セキュリティで保護された電子メールのTLDに基づいて電子メールのURLをブロック

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

- [ステップ 1：フィルタの作成](#)
- [ステップ 2：正規表現の使用](#)
- [ステップ 3：モニタモードでのテスト](#)
- [パフォーマンスに関する考慮事項](#)

[結論](#)

はじめに

このドキュメントでは、特定のトップレベルドメイン(TLD)に基づいてCisco Secure Email(CSE)のURLをブロックする方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Secure Emailに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

特定のTLDに基づいてURLをブロックすることは、潜在的な脅威から電子メールシステムを保護するための効果的な方法です。Cisco Eメールセキュリティゲートウェイ(CES/ESA)は、URLのレピュテーションを分析し、さまざまな基準に基づいてURLを実行します。

ただし、会社のポリシーで特定のTLDをブロックする必要がある場合は、この手順で、電子メールシステムのフィルタと辞書を使用してTLDをブロックする方法を説明します。

ステップ 1：フィルタの作成

TLD全体をブロックするには、最初に電子メールシステムでコンテンツフィルタを作成する必要があります。このフィルタは、制限するTLDを含むURLを識別し、ブロックします。辞書を使用してTLDのリストを管理し、関連する正規表現を組み込むことによって、このプロセスを強化できます。これらの正規表現を辞書に追加すると、フィルタリング条件を効率的に管理および適用できます。

ステップ 2：正規表現の使用

正規表現(regex)は、URLの特定のパターンを特定するための強力なツールです。

TLDに基づいてURLを効果的にブロックするために、これらの正規表現をディクショナリに追加できます。このアプローチにより、フィルタリング基準の管理と更新が容易になります。

