Résoudre les problèmes liés à " ; Arrêté par le filtrage par réputation IP" ;

Table des matières

Introduction

Ce document décrit une requête courante sur des rapports indiquant des e-mails arrêtés par le « filtrage de réputation IP ».

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil de messagerie électronique sécurisé Cisco

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil de messagerie électronique sécurisé Cisco

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le filtrage par réputation IP est la première couche de protection contre le spam qui permet de contrôler les messages passant par la passerelle de messagerie en fonction de la fiabilité de l'expéditeur, telle que déterminée par le service de réputation IP de l'expéditeur. Cet article explique comment résoudre les problèmes liés au filtrage par réputation IP.

Problème

Lorsque vous accédez à des rapports dans l'appliance ESA/CES en naviguant vers Monitor > Incoming Mail, certains e-mails semblent être bloqués par le « filtrage de réputation IP ». Dans certains cas, le nombre total de tentatives d'e-mails correspond à ceux bloqués par le filtrage par réputation IP, ce qui soulève des inquiétudes quant à sa précision. En outre, il peut être difficile de localiser des e-mails spécifiques qui ont été bloqués.

L'incapacité à générer une liste des e-mails bloqués par le filtrage par réputation IP est une préoccupation courante, ce qui entraîne une certaine confusion quant à savoir si les e-mails légitimes ont été filtrés par erreur.

