Guia do melhor prática para o Anti-Spam, anti-vírus, o Graymail e os filtros da manifestação

Índice

Visão geral

A grande maioria das ameaças, os ataques, e os incômodos enfrentados por uma organização através do email vêm sob a forma do Spam, do malware, e dos ataques misturados. A ferramenta de segurança do email de Cisco (ESA) inclui diversas Tecnologias e características diferentes para cortar fora estas ameaças no gateway antes que incorporem a organização. Este documento descreverá as aproximações do melhor prática para configurar o Anti-Spam, anti-vírus, o Graymail e os filtros da manifestação, no fluxo de entrada e de partida do email.

Anti-Spam

A proteção do Anti-Spam endereça uma gama completa de ameaças conhecidas que incluem ataques do Spam, do phishing e do zombi, assim como duro-à-detecta o volume baixo, breves ameaças do email tais como “419" embustes. Além, a proteção do Anti-Spam identifica ameaças misturadas novas e em desenvolvimento tais como os ataques do Spam que distribuem o índice malicioso com uma transferência URL ou um executável.

Cisco envia por correio eletrónico a Segurança oferece as seguintes soluções do anti-Spam:

- Filtração do Anti-Spam de IronPort (IPA)

- Filtração inteligente da Multi-varredura de Cisco (IMS)

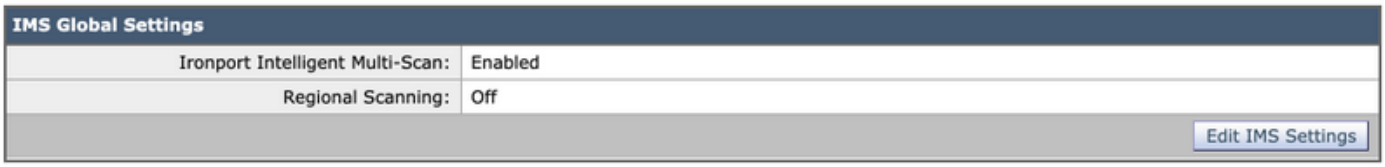
Você pode licenciar e permitir ambas as soluções em seu ESA mas somente pode usar um em uma política particular do correio. A fim este documento do melhor prática, nós está indo usar a característica IMS.

Verifique a chave de recurso

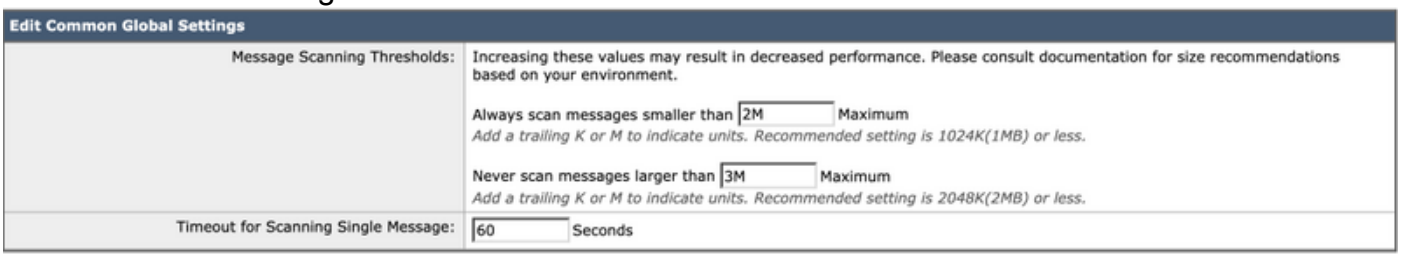
- No ESA, navegue à **administração do sistema** > às **chaves de recurso**
- Procure a licença inteligente da Multi-varredura e certifique-se que é ativa.

Permita a Multi-varredura inteligente (IMS) globalmente

- No ESA, navegue aos **Serviços de segurança** > ao **IMS e ao Graymail**
- Clique o **Enablebutton em configurações globais IMS**:



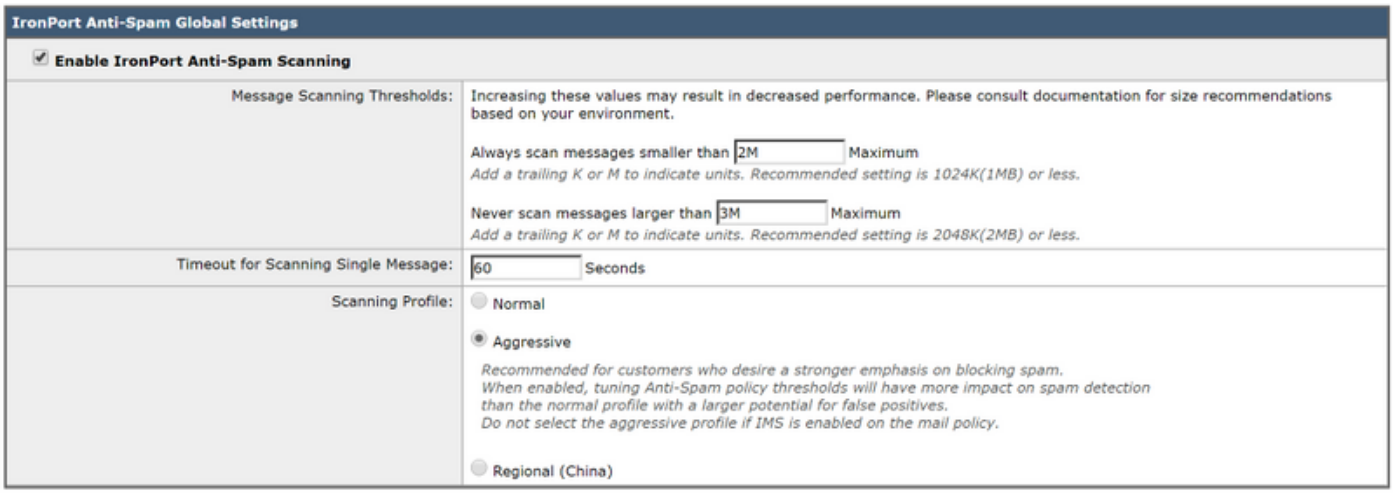
- Procure **configurações globais comuns** e o clique **edita configurações globais**
- Aqui você pode configurar ajustes múltiplos. As configurações recomendadas são mostradas na imagem abaixo:



- O clique **Submitand compromete suas mudanças**.

Se você não tem uma assinatura da licença IMS:

- Navegue aos **Serviços de segurança > ao Anti-Spam de IronPort**
- Clique o **Enablebutton na vista geral do Anti-Spam de IronPort**
- O clique **edita configurações globais**
- Aqui você pode configurar ajustes múltiplos. As configurações recomendadas são mostradas na imagem abaixo:

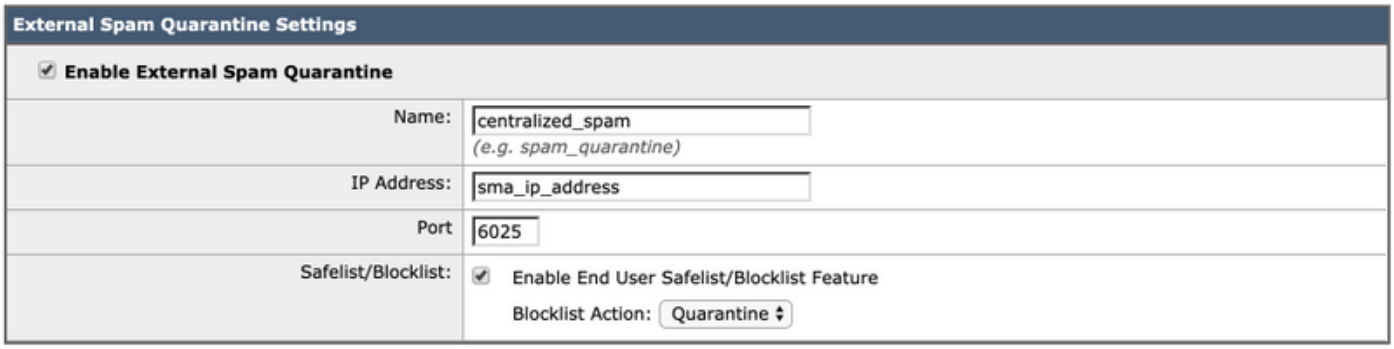


- Cisco recomenda selecionar o perfil **agressivo da** exploração para um cliente que deseje uma ênfase forte em obstruir o Spam.
- O clique **Submitand compromete suas mudanças**

Enable centralizou a quarentena do Spam

Desde que o Anti-Spam tem a opção a ser enviada para quarantine, é importante assegurar-se de que a quarentena do Spam se estabeleça:

- Navegue aos **Serviços de segurança** > à **quarentena do Spam**
- Clicar o **Configurebutton** tomá-lo-á à seguinte página.
- Aqui você pode permitir a quarentena verificando o **enablebox** e apontar a quarentena a ser centralizada em um dispositivo de SecurityManagement (S A) que byfilling no **IP address** SMANAMEAND. As configurações recomendadas são mostradas abaixo:



- O clique **Submitand compromete suas mudanças**

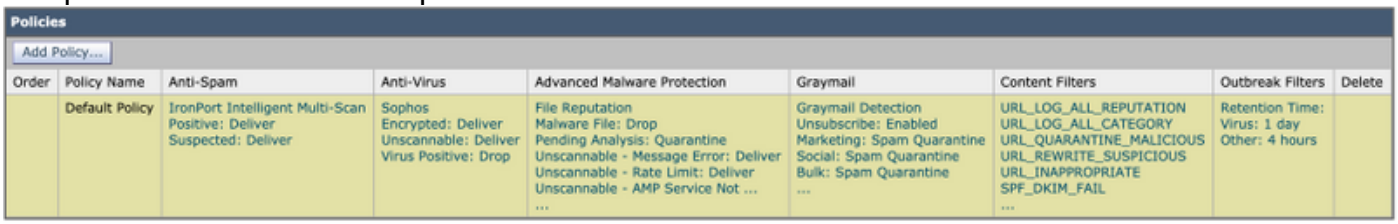
Para obter mais informações sobre da fundação e das quarentena centralizadas, refira por favor o documento dos melhores prática:
Melhores prática para a política, instalação das quarentena do vírus e da manifestação, e migração centralizadas do ESA ao S A

