根據安全電子郵件中的TLD阻止電子郵件中的URL

目錄

簡介

本檔案介紹如何根據特定頂層網域(TLD)封鎖思科安全電子郵件中的URL。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據思科安全電子郵件。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

基於特定頂級域(TLD)阻止URL是保護您的電子郵件系統免受潛在威脅的有效方法。Cisco Email Security Gateway(CES/ESA)會分析URL的信譽，並根據各種標準執行它們。

但是，如果您的公司策略要求阻止某些TLD，則此過程將說明如何使用電子郵件系統中的過濾器和詞典來實現此功能。

步驟1.建立篩選條件

要阻止整個TLD，您首先需要在電子郵件系統中建立一個內容過濾器。此過濾器標識並阻止包含您要限制的TLD的URL。您可以使用詞典管理TLD清單並合併相關的正規表示式，從而增強此過程。通過將這些正規表示式新增到詞典，您可以有效地管理和應用過濾條件。

步驟2.使用正規表示式

正規表示式(regex)是識別URL中特定模式的強大工具。

要有效地阻止基於TLD的URL，可以將這些正規表示式新增到詞典中。此方法允許輕鬆管理和更新您的過濾條件：

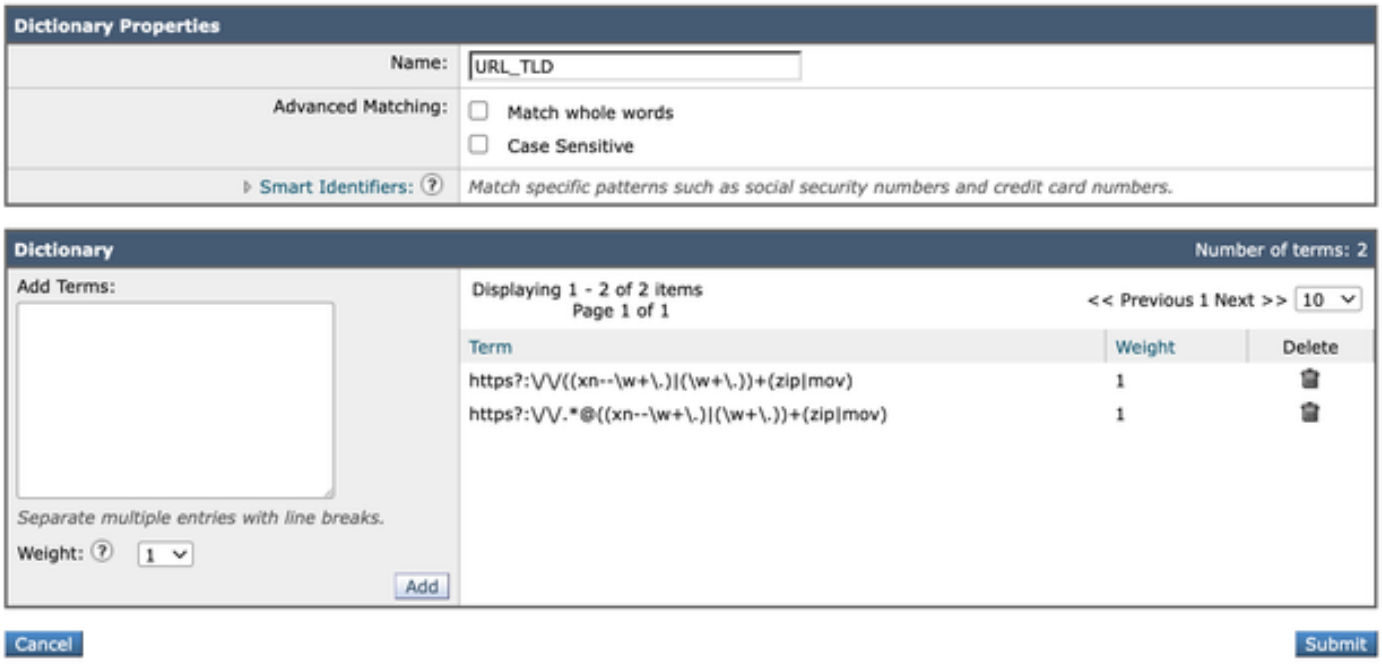
1. 用於阻止以http或https開頭的URL的正規表示式，包括對Punycode域的支援：

