

Configurar o filtro de conteúdo para monitorar a verificação de SPF e DKIM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Informações de Apoio](#)

[O que é SPF e DKIM](#)

[Configurar](#)

[Verifique os resultados](#)

[Monitorar via GUI](#)

[Monitorar via CLI](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como criar um filtro de conteúdo para monitorar mensagens do Email Security Appliance (ESA) que podem falhar com SPF e DKIM.

Pré-requisitos

- Conhecimento do produto Cisco Email Security Appliance
- Conhecimento dos conceitos básicos dos métodos de autenticação de e-mail Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM).

Requisitos

- Verificação de SPF e DKIM habilitada em qualquer uma de suas políticas de fluxo de email.
- Uma função de usuário apropriada onde você pode criar e implementar filtros de conteúdo.
- Acesso do CLI ao seu equipamento se você quiser usar a opção de linha de comando para procurar por coincidências de filtro.

Informações de Apoio

Ao implementar um filtro de conteúdo para monitorar esses dois mecanismos, você tem a vantagem de fornecer visibilidade, rastrear e até mesmo a capacidade de exportar mensagens que podem falhar com essas tecnologias de autenticação de e-mail para referência futura e necessidades baseadas na sua empresa, que também podem ajudá-lo a tomar decisões de implementação futuras.

O que é SPF e DKIM

SPF e DKIM são mecanismos que mantêm a segurança das mensagens de e-mail. Esses protocolos têm a capacidade de impedir que servidores não autorizados enviem mensagens como se elas fossem de seu domínio e também oferecem aos destinatários uma maneira de verificar se os e-mails vêm de sua organização.

O registro SPF melhora a cobertura de autenticação, a entrega e ajuda a promover o nível desejado de segurança para seus domínios. O SPF é aplicado no servidor de e-mail do receptor e verifica o endereço IP do remetente, o domínio no cabeçalho FROM do e-mail e a lista de remetentes permitidos no registro DNS SPF desse domínio. A entrega poderá falhar se o IP do remetente não estiver na lista.

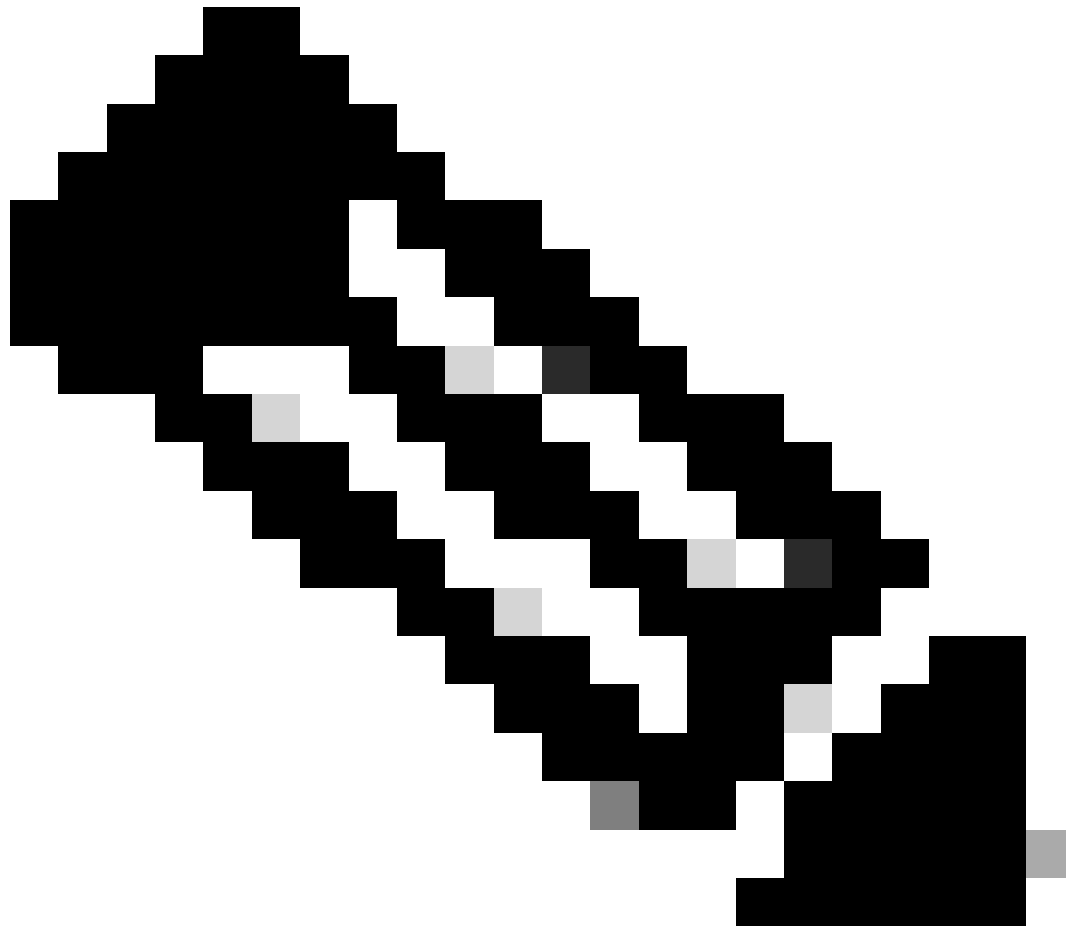
Enquanto o SPF indica se um servidor pode enviar como seu domínio, o DKIM examina e-mails. É uma forma de assinatura que permite aos servidores destinatários rastrear e-mails de volta à sua origem.

