Problemen met betrekking tot "a oplossen;Gestopt door filtering en quot van IP-reputatie;

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

Probleem

Oplossing

IP-reputatie filtering begrijpen

Geblokkeerde e-mails controleren

Gerelateerde informatie

Inleiding

Dit document beschrijft een veelvoorkomend onderzoek naar meldingen die aangeven dat e-mails zijn gestopt door "IP reputation filtering".

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco beveiligde e-mail applicatie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco beveiligde e-mail applicatie

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

IP Reputation filtering is de eerste laag van spambescherming die controle over berichten toestaat die door de e-mailgateway gaan die op de betrouwbaarheid van de afzender wordt gebaseerd, zoals die door de Dienst van de Reputatie van de Afzender IP wordt bepaald. In dit artikel wordt besproken hoe u problemen kunt aanpakken die verband houden met IP Reputation Filtering.

Probleem

Wanneer u rapporten in het ESA/CES-apparaat opent door te navigeren naar Monitor > Incoming Mail, lijken bepaalde e-mails geblokkeerd te worden door "IP-reputatieschakeling filtering". In sommige gevallen komt het totale aantal pogingen tot het verzenden van e-mails overeen met het aantal pogingen dat is gestopt door IP-reputatie filtering, wat vragen oproept over de nauwkeurigheid ervan. Bovendien kan het moeilijk zijn om specifieke e-mails te vinden die zijn geblokkeerd.

Een veel voorkomende zorg is het onvermogen om een lijst van e-mails te genereren geblokkeerd door IP reputatie filtering, wat leidt tot verwarring over of legitieme e-mails verkeerd gefilterd zijn.

