mails durch "IP-Reputationsfilterung" gestoppt wurden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure E-Mail Appliance

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure E-Mail Appliance

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die IP-Reputationsfilterung ist die erste Ebene des Spam-Schutzes, der die Kontrolle über Nachrichten ermöglicht, die das E-Mail-Gateway passieren. Dies hängt von der Vertrauenswürdigkeit des Absenders ab, die vom IP-Reputationsdienst des Absenders festgelegt wird. In diesem Artikel wird erläutert, wie Sie Probleme im Zusammenhang mit der IP-Reputationsfilterung beheben.

Problem

Wenn Sie auf Berichte in der ESA/CES-Appliance zugreifen, indem Sie zu Monitor > Incoming Mail navigieren, werden bestimmte E-Mails anscheinend durch "IP-Reputationsfilterung" blockiert. In einigen Fällen stimmt die Gesamtzahl der versuchten E-Mails mit der Anzahl der durch die IP-Reputationsfilterung gestoppten E-Mails überein, was Bedenken hinsichtlich ihrer Genauigkeit aufkommen lässt. Darüber hinaus kann es schwierig sein, bestimmte E-Mails zu finden, die blockiert wurden.

Häufig wird befürchtet, dass keine Liste der durch die IP-Reputationsfilterung blockierten E-Mails erstellt werden kann, was zu Verwirrung darüber führt, ob legitime E-Mails irrtümlicherweise gefiltert wurden.

