Esempio di configurazione di ESA Email Encryption

Sommario

Introduzione

In questo documento viene descritto come configurare la crittografia e-mail su Email Security Appliance (ESA).

Prerequisiti

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Modello: Tutti i proiettori della serie C e X
- Funzionalità di crittografia della busta (PostX) installata

Configurazione

Abilitazione della crittografia e-mail sull'ESA

Eseguire questi passaggi dalla GUI:

1. In Security Services, scegliere **Cisco IronPort Email Encryption > Enable Email Encryption**, quindi fare clic su **Edit Settings**.

2. Per creare un nuovo profilo di crittografia, fare clic su **Add Encryption Profile** (Aggiungi profilo di crittografia).

3. Per il tipo di servizio chiave, selezionare **Cisco Registered Envelope Service** o **Cisco IronPort**

Encryption Appliance (se l'appliance di crittografia è stata acquistata).

4. Fare clic su **Invia e conferma modifiche**.

5. Dopo aver creato il profilo di crittografia, è possibile decidere di eseguirne il provisioning sul server Cisco Registered Envelope Service (CRES). Accanto al nuovo profilo dovrebbe essere visualizzato il pulsante Provisioning. Fare clic su **Assegna ruoli**.

Creare un filtro contenuto in uscita

Completare questa procedura dalla GUI per creare un filtro dei contenuti in uscita per implementare il profilo di crittografia. Nell'esempio seguente, il filtro attiverà la crittografia per qualsiasi messaggio in uscita con la stringa "Secure:" nell'intestazione dell'oggetto:

1. In Criteri di posta, scegliere i filtri contenuti in uscita e fare clic su **Aggiungi filtro**.

2. Aggiungere un nuovo filtro con la condizione Subject Header come subject == "Secure:" e l'azione Encrypt and Deliver Now (azione finale). Fare clic su **Invia**.

3. In Criteri di posta, scegliere i Criteri posta in uscita e abilitare questo nuovo filtro nel criterio di posta predefinito o nei criteri di posta appropriati.

4. Eseguire il commit delle modifiche.

Verifica

In questa sezione viene descritto come verificare il funzionamento della crittografia.

1. Per procedere alla verifica, genera un nuovo messaggio con **Secure:** nell'oggetto e inviare l'e-mail a un account Web (Hotmail, Yahoo, Gmail) per determinare se è crittografata.

2. Controllare i log di posta come descritto nella sezione successiva per assicurarsi che il messaggio sia crittografato tramite il filtro contenuti in uscita.

Convalida elaborazione filtro crittografia in Mail_logs

Queste voci di log di posta mostrano che i messaggi corrispondono al filtro di crittografia 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
```

Per istruzioni sull'uso dei comandi **grep** o **findevent** per raccogliere informazioni dai log, consultare il documento ESA Message Disposition Determination (Determinazione della disposizione del messaggio ESA) come mostrato in questa sezione.

Risoluzione dei problemi

Se il filtro di crittografia non viene attivato, verificare nei log di posta il criterio di posta utilizzato dal messaggio di prova. Verificare che il filtro sia abilitato nel criterio di posta e che non sia presente alcun filtro precedente abilitato nel criterio con un'azione **Ignora filtri contenuti rimanenti**.

Verificare che i messaggi nella verifica messaggi utilizzino la stringa corretta o il tag dell'oggetto designato per attivare la crittografia tramite il filtro contenuti.