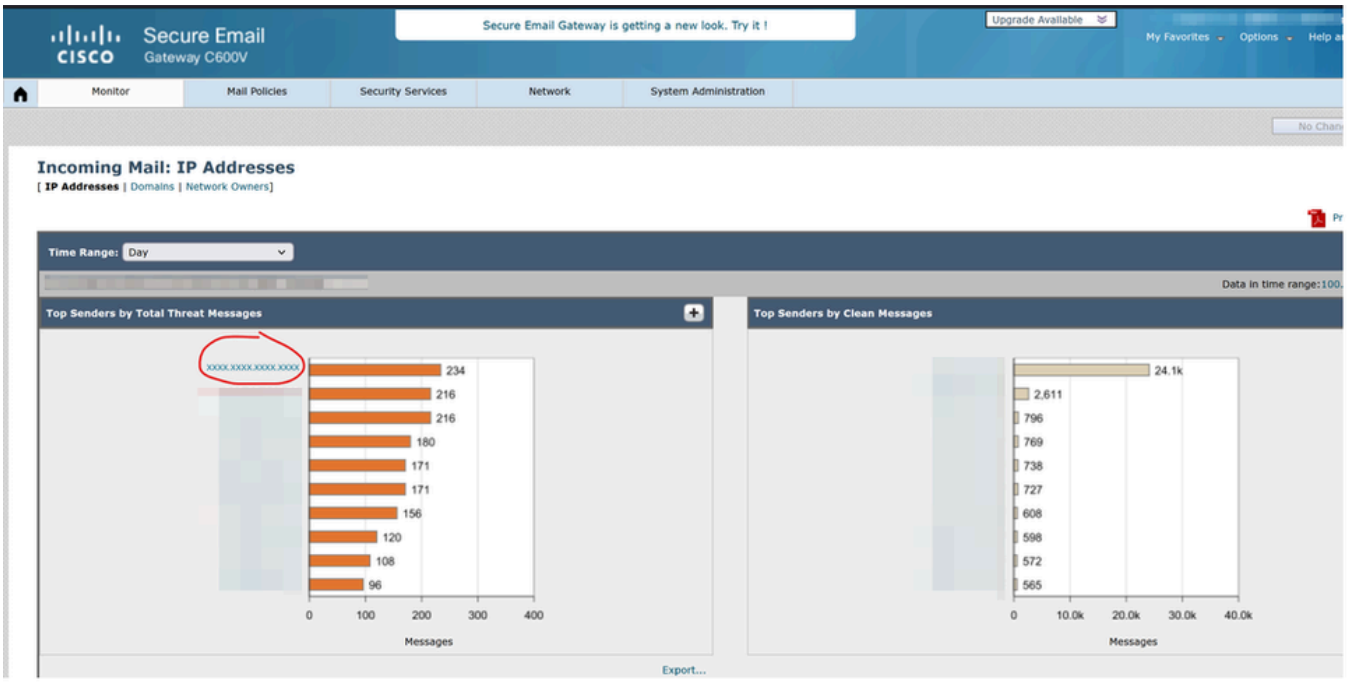
Oplossing

IP-reputatie filtering functies vergelijkbaar met de Sender Base Reputation Scores (SBRS) in ESA-apparaten, met gebruik van een vergelijkbare berekeningsmethode.

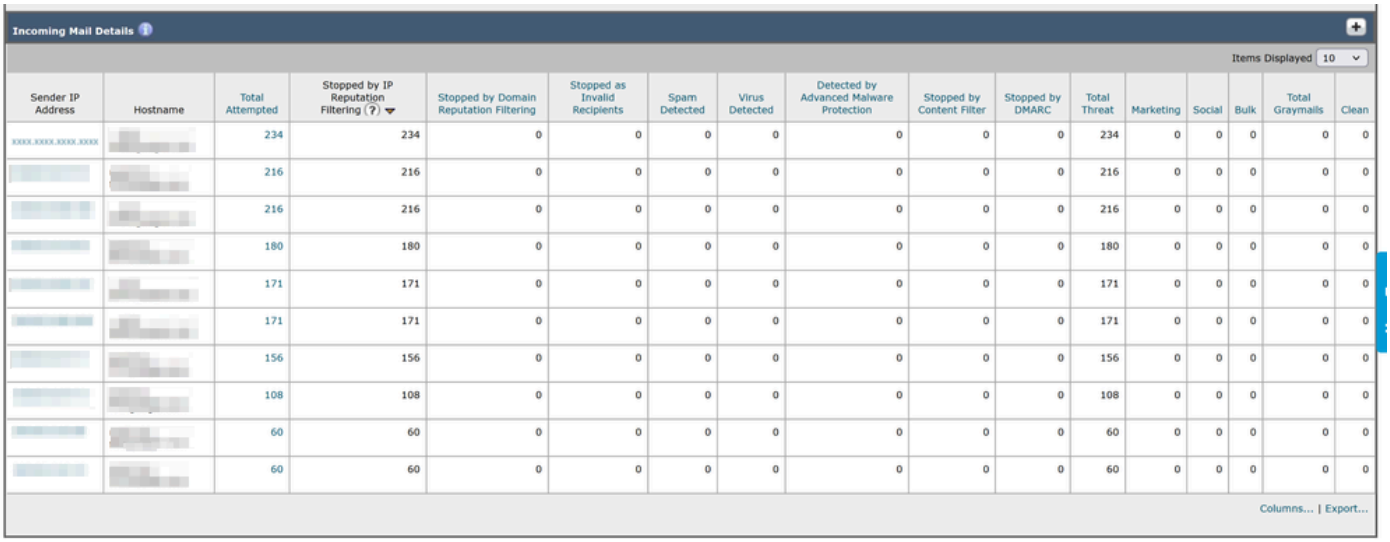
IP-reputatie filtering begrijpen

IP van de afzender de reputatie filtering is de eerste laag van spambescherming, die controle over berichten toestaan die door de e-mailgateway komen die op de betrouwbaarheid van de afzenders wordt gebaseerd zoals die door de Dienst van de Reputatie van de Afzender IP wordt bepaald. De IP Reputation Service, met behulp van wereldwijde gegevens van het Talos Affiliate netwerk, kent een IP Reputation Score (IPRS) toe aan e-mailafzenders op basis van klachtentarieven, statistieken over het berichtenvolume, en gegevens van publiekelijk geblokkeerde lijsten en open proxylijsten. De IP Reputation Score helpt om legitieme afzenders te onderscheiden van spambronnen. U kunt de drempel bepalen voor het blokkeren van berichten van afzenders met lage reputatiescores. Talos Intelligence (Talos Intelligence) biedt een globaal overzicht van de laatste e-mail en web-based bedreigingen, toont het huidige e-mailverkeer volume per land, en stelt u in staat om reputatiescores op te zoeken op basis van IP adres, URI, of Domein.

Het voorbeeld verklaart het werken van IP reputatie het filtreren:

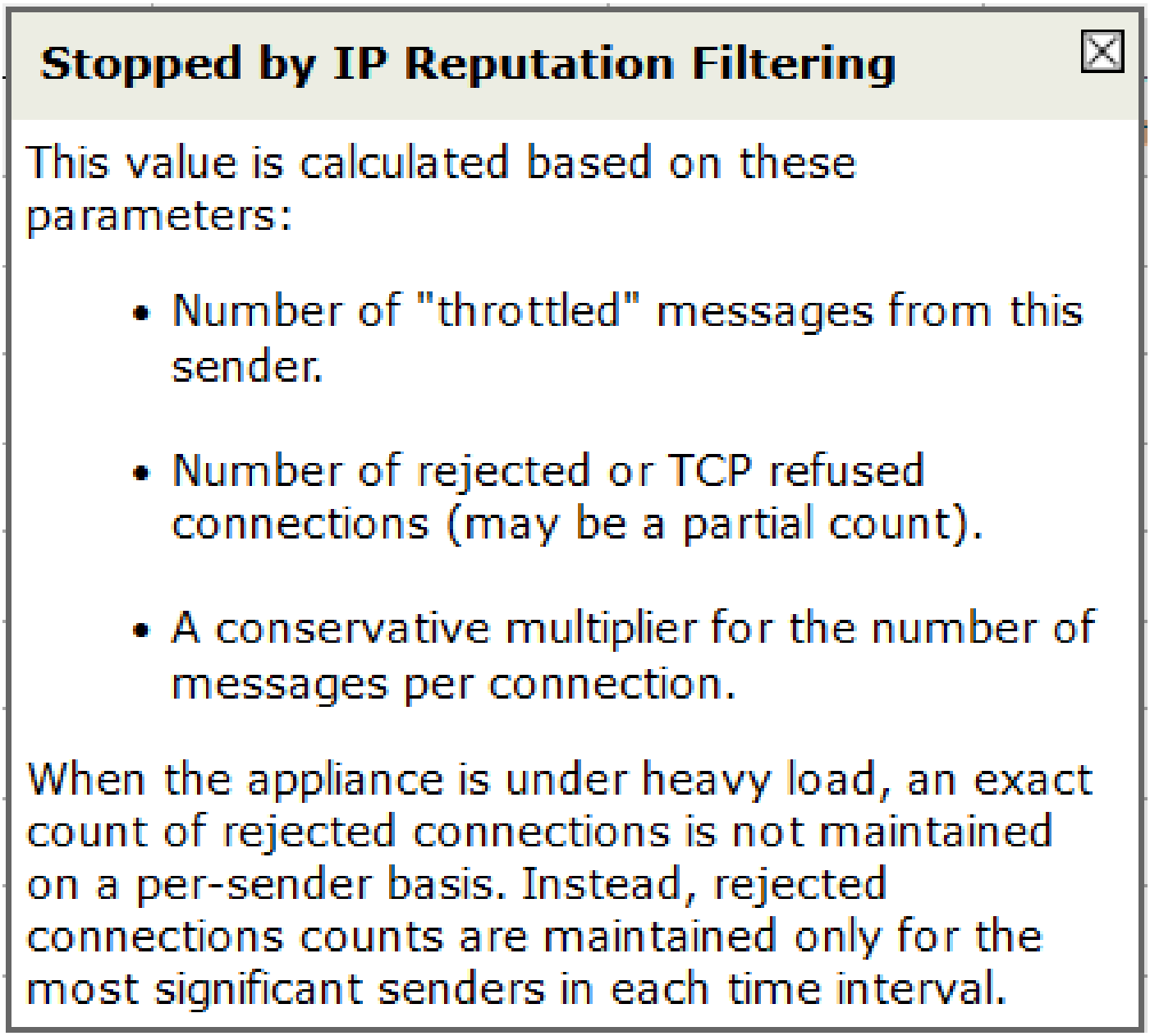


Topafzenders



Gegevens inkomende post

IP XXXX.XXXX.XXXX.XXXX heeft 234 e-mails verzonden, die allemaal lijken te zijn geblokkeerd door IP-reputatifiltering. Uit een analyse van het bijhouden van berichten en mail_logs in het apparaat blijkt echter dat e-mails van dit IP-adres met succes zijn afgeleverd, zonder bewijs van blokkering door IP-reputatifiltering.



Voorwaarden voor IP-reputatie filtering

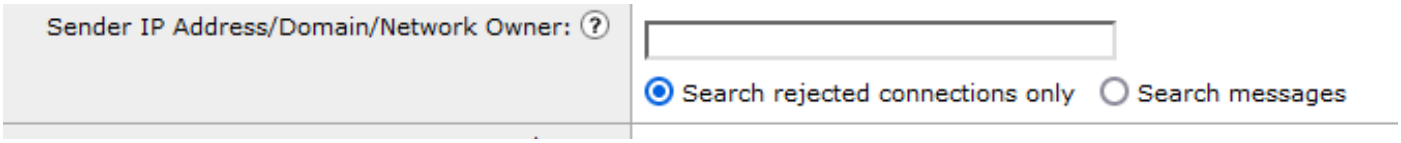
IP-reputatieschermfiltering wordt berekend op basis van specifieke parameters, zoals wordt weergegeven in de referentiescreenshot. In bepaalde gevallen kunnen e-mails zich op de derde voorwaarde richten - een conservatieve multiplier voor het aantal berichten per verbinding. De logboeken van de afwijzing zijn slechts zichtbaar als e-mails aan de eerste twee voorwaarden voldoen. Het apparaat kan echter een geschat aantal berichten weergeven op basis van deze multiplier.

Het rapport kan bij benadering een aantal aansluitingen weergeven, waarvan sommige het apparaat niet echt kunnen bereiken. Zo is bijvoorbeeld een Simple Mail Transfer Protocol (SMTP)-verbinding tot stand gebracht, maar deze wordt later verbroken vanwege een netwerkprobleem. De derde voorwaarde verklaart dergelijke scenario's, die een geschatte analyse verstrekken van of de verbinding de IP reputatiecontrole overging of ontbrak. Dit betekent niet per se dat alle vermelde berichten werden geblokkeerd door IP-reputatiescherm filtering.

Geblokkeerde e-mails controleren

Om te bepalen of berichten daadwerkelijk zijn geblokkeerd:

- Controleer de lijst met geblokkeerde zenders: Berichten die zijn geblokkeerd door IP-reputatie filtering, worden gecategoriseerd onder de groep van afzenders met een blokklijst.
- Berichttracering gebruiken: Navigeer naar Geavanceerde opties, voer het IP-adres in om te zoeken en selecteer Alleen afgewezen verbindingen zoeken.



Geweigerde verbindingen zoeken in berichttracering

- Beoordeel Mail Logs: E-mails die worden geblokkeerd door de blokklijst sender groep kunnen worden geïdentificeerd in mail_logs.
- Vertraagde hat afwijzing: IP-filtering wordt op het niveau van de SMTP-verbinding afgedwongen en de functie Delayed Host Access Table (HAT) Reject op ESA kan worden gebruikt om de oorzaak te begrijpen.

Gerelateerde informatie

- Vertraagde afwijzing Veelgestelde vragen
- Cisco ESA-gebruikershandleiding
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.