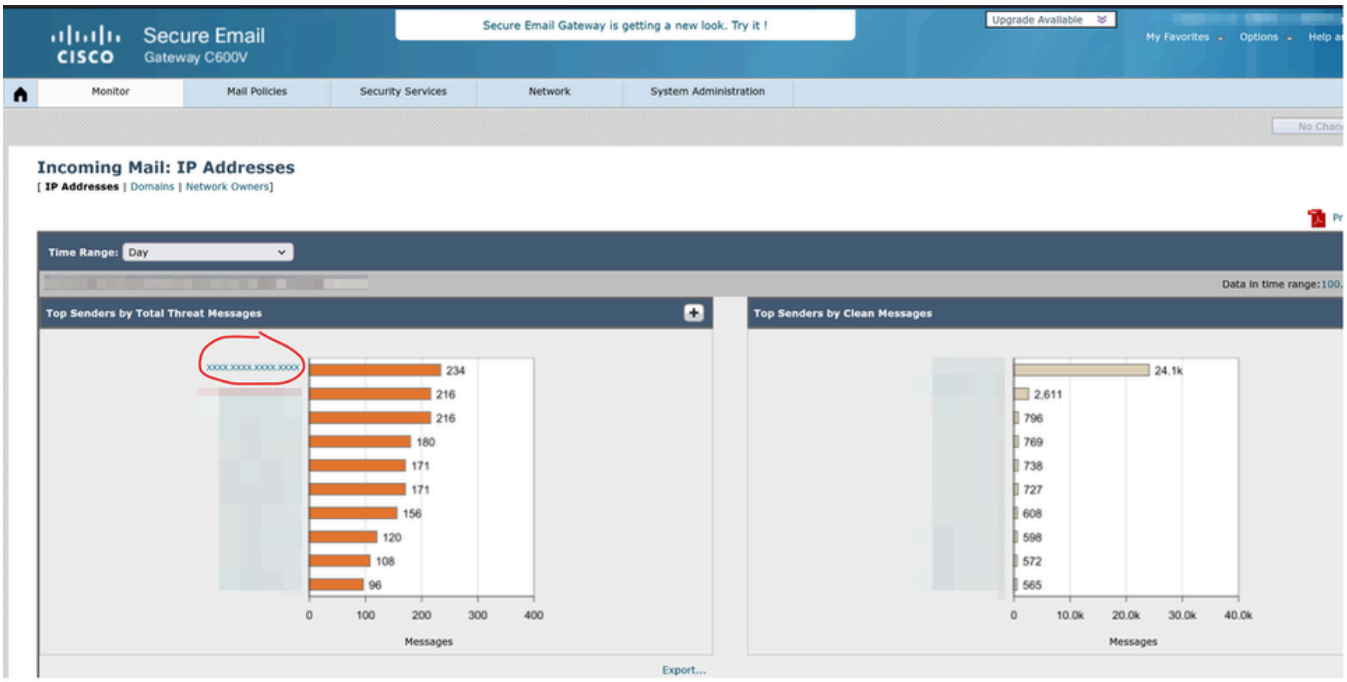
Lösung

Die IP-Reputationsfilterung funktioniert ähnlich wie die Sender Base Reputation Scores (SBRS) in ESA-Appliances, wobei eine vergleichbare Berechnungsmethode verwendet wird.

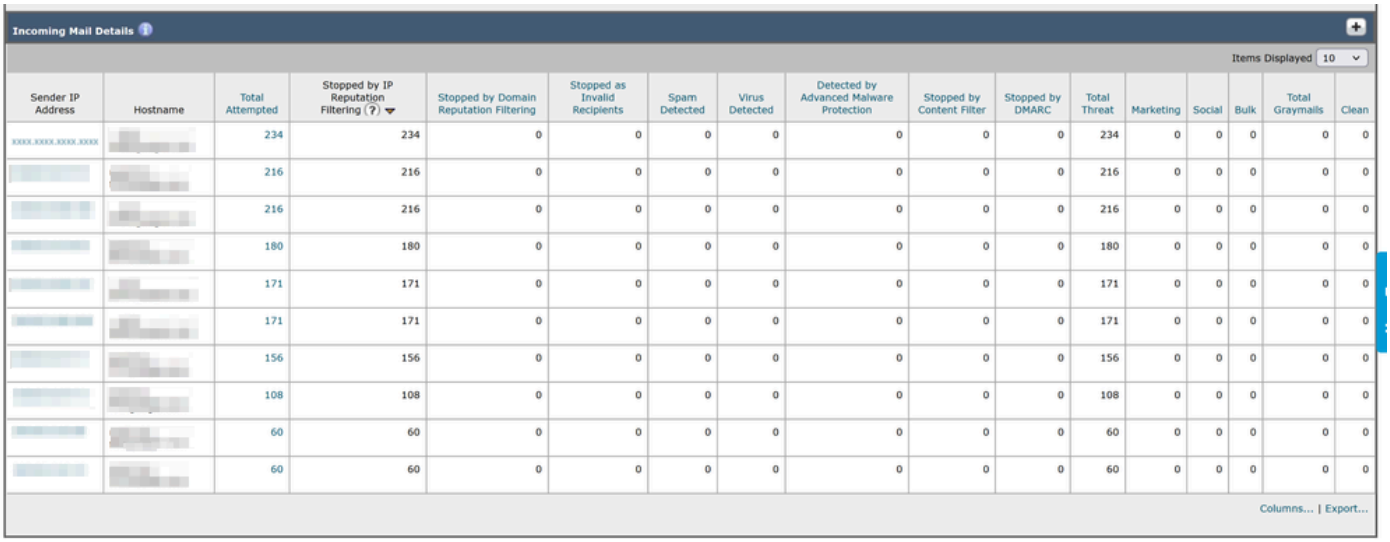
IP-Reputationsfilterung verstehen

Die IP-Reputationsfilterung für Absender ist die erste Ebene des Spam-Schutzes und ermöglicht die Kontrolle über Nachrichten, die über das E-Mail-Gateway eingehen. Dies hängt von der Vertrauenswürdigkeit des Absenders ab, die vom IP-Reputationsdienst des Absenders festgelegt wurde. Der IP Reputation Service weist E-Mail-Absendern unter Verwendung globaler Daten aus dem Talos Affiliate-Netzwerk eine IP Reputation Score (IPRS) zu. Diese Bewertung basiert auf der Anzahl der Beschwerden, auf Statistiken zum Nachrichtenvolumen sowie auf Daten aus öffentlich gesperrten Listen und offenen Proxylisten. Die IP-Reputationsbewertung hilft dabei, legitime Absender von Spam-Quellen zu unterscheiden. Sie können den Schwellenwert für das Blockieren von Nachrichten von Absendern mit schlechter Reputationsbewertung festlegen. Die Talos-Informationen (Talos Intelligence) bieten einen globalen Überblick über die neuesten E-Mail- und webbasierten Bedrohungen, zeigen das aktuelle E-Mail-Datenverkehrsvolumen nach Land an und ermöglichen das Nachschlagen der Reputationsbewertungen auf Basis von IP-Adresse, URI oder Domäne.

