Konfigurieren der Sicherheitsstufen im CRES-Verschlüsselungsprofil der ESA

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der Cisco Registered Envelope Service Encryption (CRES)-Profile in der E-Mail Security Appliance (ESA) mit Schwerpunkt auf den verschiedenen zulässigen Sicherheitsstufen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkonfiguration der ESA
- Verschlüsselung auf Basis der Content-Filter-Konfiguration
- Cisco Registered Envelope Service

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Erstellung des CRES-Profils ist eine Kernaufgabe für die Aktivierung und Nutzung des Verschlüsselungsdienstes über die ESA. Stellen Sie vor der Erstellung mehrerer Profile sicher, dass Sie ein für eine ESA bereitgestelltes Konto mit der Erstellung eines CRES-Kontos abgeschlossen haben.

Es kann mehr als ein Profil geben, und jedes Profil kann mit einer anderen Sicherheitsstufe konfiguriert werden. Auf diese Weise kann das Netzwerk unterschiedliche Sicherheitsstufen nach Domäne, Benutzer oder Gruppe aufrechterhalten.

Konfigurieren

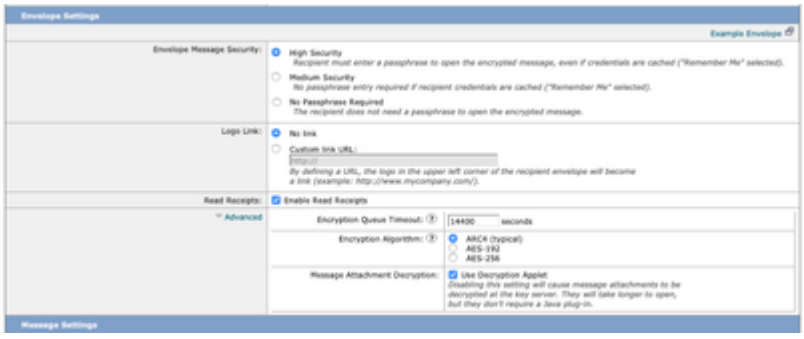
Sie können ein Verschlüsselungsprofil mit dem CLI-Befehl encryptionconfig aktivieren und konfigurieren oder über Security Services > Cisco IronPort Email Encryption in der GUI.

Konfiguration über GUI

Navigieren Sie von der ESA zu Security Services > Cisco IronPort Email Encryption > Add Encryption Profile.

Es wird ein Bildschirm mit den Verschlüsselungsprofileinstellungen angezeigt. Der Profilname und der Rest der Konfiguration können angepasst werden und hängen von Identifizierungsmarkierungen oder Methoden der Organisation ab.

Die Konfiguration, die die Sicherheitsstufe für die einzelnen Profile definiert, lautet "Envelope Settings" (Umschlageinstellungen), wie im Bild gezeigt:



Anmerkung: Es wird empfohlen, dass der Profilname Folgendes enthält: "Hoch", "Niedrig" usw., um die konfigurierte Sicherheitsstufe oder den Namen der Gruppe, der das Profil zugeordnet ist, für eine schnelle Identifizierung bei der Erstellung von Content-Filtern und der Verifizierung anzupassen.

Die drei von der ESA zugelassenen Sicherheitsstufen sind:

- Hohe Sicherheit: Der Empfänger muss immer eine Passphrase eingeben, um verschlüsselte Nachrichten öffnen zu können.
- Mittlere Sicherheit: Der Empfänger muss keine Anmeldeinformationen eingeben, um die verschlüsselte Nachricht zu öffnen, wenn die Anmeldeinformationen des Empfängers zwischengespeichert werden.
- Keine Passphrase erforderlich: Dies ist die niedrigste Sicherheitsstufe für verschlüsselte Nachrichten. Der Empfänger muss keine Passphrase eingeben, um die verschlüsselte Nachricht zu öffnen. Sie können weiterhin die Funktionen Lesebestätigungen, Sichere Antwort an alle und Sichere Nachrichtenweiterleitung für Umschläge aktivieren, die nicht durch eine Passphrase geschützt sind.

