# FOIRE AUX QUESTIONS CRES : Comment est-ce que j'emploie le TLS pour sécuriser des réponses décryptées CRES ?

## Contenu



## Introduction

Ce document décrit comment employer le Transport Layer Security (TLS) pour sécuriser des réponses du service d'enveloppe recommandée de Cisco (CRES), qui permet à un utilisateur pour ne pas avoir besoin de les déchiffrer, en association avec l'appliance de sécurité du courrier électronique de Cisco (ESA).

## Comment est-ce que j'emploie le TLS pour sécuriser des réponses décryptées CRES ?

Par défaut, des réponses à un email sécurisé sont chiffrées par CRES et en fonction envoyées à votre mail gateway. Ils traversent alors à vos serveurs de messagerie chiffrés pour que l'utilisateur final s'ouvre avec leurs qualifications CRES.

Afin d'éviter le besoin de l'utilisateur d'authentifier avec CRES pour ouvrir la réponse sécurisée, CRES livre sous une forme « décryptée » pour envoyer par mail les passerelles qui prennent en charge le TLS. Dans la plupart des cas le mail gateway est l'ESA, et cet article est applicable.

Cependant, s'il y a un autre mail gateway qui se repose devant l'ESA tel qu'un filtre externe de Spam, là n'est aucun besoin de certificate/TLS/mail circulent la configuration sur votre ESA. Dans ce cas, vous pouvez ignorer les étapes 1 3 dans la partie Solution de ce document. Pour que les réponses décryptées fonctionnent dans cet environnement, le filtre externe de Spam (mail gateway) est l'appliance qui doit prendre en charge le TLS. S'ils prennent en charge le TLS, vous pouvez faire confirmer CRES ceci et vous obtenir installez pour des réponses « décryptées » afin de sécuriser des emails.

### Sender Policy Framework

Afin d'éviter des pannes de vérification de Sender Policy Framework (SPF), vous devez ajouter le MX : res.cisco.com, mxnat1.res.cisco.com, et mxnat3.res.cisco.com à votre enregistrement SPF.

Là où et comment vous ajoutez CRES à votre enregistrement SPF dépend de la façon dont le

Système de noms de domaine (DNS) est mis en application en votre topologie du réseau. Entrez en contact avec votre pour en savoir plus d'administrateur de DN.

Si des DN n'est pas configurés pour inclure CRES, si sécurisé composez et sécurisez les réponses sont générés et livré par les serveurs principaux hébergés, l'adresse IP sortante n'appariera pas les adresses IP énumérées aux destinataires finissent, ayant pour résultat une panne de vérification SPF.

### Adresses Internet et adresses IP

| Nom de l'hôte | Adresse IP | Type d'enregistrement |
|---|---|---|
| res.cisco.com | 184.94.241.74 | 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 |
| ---- ---- ---- | ---- ---- ---- | ---- ---- ---- |
| mxnat1.res.cisco.com | 208.90.57.32 | A |
| mxnat3.res.cisco.com | 184.94.241.96 | A |

*Les adresses Internet et les adresses IP sont sujettes à la modification basée sur le service/maintenance du réseau et entretiennent/croissances de réseau.*

## Solution

1. Obtenez et installez un certificat signé et le certificat intermédiaire sur l'ESA. **Note**: Il est important vous obtiennent le certificat intermédiaire de votre autorité de signature comme certificat de démonstration qui est livré sur l'appliance fait échouer le processus de vérification CRES.
2. Créez une nouvelle stratégie de flux de courrier : Du GUI, choisissez les **stratégies de messagerie > les stratégies de flux de courrier > ajoutent la stratégie…**.Écrivez un nom et laissez tout le reste au par défaut excepté des *fonctionnalités de sécurité : TLS.* Placez ceci à **requis**.
3. Créez un nouveau groupe d'expéditeur : Du GUI, choisissez les **stratégies de messagerie > l'aperçu de CHAPEAU > ajoutent le groupe d'expéditeur…**.Écrivez un nom et placez le numéro de commande à #1.  Vous pouvez également écrire un commentaire facultatif. Choisissez la stratégie de flux de courrier que vous avez créé dans le congé d'étape 2. tout autrement blanc.Cliquez sur Submit **et ajoutez les expéditeurs >>**.
4. Dans le domaine d'expéditeur, entrez dans ces plages et adresses Internet IP :
```
.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)
```
5. Soumettez et commettez les modifications.
6. Après que vous soyez sûr est-ce queESA est-il préparé pour le TLS des serveurs CRES, suivent les étapes dans la façon dont fais je teste si mon domaine prend en charge le TLS avec CRES ? afin d'inviter les serveurs CRES à commencer à utiliser le TLS.

## Informations connexes

- FOIRE AUX QUESTIONS ESA : Quels sont les IPS et les adresses Internet du CRES introduisent des serveurs ?
- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems