Block URLs in Emails Based on TLD in Secure Email

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Step 1. Create a Filter
- Step 2. Use Regular Expressions
- Step 3. Test in Monitor Mode
- Performance Considerations

Conclusion

Introduction

This document describes how to block URLs in Cisco Secure Email based on specific top-level domains (TLDs).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Blocking URLs based on specific TLDs can be an effective way to protect your email system from potential threats. Cisco Email Security Gateway (CES/ESA) analyzes the reputation of URLs and executes them based on various criteria.

However, if your company policy requires blocking certain TLDs, this procedure explains how to achieve it using filters and dictionaries in your email system.

Step 1. Create a Filter

In order to block an entire TLD, you first need to create a content filter in your email system. This filter identifies and blocks URLs containing the TLDs you wish to restrict. You can enhance this process by using dictionaries to manage lists of TLDs and incorporate relevant regular expressions. By adding these regular expressions to a dictionary, you can efficiently manage and apply your filtering criteria.

Step 2. Use Regular Expressions

Regular expressions (regex) are a powerful tool for identifying specific patterns in URLs.

In order to effectively block URLs based on TLDs, you can add these regular expressions to a dictionary. This approach allows for easy management and updates to your filtering criteria:

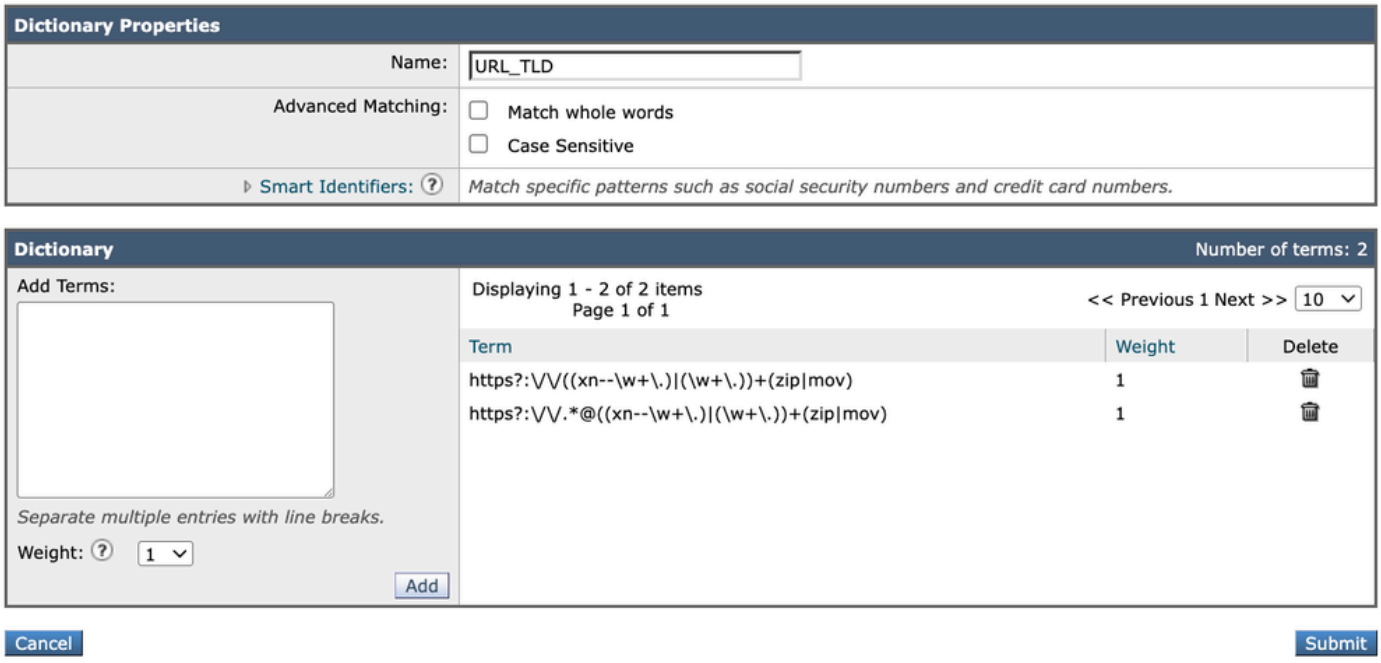
1. Regular expression for blocking URLs starting with HTTP or HTTPS, including support for Punycode domains:

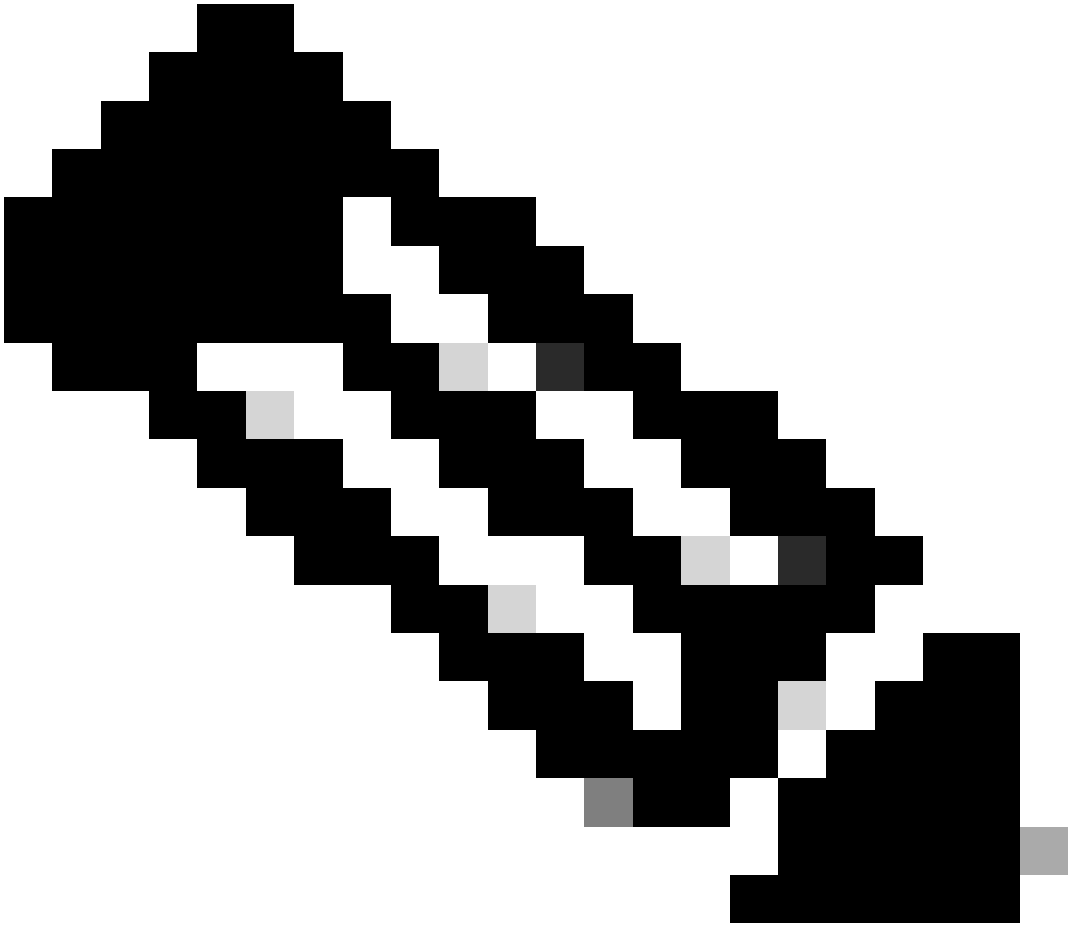
```
(?i)https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)
```

2. Regular expression for blocking URLs using an email format, also supporting Punycode:

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

By adding these regular expressions to a dictionary, you can streamline the process of filtering URLs, ensuring that your email system efficiently blocks the specified TLDs.





Note: If you need to consider Unicode characters such as U+2215 (∕) and U+2044 (⁄), additional adjustments to your regular expression can be necessary.