O DKIM fornece uma maneira de verificar se um e-mail é autêntico, se não foi modificado em trânsito e se foi realmente enviado pelo seu servidor. Quando o DKIM falhar, o destinatário poderá tratar o e-mail como não confiável e caberá ao destinatário decidir o que fazer com o e-mail. Provavelmente, ele acaba em alguma pasta de spam do destinatário, mas também pode ser descartado por completo.

Configurar

Crie um filtro de Conteúdo de Entrada para o monitor SPF.

1. Na GUI do ESA, navegue para Políticas de e-mail > Filtros de conteúdo de entrada.
2. Clique em Adicionar filtro.
3. No campo de nome, use um nome apropriado para identificar o filtro. Nesse caso, SPF_FAILED_MONITOR.
4. Clique em Adicionar condição.
5. À esquerda, procure Verificação SPF. Aqui: Nenhum, Falha temporária, Erro temporário, Erro permanente.
6. Depois de marcar essas opções, clique em Ok na parte inferior da janela.
7. Agora, clique em Add Action e, no lado esquerdo, escolha Add Log Entry.
8. No campo de texto, você pode adicionar o texto mais adequado, neste caso, como este: —>
\$FilterName triggered <—



Note: Uma entrada de registro pode fornecer mais controle e visibilidade de quando esse filtro é disparado dentro do seu ESA e quando você está solucionando problemas através da linha de comando, por exemplo, fornece uma melhor visibilidade sobre os filtros que foram ativados.

Exemplo:

Edit Incoming Content Filter

Content Filter Settings			
Name:	<input type="text" value="SPF_FAILED_MONITOR"/>		
Currently Used by Policies:	Default Policy		
Description:	<input type="text"/>		
Order:	1 <input type="button" value="v"/> (of 15)		

Conditions			
<input type="button" value="Add Condition..."/>			
Order	Condition	Rule	Delete
1	SPF Verification	spf-status == "none,softfail,fail,temperror,permerror"	<input type="button" value="Delete"/>

Actions			
<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("--> \$FilterName triggered <--")	<input type="button" value="Delete"/>

Crie um filtro de Conteúdo de Entrada para o Monitor DKIM.

1. Na GUI do ESA, navegue para Políticas de e-mail > Filtros de conteúdo de entrada.
2. Clique em Adicionar filtro.
3. No campo de nome, use um nome apropriado para identificar o filtro. Nesse caso, use DKIM_FAILED_MONITOR.
4. Clique em Adicionar condição.
5. No lado esquerdo, procure Autenticação DKIM. Aqui, use: nenhum, hardfail, permerror, temperror.
6. Depois de marcar essas opções, clique em Ok na parte inferior da janela.
7. Diferentemente da configuração SPF, neste filtro de conteúdo DKIM, você precisa adicionar uma condição para cada Resultado de autenticação.
8. Depois de adicionar as condições, clique em Add Action e, no lado esquerdo, escolha Add Log Entry.
9. No campo de texto, você pode adicionar o texto mais adequado para você. Neste caso, como este: —> \$FilterName acionado <—

Exemplo:

Edit Incoming Content Filter

Content Filter Settings

Name:	<input type="text" value="DKIM_FAILED_MONITOR"/>
Currently Used by Policies:	Default Policy
Description:	<input type="text"/>
Order:	<input type="text" value="2"/> (of 15)

Conditions

Apply rule:

Order	Condition	Rule	Delete
1	DKIM Authentication	dkim-authentication == "none"	<input type="button" value="Delete"/>
2	DKIM Authentication	dkim-authentication == "hardfail"	<input type="button" value="Delete"/>
3	DKIM Authentication	dkim-authentication == "permerror"	<input type="button" value="Delete"/>
4	DKIM Authentication	dkim-authentication == "temperror"	<input type="button" value="Delete"/>

Actions

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("--> \$FilterName triggered <--")	<input type="button" value="Delete"/>

Ative os filtros de conteúdo de entrada na política de e-mails recebidos.