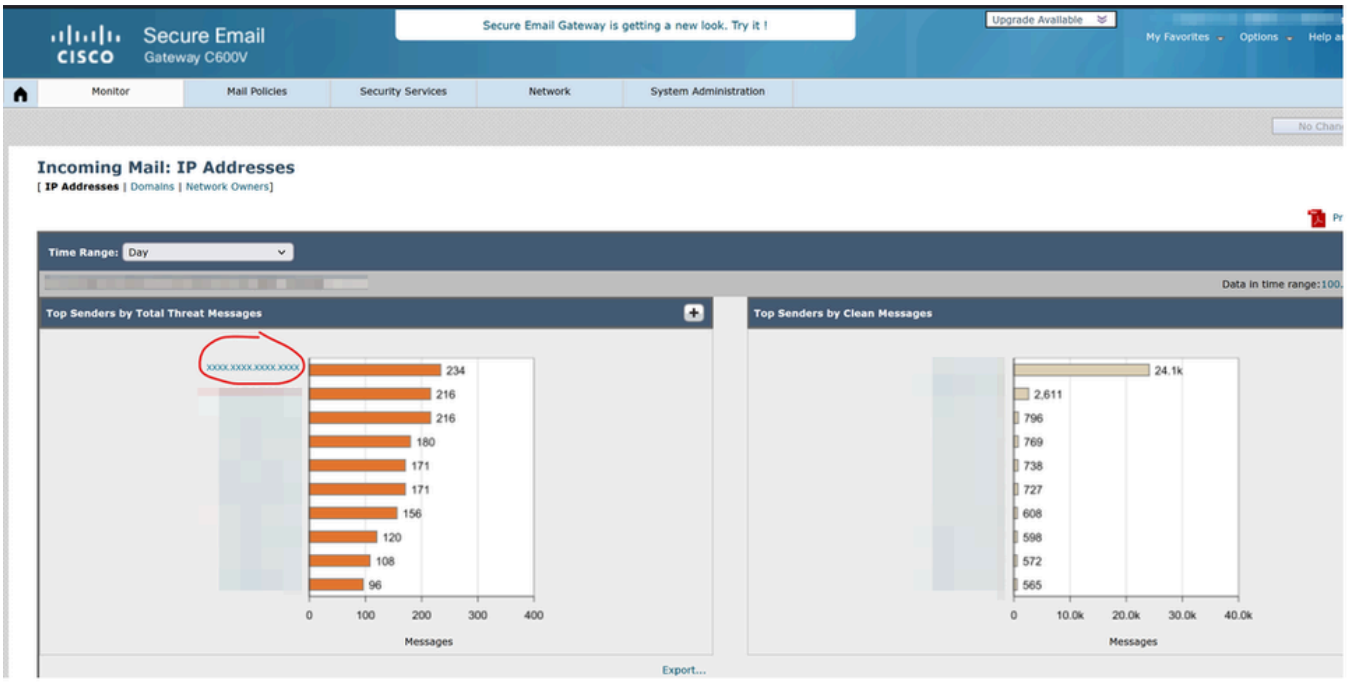
Solution

Le filtrage par réputation IP fonctionne de la même manière que les SBRS (Sender Base Reputation Scores) dans les appliances ESA, à l'aide d'une méthode de calcul comparable.

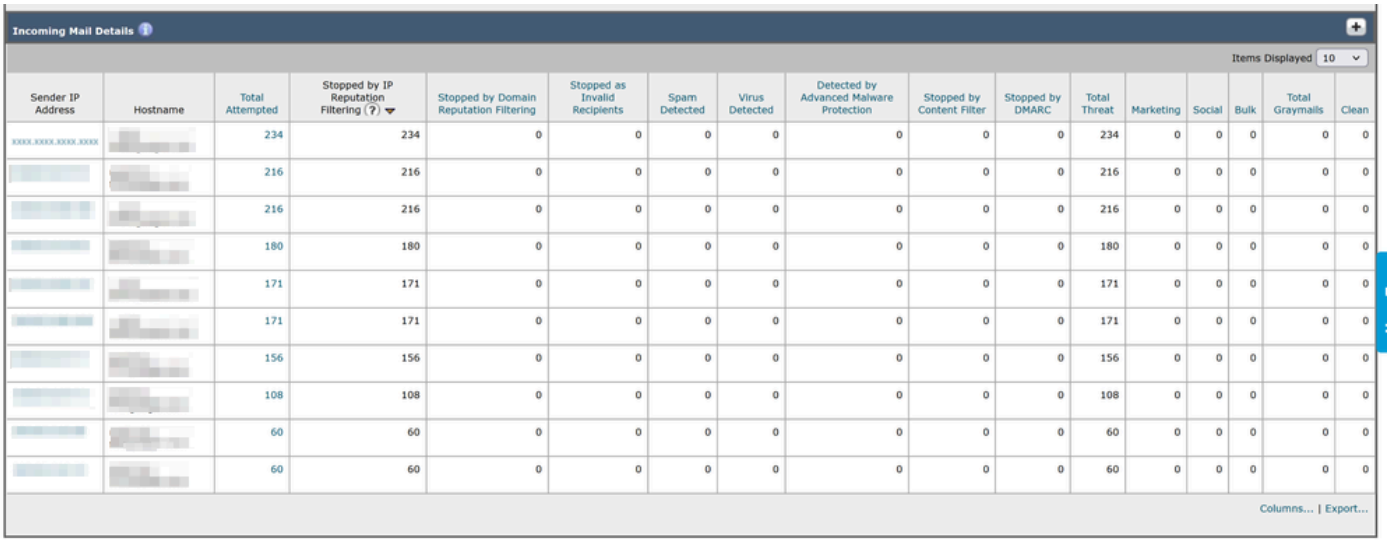
Comprendre le filtrage par réputation IP

Le filtrage par réputation IP de l'expéditeur est la première couche de protection contre le courrier indésirable. Il permet de contrôler les messages qui transitent par la passerelle de messagerie en fonction de la fiabilité de l'expéditeur, telle que déterminée par le service de réputation IP de l'expéditeur. Le service de réputation IP, qui utilise les données globales du réseau de l'affiliée Talos, attribue un score de réputation IP (IPRS) aux expéditeurs d'e-mails en fonction des taux de plaintes, des statistiques de volume de messages et des données des listes publiquement bloquées et des listes de proxy ouvertes. Le score de réputation IP permet de différencier les expéditeurs légitimes des sources de spam. Vous pouvez déterminer le seuil de blocage des messages provenant d'expéditeurs dont le score de réputation est faible. Talos Intelligence (Talos Intelligence) fournit une vue d'ensemble globale des dernières menaces par e-mail et Web, affiche le volume de trafic de messagerie électronique actuel par pays et vous permet de rechercher des scores de réputation basés sur l'adresse IP, l'URI ou le domaine.

