Konfigurationsbeispiel für E-Mail-Verschlüsselung der ESA

Inhalt

Einführung

Dieses Dokument beschreibt, wie Sie die E-Mail-Verschlüsselung auf der E-Mail Security Appliance (ESA) einrichten.

Voraussetzungen

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Modell: Alle C-Serien und X-Serien
- Installierte Umschlagverschlüsselungsfunktion (PostX)

Konfigurieren

E-Mail-Verschlüsselung auf der ESA aktivieren

Führen Sie die folgenden Schritte über die Benutzeroberfläche aus:

1. Wählen Sie unter Sicherheitsdienste **Cisco IronPort Email Encryption > Enable Email Encryption aus**, und klicken Sie auf **Edit Settings**.

2. Klicken Sie auf **Verschlüsselungsprofil hinzufügen**, um ein neues Verschlüsselungsprofil zu erstellen.

3. Wählen Sie **Cisco Registered Envelope Service** oder **Cisco IronPort Encryption Appliance**

(wenn die Verschlüsselungs-Appliance erworben wurde) als Key-Service-Typ aus.

4. Klicken Sie auf **Änderungen senden und bestätigen**.

5. Nachdem das Verschlüsselungsprofil erstellt wurde, können Sie es dem CRES-Server (Registered Envelope Service) von Cisco bereitstellen. Neben dem neuen Profil sollte eine Provisioning-Schaltfläche angezeigt werden. Klicken Sie auf **Bereitstellung**.

Erstellen eines ausgehenden Content-Filters

Führen Sie diese Schritte in der GUI aus, um einen Content-Filter für ausgehenden Datenverkehr zu erstellen und das Verschlüsselungsprofil zu implementieren. Im folgenden Beispiel löst der Filter eine Verschlüsselung für ausgehende Nachrichten aus, wobei die Zeichenfolge "Secure:" im Betreff-Header lautet:

1. Wählen Sie unter Mail-Policys die Filter für ausgehende Inhalte aus, und klicken Sie auf **Filter hinzufügen**.

2. Fügen Sie einen neuen Filter mit der Bedingung Betreff-Header als Betreff == "Sicher:" und der Aktion "Verschlüsseln und jetzt bereitstellen" (abschließende Aktion) hinzu. Klicken Sie auf **Senden**.

3. Wählen Sie unter Mail-Policys die Richtlinien für ausgehende Nachrichten aus, und aktivieren Sie diesen neuen Filter in der Standard-Mail-Richtlinie oder den entsprechenden Mail-Richtlinien.

4. Änderungen bestätigen.

Überprüfen

In diesem Abschnitt wird beschrieben, wie Sie überprüfen, ob die Verschlüsselung funktioniert.

1. Erstellen Sie zum Verifizieren eine neue E-Mail mit **Secure:** im Betreff und senden Sie die E-Mail an ein Web-Konto (Hotmail, Yahoo, Gmail), um festzustellen, ob es verschlüsselt ist.

2. Überprüfen Sie die E-Mail-Protokolle wie im nächsten Abschnitt beschrieben, um sicherzustellen, dass die Nachricht über den Filter für ausgehende Inhalte verschlüsselt wird.

Validieren Sie die Verarbeitung des Verschlüsselungsfilters in den Mail_logs.

Diese mail_log-Einträge zeigen, dass die Nachrichten dem Verschlüsselungsfilter Encrypt_Message zugeordnet wurden.

```
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
```

Informationen zur Verwendung der Befehle **grep** oder **findevent** zum Erfassen von Informationen aus den Protokollen finden Sie unter ESA Message Disposition Determination (Bestimmung der Löschung von Nachrichten oder **Findevent**).

Fehlerbehebung

Wenn der Verschlüsselungsfilter nicht auslöst, überprüfen Sie die E-Mail-Protokolle auf die Mail-Richtlinie, die die Testnachricht verwendet. Stellen Sie sicher, dass der Filter in dieser Mail-Richtlinie aktiviert ist und dass in dieser Richtlinie kein vorheriger Filter aktiviert ist, der die Aktion **Verbleibende Content-Filter überspringen** enthält.

Stellen Sie sicher, dass die Nachrichten in der Nachrichtenverfolgung die richtige Zeichenfolge oder das angegebene Betreff-Tagging verwenden, um die Verschlüsselung über den Content-Filter auszulösen.