URLs in E-Mails basierend auf TLD in sicherer E-Mail blockieren

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

- Schritt 1: Filter erstellen
- Schritt 2: Verwenden regulärer Ausdrücke
- Schritt 3: Test im Überwachungsmodus
- Überlegungen zur Leistung

Schlussfolgerung

Einleitung

In diesem Dokument wird beschrieben, wie URLs in Cisco Secure Email auf der Basis bestimmter Top-Level-Domains (TLDs) blockiert werden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure Email.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Blockieren von URLs auf Basis bestimmter Domänen oberster Ebene (TLDs) kann eine effektive Möglichkeit darstellen, Ihr E-Mail-System vor potenziellen Bedrohungen zu schützen. Cisco Email Security Gateway (CES/ESA) analysiert die Reputation von URLs und führt sie anhand verschiedener Kriterien aus.

Wenn jedoch gemäß Ihrer Unternehmensrichtlinie bestimmte TLDs blockiert werden müssen, wird in diesem Verfahren erläutert, wie Sie dies mithilfe von Filtern und Wörterbüchern in Ihrem E-Mail-System erreichen.

Schritt 1: Filter erstellen

Um eine ganze TLD zu blockieren, müssen Sie zunächst einen Content-Filter in Ihrem E-Mail-System erstellen. Dieser Filter identifiziert und blockiert URLs, die TLDs enthalten, die Sie einschränken möchten. Sie können diesen Prozess optimieren, indem Sie mithilfe von Wörterbüchern Listen von TLDs verwalten und relevante reguläre Ausdrücke integrieren. Wenn Sie diese regulären Ausdrücke einem Wörterbuch hinzufügen, können Sie Ihre Filterkriterien effizient verwalten und anwenden.

Schritt 2: Verwenden regulärer Ausdrücke

Reguläre Ausdrücke (regex) sind ein leistungsstarkes Werkzeug zur Identifizierung bestimmter Muster in URLs.

Um auf TLDs basierende URLs effektiv zu blockieren, können Sie diese regulären Ausdrücke einem Wörterbuch hinzufügen. Dieser Ansatz ermöglicht eine einfache Verwaltung und Aktualisierungen Ihrer Filterkriterien:

1. Regulärer Ausdruck zum Blockieren von URLs, die mit http oder https beginnen, einschließlich Unterstützung für Punycode-Domänen:

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

2. Regulärer Ausdruck zum Blockieren von URLs im E-Mail-Format, der auch Punycode unterstützt:

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

Indem Sie diese regulären Ausdrücke zu einem Wörterbuch hinzufügen, können Sie den Prozess des Filterns von URLs optimieren und sicherstellen, dass Ihr E-Mail-System die angegebenen TLDs effizient blockiert.