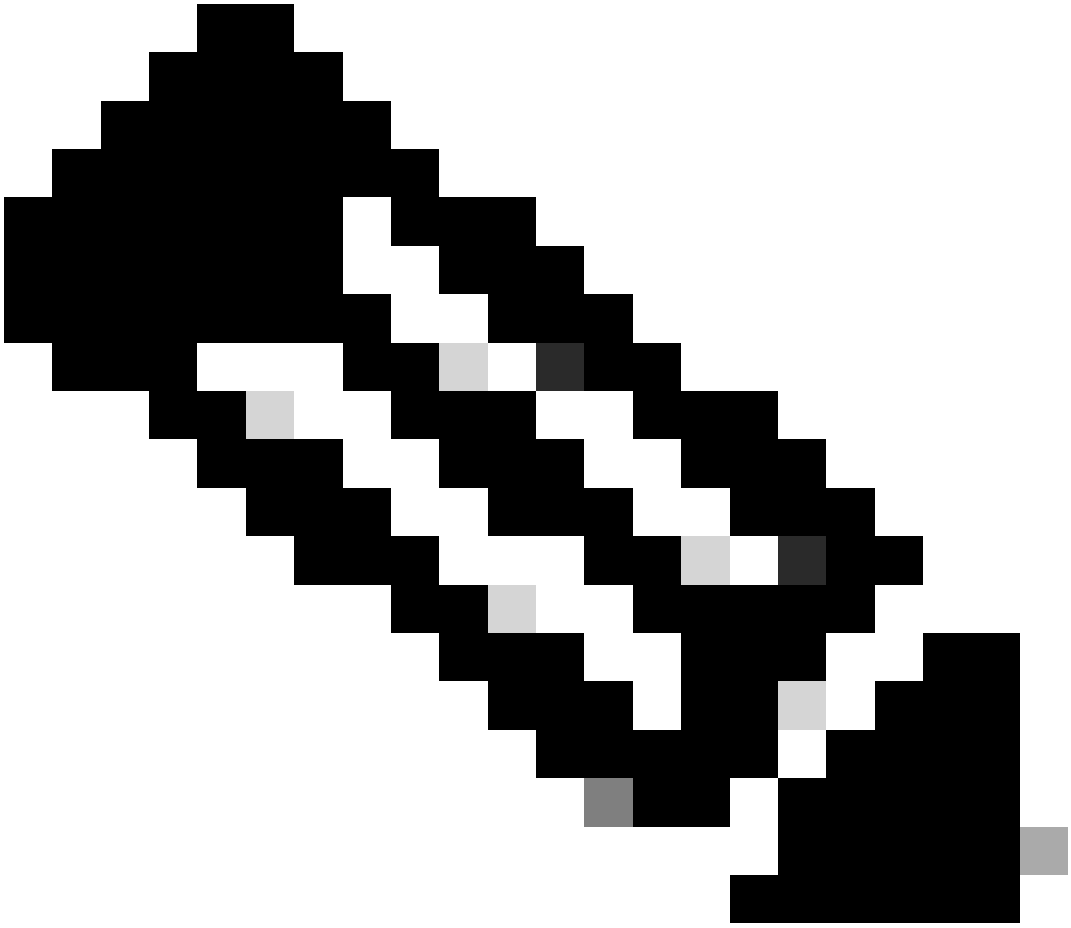
```
(?i)https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)
```

2. 使用電子郵件格式阻止URL的正規表示式，也支援Punycode:

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

通過將這些正規表示式新增到詞典中，可以簡化篩選URL的過程，確保您的電子郵件系統有效地阻止指定的TLD。





附註：如果需要考慮Unicode字元，如U+2215(∕)和U+2044(⁄)，可能需要對正規表示式進行其他調整。

步驟3.在監控模式下測試

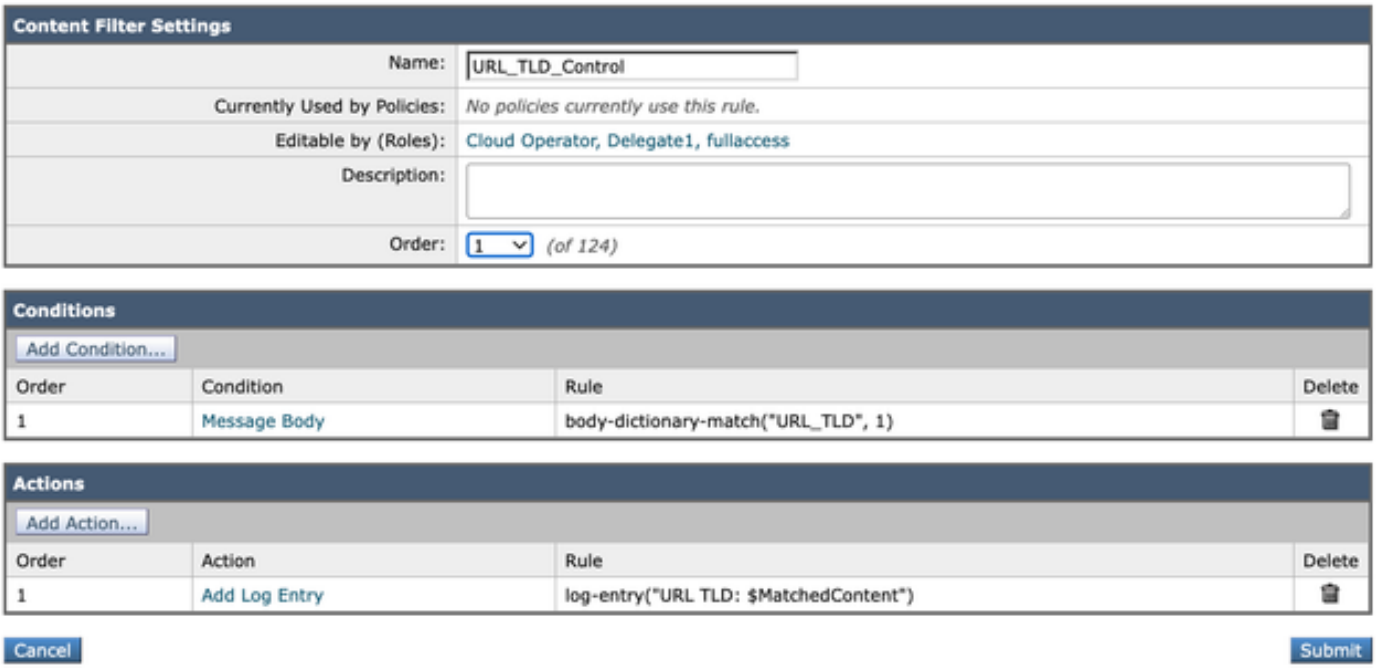
在生產環境中實施這些篩選器之前，建議在監控模式下使用它們。此方法允許您評估過濾器的有效性，而不會立即阻止電子郵件，從而避免您的電子郵件系統遭受任何意外中斷。

在監控模式下，系統會記錄與URL匹配指定條件的例項，從而使您可以觀察結果並進行必要的調整。為便於執行，您可以配置日誌條目操作，以捕獲有關匹配的URL的相關資訊。例如，您可以使用此日誌條目操作：

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

此操作會記錄與您的過濾器條件匹配的特定內容，從而提供在過濾器處於活動狀態時將阻止的URL的有價值見解。通過檢視這些日誌，您可以微調正規表示式和字典條目，以確保它們準確捕獲預期的URL，而不會影響合法電子郵件。

此外，通過監控一段時間內的日誌，您可以評估過濾器的效能影響，並根據需要進行最佳化。一旦您確信過濾器按預期方式工作，您就可以從monitor轉換為active blocking模式：



效能注意事項

對正規表示式的廣泛使用可能會影響電子郵件系統的效能。因此，有必要進行必要的測試和最佳化。

結論

基於特定TLD阻止URL可增強您的電子郵件系統的安全性。值得注意的是，Google推出的新版TLD(如.zip和.mov)與流行的副檔名類似，因此引起了安全方面的擔憂。仔細測試您的過濾器並考慮其對效能的影響有助於保持一個高效而安全的系統。

Google Registry宣佈了8個新的TLD:.dad、.phd、.prof、.esq、.foo、.zip、.mov和.nexus。但是，.zip和.mov尤其受到關注，因為它們與廣泛使用的副檔名相似，因此必須在安全措施中解決這些問題。

有關.zip TLD安全影響的更多見解，請參閱Talos Intelligence部落格：ZIP TLD資訊洩漏。這一資源進一步說明了與這些臨時診斷工具有關的潛在風險，並強調實施適當篩選戰略的重要性。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。