# 如何捕獲和阻止具有執行檔的嵌入超連結？

## 目錄



## 問題

如何捕獲和阻止具有執行檔的嵌入超連結？

## 答案

您可以使用郵件過濾器掃描正文和任何HTML附件。通常，這些電子郵件會通過HTML電子郵件送入。 為了使掃描引擎檢測到它，必須使用body-contains條件。如果只處理出站郵件，則可以使用「only-body-contains」條件。

以下消息過濾器將查詢以執行檔結尾的任何長度超連結。滿足條件後，將啟用兩個操作。第一個操作是通過向admin@example.com傳送電子郵件來通知本地管理員。

第二步是最終刪除電子郵件。電子郵件不需要丟棄，而是可以隔離。 刪除'drop();'下面的操作可以替換為'quarantine('Policy');'

必須定義隔離區，否則篩選器引擎將不允許篩選器。您可以使用預設策略隔離區，也可以建立自己的隔離區（請參閱手冊中的隔離區以建立或刪除隔離區）。

```
Block_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
notify ("admin@example.com");
drop();
}
```

您也可以使用此版本，從正文中刪除錯誤的URL，並將其替換為URL REMOVED。

```
remove_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
edit-body-text("://\\S*\\.exe(\\s|\\b|$)", "URL REMOVED");
}
```

有關如何輸入郵件過濾器的詳細說明，請檢視如何向Cisco IronPort裝置新增新的郵件過濾器？

請參閱《思科ESA AsyncOS郵件安全裝置高級使用手冊》中名為「策略實施」的部分來檢視郵件過

濾器。