Bloquear URLs em e-mails com base em TLD em e-mail seguro

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Informações de Apoio

- Etapa 1. Criar um Filtro
- Etapa 2. Usar Expressões Regulares
- Etapa 3. Testar no modo de monitor
- Considerações de desempenho

Conclusão

Introdução

Este documento descreve como bloquear URLs no Cisco Secure Email com base em domínios de nível superior (TLDs) específicos.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure Email.

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

O bloqueio de URLs com base em TLDs específicos pode ser uma maneira eficaz de proteger seu sistema de e-mail contra possíveis ameaças. O Cisco Email Security Gateway (CES/ESA) analisa a reputação dos URLs e os executa com base em vários critérios.

No entanto, se a política da sua empresa exigir o bloqueio de certos TLDs, este procedimento explica como conseguir isso usando filtros e dicionários no seu sistema de e-mail.

Etapa 1. Criar um Filtro

Para bloquear um TLD inteiro, primeiro você precisa criar um filtro de conteúdo em seu sistema de e-mail. Este filtro identifica e bloqueia URLs que contêm os TLDs que você deseja restringir. Você pode aprimorar esse processo usando dicionários para gerenciar listas de TLDs e incorporar expressões regulares relevantes. Ao adicionar essas expressões regulares a um dicionário, você pode gerenciar e aplicar seus critérios de filtragem com eficiência.

Etapa 2. Usar Expressões Regulares

Expressões regulares (regex) são uma ferramenta poderosa para identificar padrões específicos em URLs.

Para bloquear efetivamente URLs baseados em TLDs, você pode adicionar essas expressões regulares a um dicionário. Essa abordagem facilita o gerenciamento e as atualizações de seus critérios de filtragem:

1. Expressão regular para bloquear URLs, começando por HTTP ou HTTPS; incluindo suporte para domínios Punycode:

```
(?i)https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)
```

2. Expressão regular para bloquear URLs utilizando um formato de e-mail, também suportando Punycode:

```
(?i)https?:\/\/.*@((xn--\w+\.)|(\w+\.))+(zip|mov)
```

Ao adicionar essas expressões regulares a um dicionário, você pode simplificar o processo de filtragem de URLs, garantindo que seu sistema de e-mail bloqueie eficientemente os TLDs especificados.

Dictionary Properties

Name: URL_TLD

Advanced Matching: ☐ Match whole words ☐ Case Sensitive

▷ Smart Identifiers: *Match specific patterns such as social security numbers and credit card numbers.*

Dictionary Number of terms: 2

Add Terms:

Separate multiple entries with line breaks.