Configurar o Anti-Spam nas políticas

Uma vez que a Multi-varredura inteligente foi configurada globalmente, você pode agora aplicar a Multi-varredura inteligente para enviar políticas:

- Navegue **para enviar políticas > políticas do correio recebido**
- As políticas do correio recebido usam ajustes do Anti-Spam de IronPort à revelia.
- Clicar o link azul sob o Anti-**Spam** permitirá essa política particular usar ajustes

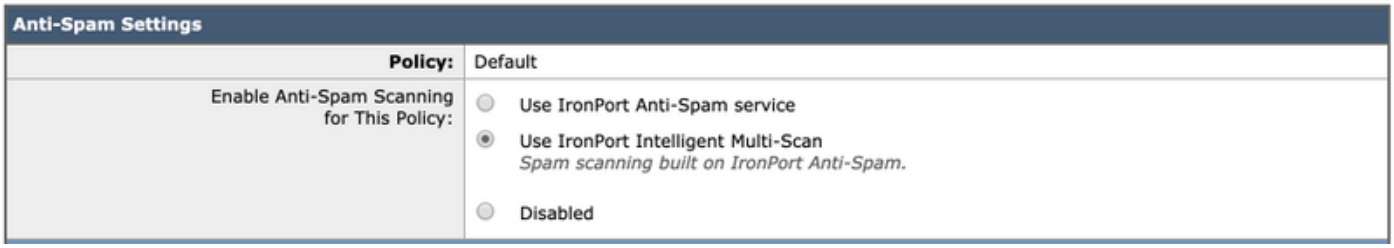
personalizados do Anti-Spam.
- Abaixo de você verá um exemplo que mostre a política padrão usando ajustes personalizados do Anti-Spam:



Personalize ajustes do Anti-Spam para uma política do correio recebido clicando o link azul sob o Anti-**Spam** para a política que você deseja personalizar.

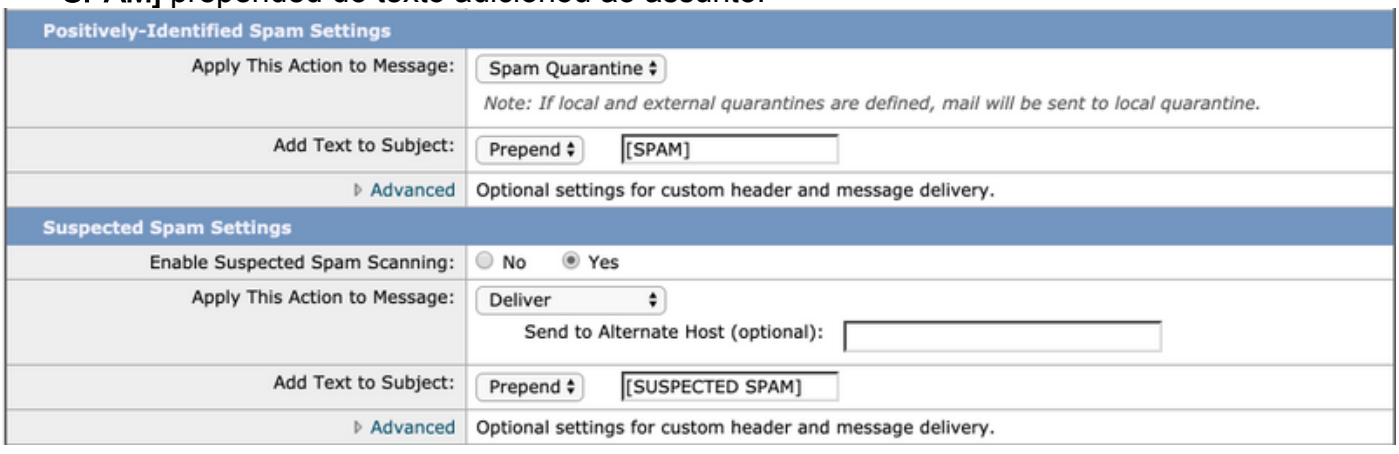
Aqui você pode selecionar a opção que da exploração do Anti-Spam você deseja permitir para esta política.