Depois de ter ambos os filtros de conteúdo configurados, você precisa ativá-los em sua Política de recebimento de e-mail. Para fazer isso, você pode executar estas etapas.

1. Na GUI do ESA, navegue para Políticas de e-mail > Políticas de recebimento de e-mail.
2. Você precisa escolher qual política é onde os filtros de conteúdo funcionam. Nesse caso, use a Política padrão.
3. Vá para a 7ª coluna, a que está relacionada a Filtros de conteúdo e clique nos campos que aparecem nessa coluna.
4. Será exibida uma janela chamada Filtragem de conteúdo para: Default Policy (Política padrão).
5. Quando estiver lá, escolha a opção Ativar filtros de conteúdo (Personalizar configurações). Com essa opção, você tem a possibilidade de escolher quais filtros de conteúdo deseja ativar nessa política.

Mail Policies: Content Filters

Content Filtering for: Default Policy

Content Filters

Order	Filter Name	Description	Enable
1	SPF_FAILED_MONITOR		<input checked="" type="checkbox"/>
2	DKIM_FAILED_MONITOR		<input checked="" type="checkbox"/>

6. Depois, clique em Submit.

7. Depois de clicar em Enviar, a janela retornará você às Políticas de recebimento de e-mail e, na coluna Filtros de conteúdo, você verá que novos filtros foram adicionados.

Incoming Mail Policies

The screenshot displays the 'Incoming Mail Policies' interface. At the top, there is a 'Find Policies' section with an 'Email Address:' input field, radio buttons for 'Recipient' (selected) and 'Sender', and a 'Find Policies' button. Below this is a table of policies. The 'Content Filters' column is highlighted with a red box, showing the following filters: SPF_FAILED_MONITOR, DKIM_FAILED_MONITOR, and ExternalTagging. A legend at the bottom right indicates that yellow cells represent 'Default', white cells represent 'Custom', and gray cells represent 'Disabled'.

