

使用TLS加密配置CRES安全加密服務郵件回覆

目錄

[簡介](#)

[Cisco RES：如何使用TLS保護未加密的RES回覆](#)

[發件人策略框架](#)

[主機名和IP地址](#)

[解決方案](#)

[相關資訊](#)

簡介

本文檔介紹為CRES入站安全答覆而非安全信封附件配置TLS加密的操作。

Cisco RES：如何使用TLS保護未加密的RES回覆

預設情況下，對安全電子郵件的回覆由Cisco RES加密並傳送到您的郵件網關。然後，它們會傳遞到您的郵件伺服器，這些郵件伺服器經過加密，以便終端使用者使用其Cisco RES憑證開啟。

為了在開啟Cisco RES安全郵件回覆時消除使用者身份驗證的需要，Cisco RES以「未加密」的形式向支援傳輸層安全(TLS)的郵件網關提供。大多數情況下，郵件網關是思科郵件安全裝置(ESA)，本文適用。

但是，如果有另一個位於ESA前面的郵件網關（例如外部垃圾郵件過濾器），則不需要在ESA上配置證書/TLS/郵件流。在這種情況下，您可以跳過本文檔的解決方案部分中的步驟1 - 3。對於在此環境中工作的未加密回覆，外部垃圾郵件過濾器（郵件網關）是需要支援TLS的裝置。如果他們支援TLS，您可以讓Cisco RES確認這一點，並設定您對安全郵件進行「未加密」回覆。

發件人策略框架

為了避免發件人策略框架(SPF)驗證失敗，請將這些值新增到SPF記錄中。

Cisco Registered Envelope Service(CRES)SPF記錄值與此表「主機名和IP地址」的IP/主機名匹配。

使用Cisco提供的SPF機制的輸出：

```
<#root>
~ dig txt
res.cisco.com
+short
"v=spf1
```

```
mx:res.cisco.com
```

```
exists:%{i}.spf.res.cisco.com  
-all"
```

將此機制新增到現有SPF記錄：

```
<#root>  
include:res.cisco.com
```

包含新的res.cisco.com機制的FAKE/test SPF記錄示例：

```
<#root>  
"v=spf1 mx:sampleorg1.com ip4:1.2.3.4  
include:res.cisco.com  
-all"
```


將Cisco RES新增到SPF記錄中的位置及方式取決於網路拓撲中網域名稱系統(DNS)的實作方式。請務必與DNS管理員聯絡以獲取更多資訊。

如果未將DNS配置為包括Cisco RES，則在通過託管金鑰伺服器生成並傳送安全合成和安全應答時，傳出IP地址與收件人末尾列出的IP地址不匹配，導致SPF驗證失敗。

主機名和IP地址


主機名	IP 位址	記錄型別
res.cisco.com	184.94.241.74	A
mxnat1.res.cisco.com	208.90.57.32	A
mxnat2.res.cisco.com	208.90.57.33	A
mxnat3.res.cisco.com	184.94.241.96	A

主機名	IP 位址	記錄型別
mxnat4.res.cisco.com	184.94.241.97	A
mxnat5.res.cisco.com	184.94.241.98	A
mxnat6.res.cisco.com	184.94.241.99	A
mxnat7.res.cisco.com	208.90.57.34	A
mxnat8.res.cisco.com	208.90.57.35	A
esa1.cres.iphmx.com	68.232.140.79	MX
esa2.cres.iphmx.com	68.232.140.57	MX
esa3.cres.iphmx.com	68.232.135.234	MX
esa4.cres.iphmx.com	68.232.135.235	MX

 注意：主機名和IP地址可能會因服務/網路維護或服務/網路增長而更改。並非所有主機名和IP地址都用於服務。此處提供以供參考。

解決方案

- 在ESA上獲取並安裝簽名證書和中間證書。

 注意：您必須從您的簽名機構獲取中間證書，因為裝置上的演示證書會導致CRES驗證過程失敗。

- 建立新的郵件流策略：
 - 在GUI中選擇Mail Policies > Mail Flow Policies > Add Policy。
 - 輸入名稱，並將除「安全功能：TLS」之外的所有其他內容保留為預設值。將此項設定為**Required**。
- 建立新的發件人組：

a. 在GUI中選擇Mail Policies > HAT Overview > Add Sender Group。

- 輸入名稱，並將訂單編號設定為#1。您也可以輸入可選註釋。選擇您在步驟2中建立的郵件流策略。把其他所有東西都留空。
- 按一下「Submit and」 Add Senders。

- 在Sender欄位中，輸入以下IP範圍和主機名：

.res.cisco.com
.cres.iphmx.com
208.90.57.0/26 (current CRES IP network range)
204.15.81.0/26 (old CRES IP network range)

•

提交並提交更改。

- 當您確信了ESA已準備好從Cisco RES伺服器協商TLS加密後，請執行CRES管理門戶中的步驟[如何測試我的域是否支援使用Cisco RES的TLS?](#)

相關資訊

- [Cisco RES：關鍵伺服器的IP地址和主機名](#)
- [Cisco Email Security Appliance — 最終使用手冊](#)
- [技術支援與文件 - Cisco Systems](#)

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）。