Configurer le service de chiffrement sécurisé CRES Réponses aux messages à l'aide du chiffrement TLS

Table des matières

Introduction

Ce document décrit les actions pour configurer le chiffrement TLS pour les réponses sécurisées entrantes CRES au lieu d'une pièce jointe d'enveloppe sécurisée.

Cisco RES : Comment utiliser TLS pour sécuriser les réponses RES non chiffrées

Par défaut, les réponses à un e-mail sécurisé sont chiffrées par Cisco RES et envoyées à votre passerelle de messagerie. Ils sont ensuite transmis à vos serveurs de messagerie cryptés pour que l'utilisateur final puisse les ouvrir avec ses identifiants Cisco RES.

Afin d'éliminer le besoin d'authentification des utilisateurs lors de l'ouverture d'une réponse de message sécurisé Cisco RES, Cisco RES fournit sous une forme « non chiffrée » aux passerelles de messagerie qui prennent en charge la sécurité de la couche transport (TLS). Dans la plupart des cas, la passerelle de messagerie est l'appliance de sécurisation de la messagerie Cisco (ESA), et cet article s'applique.

Cependant, si une autre passerelle de messagerie se trouve devant l'ESA, par exemple un filtre de spam externe, il n'est pas nécessaire de configurer le certificat/TLS/flux de messagerie sur votre ESA. Dans ce cas, vous pouvez ignorer les étapes 1 à 3 de la section Solution de ce document. Pour que les réponses non chiffrées fonctionnent dans cet environnement, le filtre de courrier indésirable externe (passerelle de messagerie) est l'appliance qui doit prendre en charge TLS. S'ils prennent en charge le protocole TLS, vous pouvez demander à Cisco RES de le confirmer et de vous configurer pour des réponses « non chiffrées » aux e-mails sécurisés.

Sender Policy Framework

Afin d'éviter les échecs de vérification SPF (Sender Policy Framework), ajoutez ces valeurs à votre enregistrement SPF.

La valeur de l'enregistrement SPF du service d'enveloppe enregistré Cisco (CRES) correspond aux adresses IP/noms d'hôte de cette table, « Noms d'hôte et adresses IP ».

Le résultat obtenu à l'aide du mécanisme SPF fourni par Cisco :

<#root>

```
~ dig txt
res.cisco.com
 +short
"v=spf1
mx:res.cisco.com
exists:%{i}.spf.res.cisco.com
 -all"
```

Ajoutez ce mécanisme à votre enregistrement SPF existant :

<#root>

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

Exemple d'enregistrement FAKE/test SPF contenant le nouveau mécanisme res.cisco.com :

<#root>

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

L'emplacement et le mode d'ajout de Cisco RES à votre enregistrement SPF dépendent de la manière dont votre système de noms de domaine (DNS) est mis en oeuvre dans votre topologie de réseau. N’oubliez pas de contacter votre administrateur DNS pour plus d’informations.

Si DNS n'est pas configuré pour inclure Cisco RES, lorsque des réponses composées et sécurisées sont générées et transmises via les serveurs de clés hébergés, l'adresse IP sortante

ne correspond pas aux adresses IP répertoriées à la fin du destinataire, ce qui entraîne un échec de la vérification SPF.

Noms d'hôte et adresses IP

Nom de l'hôte	Adresse IP	Type d'enregistrement
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
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

Remarque : le nom d'hôte et les adresses IP peuvent être modifiés en fonction de la maintenance du service/réseau ou de la croissance du service/réseau. Tous les noms d'hôte et adresses IP ne sont pas utilisés pour le service. Ils sont fournis ici à titre de référence.

Solution

- Obtenez et installez un certificat signé et un certificat intermédiaire sur l'ESA.

Remarque : vous devez obtenir le certificat intermédiaire auprès de votre autorité de signature, car le certificat de démonstration fourni sur l'appliance entraîne l'échec du processus de vérification CRES.

- Créer une nouvelle stratégie de flux de messagerie :
  a. Dans l'interface utilisateur graphique, sélectionnez Mail Policies > Mail Flow Policies > Add Policy.

  - Entrez un nom et conservez tous les autres par défaut, à l'exception de « Fonctions de sécurité : TLS ». Définissez cette option sur **Obligatoire**.

- Créer un nouveau groupe d'expéditeurs :

  a. Dans l'interface utilisateur graphique, sélectionnez Mail Policies > HAT Overview > Add Sender Group.

  - Entrez un nom et définissez le numéro de commande sur #1. Vous pouvez également saisir un commentaire facultatif. Sélectionnez la stratégie de flux de messagerie que vous avez créée à l'étape 2. Laissez tout le reste en blanc.

  - Cliquez sur Submit et surAdd Senders.

- Dans le champ Sender, saisissez les plages IP et les noms d'hôte suivants :

```
.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)
```

-

Envoyez et validez les modifications.

- Une fois que vous êtes certain que l'ESA est prêt à négocier le cryptage TLS à partir des serveurs Cisco RES, suivez les étapes du portail d'administration CRES. Comment puis-je tester si mon domaine prend en charge TLS avec Cisco RES ?

Informations connexes

- Cisco RES : adresses IP et noms d'hôte pour les serveurs clés
- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.