Solucionar problemas relacionados a "interrompido pelo filtro de reputação de IP"

Contents

Introdução

Este documento descreve uma consulta comum em relatórios que indicam e-mails interrompidos pela "filtragem de reputação de IP".

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Email Appliance

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Email Appliance

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A filtragem de Reputação de IP é a primeira camada de proteção contra spam que permite o controle sobre mensagens que passam pelo gateway de e-mail com base na confiabilidade do remetente, conforme determinado pelo Serviço de Reputação de IP do Remetente. Este artigo discute como resolver problemas relacionados à filtragem de reputação de IP.

Problema

Ao acessar relatórios no dispositivo ESA/CES navegando para Monitor > Incoming Mail, alguns e-mails parecem ser bloqueados pela "filtragem de reputação de IP". Em alguns casos, o número total de tentativas de e-mail corresponde àquelas interrompidas pela filtragem de reputação de IP, o que gera preocupações sobre sua precisão. Além disso, pode ser difícil localizar e-mails específicos que foram bloqueados.

Uma preocupação comum é a incapacidade de gerar uma lista de e-mails bloqueados pela filtragem de reputação de IP, levando à confusão sobre se e-mails legítimos foram filtrados por engano.

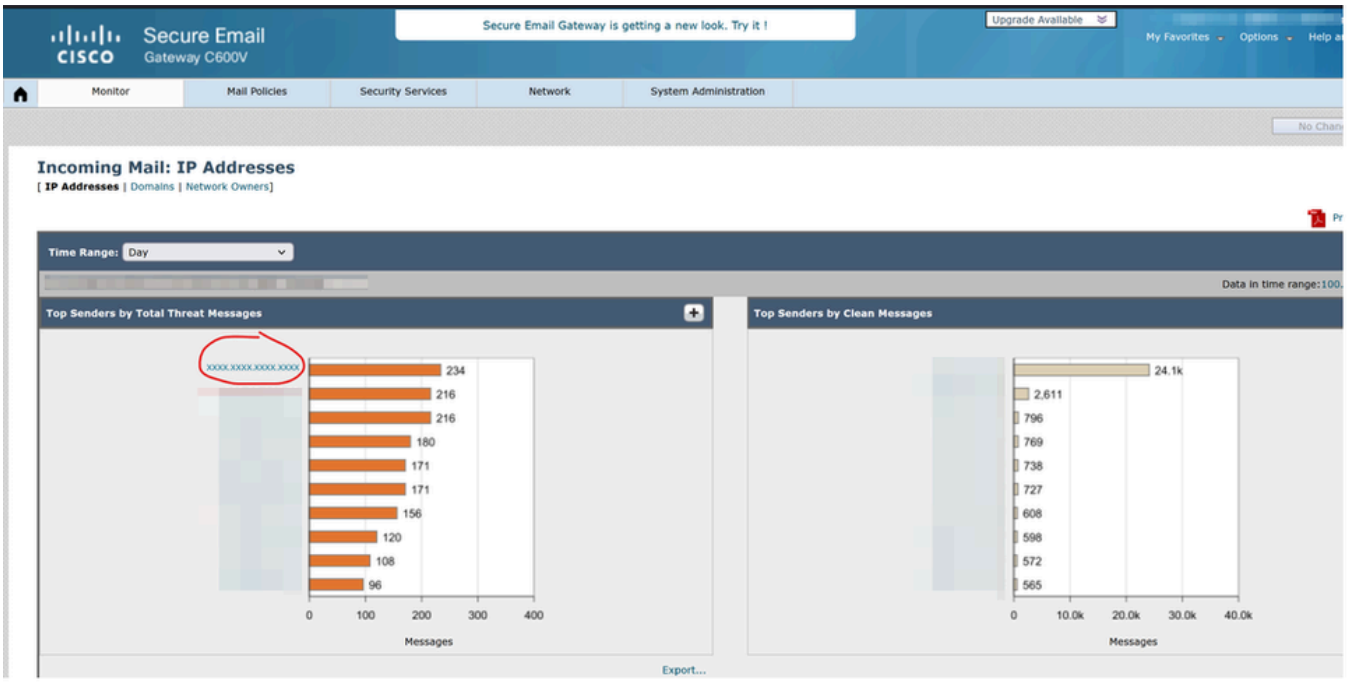
Solução

As funções de filtragem de reputação IP são semelhantes às Sender Base Reputation Scores (SBRS) em dispositivos ESA, usando um método de cálculo comparável.