Sie können die verschiedenen Sicherheitsstufen für die folgenden Objekte konfigurieren:

Umschläge für Nachrichtensicherheit:

- · Hohe Sicherheit
- Mittlere Sicherheit
- Keine Passphrase erforderlich

Logo-Link: Um Benutzern das Öffnen der URL Ihrer Organisation zu ermöglichen, klicken Sie auf das entsprechende Logo. Sie können dem Logo einen Link hinzufügen. Wählen Sie eine der folgenden Optionen aus:

- Kein Link. Dem Nachrichtenumschlag wurde kein Live-Link hinzugefügt.
- URL für benutzerdefinierten Link. Geben Sie die URL ein, um dem Nachrichtenumschlag einen Live-Link hinzuzufügen.

Lesebestätigungen: Wenn Sie diese Option aktivieren, erhält der Absender eine Quittung, wenn der Empfänger den sicheren Umschlag öffnet. Dies ist eine optionale Auswahl.

Erweitert:

Timeout der Verschlüsselungswarteschlange: Geben Sie die Zeitdauer (in Sekunden) ein, nach der eine Nachricht in der Verschlüsselungswarteschlange verbleiben kann, bevor sie abgelaufen ist. Sobald eine Nachricht eine Zeitüberschreitung aufweist, sendet die Appliance eine Bounce-Nachricht und sendet eine Benachrichtigung an den Absender.

Verschlüsselungsalgorithmus:

- ARC4. ARC4 ist die häufigste Wahl, es bietet starke Verschlüsselung mit minimalen Entschlüsselungsverzögerungen für Nachrichtenempfänger.
- AES: AES bietet eine stärkere Verschlüsselung, aber die Entschlüsselung dauert auch länger, es führt zu Verzögerungen bei den Empfängern. AES wird in der Regel in Behörden- und Bankenanwendungen verwendet.

Entschlüsselung von Nachrichtenanlagen: Aktivieren oder deaktivieren Sie das Entschlüsselungs-Applet. Nachdem Sie diese Option aktiviert haben, wird der Nachrichtenanhang in der Browserumgebung geöffnet. Wenn Sie diese Option deaktivieren, werden Nachrichtenanhänge auf dem Schlüsselserver entschlüsselt. Standardmäßig ist Java Applet im Umschlag deaktiviert.

Anmerkung: Die am häufigsten verwendeten Browser haben Java Applet aus Sicherheitsgründen deaktiviert.

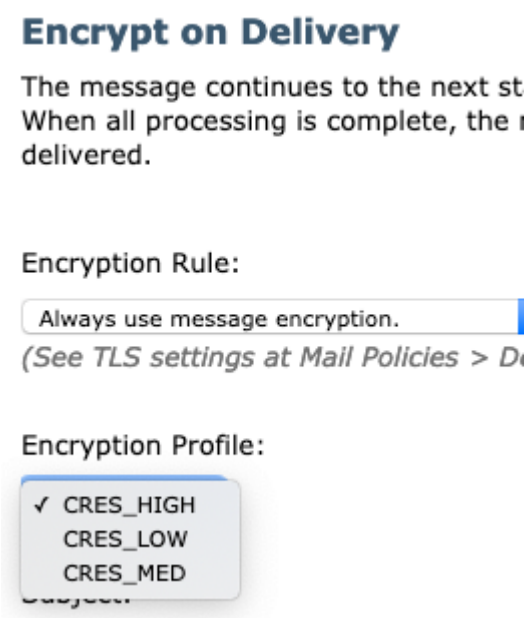
Sobald die Verschlüsselungsprofile erstellt wurden. Stellen Sie sicher, dass sie wie im Bild dargestellt bereitgestellt wird:

Jedes dieser Profile muss über einen Content-Filter zugeordnet werden, damit es angewendet werden kann.

