Exemple de configuration de chiffrement d'email ESA

Contenu

Introduction

Ce document décrit comment installer le cryptage d'email sur l'appliance de sécurité du courrier électronique (ESA).

Conditions préalables

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Modèle : Toutes les série C et X-gamme
- Caractéristique de cryptage d'enveloppe (PostX) installée

Configurez

Cryptage d'email d'enable sur l'ESA

Terminez-vous ces étapes du GUI :

1. Sous des Services de sécurité, choisissez le **cryptage d'email d'IronPort Cisco > le cryptage d'email d'enable**, et cliquez sur Edit les **configurations**.

2. Cliquez sur Add le **profil de cryptage** afin de créer un nouveau profil de cryptage.

3. Choisissez l'**appliance de service** ou de **Chiffrement Cisco IronPort d'enveloppe recommandée de Cisco** (si l'appliance de cryptage est achetée) pour le type de service

principal.

4. Cliquez sur Submit **et commettez les modifications**.

5. Après que le profil de cryptage ait été créé, vous êtes donné l'option de provision l'au serveur du service de l'enveloppe recommandée de Cisco (CRES). Un bouton de disposition devrait afficher à côté du nouveau profil. **Disposition de** clic.

Créez un filtre satisfait sortant

Terminez-vous ces étapes du GUI afin de créer un filtre satisfait sortant pour implémenter le profil de cryptage. Dans l'exemple suivant, le filtre déclenchera le cryptage pour n'importe quel message sortant avec la chaîne « sécurisent : » dans l'en-tête soumise :

1. Dans le cadre des stratégies de messagerie, choisissez les filtres satisfaits sortants, et cliquez sur Add le **filtre**.

2. Ajoutez un nouveau filtre avec l'état de l'en-tête soumise comme le == soumis « sécurisent : » et l'action Encrypt et livrent maintenant (mesure finale). Cliquez sur **Submit**.

3. Dans le cadre des stratégies de messagerie, choisissez les stratégies de mail sortant, et activez ce nouveau filtre dans la stratégie par défaut de messagerie ou les stratégies appropriées de messagerie.

4. Modifications de validation.

Vérifiez

Cette section décrit comment vérifier que le cryptage fonctionne.

1. Afin de vérifier, générez une nouvelle messagerie avec **sécurisé :** dans le sujet et envoyez l'email à un compte de Web (Hotmail, Yahoo, Gmail) afin de déterminer s'il est chiffré.

2. Vérifiez les logs de messagerie comme décrit dans la section suivante afin de s'assurer que le message est chiffré par l'intermédiaire du filtre satisfait sortant.

Validez le filtre de cryptage traitant dans le Mail_logs

Ces entrées de mail_log prouvent que les messages ont apparié le filtre de cryptage appelé Encrypt_Message.

```
Wed Oct 22 17:06:46 2008 Info: MID 116 was generated based on MID 115 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:07:22 2008 Info: MID 118 was generated based on MID 117 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:31:21 2008 Info: MID 120 was generated based on MID 119 by encrypt
filter ''Encrypt_Message
```

Référez-vous à la détermination de disposition de message ESA pour l'instruction sur la façon

dont employer le **grep** ou les commandes **findevent** afin de recueillir des informations des logs suivant les indications de ceci section.

Dépannez

Si le filtre de cryptage ne déclenche pas, vérifiez les logs de messagerie pour la stratégie de messagerie que le message-test l'utilise. Assurez-vous que le filtre est activé dans cette stratégie de messagerie, et également ce là n'est aucun filtre précédent activé dans cette stratégie avec une action **restante de filtres de contenu de saut**.

Assurez-vous que les messages dans l'utilisation de cheminement de message la chaîne correcte ou le sujet indiqué étiquetant afin de déclencher le cryptage par le filtre satisfait.