Diferenças entre filtros de mensagens e filtros de conteúdo no ESA

Contents

Introduction
Diferenças entre filtros de mensagens e filtros de conteúdo
Filtros de conteúdo
Filtros de mensagem
Ações para todos os destinatários

Introduction

Este documento descreve as diferenças entre filtros de mensagens e filtros de conteúdo no Cisco Email Security Appliance (ESA) e descreve qual filtro é melhor para qual tipo de ação.

Diferenças entre filtros de mensagens e filtros de conteúdo

Os filtros de mensagens e os filtros de conteúdo usam o mesmo idioma de script e correspondência de expressão regular.

Filtros de conteúdo

Os filtros de conteúdo suportam um subconjunto das regras e ações usadas pelos filtros de mensagens. Os filtros de conteúdo incluem todas as regras e ações necessárias para identificar e agir sobre o conteúdo de uma mensagem e são fáceis de configurar na GUI.

Filtros de mensagem

Os filtros de mensagens são mais flexíveis e dão acesso aos metadados de uma mensagem, como o ouvinte de recebimento, o IP do remetente, a pontuação de reputação SenderBase do remetente, o número de destinatários na mensagem, o tamanho da mensagem ou dos anexos. Um subconjunto dos metadados também está disponível nos Filtros de conteúdo. Os Filtros de Mensagens são aplicados como a **primeira** etapa de processamento de Política no pipeline de emails ESA. Quando um filtro de mensagens é aplicado, suas ações se aplicam a todos os destinatários da mensagem. Isso significa que, se a ação for Ignorar, nenhum destinatário receberá a mensagem, mesmo que a regra que correspondeu à mensagem correspondesse a apenas um destinatário.

Ações para todos os destinatários

Os Filtros de conteúdo são aplicados como a **última** etapa de processamento de política no pipeline de e-mails, depois que as mensagens são **divididas** em cópias separadas, dependendo das Políticas de e-mail (e, portanto, de diferentes grupos de destinatários) definidas em sua configuração. Por causa disso, os Filtros de conteúdo podem ser aplicados a um grupo mais detalhado de remetentes ou destinatários. Se você executar uma ação em todos os destinatários, será mais eficiente fazê-lo em um filtro de mensagens antes que ocorra a divisão de mensagens. Isso é especialmente verdadeiro no caso da verificação de conteúdo (regra de corpo ou anexo contém) ou se a ação é descartar ou devolver uma mensagem, o que evitaria a varredura de antivírus e antisspam em uma mensagem destinada a não entrega.