- Para fins deste documento do melhor prática, clique o botão de rádio ao lado da Multi-**varredura inteligente de IronPort do** uso:

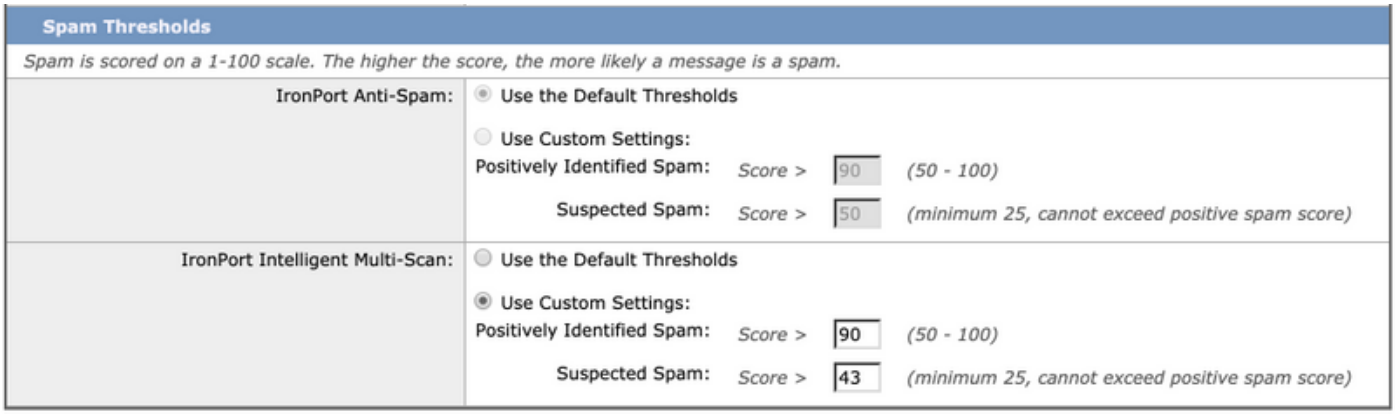


As duas seções seguintes incluem **ajustes Positivo-identificados do Spam** e **ajustes suspeitados do Spam:**

- O melhor prática recomendado é configurar a ação da **quarentena no** ajuste do **Spam Positivo-Identificar** com o **[SPAM]** prepended do texto adicionado ao assunto e;
- Aplique **para entregar** como a ação para **ajustes do Spam Suspected** com o **[SUSPECTED SPAM]** prepended do texto adicionou ao assunto:



- **A configuração de limiar do Spam** pode ser mudada, e as configurações recomendadas são personalizar a contagem Positivo-**identificada do Spam a 90** e a contagem **suspeitada do Spam a 43**:



- O clique **Submitand compromete suas mudanças**

Anti-vírus

A proteção anti-vírus é fornecida através de dois motores da terceira parte – Sophos e McAfee. Estes motores filtrarão todas as ameaças maliciosas conhecidas, deixando cair, limpando ou quarantining as como configuradas.

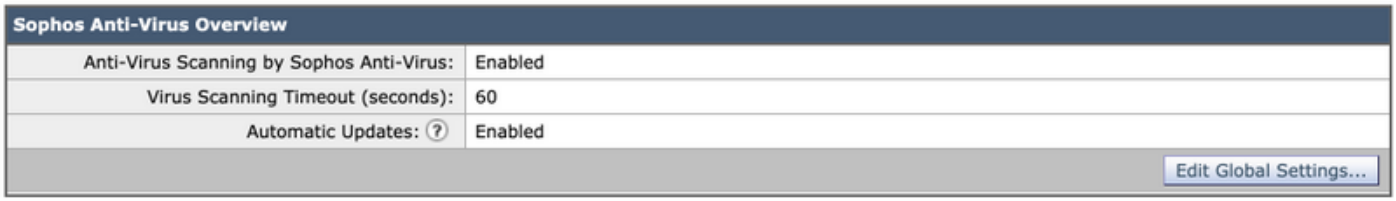
Verifique chaves de recurso

Para certificar-se de ambas as chaves de recurso estejam permitidas e active:

- Vá à **administração do sistema** > às **chaves de recurso**
- Certifique-se que **Sophos** licenças **anti-vírus** e da **McAfee** é ativo.

Permita a exploração anti-vírus

- Navegue aos **Serviços de segurança > anti-vírus - Sophos**
- Clique o **Enablebutton**.
- Certifique-se que a **atualização automática está permitida** e a atualização anti-vírus dos arquivos de Sophos está trabalhando muito bem. Caso necessário, **atualização do** clique **agora** para iniciar imediatamente a atualização do arquivo:



- O clique **Submitand compromete suas mudanças**.

Se a licença da McAfee é ativa também, navegue aos **Serviços de segurança > anti-vírus - McAfee**

- Clique o **Enablebutton**.