L'exemple explique le fonctionnement du filtrage par réputation IP :

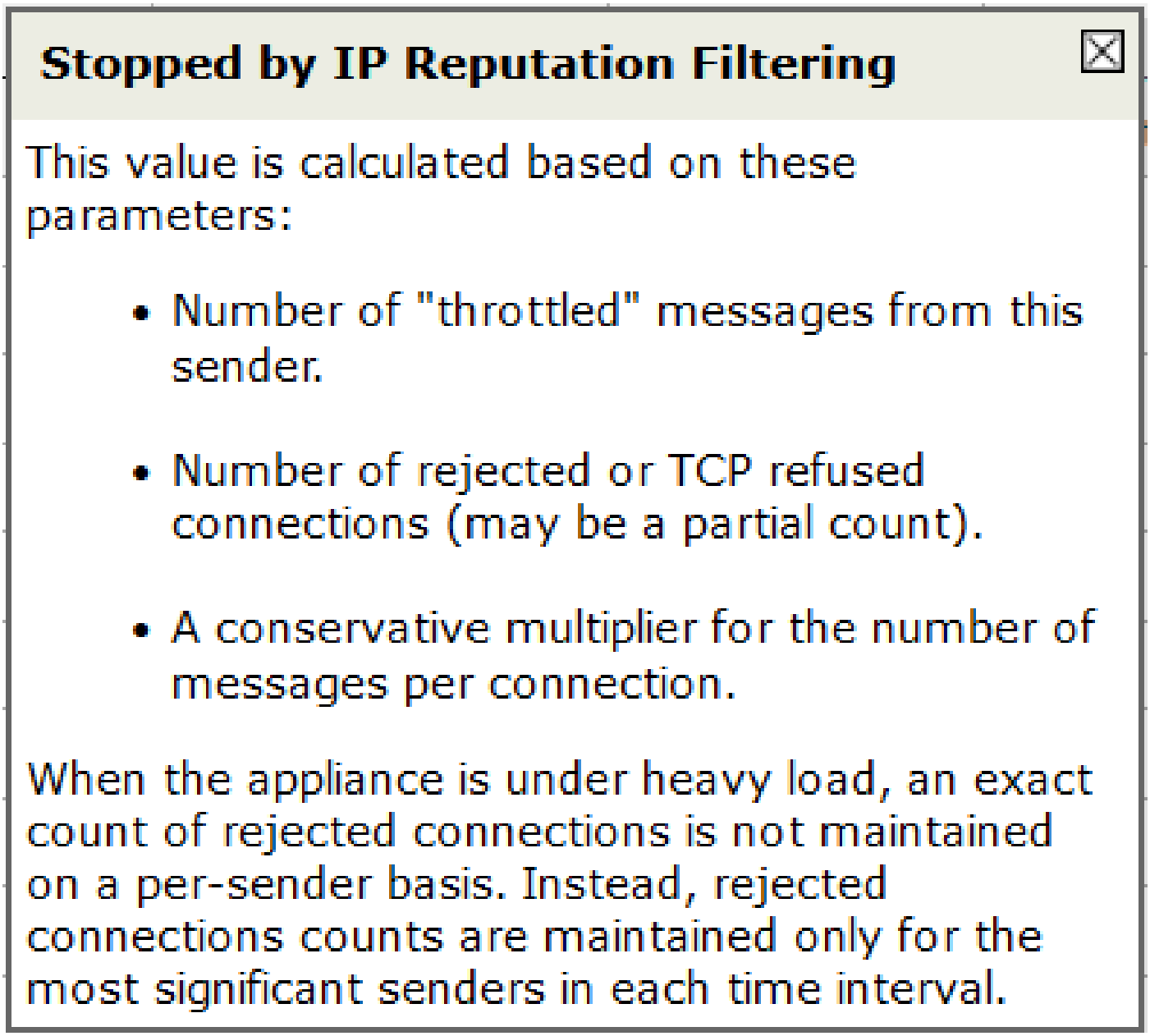


Principaux expéditeurs



Détails des messages entrants

L'adresse IP XXXX.XXXX.XXXX.XXXX a envoyé 234 e-mails, qui semblent tous avoir été bloqués par le filtrage par réputation IP. Cependant, une analyse du suivi des messages et des journaux de messages au sein de l'appliance montre que les e-mails de cette adresse IP ont été remis avec succès, sans preuve de blocage par le filtrage par réputation IP.



Conditions applicables au filtrage par réputation IP

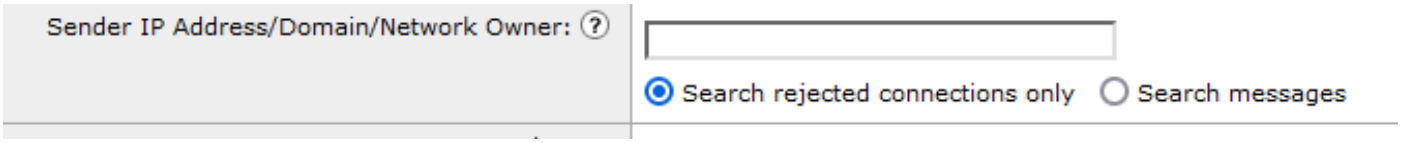
Le filtrage par réputation IP est calculé en fonction de paramètres spécifiques, comme indiqué dans la capture d'écran référencée. Dans certains cas, les e-mails peuvent correspondre à la troisième condition : un multiplicateur prudent pour le nombre de messages par connexion. Les journaux de rejet ne sont visibles que si les e-mails remplissent les deux premières conditions. Cependant, l'appliance peut afficher un nombre estimé de messages en fonction de ce multiplicateur.

Le rapport peut refléter un nombre approximatif de connexions, dont certaines ne peuvent pas réellement atteindre l'appliance. Par exemple, une connexion SMTP (Simple Mail Transfer Protocol) est établie, mais