Weight: 1

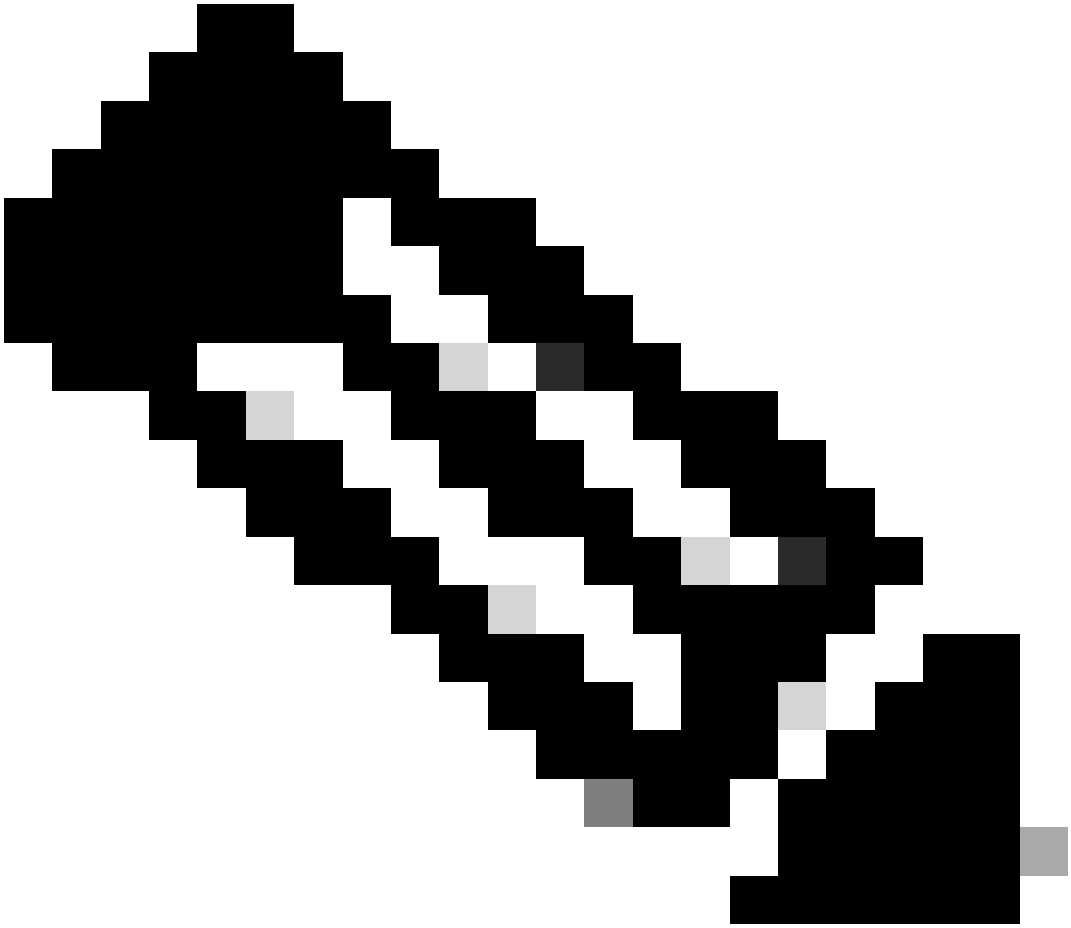
Add

Displaying 1 - 2 of 2 items
Page 1 of 1

<< Previous 1 Next >> 10

Term	Weight	Delete
https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)	1	
https?:\/\/.*@((xn--\w+\.)|(\w+\.))+(zip|mov)	1	

Cancel Submit



> Note: Se você precisar considerar caracteres Unicode, como U+2215 (⁄) e U+2044 (/), ajustes adicionais em sua expressão regular podem ser necessários.