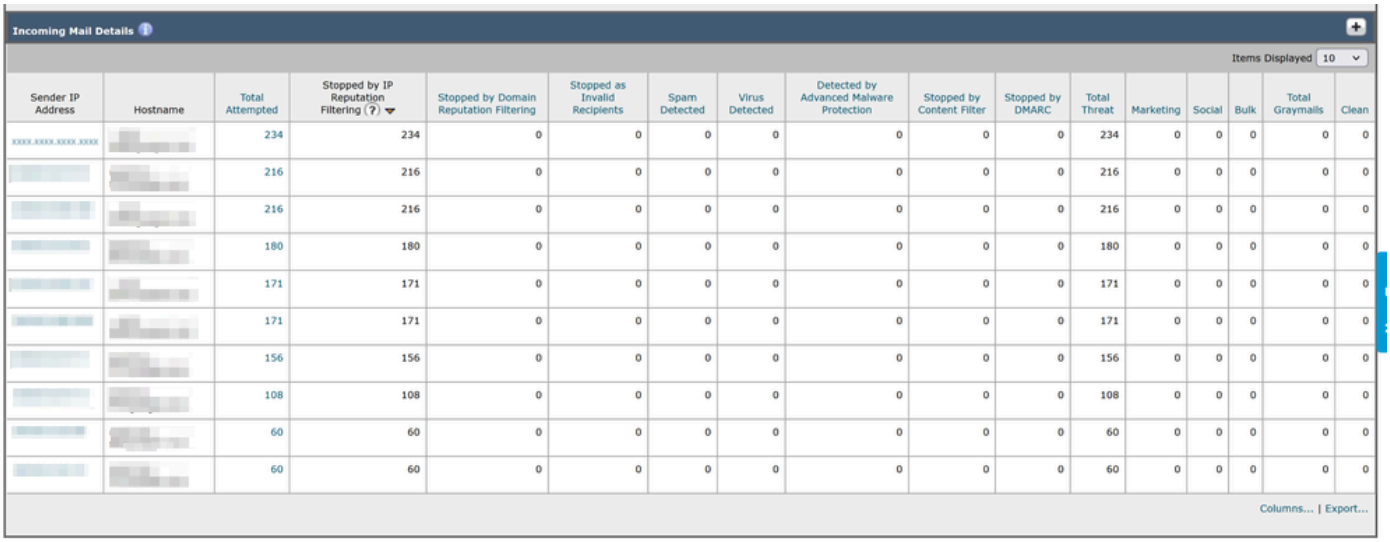
Entender a filtragem de reputação de IP

A filtragem de reputação de IP do remetente é a primeira camada de proteção contra spam, permitindo o controle sobre as mensagens que chegam pelo gateway de e-mail com base na confiabilidade dos remetentes, conforme determinado pelo serviço de reputação de IP do remetente. O IP Reputation Service, usando dados globais da rede de afiliados Talos, atribui uma pontuação de reputação IP (IPRS) a remetentes de e-mail com base em taxas de reclamação, estatísticas de volume de mensagens e dados de listas publicamente bloqueadas e listas de proxy abertas. A pontuação de reputação de IP ajuda a diferenciar remetentes legítimos de fontes de spam. Você pode determinar o limite para bloquear mensagens de remetentes com pontuações baixas de reputação. A inteligência do Talos (Talos Intelligence) fornece uma visão geral global das ameaças mais recentes de email e baseadas na Web, exibe o volume de tráfego de email atual por país e permite pesquisar as pontuações de reputação com base no endereço IP, URI ou domínio.

O exemplo explica o funcionamento da filtragem de reputação de IP:

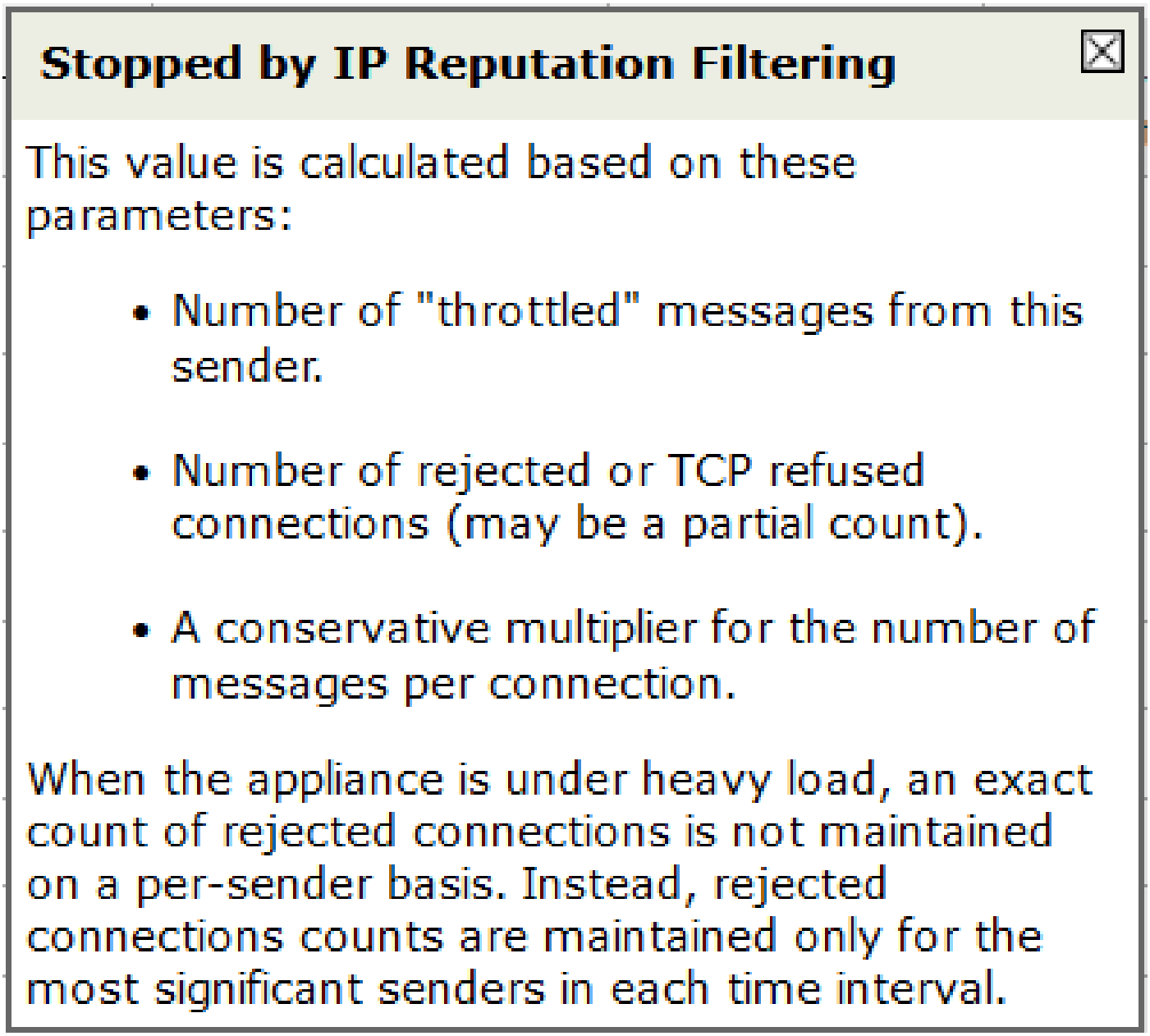


Principais remetentes



Detalhes de e-mails recebidos

O IP XXXX.XXXX.XXXX.XXXX enviou 234 emails, todos aparentemente bloqueados pela filtragem de reputação de IP. No entanto, uma análise do rastreamento de mensagens e mail_logs no dispositivo mostra que os e-mails desse IP foram entregues com êxito, sem evidências de bloqueio por filtragem de reputação de IP.



Condições aplicáveis para filtragem de reputação de IP

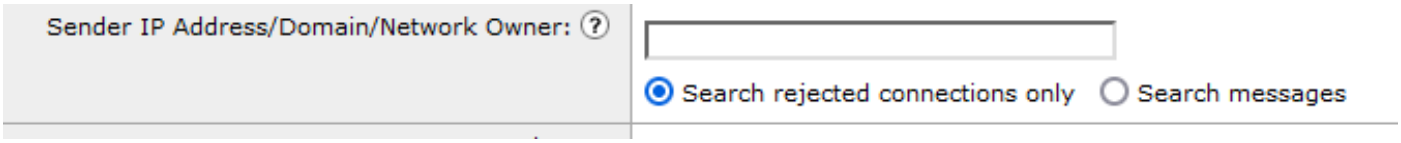
A filtragem de reputação de IP é calculada com base em parâmetros específicos, como mostrado na captura de tela mencionada. Em certos casos, os e-mails podem se alinhar com a terceira condição - um multiplicador conservador para o número de mensagens por conexão. Os logs de rejeição só serão visíveis se os emails atenderem às duas primeiras condições. No entanto, o dispositivo pode exibir um número estimado de mensagens com base nesse multiplicador.

O relatório pode refletir um número aproximado de conexões, algumas das quais não podem realmente alcançar o dispositivo. Por exemplo, uma conexão Simple Mail Transfer Protocol (SMTP) é estabelecida, mas é posteriormente descartada devido a um problema de rede. A terceira condição é responsável por tais cenários, fornecendo uma análise estimada se a conexão foi aprovada ou reprovada na verificação de reputação de IP. Isso não indica necessariamente que todas as mensagens listadas foram bloqueadas pela filtragem de reputação de IP.

Verificar e-mails bloqueados

Para determinar se as mensagens foram realmente bloqueadas:

- Verificar Grupo de Remetentes da Lista de Bloqueio: As mensagens bloqueadas pela filtragem de reputação de IP são categorizadas no grupo de remetentes da lista de bloqueio.
- Usar Rastreamento de Mensagem: Navegue até Advanced Options, insira o endereço IP a ser pesquisado e selecione Search rejected connections only.



Pesquisar Conexões Rejeitadas no Rastreamento de Mensagem

- Revisar logs de e-mail: Os e-mails bloqueados pelo grupo de remetentes da lista de bloqueio podem ser identificados em mail_logs.
- Rejeição de HAT atrasada: A filtragem de IP é aplicada no nível de conexão SMTP e o recurso de rejeição de tabela de acesso de host atrasada (HAT) no ESA pode ser usado para entender a causa.

Informações Relacionadas

- Perguntas Frequentes de Rejeição Atrasada de HAT
- Guia do usuário do Cisco ESA
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.