Step 3. Test in Monitor Mode

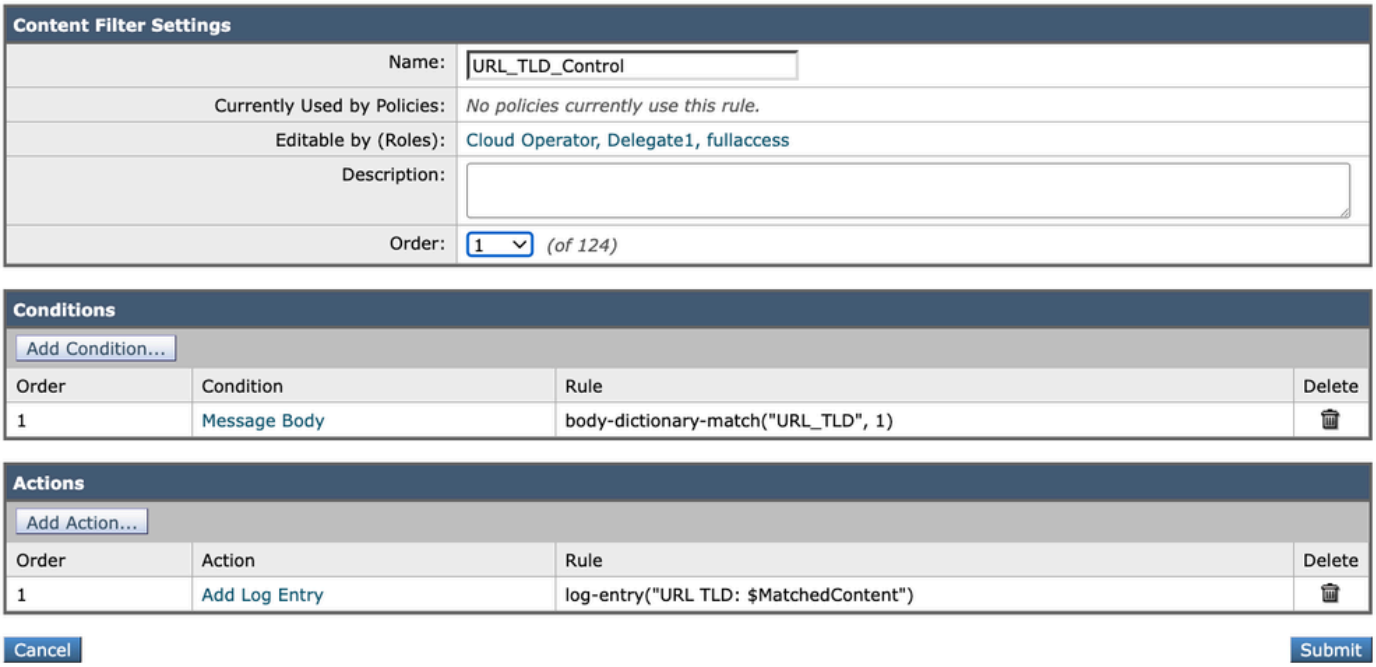
Before implementing these filters in a production environment, it is advisable to use them in monitor mode. This approach allows you to assess the effectiveness of your filters without immediately blocking emails, thereby avoiding any unintended disruptions to your email system.

In monitor mode, the system logs instances where URLs match your specified criteria, enabling you to observe the results and make necessary adjustments. In order to facilitate this, you can configure a log entry action that captures relevant information about the matched URLs. For example, you can use this log entry action:

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

This action logs the specific content that matched your filter criteria, providing valuable insights into the URLs that will be blocked if the filter is active. By reviewing these logs, you can fine-tune your regular expressions and dictionary entries in order to ensure they accurately capture the intended URLs without impacting legitimate emails.

Additionally, monitoring the logs over a period of time allows you to evaluate the performance impact of your filters and make optimizations as needed. Once you are confident that the filters are functioning as intended, you can transition from **monitor** to **active blocking** mode:



Performance Considerations

Extensive use of regular expressions can impact the performance of your email system. Therefore, it is essential to test and optimize as needed.

Conclusion

Blocking URLs based on specific TLDs can enhance the security of your email system. Notably, new TLDs introduced by Google, such as **.zip** and **.mov**, have raised security concerns due to their similarity to popular file extensions. Testing your filters carefully and considering the impact on performance helps maintain an efficient and secure system.

Google Registry announced eight new TLDs: **.dad**, **.phd**, **.prof**, **.esq**, **.foo**, **.zip**, **.mov**, and **.nexus**. However, **.zip** and **.mov** have particularly drawn attention due to their resemblance to widely used file extensions, making it crucial to address these in your security measures.

For more insights into the security implications of the **.zip** TLD, you can refer to the Talos Intelligence blog post: ZIP TLD Information Leak. This resource provides additional context on the potential risks associated with these TLDs and underscores the importance of implementing appropriate filtering strategies.