est ultérieurement abandonnée en raison d'un problème réseau. La troisième condition prend en compte ces scénarios, fournissant une analyse estimée de la réussite ou de l'échec du contrôle de réputation IP. Cela n'indique pas nécessairement que tous les messages répertoriés ont été bloqués par le filtrage par réputation IP.

Vérifier les e-mails bloqués

Pour déterminer si les messages ont été réellement bloqués :

- Vérifier le groupe d'expéditeurs de liste de blocage : Les messages bloqués par le filtrage par réputation IP sont classés dans le groupe d'expéditeurs de la liste de blocage.
- Utiliser le suivi des messages : Accédez à Options avancées, entrez l'adresse IP à rechercher et sélectionnez Rechercher uniquement les connexions rejetées.



Rechercher les connexions rejetées dans le suivi des messages

- Consulter les journaux de messagerie : Les e-mails bloqués par le groupe d'expéditeurs de la liste de blocage peuvent être identifiés dans mail_logs.
- Rejet HAT différé : Le filtrage IP est appliqué au niveau de la connexion SMTP et la fonction de rejet HAT (Delayed Host Access Table) sur ESA peut être utilisée pour comprendre la cause.

Informations connexes

- FAQ sur le rejet différé HAT
- Guide de l'utilisateur Cisco ESA
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.