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

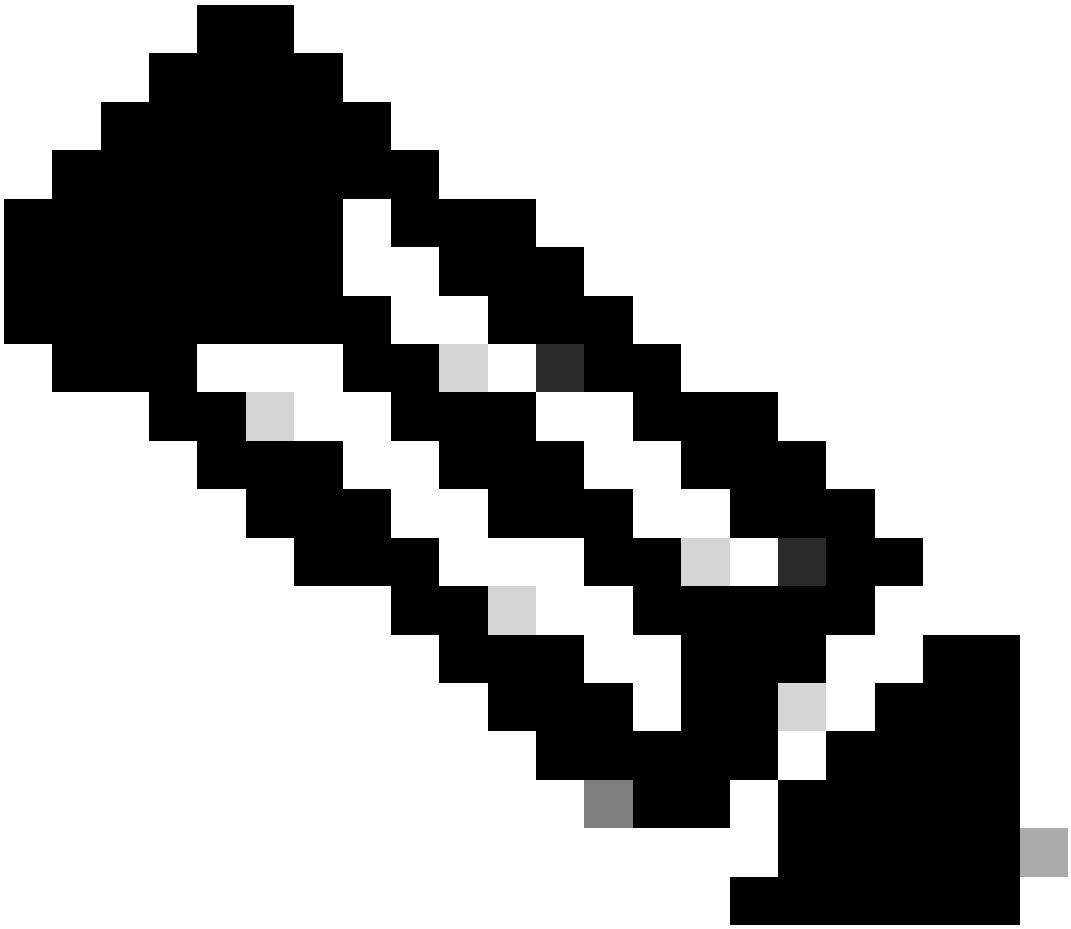
Add

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



> Anmerkung: Wenn Sie Unicode-Zeichen wie U+2215 (⁄) und U+2044 (/) berücksichtigen müssen, können zusätzliche Anpassungen an Ihrem regulären Ausdruck erforderlich sein.

Schritt 3: Test im Überwachungsmodus

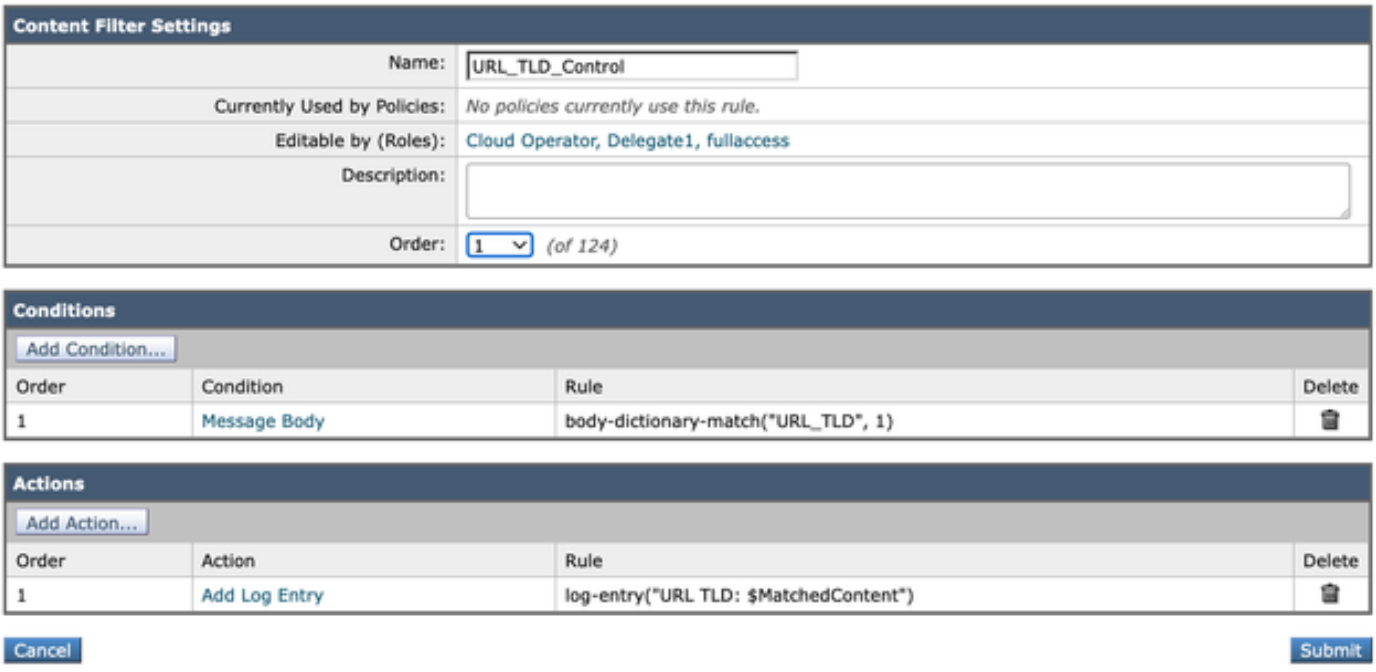
Vor der Implementierung dieser Filter in einer Produktionsumgebung ist es ratsam, sie im Überwachungsmodus zu verwenden. Dieser Ansatz ermöglicht es Ihnen, die Effektivität Ihrer Filter zu bewerten, ohne E-Mails sofort zu blockieren, wodurch unbeabsichtigte Unterbrechungen Ihres E-Mail-Systems vermieden werden.

