

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

## Índice

[Overview](#)

[Anti-Spam](#)

[Verifique a chave de recurso](#)

[Permita a Multi-varredura inteligente \(IMS\) globalmente](#)

[Enable centralizou a quarentena do Spam](#)

[Configurar o Anti-Spam nas políticas](#)

[Anti-vírus](#)

[Verifique chaves de recurso](#)

[Permita a exploração anti-vírus](#)

[Configurar anti-vírus em políticas do correio](#)

[Graymail](#)

[Verifique a chave de recurso](#)

[Permita Graymail e serviços seguros do cancelar assinatura](#)

[Configurar Graymail e o cancelar assinatura seguro nas políticas](#)

[Filtros da manifestação](#)

[Verifique a chave de recurso](#)

[Permita o serviço dos filtros da manifestação](#)

[Configurar filtros da manifestação nas políticas](#)

[Conclusão](#)

## 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 eletrônico 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 **Enable** button em **configurações globais IMS**:

IMS Global Settings	
Ironport Intelligent Multi-Scan:	Enabled
Regional Scanning:	Off
<a href="#">Edit IMS Settings</a>	

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

Edit Common Global Settings	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum  <small>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</small></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum  <small>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</small></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

- O clique **Submit** and compromete suas mudanças.

Se você não tem uma assinatura da licença IMS:

- Navegue aos **Serviços de segurança** > ao **Anti-Spam de IronPort**
- Clique o **Enable** button 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:

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> <b>Enable IronPort Anti-Spam Scanning</b>	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<p><input type="radio"/> Normal</p> <p><input checked="" type="radio"/> <b>Aggressive</b> <i>Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</i></p> <p><input type="radio"/> Regional (China)</p>

- 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:

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> <b>Enable External Spam Quarantine</b>	
Name:	<input type="text" value="centralized_spam"/> <i>(e.g. spam_quarantine)</i>
IP Address:	<input type="text" value="sma_ip_address"/>
Port	<input type="text" value="6025"/>
Safelist/Blocklist:	<input checked="" type="checkbox"/> <b>Enable End User Safelist/Blocklist Feature</b> Blocklist Action: <input type="text" value="Quarantine"/>

- 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:

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver	Sophos: Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ... ...	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	

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**:

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan Spam scanning built on IronPort Anti-Spam. <input type="radio"/> Disabled

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:

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine <small>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</small>
Add Text to Subject:	Prepend [SPAM]
Advanced	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	No Yes
Apply This Action to Message:	Deliver Send to Alternate Host (optional):
Add Text to Subject:	Prepend [SUSPECTED SPAM]
Advanced	Optional settings for custom header and message delivery.

- 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**:

Spam Thresholds	
<i>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</i>	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input type="radio"/> Use the Default Thresholds <input checked="" type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="43"/> (minimum 25, cannot exceed positive spam score)

- 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:

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: (?)	Enabled
<a href="#">Edit Global Settings...</a>	

Current Sophos Anti-Virus files			
File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Wed Nov 6 10:04:30 2019	3.2.07.377.1_5.68	Not Available
Sophos IDE Rules	Wed Nov 6 12:03:56 2019	2019110602	Not Available
No updates in progress.			<a href="#">Update Now</a>

- 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**:

Anti-Virus Settings	
<b>Policy:</b>	DEFAULT
<b>Enable Anti-Virus Scanning for This Policy:</b>	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> No

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

Message Scanning	
	Scan for Viruses only <input type="button" value="v"/> <input type="checkbox"/> Drop infected attachments if a virus is found <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	<input type="text" value="Deliver As Is"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	<input type="text" value="[WARNING: VIRUS REMOVED]"/>
<a href="#">Advanced</a>	Optional settings for custom header and message delivery.

- 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:

Encrypted Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
▶ Advanced	Optional settings for custom header and message delivery.

- O clique **Submit** 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 Settings** button em configurações globais de Graymail
- Selecione todas as opções - **Permita a detecção de Graymail**, **permita o cancelar assinatura seguro** e **permita atualizações automáticas**:



Graymail Global Settings	
Graymail Detection	Enabled
Safe Unsubscribe	Enabled
Automatic Updates <sup>?</sup>	Enabled

[Edit Graymail Settings](#)

- O clique **Submit** 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 Graymail options 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:**

Graymail Settings	
<b>Policy:</b>	DEFAULT
<b>Enable Graymail Detection for This Policy:</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<b>Enable Graymail Unsubscribing for This Policy:</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Perform this action for: <input checked="" type="radio"/> All Messages (Recommended) <input type="radio"/> Unsigned Messages

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:

<b>✓ Action on Marketing Email</b>	
Apply this action to Message:	Deliver <input type="text" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[MARKETING]"/>
<b>Advanced</b>	<i>Optional settings for custom header and message delivery.</i>
<b>✓ Action on Social Network Email</b>	
Apply this action to Message:	Deliver <input type="text" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[SOCIAL NETWORK]"/>
<b>Advanced</b>	<i>Optional settings for custom header and message delivery.</i>
<b>✓ Action on Bulk Email</b>	
Apply this action to Message:	Deliver <input type="text" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[BULK]"/>
<b>Advanced</b>	<i>Optional settings for custom header and message delivery.</i>



- 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 eletrônico 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 **Enable** button na vista geral dos **filtros da manifestação**
- Aqui você pode configurar ajustes múltiplos. As configurações recomendadas são mostradas na imagem abaixo:

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> <b>Enable Outbreak Filters</b>	
Adaptive Rules:	<input checked="" type="checkbox"/> <b>Enable Adaptive Rules</b>
Maximum Message Size to Scan:	<input type="text" value="3M"/> Maximum <small>Add a trailing K or M to indicate units.</small>
Emailed Alerts: (?)	<input checked="" type="checkbox"/> <b>Receive Emailed Alerts</b>
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> <b>Enable Web Interaction Tracking</b>

- 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 tomal 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:

Outbreak Filter Settings	
Quarantine Threat Level: (?)	<input type="text" value="3"/>
Maximum Quarantine Retention:	Viral Attachments: <input type="text" value="1"/> <input type="text" value="Days"/>
	Other Threats: <input type="text" value="4"/> <input type="text" value="Hours"/>
	<input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▶	None configured

- Os filtros da manifestação podem reescrever URL se são julgados maliciosos, suspeitos, ou phish. Seletor **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:

Message Modification	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: ?	3
Message Subject:	Prepend [Possible \$threat_category Fraud] <a href="#">Insert Variables</a>   <a href="#">Preview Text</a>
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	<input type="text"/> <small>(examples: example.com, 10.0.0.1, 2001:420:80:1::5)</small>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
	Bypass Domain Scanning ? <input type="text"/> <small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</small>
Threat Disclaimer:	System Generated <a href="#">Preview Disclaimer</a> <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies &gt; Text Resources &gt; Disclaimers</small>

- 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.