瞭解CES SPF記錄

目錄

簡介

本文檔介紹思科為CES託管客戶推薦的SPF記錄如何運行。

需求

1. 對DNS工作方式有基礎認識。

SPF宏的重要性

Cisco推薦的記錄使用RFC7208第7節中定義的SPF宏。在這種情況下，使用宏來減少允許CES裝置通過SPF驗證所需的DNS查詢量。這一點非常重要，因為SPF根據RFC7208 4.6.4節，將每個SPF驗證的DNS查詢量限製為10。如果需要的DNS查詢超過10個，則SPF驗證結果將是永久錯誤。這可能不是問題，但如果調配了更多託管的ESA，將需要更多DNS查詢。

可以將每個託管ESA的IP地址新增到SPF記錄。在SPF驗證期間，這將不需要任何額外的DNS查詢。但是，此方法的缺點是，每當調配任何新的ESA或現有ESA的IP地址發生更改時，您必須更改SPF記錄。新增記錄後，思科建議的SPF記錄不需要您進行任何管理。

已解釋SPF記錄

以下是SPF記錄的示例：

```
$ dig acme.com txt +short
"v=spf1 exists:%{i}.spf.acme.iphmx.com ~all"
```

> **附註**：*此SPF記錄的「acme」部分被視為分配名稱。您的CES託管的群集具有唯一的分配名稱，如果您將此SPF記錄新增到DNS，則應使用它來代替「acme」。*

在此SPF記錄中，使用了宏「%{i}」。此宏用作變數，在SPF驗證進行時，該變數將被連線主機的IP地址替換。例如，如果192.168.0.1是傳送主機，則主機名「%{i}.spf.acme.iphmx.com」將擴展為「192.168.0.1.spf.acme.iphmx.com」。

「exists」機制在RFC7208 Section-5.7中定義，如果主機名「%{i}.spf.acme.iphmx.com」在DNS中具有A記錄，則會匹配。例如，假設192.168.0.1再次是傳送主機。主機名「

%{i}.spf.acme.iphmx.com」將擴展到「192.168.0.1.spf.acme.iphmx.com」，驗證主機將執行以下DNS查詢：

```
$ dig 192.168.0.1.spf.acme.iphmx.com a +short
127.0.0.2
```

> **附註**：域iphmx.com由思科管理。因此，只有思科才能新增/刪除/修改該域的DNS記錄，如上述記錄。這對您來說意味著您無需在向CES集群調配新的ESA時新增這些記錄。思科有責任確保這些記錄得以新增並正確無誤。

因為返回了IP地址127.0.0.2，所以存在機制將匹配，SPF驗證結果將通過。

假設傳送主機是10.0.0.1。主機名「%{i}.spf.acme.iphmx.com」將擴展到「10.0.0.1.spf.acme.iphmx.com」，驗證主機將執行以下DNS查詢：

```
$ dig 10.0.0.1.spf.acme.iphmx.com a +short
$
```

由於沒有返回結果，現有的機制不匹配，SPF驗證結果將軟失敗。

其他資訊

SPF技術可能很複雜，具體取決於您要授權為域轉發郵件的主機數量。如果CES託管的裝置是唯一授權為您的域轉發郵件的主機，則上述記錄對您非常有用。否則，您必須修改我們提供的SPF記錄，以便它將授權您需要它的所有主機。

如果您有現有的SPF記錄，則「exists:%{i}.spf.acme.iphmx.com」可以新增到該SPF記錄中。