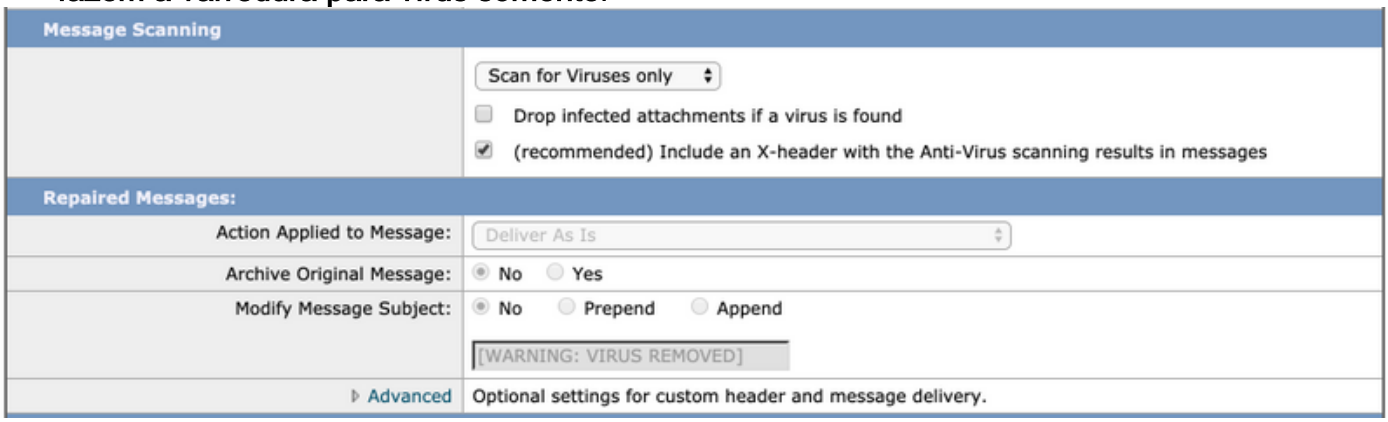
- Certifique-se que a **atualização automática está permitida** e a atualização anti-vírus dos arquivos da McAfee está trabalhando muito bem. Caso necessário, a **atualização do** clique **agora** para iniciar o arquivo atualiza imediatamente.
- O clique **Submitand compromete suas mudanças**

Configurar anti-vírus em políticas do correio

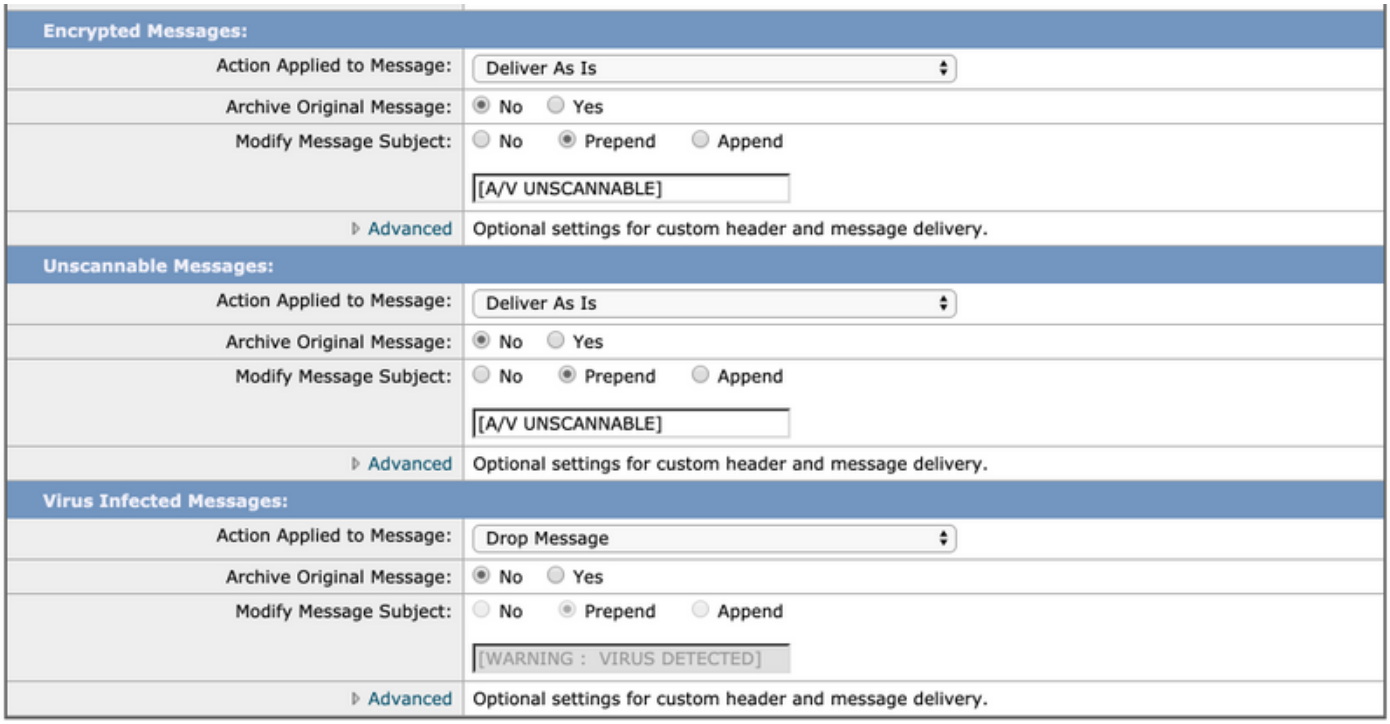
Em uma política do correio recebido, o seguinte é recomendado:

- Navegue **para enviar políticas > políticas do correio recebido**
- Personalize ajustes **anti-vírus** para uma política do correio recebido clicando o link azul sob anti-vírus para a política que você deseja personalizar.
- Aqui você pode selecionar a opção que anti-vírus da exploração você deseja permitir para esta política.
- Para fins deste documento do melhor prática, selecione a **McAfee** e o **Sophos anti-vírus**:

- Nós não tentamos reparar um arquivo, assim que as sobras da exploração da mensagem **fazem a varredura para vírus somente**:



- A ação recomendada para **mensagens cifrada** e de **Unscannable** é **entregar real** com uma linha de assunto alterada para sua atenção.
- A política recomendada para o Antivirus é **gota** todas as **mensagens Vírus-contaminadas** segundo as indicações da imagem abaixo:



- O clique **Submitand compromete suas mudanças**

Uma política similar é recomendada para políticas que parte do correio, contudo, nós não recomendamos alterar a linha de assunto no email de partida.

