Bloquear URL en correos electrónicos basados en TLD en correos electrónicos seguros

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

- Paso 1. Crear un filtro
- Paso 2. Utilizar expresiones regulares
- Paso 3. Prueba en modo Monitor
- Consideraciones de rendimiento

Conclusión

Introducción

Este documento describe cómo bloquear las URL en Cisco Secure Email en función de dominios de nivel superior (TLD) específicos.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Secure Email.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El bloqueo de URL basadas en TLD específicos puede ser una forma eficaz de proteger su sistema de correo electrónico de posibles amenazas. Cisco Email Security Gateway (CES/ESA) analiza la reputación de las URL y las ejecuta según diversos criterios.

Sin embargo, si la política de su empresa requiere el bloqueo de determinados TLD, este procedimiento explica cómo conseguirlo utilizando filtros y diccionarios en su sistema de correo electrónico.

Paso 1. Crear un filtro

Para bloquear un TLD completo, primero debe crear un filtro de contenido en su sistema de correo electrónico. Este filtro identifica y bloquea las URL que contienen los TLD que desea restringir. Puede mejorar este proceso mediante el uso de diccionarios para administrar listas de TLD e incorporar expresiones regulares relevantes. Al agregar estas expresiones regulares a un diccionario, puede administrar y aplicar eficazmente los criterios de filtrado.

Paso 2. Utilizar expresiones regulares

Las expresiones regulares (regex) son una herramienta eficaz para identificar patrones específicos en URL.

Para bloquear eficazmente las URLs basadas en TLDs, puede agregar estas expresiones regulares a un diccionario. Este enfoque facilita la gestión y permite actualizar los criterios de filtrado:

1. Expresión regular para el bloqueo de URL que comienzan con HTTP o HTTPS, incluida la compatibilidad con dominios Punycode:

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

2. Expresión regular para bloquear URLs usando un formato de correo electrónico, también soportando Punycode:

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

Al agregar estas expresiones regulares a un diccionario, puede agilizar el proceso de filtrado de URL, asegurándose de que su sistema de correo electrónico bloquea eficazmente los TLD 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

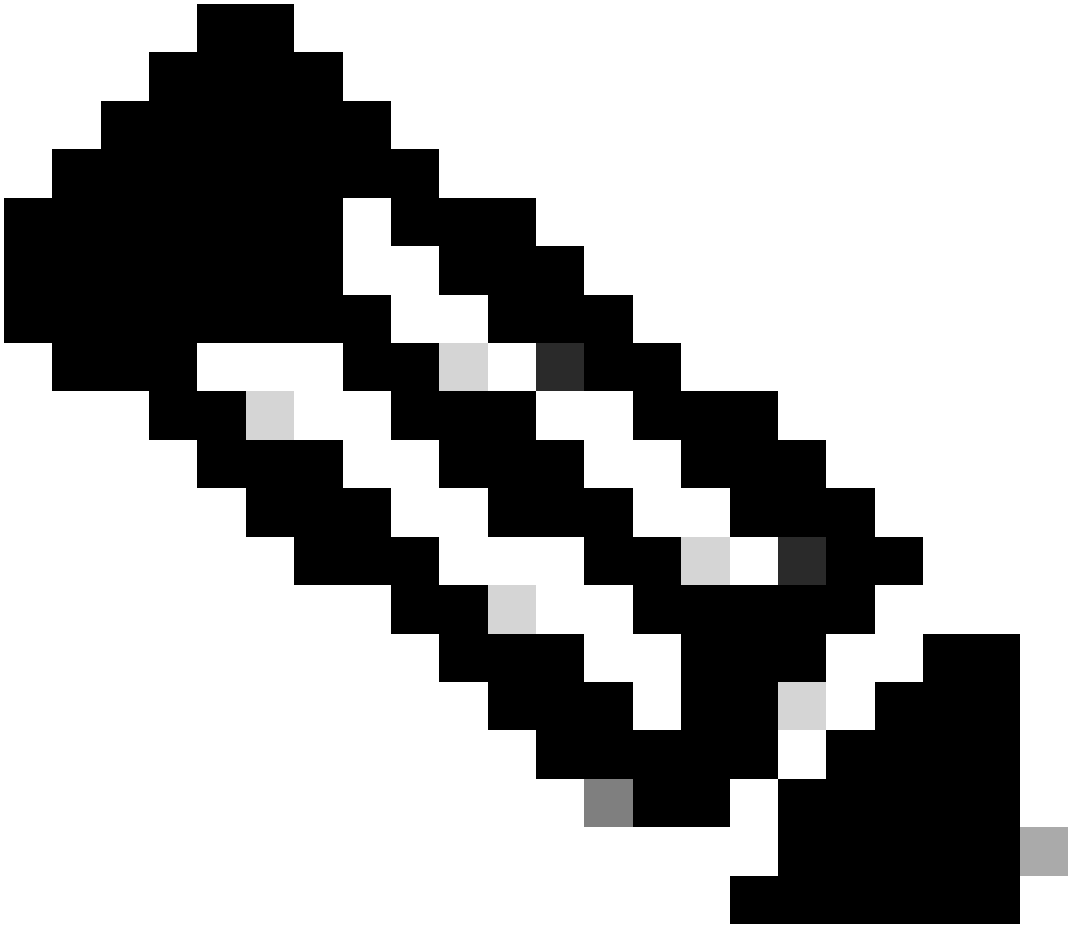
Add

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



Nota: Si necesita tener en cuenta caracteres Unicode como U+2215 (∕) y U+2044 (⁄), puede que sea necesario realizar ajustes adicionales en la expresión regular.