Vorsicht: Wenn das Profil nicht von einem Content-Filter aufgerufen wird, können die Verschlüsselungseinstellungen nicht angewendet werden.

Navigieren Sie von der ESA zu Mail-Policys > Filter für ausgehenden Inhalt > Filter hinzufügen

Sobald die Bedingung für Benutzer, Betreff, Gruppe, Absender usw. innerhalb des Filters konfiguriert wurde, definieren Sie die Verschlüsselungsstufe für den ausgehenden Filter, wie im Bild gezeigt:



Vorsicht: Alle Content-Filter müssen mit Richtlinien für ausgehende E-Mails verknüpft sein, damit sie ordnungsgemäß funktionieren.

Anmerkung: Sie können mehrere Verschlüsselungsprofile für einen gehosteten Schlüsseldienst konfigurieren. Wenn Ihr Unternehmen über mehrere Marken verfügt, können Sie auf diese Weise auf verschiedene Logos verweisen, die auf dem Schlüsselserver für die PXE-Umschläge gespeichert sind.

Konfiguration über CLI

Geben Sie in der ESA-CLI den Befehl encryptionconfig ein:

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service

[]> profiles

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIGH-CRES              Hosted Service         No          Not Provisioned
Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]> new

1. Cisco Registered Envelope Service
2. IronPort Encryption Appliance (in network)
Choose a key service:
[1]>

Enter a name for this encryption profile:
[]> HIGH

Current Cisco Registered Key Service URL: https://res.cisco.com
Do you wish to alter the Cisco Registered Envelope Service URL? [N]> N

1. ARC4
2. AES-192
3. AES-256
Please enter the encryption algorithm to use when encrypting envelopes:
[1]>

1. Use envelope service URL with HTTP (Recommended). Improves performance for opening envelopes.
2. Use the envelope service URL with HTTPS.
3. Specify a separate URL for payload transport.
Configure the Payload Transport URL
[1]>

1. High Security (Recipient must enter a passphrase to open the encrypted message, even if credentials
2. Medium Security (No passphrase entry required if recipient credentials are cached ("Remember Me" sel
3. No Passphrase Required (The recipient does not need a passphrase to open the encrypted message.)
Please enter the envelope security level:
[1]>

Would you like to enable read receipts? [Y]>
```

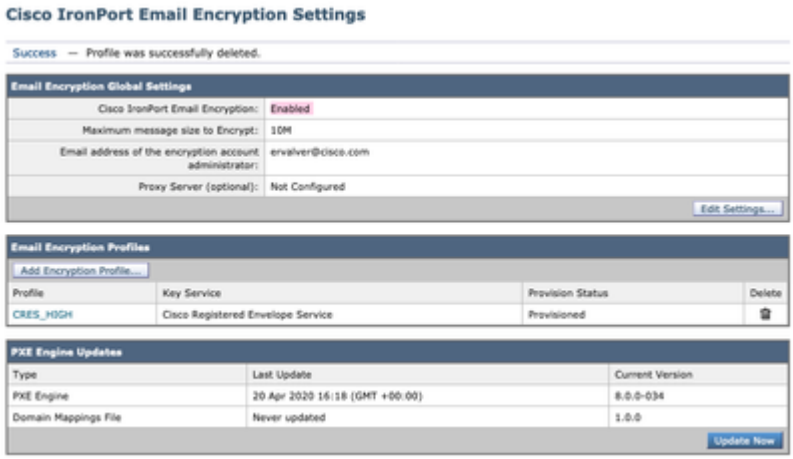
```
Would you like to enable "Secure Reply All"? [N]> y

Would you like to enable "Secure Forward"? [N]> y

Enter a URL to serve as a link for the envelope logo image (may be blank):
[]>

Would you like envelopes to be displayed in a language other than English ? [N]>

Enter the maximum number of seconds for which a message could remain queued waiting to be encrypted. De
[14400]>

Enter the subject to use for failure notifications:
[[ENCRYPTION FAILURE]]>

Please enter file name of the envelope attached to the encryption notification:
[securedoc_${date}T${time}.html]>


A Cisco Registered Envelope Service profile "HIGH" was added.

