Contenu

Introduction

Par défaut l'appliance de sécurité du courrier électronique de Cisco (ESA) n'empêche pas la livraison d'arrivée des messages qui sont adressés ? de ? le même domaine allant au même domaine. Ceci permet à des messages pour être ? charrié ? par les sociétés extérieures qui légitiment l'entreprise avec le client. Quelques sociétés comptent sur l'organisation de tiers pour envoyer l'email au nom de la société telle que la santé, des agences de voyages, etc.

Charriez la protection utilisant la vérification d'expéditeur

Configurez la stratégie de flux de courrier (MFP)

1. À partir de la GUI : **Les stratégies de messagerie > les stratégies de flux de courrier > ajoutent la stratégie…**
2. Créez un nouveau MFP utilisant un nom qui est approprié comme SPOOF_ALLOW
3. Dans la section de *vérification d'expéditeur*, changez la configuration de *Tableau d'exception de vérification d'expéditeur d'utilisation du* **par défaut d'utilisation à HORS FONCTION**.
4. Dans des **stratégies de messagerie > des stratégies de flux de courrier > des paramètres de stratégie par défaut**, placez la configuration de *Tableau d'exception de vérification d'expéditeur d'utilisation à* **en fonction**.

Configurez le CHAPEAU

1. À partir de la GUI : **Les stratégies de messagerie > l'aperçu de CHAPEAU > ajoutent le groupe d'expéditeur…**
2. Placez le nom en conséquence au MFP créé plus tôt, c.-à-d. SPOOF_ALLOW.
3. Placez la commande ainsi elle est des groupes au-dessus WHITELIST et de LISTE NOIRE d'expéditeur.
4. Assignez la stratégie **SPOOF_ALLOW aux** configurations de ce groupe d'expéditeur.
5. Cliquez sur Submit **et ajoutez les expéditeurs…**
6. Ajoutez l'IP ou les domaines pour tous les interlocuteurs externes aux lesquels vous voulez permettre pour charrier le domaine interne.

Configurez le Tableau d'exception

1. À partir de la GUI : **Le Tableau de stratégies > d'exception de messagerie > ajoutent l'exception de vérification d'expéditeur…**
2. Ajoutez le domaine local au Tableau d'exception de vérification d'expéditeur
3. Placez le *comportement* **pour rejeter**

Vérifiez

En ce moment, la messagerie provenant *your.domain à* your.domainwould soit rejetée à moins que l'expéditeur soit répertorié dans le groupe SPOOF_ALLOW d'expéditeur, car il serait associé à un MFP qui n'utilise pas la table d'exception de vérification d'expéditeur.

Un exemple de ceci serait vu en se terminant une session de telnet manuelle à l'auditeur :

La réponse du SMTP 553 est un résultat de réponse directe de la table d'exception comme configurée sur l'ESA des étapes ci-dessus.

Des logs de messagerie, vous pouvez voir que l'adresse IP de 192.168.0.9 n'est pas dans l'adresse IP valide pour le groupe correct d'expéditeur :

Une adresse IP permise s'assortissant avec l'exemple de configuration des étapes ci-dessus serait vue comme suit :

Informations connexes

- Grep ESA, SMA, et WSA avec l'expression régulière pour rechercher des logs
- Détermination de disposition de message ESA
- Support et documentation techniques - Cisco Systems