

在Cisco ESA上為網路釣魚教育測試建立白名單策略

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[背景資訊](#)

[設定](#)

[建立發件人組](#)

[建立郵件過濾器](#)

[驗證](#)

簡介

本文檔介紹如何在思科郵件安全裝置(ESA)或雲郵件安全(CES)例項上建立白名單策略，以允許進行網路釣魚教育測試/活動。

必要條件

需求

思科建議您瞭解以下主題：

- 在WebUI上的Cisco ESA/CES上導航和配置規則。
- 在命令列介面(CLI)上的Cisco ESA/CES上建立消息過濾器。
- 網路釣魚活動/測試所用資源的知識。

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

執行網路釣魚教育測試或活動的管理員將生成電子郵件，其中包含根據防垃圾郵件和/或爆發過濾器規則集上的當前Talos規則匹配的資訊。在這種情況下，網路釣魚活動電子郵件將不會到達終端使用者，並且由Cisco ESA/CES本身操作，從而導致測試停止。管理員需要確保ESA/CES允許通過這些電子郵件執行活動/測試。

設定

警告：不允許思科在全球範圍內將網路釣魚模擬和教育供應商列入白名單。我們建議管理員使用網路釣魚模擬器服務(例如：*PhishMe*)獲取其IP，然後將其本地新增到白名單。思科必須保護我們的ESA/CES客戶免受這些IP的侵害，以防他們易手或成為威脅。

注意：在測試時，管理員應僅將這些IP儲存在白名單中，如果外部IP在白名單中停留較長時間，則測試後可能會向終端使用者傳送未經請求的或惡意的電子郵件，以防這些IP受到危害。

在思科郵件安全裝置(ESA)上，為網路釣魚模擬建立新的發件人組，並將其分配給\$TRUSTED郵件流策略。這將允許向終端使用者傳送所有仿冒郵件。此新發件人組的成員不受速率限制，Cisco IronPort Anti-Spam引擎不會掃描來自這些發件人的內容，但仍會掃描防病毒軟體。

附註：預設情況下，\$TRUSTED郵件流策略已啟用防病毒，但已關閉防垃圾郵件。

建立發件人組

1. 按一下 **Mail Policies** 選項卡。
2. 在 **Host Access Table** 部分下，選擇 **HAT Overview**



3. 在右側，確保當前選擇了 **InboundMail** 偵聽程式，
4. 在下面的 **Sender Group** 列中，按一下 **Add Sender Group...**

Order	Sender Group	SenderBase™ Reputation Score	External Threat Feed Sources Applied	Mail Flow Policy	Delete
1	WHITELIST	-10 -8 -6 -4 -2 0 2 4 6 8 +10	None applied	TRUSTED	
2	BLACKLIST	=====	None applied	BLOCKED	

5. 填寫 **Name** 和 **Comment** 欄位。在 **Policy** 下拉選單中選擇「**\$TRUSTED**」，然後按一下 **Submit and Add Senders >>**。

Sender Group Settings	
Name:	PHISHING_SIMULATION
Comment:	Allow 3rd Party Phishing Simulation emails
Policy:	TRUSTED
SBRS (Optional):	<input type="text"/> to <input type="text"/> <input type="checkbox"/> Include SBRS Scores of "None" <i>Recommended for suspected senders only.</i>
External Threat Feeds (Optional): <i>For IP lookups only</i>	To add and configure Sources, go to Mail Policies > External Threat Feeds
DNS Lists (Optional): ?	<input type="text"/> <i>(e.g. 'query.blacklist.example, query.blacklist2.example')</i>
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

Cancel

Submit

6. 在第一個欄位中輸入要列入白名單的IP或主機名。 您的網路釣魚模擬合作夥伴將向您提供發件人IP資訊。

Sender Details	
Sender Type:	<input checked="" type="radio"/> IP Addresses <input type="radio"/> Geolocation
Sender: ?	<input type="text" value="12.34.56.78"/> <i>(IPv4 or IPv6)</i>
Comment:	<input type="text" value="Phishing Simulation Sender IP"/>

Cancel

Submit

新增完條目後，按一下 **Submit** 按鈕。請記得按一下 **Commit Changes** 按鈕以儲存更改。

建立郵件過濾器

建立發件人組以允許繞過反垃圾郵件和防病毒後，需要郵件過濾器來跳過可能匹配網路釣魚活動/測試的其他安全引擎。

1. 連線到ESA的CLI。
2. 執行命令 **filters**。
3. 運行命令 **new** 以建立新的消息過濾器。
4. 複製並貼上以下過濾器示例，根據需要編輯實際的發件人組名稱：

```
skip_amp_graymail_vof_for_phishing_campaigns:
if(sendergroup == "PHISHING_SIMULATION")
{
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
}
```

5. 返回主CLI提示符並按Enter鍵。
6. 運行 *commit* 以儲存配置。

驗證

使用第三方資源傳送網路釣魚活動/測試，並驗證郵件跟蹤日誌的結果，以確保跳過所有引擎並傳送電子郵件。