   1. Commit this configuration change before continuing.
   2. Return to the encryptionconfig menu and select PROVISION to complete
the configuration.

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIGH-CRES            Hosted Service         No          Not Provisioned
LOW-CRES             Hosted Service         No          Not Provisioned

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service

[]> provision
```

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfung über GUI

Navigieren Sie von der ESA zu Security Services > Cisco IronPort Email Encryption, wie in der Abbildung dargestellt:



Anmerkung: Stellen Sie sicher, dass die Verschlüsselung aktiviert und das konfigurierte Profil bereitgestellt ist. wie im Bild dargestellt.

Überprüfung von CLI

Geben Sie in der CLI den Befehl encryptconfig und type profiles ein.

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> profiles

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
CRES_HIGH             Hosted Service         No          Provisioned
```

Anmerkung: Stellen Sie sicher, dass die Verschlüsselung aktiviert und das konfigurierte Profil bereitgestellt ist. wie im Bild dargestellt.

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Navigieren Sie von der ESA zu Systemverwaltung > Feature-Schlüssel.

Überprüfen Sie, ob der Feature-Schlüssel angewendet und aktiviert wurde. Der Schlüssel: Die IronPort-E-Mail-Verschlüsselung muss aktiviert sein.

Navigieren Sie von der ESA zu Security Services > Cisco IronPort Email Encryption.

Überprüfen Sie, ob der Verschlüsselungsdienst ordnungsgemäß aktiviert ist.

Vergewissern Sie sich, dass sich das Verschlüsselungsprofil nicht im Status Nicht bereitgestellt befindet, wie im Bild gezeigt:

Profile	Key Service	Provision Status
HIGH	Cisco Registered Envelope Service	Not Provisioned
LOW	Cisco Registered Envelope Service	Not Provisioned
MEDIUM	Cisco Registered Envelope Service	Not Provisioned

Überprüfen Sie die letzte Aktualisierung des Moduls, wie im Bild gezeigt:

PXE Engine Updates		
Type	Last Update	Current Version
PXE Engine	21 Jan 2020 16:01 (GMT +00:00)	7.2.1-015

Überprüfen Sie in den Details der Nachrichtenverfolgung, ob ein Fehler angezeigt wird.

Häufigste Fehler:

```
5.x.3 - Temporary PXE Encryption failure
```

Lösung: Der Dienst ist derzeit nicht verfügbar oder nicht erreichbar. Überprüfen Sie Verbindungs- und Netzwerkprobleme.

```
5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration issue. Pl
```

Lösung: Dieser Fehler ist verbunden mit:

- Lizenzprobleme. Überprüfen Sie die Feature-Schlüssel.
- Das verwendete Profil wurde nicht bereitgestellt. Identifizieren Sie aus der Nachrichtenverfolgung das Profil, das für Content-Filter und -Bereitstellung konfiguriert wurde.
- Einem Content-Filter ist kein Profil zugeordnet. Manchmal werden die Verschlüsselungsprofile gelöscht, mit anderen Namen geändert usw. Der konfigurierte Content-Filter kann das zugeordnete Profil nicht finden.

```
5.x.3 - PXE Encryption failure. (Error 30 - The message has an invalid "From" address.)
```

```
5.x.3 - PXE Encryption failure. (Error 102 - The message has an invalid "To" address.)
```

Lösung: Regelmäßig wird dieses Problem durch die automatische Eingabe der E-Mail-Adresse des Empfängers durch den internen Absender-Client (z. B. Outlook) verursacht, die eine ungültige "Von"-/"An"-Adresse enthält.

In der Regel wird dies durch Anführungszeichen um die E-Mail-Adresse oder andere unzulässige Zeichen in der E-Mail-Adresse verursacht.

Zugehörige Informationen

- Benutzerhandbuch
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.