Im Überwachungsmodus protokolliert das System Instanzen, bei denen URLs mit den angegebenen Kriterien übereinstimmen, sodass Sie die Ergebnisse beobachten und die erforderlichen Anpassungen vornehmen können. Um dies zu vereinfachen, können Sie eine Protokolleintragsaktion konfigurieren, die relevante Informationen über die zugeordneten URLs erfasst. Sie können z. B. folgende Protokolleintragsaktion verwenden:

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

Bei dieser Aktion werden die spezifischen Inhalte protokolliert, die Ihren Filterkriterien entsprechen. So erhalten Sie wertvolle Einblicke in die URLs, die blockiert würden, wenn der Filter aktiv wäre. Durch Überprüfung dieser Protokolle können Sie Ihre regulären Ausdrücke und Wörterbucheinträge optimieren, um sicherzustellen, dass die beabsichtigten URLs korrekt erfasst werden, ohne dass legitime E-Mails beeinträchtigt werden.

Außerdem können Sie durch die Überwachung der Protokolle über einen bestimmten Zeitraum die Auswirkungen Ihrer Filter auf die Leistung bewerten und ggf. Optimierungen vornehmen. Sobald Sie sicher sind, dass die Filter wie vorgesehen funktionieren, können Sie vom Überwachungs- in den aktiven Blockierungs-Modus wechseln:



Überlegungen zur Leistung

Die umfassende Verwendung von regulären Ausdrücken kann die Leistung Ihres E-Mail-Systems beeinträchtigen. Daher müssen Tests und Optimierungen nach Bedarf durchgeführt werden.

Schlussfolgerung

Das Blockieren von URLs auf Basis bestimmter TLDs kann die Sicherheit Ihres E-Mail-Systems erhöhen. Insbesondere neue TLDs, die von Google eingeführt wurden, wie .zip und .mov, haben Sicherheitsbedenken aufgrund ihrer Ähnlichkeit mit gängigen Dateierweiterungen aufgeworfen. Wenn Sie Ihre Filter sorgfältig testen und die Auswirkungen auf die Leistung berücksichtigen, können Sie ein effizientes und sicheres System aufrechterhalten.

Google Registry kündigte acht neue TLDs an: .dad, .phd, .prof, .esq, .foo, .zip, .mov und .nexus. Jedoch haben .zip und .mov aufgrund ihrer Ähnlichkeit mit weit verbreiteten Dateiendungen die Aufmerksamkeit besonders auf sich gezogen, sodass es wichtig ist, diese in Ihren Sicherheitsmaßnahmen zu beheben.

Weitere Einblicke in die Auswirkungen der ZIP-TLD auf die Sicherheit finden Sie im Blog-Beitrag von Talos Intelligence: ZIP-TLD-Informationsleck. Diese Ressource bietet zusätzlichen Kontext zu den potenziellen Risiken, die mit diesen TLDs verbunden sind, und unterstreicht die Bedeutung der Implementierung geeigneter Filterstrategien.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.