# حظر عناوين URL في رسائل البريد الإلكتروني المستندة إلى TLD في بريد إلكتروني آمن

## المحتويات


المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

الخطوة 1. إنشاء عامل تصفية

الخطوة 2. أستخدم التعبيرات المنتظمة

الخطوة 3. الاختبار في وضع الشاشة

اعتبارات الأداء

الدارق


## المقدمة

يصف هذا وثيقة كيف أن يمنع URLs في cisco أمن بريد إلكتروني يؤسس على خاص مستوى مجال (TLDs).

## المتطلبات الأساسية

### المتطلبات

ال توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى بريد Cisco الإلكتروني الآمن.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## معلومات أساسية

يمكن أن يكون حظر عناوين URL المستندة إلى TLDs عينة طريقة فعالة لحماية نظام البريد الإلكتروني من التهديدات المحتملة. تحلل عبارة Cisco Email Security Gateway (CES/ESA) سمعة عناوين URL وتقوم بتنفيذها استنادا إلى معايير مختلفة.

عل أي حال، إذا كانت سياسة شركتك تتطلب حظر بعض TLDs، فإن هذه الإجراءات كيفية تحقيق ذلك باستخدام المرشحات والقواميس في نظام البريد الإلكتروني الخاص بك.

## الخطوة 1. إنشاء عامل تصفية

لحظر TLD كامل، أنت تحتاج أولاً إلى إنشاء مرشح محتوى في نظام بريدك الإلكتروني. يقوم عامل التصفية هذا بتعريف عناوين URL التي تحتوي على عناوين TLD التي تريد تقييدها وحظرها. يمكنك تحسين هذه العملية باستخدام القواميس لإدارة قوائم TLDs وتضمين التعبيرات العادية ذات الصلة. بإضافة هذه التعبيرات المنتظمة إلى القاموس، يمكنك إدارة وتطبيق معايير التصفية الخاصة بك بكفاءة.

## الخطوة 2. أستخدم التعبيرات المنتظمة

التعبيرات العادية (regex) هي أداة قوية لتعريف أنماط معينة في عناوين الربط.

in order to منعت بشكل فعال URLs يؤسس على TLDs، أنت يستطيع أضفت هذا تعبير عادي إلى قاموس. يتيح هذا الأسلوب سهولة الإدارة وإجراء التحديثات على معايير التصفية الخاصة بك:

1. التعبير العادي لحظر عناوين URL بدءا من HTTP أو HTTPS، بما في ذلك دعم مجالات التعليمات البرمجية:

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

2. التعبير العادي لحظر عناوين URL باستخدام تنسيق البريد الإلكتروني، الذي يدعم أيضا التعليمات البرمجية:

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

بإضافة هذه التعبيرات العادية إلى قاموس، أنت يستطيع مشق عملية ترشيح URLs، ضمان أن نظام بريدك الإلكتروني يقوم بحجب TLDs المحدد بفاعلية.

**Dictionary Properties**

| | |
|---|---|
| Name: | URL_TLD |
| Advanced Matching: | ☐ Match whole words<br>☐ 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