1. HTTPまたはHTTPSで始まるURLをブロックするための正規表現、 Punycodeドメインのサポートを含む：

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

2. 電子メール形式を使用してURLをブロックするための正規表現。Punycodeもサポートします。

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

これらの正規表現を辞書に追加すると、URLをフィルタリングするプロセスを合理化でき、指定したTLDを電子メールシステムで効率的にブロックできます。

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

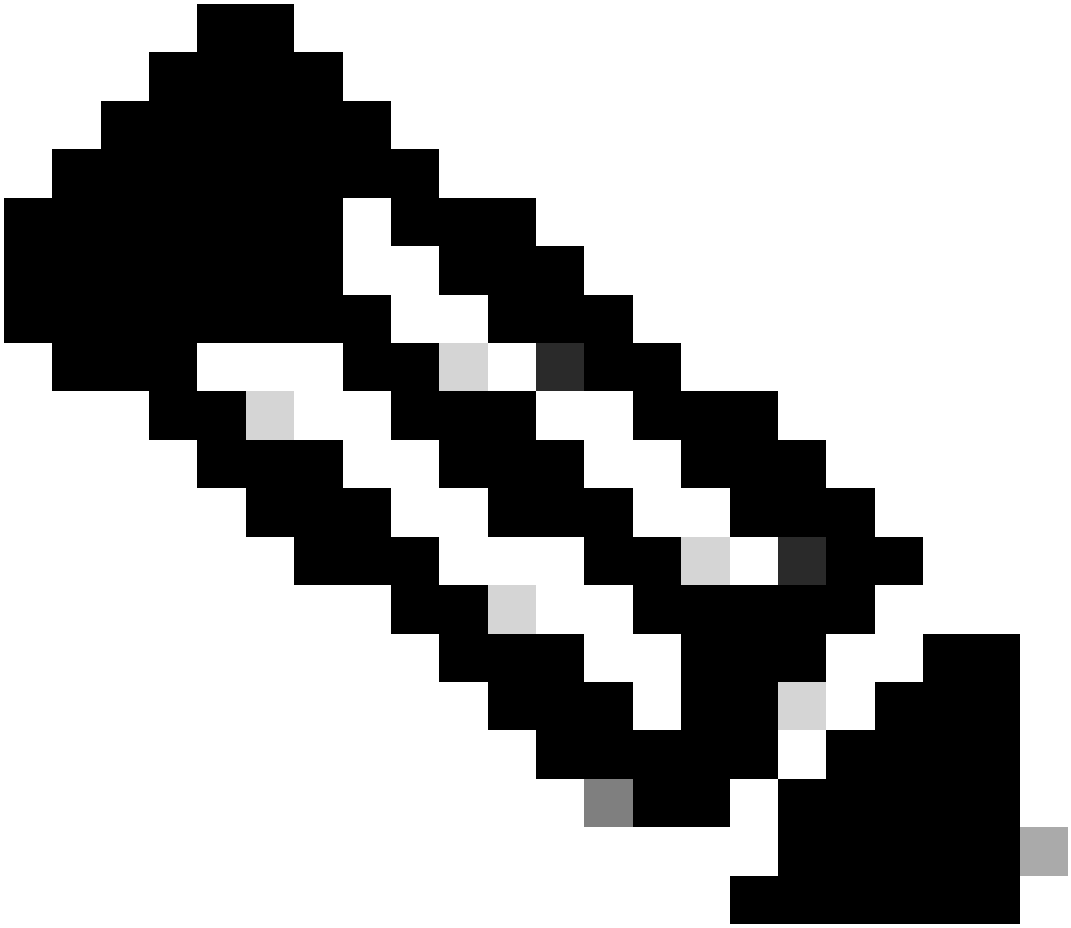
Add

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



注:U+2215(∕)やU+2044(/)などのUnicode文字を考慮する必要がある場合は、正規表現をさらに調整する必要があります。

ステップ 3：モニタモードでのテスト

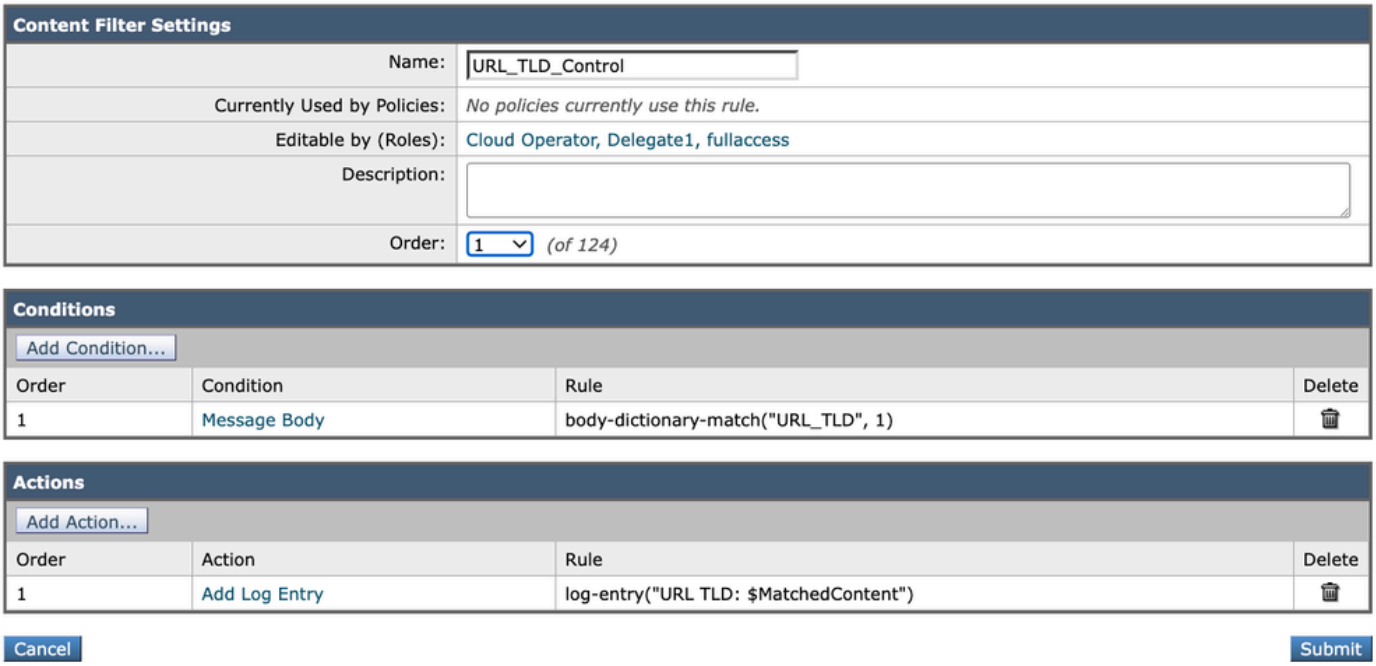
これらのフィルタを実稼働環境に実装する前に、モニタモードで使用することをお勧めします。このアプローチにより、Eメールを即時にブロックすることなくフィルタの効果を評価できるため、Eメールシステムが意図せず中断されるのを回避できます。

モニタモードでは、指定した基準に一致するURLのインスタンスがシステムによってログに記録されるため、結果を確認し、必要な調整を行うことができます。これを容易にするために、一致するURLに関する関連情報をキャプチャするログエントリアクションを設定できます。たとえば、次のログエントリアクションを使用できます。

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

このアクションは、フィルタ条件に一致した特定のコンテンツをログに記録し、フィルタがアクティブな場合にブロックされるURLに関する有益な情報を提供します。これらのログを調べることで、正規表現と辞書エントリを微調整し、正規の電子メールに影響を与えずに目的のURLを正確にキャプチャできます。

また、一定期間ログを監視することで、フィルタのパフォーマンスへの影響を評価し、必要に応じて最適化を行うことができます。フィルタが意図したとおりに機能していることを確認したら、モニタモードからアクティブブロッキングモードに移行できます。



パフォーマンスに関する考慮事項

正規表現の広範な使用は、Eメールシステムのパフォーマンスに影響を与える可能性があります。そのため、必要に応じてテストと最適化を行うことが不可欠です。

結論

特定のTLDに基づいてURLをブロックすると、Eメールシステムのセキュリティを強化できます。特に、Googleによって導入された.zipや.movなどの新しいTLDでは、一般的なファイル拡張子との類似性から、セキュリティ上の懸念が生じています。フィルタを慎重にテストし、パフォーマンスへの影響を検討することで、効率的で安全なシステムを維持できます。

Googleレジストリは、.dad、.phd、.prof、.esq、.foo、.zip、.mov、および.nexusの8つの新しいTLDを発表しました。ただし、.zipおよび.movは、広く使用されているファイル拡張子に類似しているため、特に注意を引いており、セキュリティ対策でこれらのファイル拡張子に対処することが重要です。

.zip TLDのセキュリティへの影響の詳細については、Talos Intelligenceブログの記事「ZIP TLD Information Leak」を参照してください。このリソースでは、これらのTLDに関連する潜在的なリスクに関する追加のコンテキストを提供し、適切なフィルタリング戦略を実装する重要性を強調しています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。