Configuratievoorbeeld van ESA e-mailencryptie

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Configureren](#)
[E-mailencryptie op de ESA inschakelen](#)
[Een uitgaande contentfilter maken](#)
[Verifiëren](#)
[Verifieer de verwerking van encryptie filter in de Mail_logs](#)
[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u e-mailencryptie op de e-mail security applicatie (ESA) kunt instellen.

Voorwaarden

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Model: Alle C-Series en X-Series-switches
- Invoerencryptie (PostX) optie geïnstalleerd

Configureren

E-mailencryptie op de ESA inschakelen

Volg deze stappen vanuit de GUI:

1. Kies onder Security Services **Cisco IronPort Email Encryption > E-mailencryptie inschakelen** en klik op **Instellingen bewerken**.

2. Klik op **Encryptieprofiel toevoegen** om een nieuw encryptieprofiel te maken.

3. Kies **Cisco Registered Service** of **Cisco IronPort Encryption-applicatie** (als de encryptie-applicatie is aangeschaft) voor het toetstype.

4. Klik op **Inzenden en Commit Wijzigingen**.

5. Nadat het encryptieprofiel is gemaakt, krijgt u de optie om het aan de Cisco-server voor geregistreerde services (CRES) te leveren. Naast het nieuwe profiel moet er een knop Voorziening worden weergegeven. Klik op **Voorziening**.

Een uitgaande contentfilter maken

Voltooi deze stappen vanuit de GUI om een uitgaand contentfilter te maken om het encryptieprofiel te implementeren. In het volgende voorbeeld zal het filter encryptie voor om het even welk uitgaand bericht met de string "Secure:" in de onderwerpregel activeren:

1. Selecteer onder Mail-beleid de Outverse Content Filters en klik op **Add Filter**.

2. Voeg een nieuw filter toe met de voorwaarde van Onderwerp Kop zoals onderwerp = "Beveiliging:" en actie van Encrypt and Delivery Now (Definitieve actie). Klik op **Inzenden**.

3. Selecteer onder Mail-beleid het beleid Uitgaande e-mail en laat dit nieuwe filter in het standaard postbeleid of het juiste postbeleid toe.

4. Commit change.

Verifiëren

In dit gedeelte wordt beschreven hoe u kunt controleren of de encryptie werkt.

1. Om te verifiëren moet u een nieuwe post met **Secure** genereren**:** in het onderwerp te versturen en de e-mail naar een webaccount (Hotmail, Yahoo, Gmail) te versturen om vast te stellen of de e-mail versleuteld is.

2. Controleer de e-mailbestanden zoals beschreven in de volgende sectie om er zeker van te zijn dat het bericht is versleuteld via het filter van de uitgaande inhoud.

Verifieer de verwerking van encryptie filter in de Mail_logs

Deze mail_log items tonen aan dat de berichten overeenkwamen met het encryptie filter genaamd 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
```

Raadpleeg de ESR-berichtbepaling voor instructies over het gebruik van de opdrachten om informatie te verzamelen uit de blogs, zoals in deze sectie wordt getoond.

Problemen oplossen

Als het coderingsfilter niet wordt geactiveerd, controleert u de maillogbestanden voor het postbeleid in het testbericht. Zorg ervoor dat het filter in dit e-mailbeleid is ingeschakeld en dat er ook geen vorige filter is ingeschakeld in dit beleid met een actie **Niet-opgeruimd contentfilters**.

Zorg ervoor dat de boodschap(en) in bericht tracking de juiste string of de juiste onderwerpregel gebruikt om encryptie door het contentfilter te activeren.