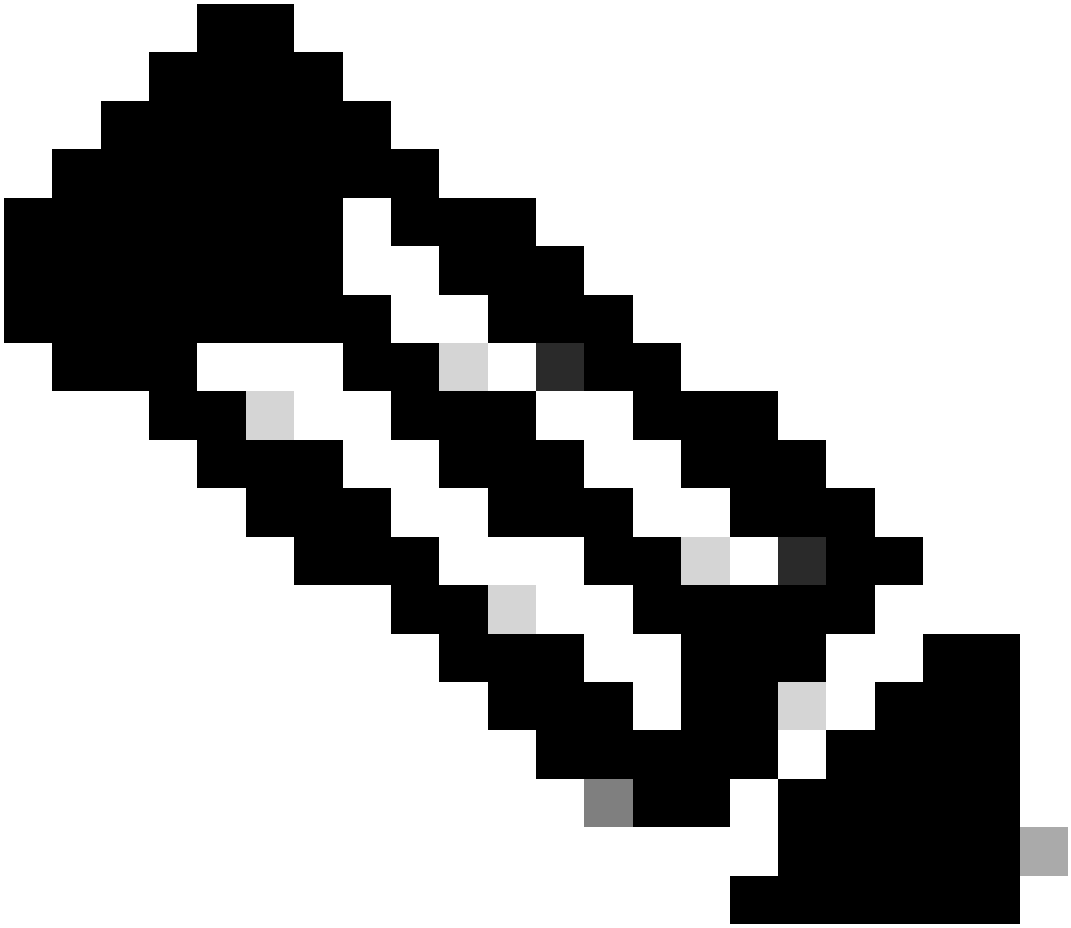
Add

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



ملاحظة: إذا كنت تحتاج أن تضع في الاعتبار حروف Unicode مثل U+2215 (∕) و U+2044 (⁄)، فإن معايرات إضافية للتعبير العادي قد تكون ضرورية.

## الخطوة 3. الاختبار في وضع الشاشة

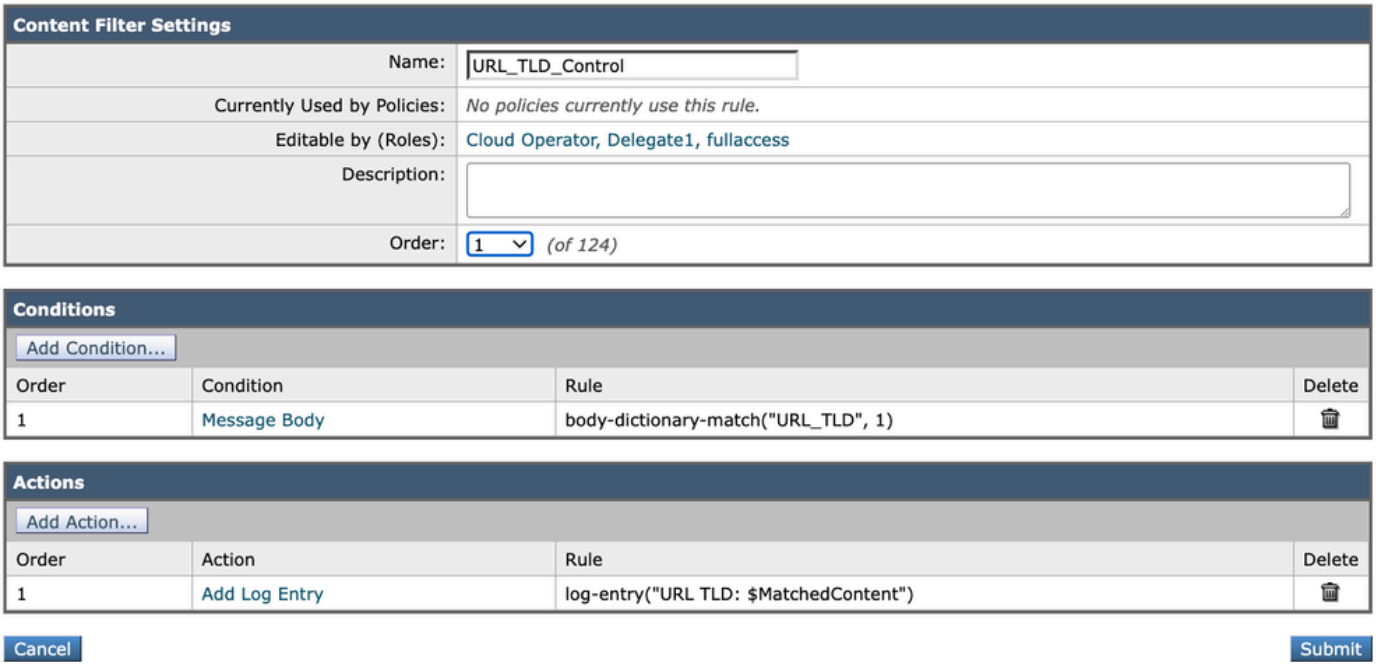
قبل تنفيذ عوامل التصفية هذه في بيئة إنتاج، من المستحسن إستخدامها في وضع المراقبة. يتيح لك هذا الأسلوب تقييم مدى فعالية عوامل التصفية لديك دون حظر رسائل البريد الإلكتروني على الفور، وبالتالي تجنب أية أعطال غير مقصودة لنظام البريد الإلكتروني الخاص بك.

في وضع المراقبة، يقوم النظام بتسجيل المثيلات التي تطابق URLs معاييرك المحددة، ممما يمكنك من ملاحظة النتائج وإجراء التعديلات اللازمة. ولتسهيل ذلك، يمكنك تكوين إجراء إدخال سجل يلتقط المعلومات ذات الصلة حول عناوين URL المتطابقة. على سبيل المثال، يمكنك إستخدام إجراء إدخال السجل هذا:

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

يقوم هذا الإجراء بتسجيل المحتوى المحدد الذي يتوافق مع معايير التصفية الخاصة بك، ممما يوفر رؤى قيمة في عناوين URL التي سيتم حظرها إذا كان عامل التصفية نشطا. من خلال مراجعة هذه السجلات، يمكنك ضبط مدخلات القاموس والتعبيرات العادية للتأكد من أنها تلتقط عناوين URL المقصودة بدقة بدون التأثير على رسائل البريد الإلكتروني الشرعية.

بالإضافة إلى ذلك، تتيح لك مراقبة السجلات على مدى فترة من الوقت إمكانية تقييم تأثير الأداء على عوامل التصفية وإجراء عمليات التحسين حسب الحاجة. بمجرد أن تكون واثقا من أن عوامل التصفية تعمل كما هو متوقع، يمكنك الانتقال من وضع المراقبة إلى وضع الحظر النشط:




### اعتبارات الأداء

يمكن أن يؤثر الاستخدام المكثف للتعبيرات المنتظمة على أداء نظام البريد الإلكتروني لديك. لذلك من الضروري ان نختبر ونحسن الامور حسب الحاجة.

## القرار

حظر عناوين URL استنادا إلى TLDs معينة يمكن أن يحسن أمن نظام بريدك الإلكتروني. ومن الجدير بالذكر أن البلدان المتقدمة الجديدة التي استحدثتها جوجل، مثل .zip و.mov، أثارت مخاوف أمنية بسبب تشابهها مع الامتدادات الشائعة للملفات. يساعد إختبار عوامل التصفية الخاصة بك بعناية ودراسة التأثير على الأداء على الحفاظ على نظام فعال وآمن.

أعلن سجل غوغل عن ثمانية TLDs جديدة: .dad و .phd و.prof و.esq و.foo و.zip و .mov و.nexus. ومع ذلك، فإن .zip و.mov قد لفتا الانتباه بشكل خاص بسبب تشابههما مع امتدادات الملفات المستخدمة على نطاق واسع، مما يجعل من الضروري معالجة هذه التمديدات في تدابيرك الأمنية.

لمزيد من المعلومات حول التأثيرات الأمنية ل .zip TLD، يمكنك الرجوع إلى مادة نشر مدونة Talos Intelligence: تسريب معلومات TLD ZIP. يوفر هذا المورد سياقا إضافيا حول المخاطر المحتملة المرتبطة بالمستويات المحلية العالية (TLDs) هذه ويؤكد على أهمية تنفيذ إستراتيجيات التصفية المناسبة.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).