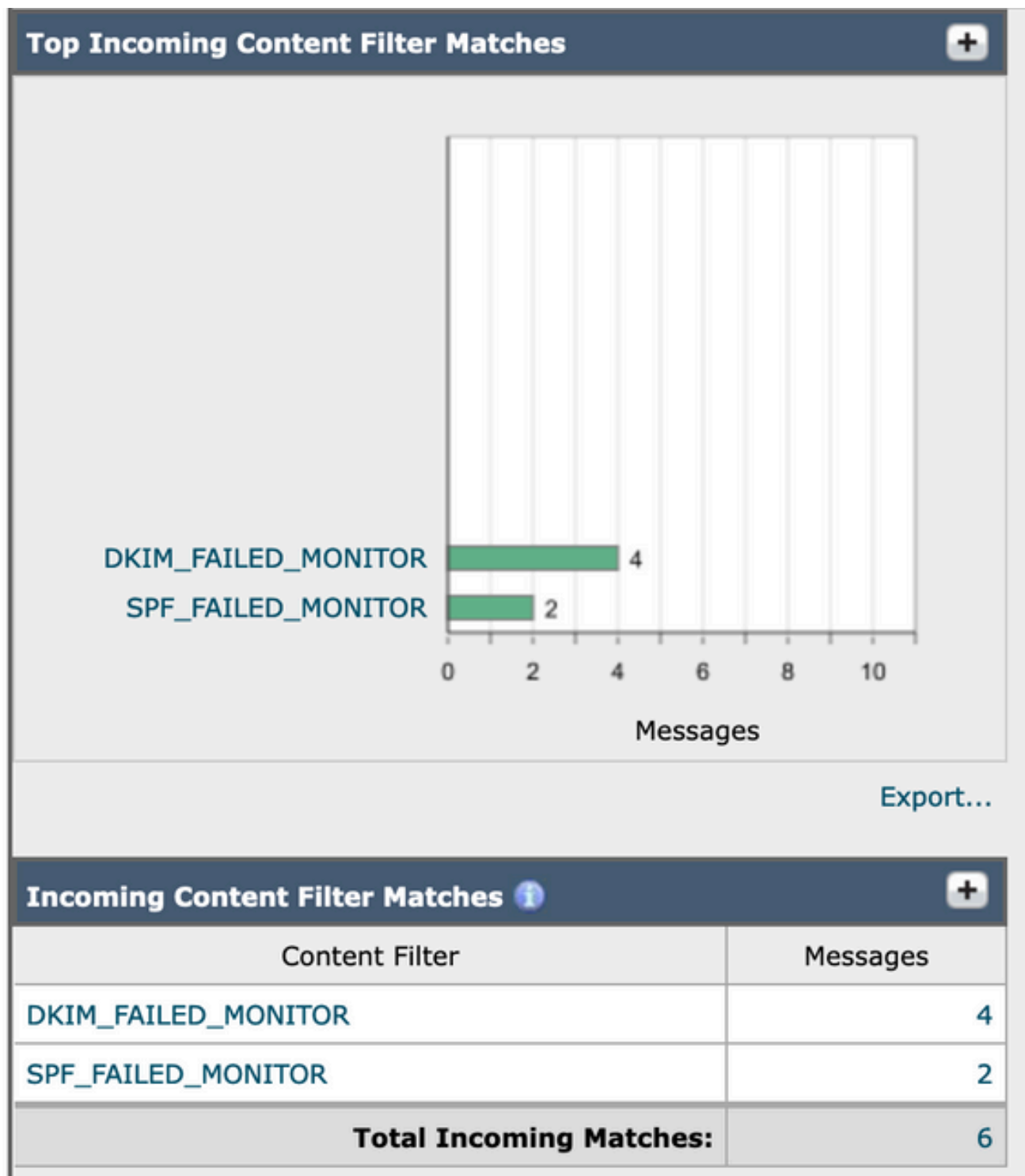
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Quarantine	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Quarantine Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection	SPF_FAILED_MONITOR DKIM_FAILED_MONITOR ExternalTagging	Disabled	Not Available	

Verifique os resultados

Para verificar os resultados desses filtros de conteúdo, você pode verificá-los na opção de monitoramento via GUI ou via acesso de linha de comando.

Monitorar via GUI

1. Na GUI do ESA/SMA, navegue para Monitor > Content Filters.
2. Localize todas as correspondências dos Filtros de conteúdo de entrada e as mensagens que correspondem às correspondências que os filtros tiveram.



3. Você pode clicar em cada uma delas e você verá as correspondências feitas.
4. Se você clicar no número de mensagens, ele o enviará ao Rastreamento de mensagens para fazer uma pesquisa global das mensagens que fizeram corresponder a esse filtro de conteúdo.

Monitorar via CLI

Esses filtros de conteúdo também podem ser monitorados via CLI com estas etapas:

1. Depois de fazer login no seu ESA via CLI, você pode digitar este comando para procurar por coincidências:

```
grep "SPF_FAILED_MONITOR" mail_logs
```

2. A saída deste comando é assim:

```
esa1.cisco.com> grep "SPF_FAILED_MONITOR" mail_logs Tue Mar 28 08:13:59 2023 Info: MID 3365 Custom Log Entry: -->
SPF_FAILED_MONITOR triggered <-- Tue Mar 28 08:22:24 2023 Info: MID 3367 Custom Log Entry: --> SPF_FAILED_MONITOR
triggered <-- =====
esa1.cisco.com> grep "DKIM_FAILED_MONITOR" mail_logs Tue Mar 28 08:09:04 2023 Info: MID 3364 Custom Log Entry: -->
DKIM_FAILED_MONITOR triggered <-- Tue Mar 28 08:13:59 2023 Info: MID 3365 Custom Log Entry: --> DKIM_FAILED_MONITOR
triggered <-- Tue Mar 28 08:17:45 2023 Info: MID 3366 Custom Log Entry: --> DKIM_FAILED_MONITOR triggered <-- Tue Mar 28
08:22:24 2023 Info: MID 3367 Custom Log Entry: --> DKIM_FAILED_MONITOR triggered <--
```

Informações Relacionadas

- [Melhor prática para autenticação de e-mail – maneiras ideais de implantar SPF, DKIM e DMARC](#)

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.