Graymail

A solução de gerenciamento do graymail na ferramenta de segurança do email compreende de dois componentes: um motor integrado da exploração do graymail e um serviço nuvem-baseado do cancelar assinatura. A solução de gerenciamento do graymail permite que as organizações identifiquem o graymail usando o motor integrado do graymail e apliquem controles de política apropriados e forneçam um mecanismo fácil para utilizadores finais ao cancelar assinatura dos mensagens não desejada usando o serviço do cancelar assinatura.

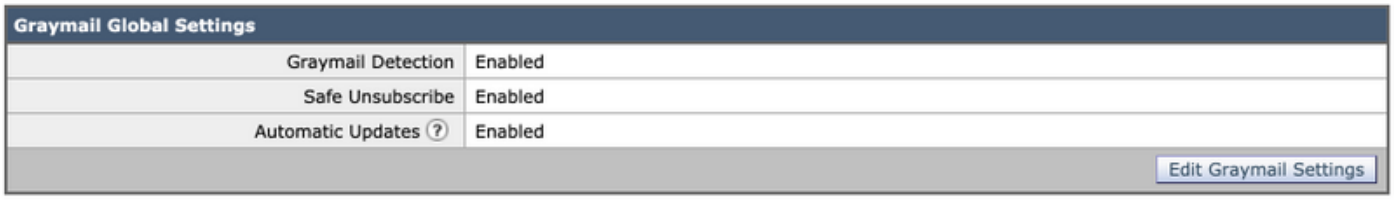
As categorias de Graymail incluem o email do mercado, o email social da rede e o email do volume. As opções avançadas incluem adicionar um encabeçamento feito sob encomenda, a emissão a um host alternativo e a arquivística da mensagem. Para este melhor prática, nós permitiremos a característica segura do cancelar assinatura de Graymail para a política do correio do padrão.

Verifique a chave de recurso

- No ESA, navegue à **administração do sistema** > às **chaves de recurso**
- Procure **Graymail Unsubscription seguro** e certifique-se que é ativo.

Permita Graymail e serviços seguros do cancelar assinatura

- No ESA, navegue aos **Serviços de segurança** > ao **IMS e ao Graymail**
- Clique a **edição Graymail Settingsbutton em configurações globais de Graymail**
- Selecione todas as opções - **Permita a detecção de Graymail**, **permita o cancelar assinatura seguro** e **permita atualizações automáticas**:



- O clique **Submitand compromete suas mudanças**

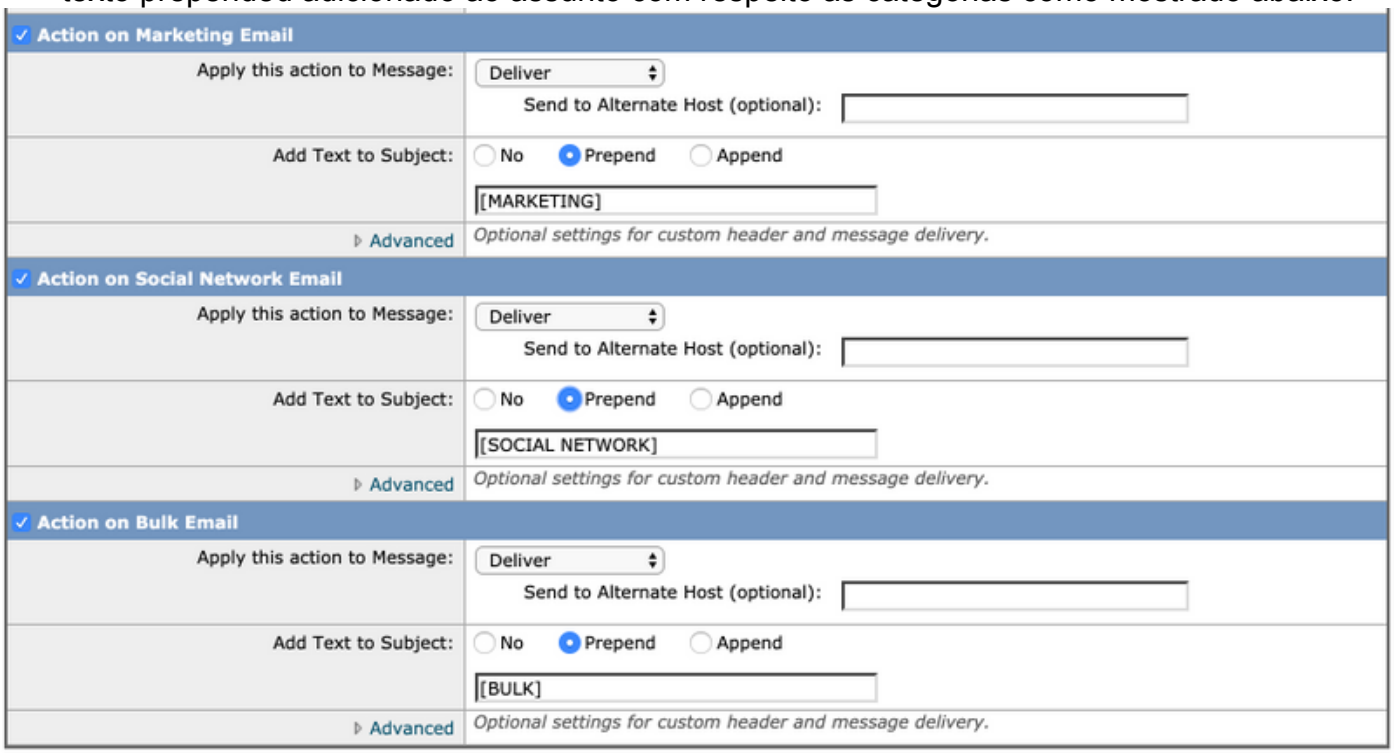
Configurar Graymail e o cancelar assinatura seguro nas políticas

