Bloquer les URL dans les e-mails en fonction du TLD dans les e-mails sécurisés

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- Étape 1. Création d'un filtre
- Étape 2. Utilisation d'expressions régulières
- Étape 3. Test en mode surveillance
- Considérations relatives aux performances

Conclusion

Introduction

Ce document décrit comment bloquer les URL dans Cisco Secure Email en fonction de domaines de premier niveau (TLD) spécifiques.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Secure Email.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le blocage des URL en fonction de TLD spécifiques peut être un moyen efficace de protéger votre système de messagerie contre les menaces potentielles. Cisco Email Security Gateway (CES/ESA) analyse la réputation des URL et les exécute en fonction de divers critères.

Cependant, si la politique de votre entreprise exige le blocage de certains TLD, cette procédure

explique comment y parvenir à l'aide de filtres et de dictionnaires dans votre système de messagerie.

Étape 1. Création d’un filtre

Pour bloquer un TLD entier, vous devez d'abord créer un filtre de contenu dans votre système de messagerie. Ce filtre identifie et bloque les URL contenant les TLD que vous souhaitez restreindre. Vous pouvez améliorer ce processus en utilisant des dictionnaires pour gérer des listes de TLD et incorporer des expressions régulières pertinentes. En ajoutant ces expressions régulières à un dictionnaire, vous pouvez gérer et appliquer efficacement vos critères de filtrage.

Étape 2. Utilisation d’expressions régulières

Les expressions régulières (regex) sont un outil puissant pour identifier des modèles spécifiques dans les URL.

Afin de bloquer efficacement les URL basées sur les TLD, vous pouvez ajouter ces expressions régulières à un dictionnaire. Cette approche facilite la gestion et la mise à jour de vos critères de filtrage :

1. Expression régulière de blocage des URL commençant par HTTP ou HTTPS, y compris le support des domaines Punycode :

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

2. Expression régulière pour bloquer les URL utilisant un format de courrier électronique, prenant également en charge Punycode :

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

En ajoutant ces expressions régulières à un dictionnaire, vous pouvez rationaliser le processus de filtrage des URL, en vous assurant que votre système de messagerie bloque efficacement les TLD spécifiés.

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

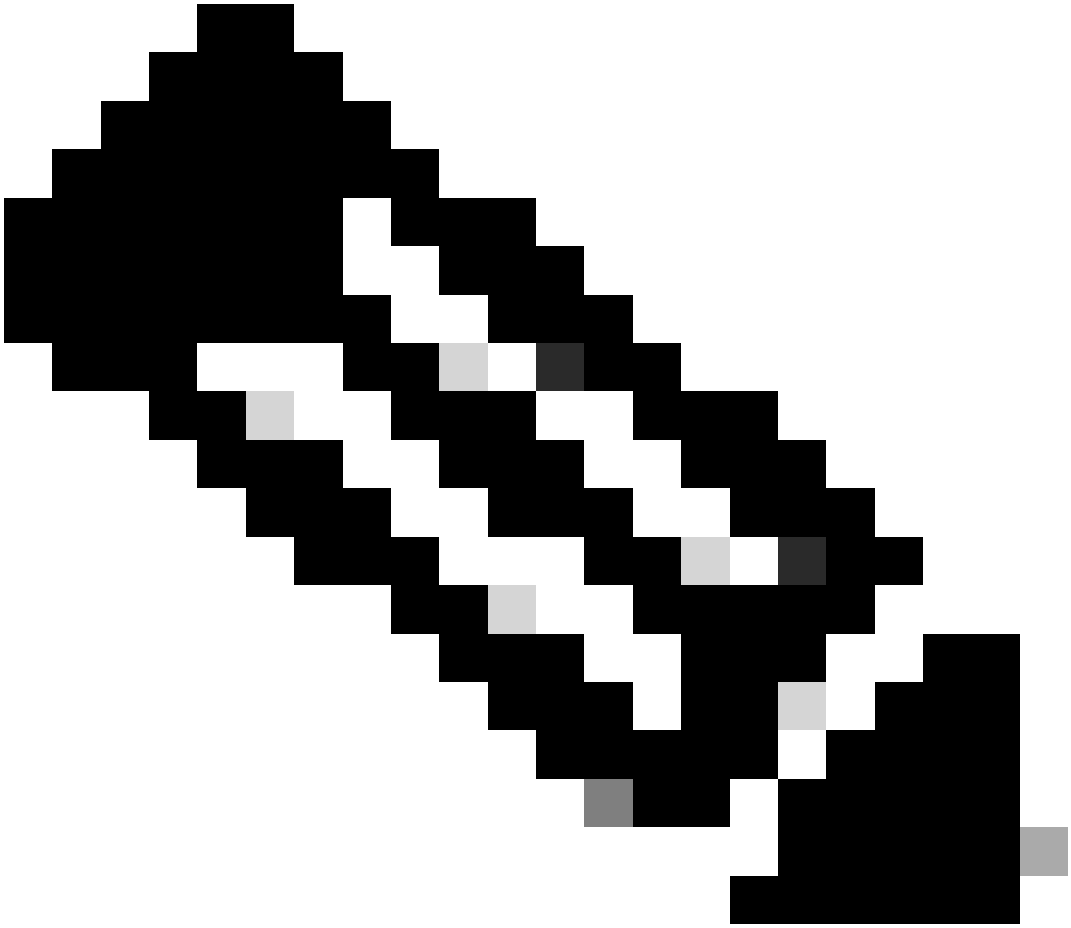
Add

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



Remarque : Si vous devez prendre en compte des caractères Unicode tels que U+2215 (∕) et U+2044 (⁄), des ajustements supplémentaires à votre expression régulière peuvent être nécessaires.