Das Beispiel erläutert die Funktionsweise der IP-Reputationsfilterung:

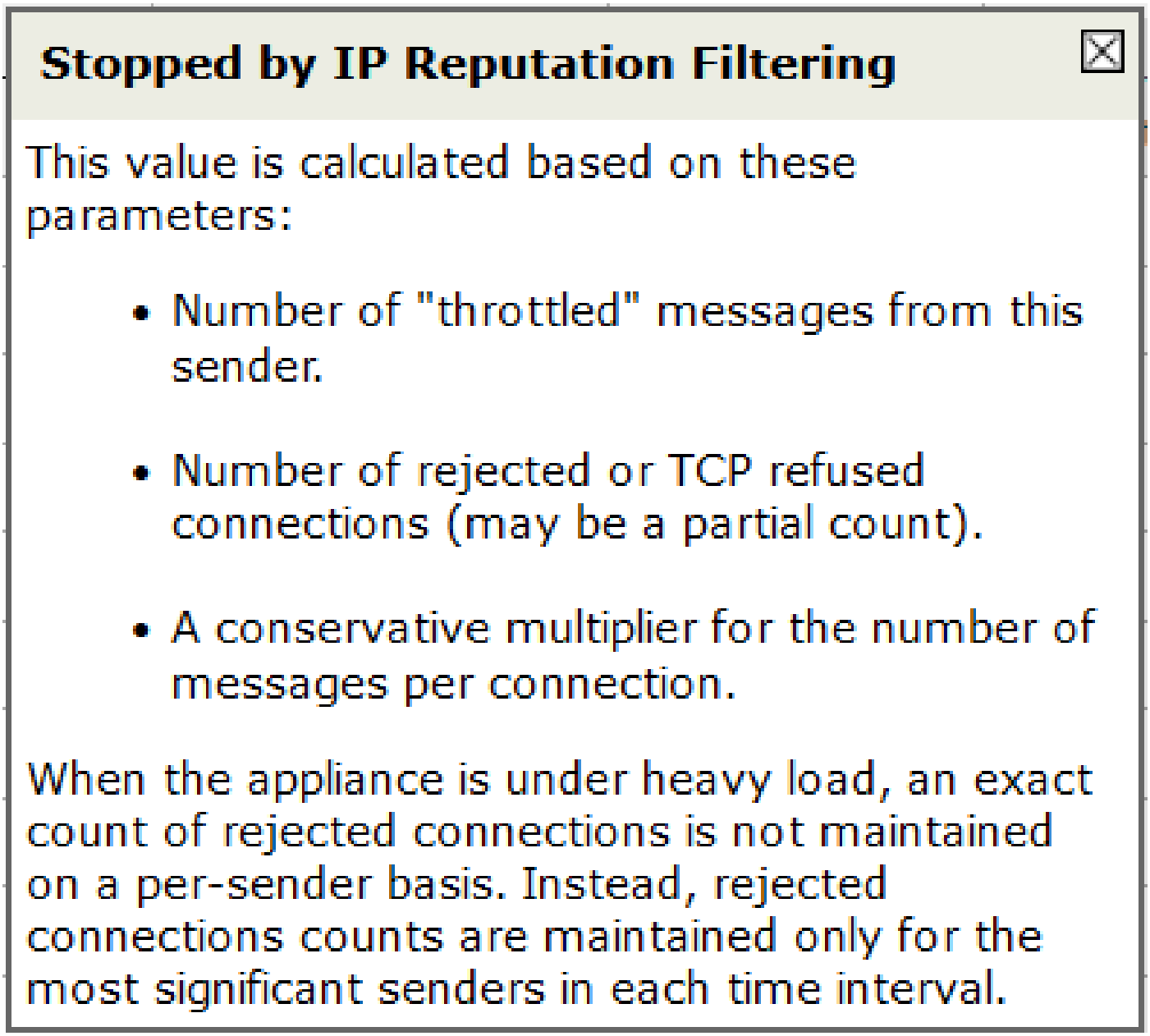


Häufigste Absender



Details zu eingehenden Mails

Die IP XXXX.XXXX.XXXX.XXXX hat 234 E-Mails versendet, die anscheinend alle durch die IP-Reputationsfilterung blockiert wurden. Eine Analyse der Nachrichtenverfolgung und von mail_logs innerhalb der Appliance zeigt jedoch, dass E-Mails von dieser IP-Adresse erfolgreich zugestellt wurden, ohne dass Hinweise auf eine Blockierung durch die IP-Reputationsfilterung vorlagen.



Bedingungen für die IP-Reputationsfilterung

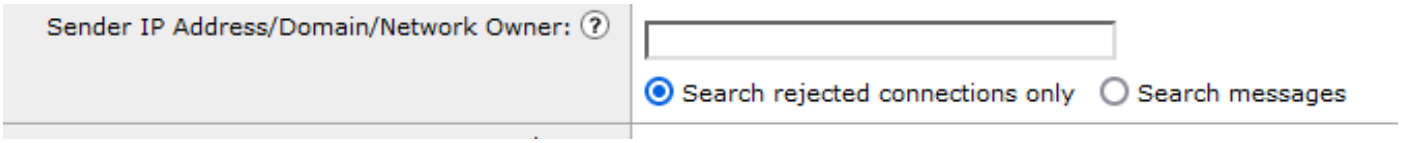
Die IP-Reputationsfilterung wird anhand bestimmter Parameter berechnet, wie im Screenshot zu sehen ist. In bestimmten Fällen können E-Mails mit der dritten Bedingung übereinstimmen - einem konservativen Multiplikator für die Anzahl der Nachrichten pro Verbindung. Ablehnungsprotokolle werden nur angezeigt, wenn die E-Mails die ersten beiden Bedingungen erfüllen. Auf Basis dieses Multiplikators kann die Appliance jedoch eine geschätzte Anzahl von Meldungen anzeigen.

Der Bericht kann eine ungefähre Anzahl von Verbindungen enthalten, von denen einige die Appliance nicht erreichen können. Beispielsweise wird eine SMTP-Verbindung (Simple Mail Transfer Protocol) hergestellt, später jedoch aufgrund eines