Uma vez que Graymail e o cancelar assinatura seguro foram configurados globalmente, você pode agora aplicar estes serviços para enviar políticas.

- Navegue **para enviar políticas > políticas do correio recebido**
- Clicar o link azul sob **Graymail** permitirá essa política particular usar ajustes personalizados de Graymail.
- Aqui você pode selecionar o Graymailoptions que você deseja permitir para esta política.
- Para fins deste documento do melhor prática, clique o botão de rádio ao lado de **permitem a detecção de Graymail para esta política** e **permitem Graymail que Unsubscribing para esta política**:

As três seções seguintes incluem a **ação em ajustes do email do mercado**, a **ação em ajustes sociais do email da rede** e a **ação em ajustes maiorias do email**.

- O melhor prática recomendado é permitir todo e permanecer a ação como **entrega** com o texto prepended adicionado ao assunto com respeito às categorias como mostrado abaixo:



- O clique **Submitand compromete suas mudanças**

A política que parte do correio deve mandar **Graymail** permanecer em condições **deficientes**.

Filtros da manifestação

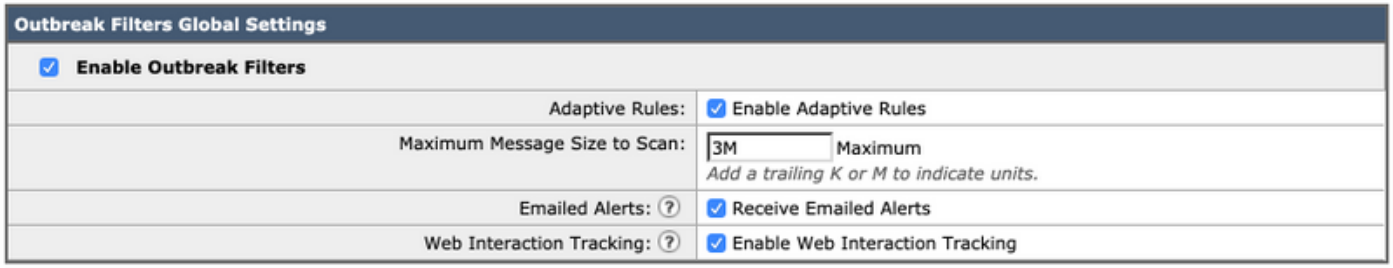
Os filtros da manifestação combinam disparadores no motor do Anti-Spam, exploração URL e Tecnologias e mais da detecção para etiquetar corretamente os artigos que caem fora da categoria verdadeira do Spam – por exemplo, o phishing enviam por correio eletrónico e os email do embuste e seguram-nos apropriadamente com notificações de usuário ou quarentena.

Verifique a chave de recurso

- No ESA, navegue à **administração do sistema** > às **chaves de recurso**
- Procure **filtros da manifestação** e certifique-se que é ativo.

Permita o serviço dos filtros da manifestação

- No ESA, navegue aos **Serviços de segurança** > aos **filtros da manifestação**
- Clique o **Enablebutton na vista geral dos filtros da manifestação**
- Aqui você pode configurar ajustes múltiplos. As configurações recomendadas são mostradas na imagem abaixo:

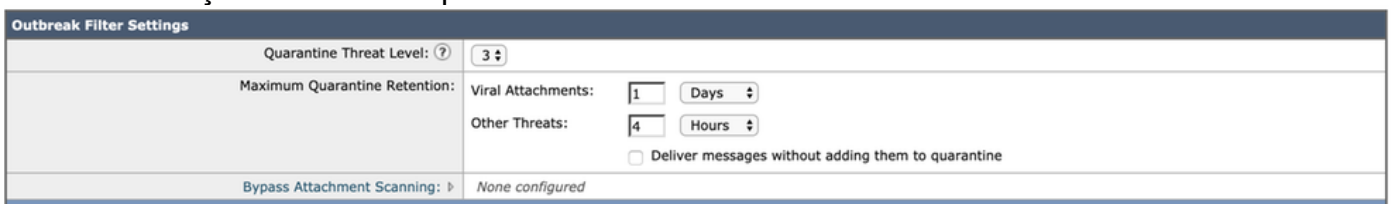


- O clique **Submitand compromete suas mudanças**.