Étape 3. Test en mode surveillance

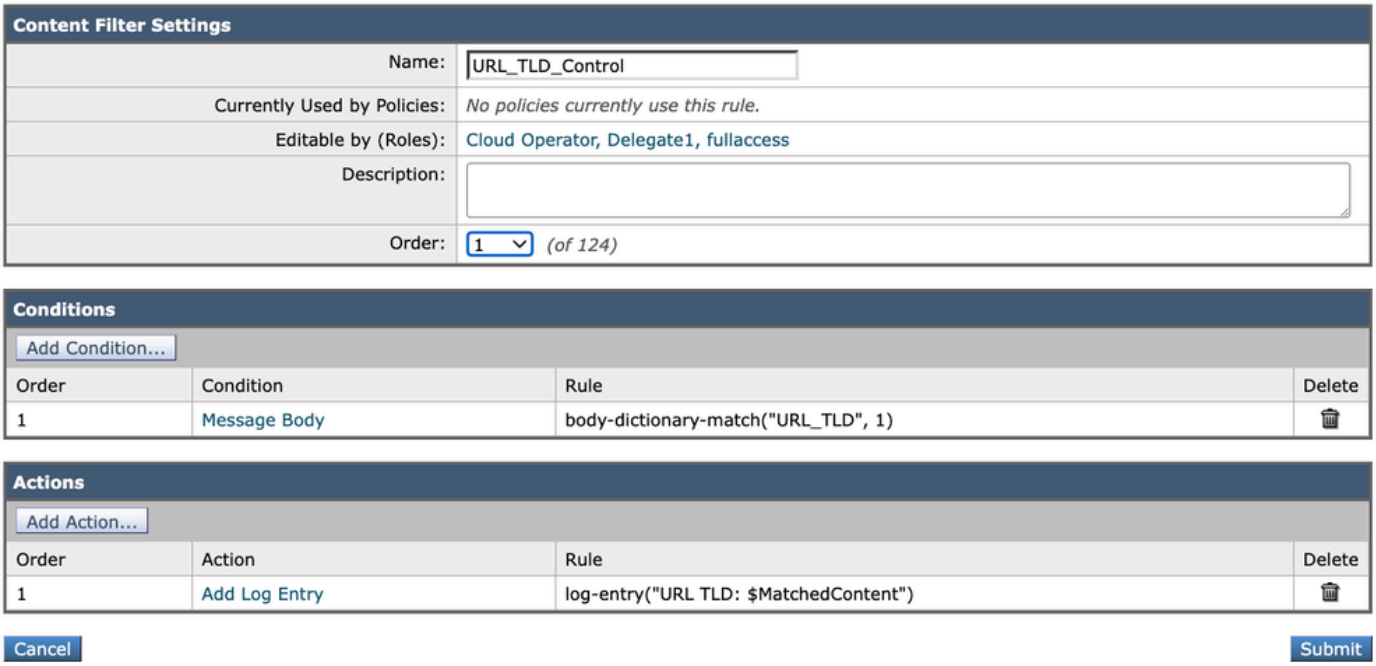
Avant d'implémenter ces filtres dans un environnement de production, il est conseillé de les utiliser en mode surveillance. Cette approche vous permet d'évaluer l'efficacité de vos filtres sans bloquer immédiatement les e-mails, évitant ainsi toute interruption involontaire de votre système de messagerie.

En mode Surveillance, le système enregistre les instances où les URL correspondent à vos critères, ce qui vous permet d'observer les résultats et d'effectuer les ajustements nécessaires. Pour faciliter cela, vous pouvez configurer une action d'entrée de journal qui capture des informations pertinentes sur les URL correspondantes. Par exemple, vous pouvez utiliser cette action d'entrée de journal :

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

Cette action consigne le contenu spécifique qui correspond à vos critères de filtre, fournissant des informations précieuses sur les URL qui seront bloquées si le filtre est actif. En examinant ces journaux, vous pouvez affiner vos expressions régulières et entrées de dictionnaire afin de vous assurer qu'elles capturent précisément les URL prévues sans affecter les e-mails légitimes.

En outre, la surveillance des journaux sur une période donnée vous permet d'évaluer l'impact de vos filtres sur les performances et d'effectuer les optimisations nécessaires. Une fois que vous êtes sûr que les filtres fonctionnent comme prévu, vous pouvez passer du mode surveillance au mode blocage actif :



Considérations relatives aux performances

L'utilisation étendue d'expressions régulières peut avoir un impact sur les performances de votre système de messagerie. Par conséquent, il est essentiel de tester et d'optimiser selon les besoins.

Conclusion

Le blocage des URL en fonction de TLD spécifiques peut améliorer la sécurité de votre système de messagerie. En particulier, les nouveaux TLD introduits par Google, tels que .zip et .mov, ont soulevé des problèmes de sécurité en raison de leur similitude avec les extensions de fichiers populaires. En testant soigneusement vos filtres et en tenant compte de l'impact sur les performances, vous pouvez maintenir un système efficace et sécurisé.

Google Registry a annoncé huit nouveaux TLD : .dad, .phd, .prof, .esq, .foo, .zip, .mov et .nexus. Cependant, .zip et .mov ont particulièrement attiré l'attention en raison de leur ressemblance avec les extensions de fichiers largement utilisées, ce qui rend crucial de les traiter dans vos mesures de sécurité.

Pour plus d'informations sur les implications pour la sécurité du TLD .zip, vous pouvez consulter le billet du blog Talos Intelligence : ZIP TLD Information Leak. Cette ressource fournit un contexte supplémentaire sur les risques potentiels associés à ces TLD et souligne l'importance de mettre en oeuvre des stratégies de filtrage appropriées.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.