Etapa 3. Testar no modo de monitor

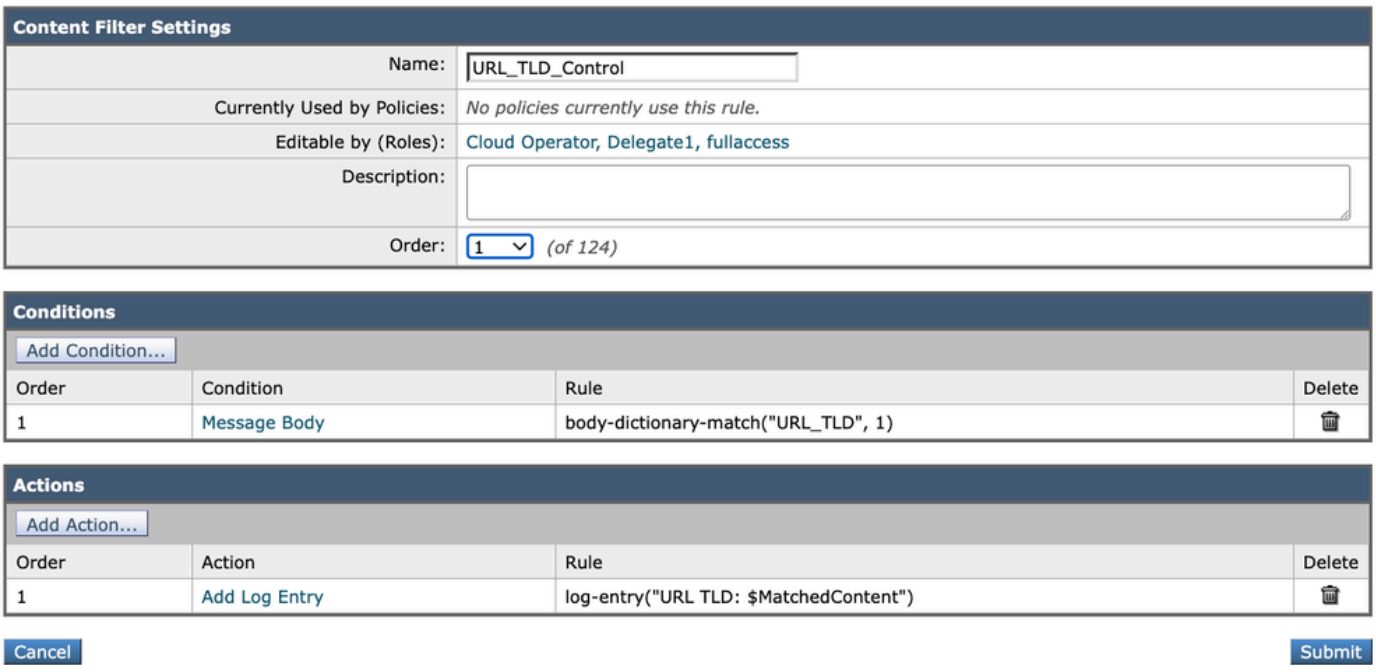
Antes de implementar esses filtros em um ambiente de produção, é aconselhável usá-los no modo de monitor. Essa abordagem permite que você avalie a eficácia dos filtros sem bloquear imediatamente os e-mails, evitando, assim, interrupções não intencionais no sistema de e-mail.

No modo de monitoramento, o sistema registra as instâncias em que os URLs correspondem aos critérios especificados, permitindo que você observe os resultados e faça os ajustes necessários. Para facilitar isso, você pode configurar uma ação de entrada de log que capture informações relevantes sobre os URLs correspondentes. Por exemplo, você pode usar esta ação de entrada de log:

```
log-entry("URL TLD: $MatchedContent")
```

Esta ação registra o conteúdo específico que correspondeu aos seus critérios de filtro, fornecendo informações valiosas sobre as URLs que serão bloqueadas se o filtro estiver ativo. Ao revisar esses logs, você pode ajustar as expressões regulares e as entradas do dicionário para garantir que eles capturem com precisão os URLs desejados sem afetar os e-mails legítimos.

Além disso, monitorar os registros durante um período permite avaliar o impacto de desempenho dos filtros e fazer otimizações conforme necessário. Depois de ter certeza de que os filtros estão funcionando conforme o esperado, você pode fazer a transição do modo de monitor para o modo de bloqueio ativo:



Considerações de desempenho

O uso extensivo de expressões regulares pode afetar o desempenho do sistema de e-mail. Portanto, é essencial testar e otimizar conforme necessário.

Conclusão

O bloqueio de URLs com base em TLDs específicos pode aumentar a segurança do seu sistema de e-mail. Notavelmente, novos TLDs introduzidos pelo Google, como .zip e .mov, levantaram preocupações de segurança devido à sua similaridade com extensões de arquivos populares. Testar os filtros com cuidado e considerar o impacto no desempenho ajuda a manter um sistema eficiente e seguro.

O Google Registry anunciou oito novos TLDs: .dad, .phd, .prof, .esq, .foo, .zip, .mov e .nexus. No entanto, .zip e .mov chamaram particularmente a atenção devido à sua semelhança com extensões de arquivo amplamente utilizadas, tornando crucial abordá-las em suas medidas de segurança.

Para obter mais informações sobre as implicações de segurança do .zip TLD, você pode consultar a publicação do blog Talos Intelligence: Vazamento de informações TLD ZIP. Este recurso fornece um contexto adicional sobre os riscos potenciais associados a estes TLD e sublinha a importância de implementar estratégias de filtragem adequadas.

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.