Configurar filtros da manifestação nas políticas

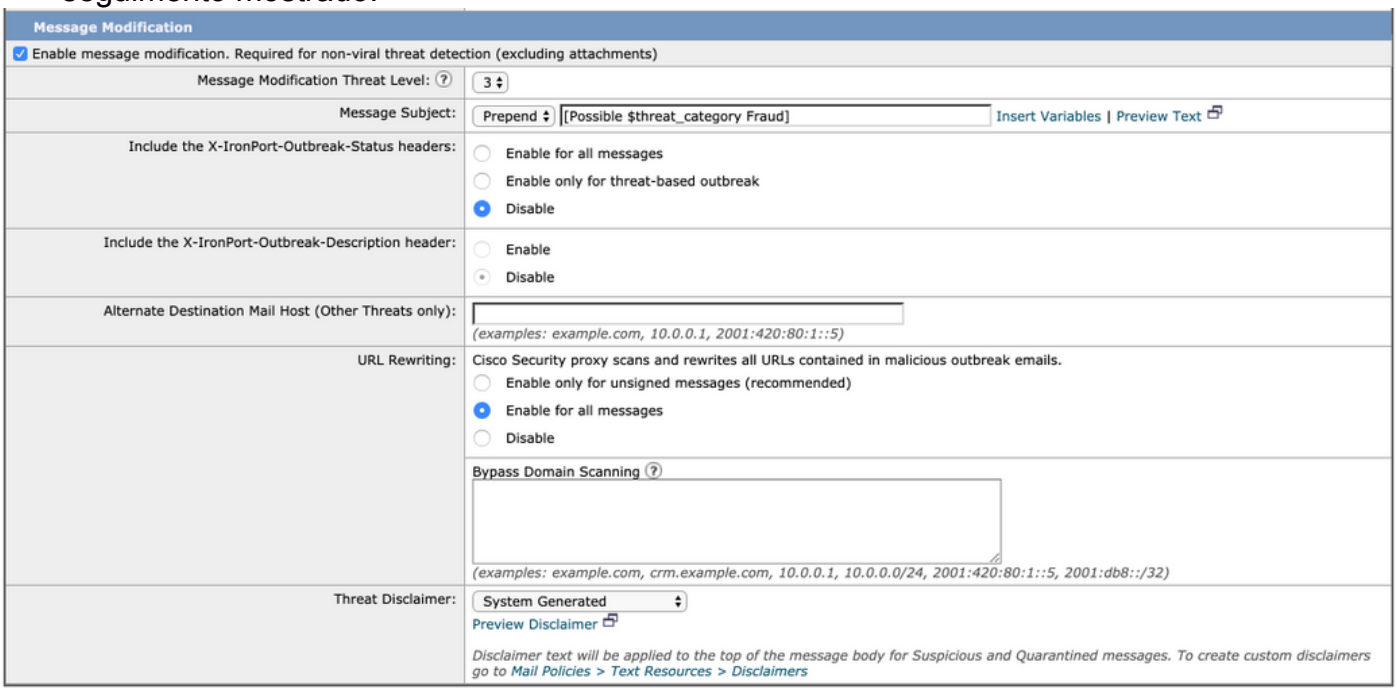
Uma vez que a manifestação Filtershas configurado globalmente, você pode agora aplicar políticas deste tomail da característica.

- Navegue **para enviar políticas > políticas do correio recebido**
- Clicar o link azul sob **filtros da manifestação** permitirá essa política particular usar ajustes personalizados dos filtros da manifestação.
- Para fins deste documento do melhor prática, nós mantemos os ajustes do filtro da manifestação com valores padrão:



- Os filtros da manifestação podem reescrever URL se são julgados maliciosos, suspeitos, ou phish. Seleto **permita a alteração da mensagem** de detectar e reescrever ameaças baseadas URL.

- Certifique-se que a opção da **reescrita URL** é **permite** para todas as mensagens como o seguimento mostrado:



- O clique **Submitand compromete suas mudanças**

A política que parte do correio deve mandar **filtros da manifestação** permanecer em condições **deficientes**.

Conclusão

Este documento apontou descrever o padrão, ou configurações do melhor prática para o Anti-Spam, anti-vírus, o Graymail e os filtros da manifestação na ferramenta de segurança do email (ESA). Todos estes filtros estão disponíveis nas políticas de entrada e de partida do email, e a configuração e a filtração estão recomendadas em ambos – quando o volume da proteção for para de entrada, filtrar o fluxo de partida fornece a proteção contra email retransmitidos ou ataques maliciosos internos.