Netzwerkproblems getrennt. Die dritte Bedingung berücksichtigt solche Szenarien und liefert eine geschätzte Analyse, ob die Verbindung die IP-Reputationsprüfung bestanden hat oder nicht. Dies bedeutet nicht unbedingt, dass alle aufgeführten Nachrichten durch IP-Reputationsfilterung blockiert wurden.

Gesperrte E-Mails überprüfen

So prüfen Sie, ob Nachrichten tatsächlich blockiert wurden:

- Sperrlistenabsendergruppe überprüfen: Nachrichten, die durch die IP-Reputationsfilterung blockiert werden, werden in der Absendergruppe der Blockliste kategorisiert.
- Nachrichtenverfolgung verwenden: Navigieren Sie zu Erweiterte Optionen, geben Sie die IP-Adresse für die Suche ein, und wählen Sie Nur abgelehnte Verbindungen durchsuchen aus.



Abgelehnte Verbindungen in der Nachrichtenverfolgung durchsuchen

- E-Mail-Protokolle überprüfen: Von der Absendergruppe der Sperrliste blockierte E-Mails können in mail_logs identifiziert werden.
- Verzögerte HAT-Ablehnung: Die IP-Filterung wird auf SMTP-Verbindungsebene erzwungen, und die Funktion zum Zurückweisen der Tabelle für verzögerten Host-Zugriff (HAT) auf der ESA kann verwendet werden, um die Ursache zu ermitteln.

Zugehörige Informationen

- Häufig gestellte Fragen zur verzögerten HAT-Zurückweisung
- Cisco ESA Benutzerhandbuch
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.