Warum schlägt die SPF-Verifizierung bei Antworten auf verschlüsselte Nachrichten oder bei E-Mails fehl, die direkt von CRES WebSafe gesendet werden?

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie den SPF-Datensatz (Sender Policy Framework) für Nachrichten vom Cisco Registered Envelope Service (CRES) einrichten.

Warum schlägt die SPF-Verifizierung bei Antworten auf verschlüsselte Nachrichten oder bei E-Mails fehl, die direkt von CRES WebSafe gesendet werden?

Bei E-Mails, die von CRES gesendet werden (sichere Antwort oder sichere Zusammenstellung von E-Mails), schlägt die SPF-Verifizierung am Empfängerende fehl. Der Grund hierfür ist, dass sichere Komprimierungs- und sichere Antworten generiert und von den gehosteten Schlüsselservern bereitgestellt werden. Die ausgehende IP-Adresse stimmt nicht mit den angegebenen IP-Adressen am Ende des Empfängers überein. Um dieses Problem zu beheben, fügen Sie diese Anweisung zum SPF-Datensatz Ihrer Domäne hinzu:

```
include:res.cisco.com
```