Paso 3. Prueba en modo Monitor

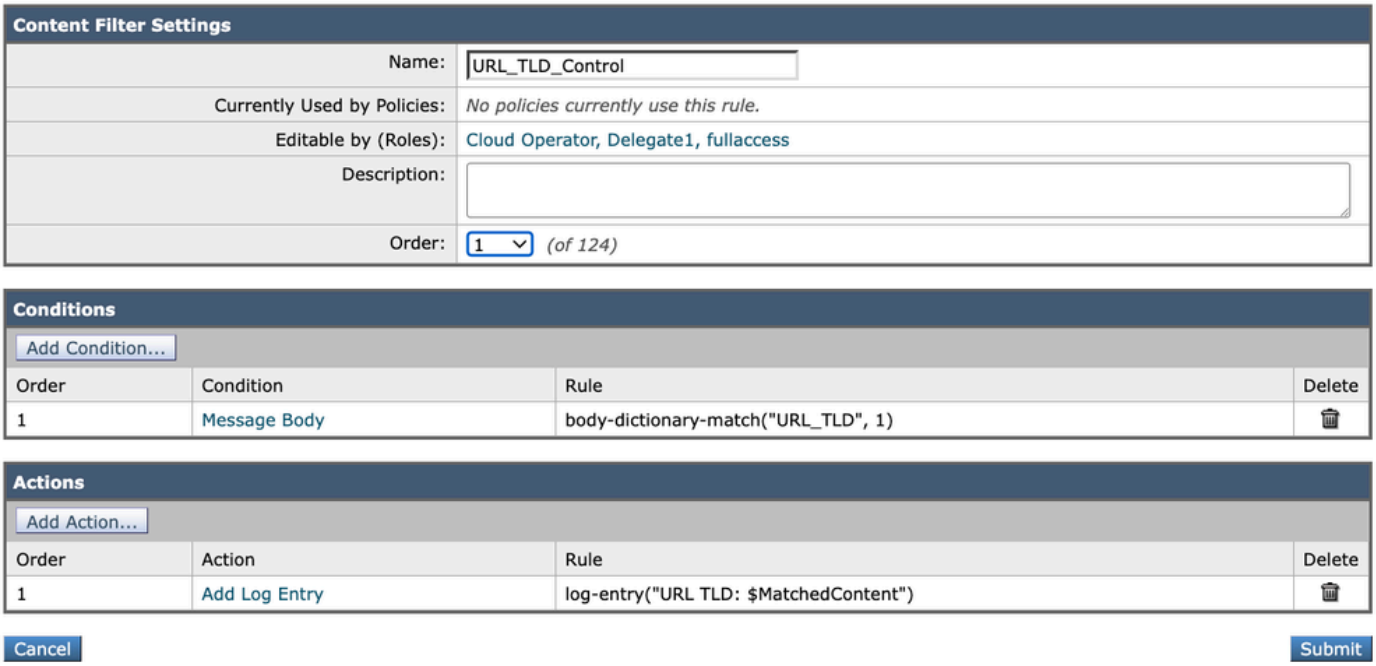
Antes de implementar estos filtros en un entorno de producción, se recomienda utilizarlos en modo de supervisión. Este enfoque le permite evaluar la eficacia de sus filtros sin bloquear inmediatamente los correos electrónicos, evitando así interrupciones no deseadas en su sistema de correo electrónico.

En el modo de supervisión, el sistema registra instancias en las que las URL coinciden con los criterios especificados, lo que le permite observar los resultados y realizar los ajustes necesarios. Para facilitar esto, puede configurar una acción de entrada de registro que capture información relevante sobre las URLs coincidentes. Por ejemplo, puede utilizar esta acción de entrada de registro:

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

Esta acción registra el contenido específico que coincide con sus criterios de filtro, lo que proporciona información valiosa sobre las URL que se bloquearán si el filtro está activo. Al revisar estos registros, puede ajustar sus expresiones regulares y entradas de diccionario para asegurarse de que capturan con precisión las URL deseadas sin afectar a los correos electrónicos legítimos.

Además, la supervisión de los registros durante un período de tiempo le permite evaluar el impacto en el rendimiento de los filtros y realizar optimizaciones según sea necesario. Una vez que esté seguro de que los filtros están funcionando correctamente, puede pasar del modo de supervisión al modo de bloqueo activo:



Consideraciones de rendimiento

El uso generalizado de expresiones regulares puede afectar al rendimiento de su sistema de correo electrónico. Por lo tanto, es esencial probar y optimizar según sea necesario.

Conclusión

El bloqueo de URL basadas en TLD específicos puede mejorar la seguridad de su sistema de correo electrónico. En particular, los nuevos TLD introducidos por Google, como .zip y .mov, han generado problemas de seguridad debido a su similitud con las extensiones de archivos más populares. La prueba de sus filtros cuidadosamente y teniendo en cuenta el impacto en el rendimiento ayuda a mantener un sistema eficiente y seguro.

Google Registry anunció ocho nuevos TLD: .dad, .phd, .prof, .esq, .foo, .zip, .mov y .nexus. Sin embargo, .zip y .mov han llamado especialmente la atención debido a su semejanza con las extensiones de archivo ampliamente utilizadas, por lo que es crucial para abordar estos problemas en sus medidas de seguridad.

Para obtener más información sobre las implicaciones de seguridad del TLD .zip, consulte la entrada del blog Talos Intelligence: Fuga de información de ZIP TLD. Este recurso proporciona contexto adicional sobre los riesgos potenciales asociados con estos TLDs y subraya la importancia de implementar estrategias de filtrado apropiadas.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).