Beveiligingsniveaus configureren in het CRES-coderingsprofiel van ESA

Inhoud

Inleiding

In dit document wordt de configuratie beschreven van de CRES-profielen (Registered Envelope Service Encryption) van Cisco binnen de Email Security Appliance (ESA), die gericht zijn op de verschillende toegestane beveiligingsniveaus.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ESA-basisconfiguratie
- Codering op basis van de configuratie van het inhoudsfilter
- Cisco Registered Envelope Service

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het opstellen van het CRES-profiel is een kerntaak voor de activering en het gebruik van de encryptiedienst via het ESA. Voordat u meerdere profielen maakt, moet u ervoor zorgen dat u een volledige account hebt voor een ESA met het maken van een CRES-account.

Er kan meer dan één profiel zijn en elk profiel kan worden geconfigureerd met een ander beveiligingsniveau. Hierdoor kan het netwerk verschillende beveiligingsniveaus handhaven per domein, gebruiker of groep.

Configureren

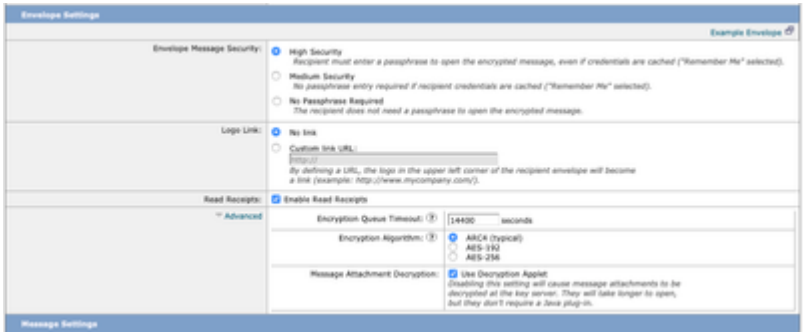
U kunt een coderingsprofiel inschakelen en configureren met de CLI-opdracht coderingsconfiguratie of via Beveiligingsservices > Cisco IronPort Email Encryption in de GUI.

Configuratie vanuit GUI

Navigeer van ESA naar Beveiligingsservices > Cisco IronPort-e-mailcodering > Coderingsprofiel toevoegen.

Er wordt een scherm weergegeven met de instellingen voor het coderingsprofiel. De profielnaam en de rest van de configuratie kunnen worden aangepast en zijn afhankelijk van identificatietags of -methoden van de organisatie.

De configuratie die het beveiligingsniveau per profiel definieert, is Envelope Settings (Envelope-instellingen), zoals wordt weergegeven in de afbeelding:



Opmerking: De profielnaam bevat: "Hoog", "Laag", enz. om overeen te komen met het geconfigureerde beveiligingsniveau of de naam van de groep waaraan het profiel is gekoppeld, voor snelle identificatie bij het maken van inhoudsfilters en verificatie.

De drie door het ESA toegestane beveiligingsniveaus zijn:

- Hoge beveiliging: De ontvanger moet altijd een wachtwoordgroep invoeren om versleutelde

berichten te openen.
- Middelgrote beveiliging: de ontvanger hoeft geen referenties in te voeren om het gecodeerde bericht te openen als de referenties van de ontvanger in de cache zijn opgeslagen.
- Geen wachtwoordzin vereist: dit is het laagste niveau van gecodeerde berichtbeveiliging. De ontvanger hoeft geen wachtwoordzin in te voeren om het gecodeerde bericht te openen. U kunt nog steeds de leesbonnen, Secure Reply All en Secure Message Forwarding-functies inschakelen voor enveloppen die niet met een wachtwoord zijn beveiligd.

U kunt de verschillende beveiligingsniveaus voor deze objecten configureren:

Beveiliging van enveloppen:

- · Hoge veiligheid
- middelzware beveiliging
- Geen wachtwoordgroep vereist

Logo Link: Om gebruikers in staat te stellen de URL van uw organisatie te openen, klikt u op het logo, kunt u een link naar het logo toevoegen. Kies uit de volgende opties:

- Geen link. Een live link wordt niet toegevoegd aan de berichtenenveloppe.
- Aangepaste link-URL. Voer de URL in om een live link aan de berichtenenveloppe toe te voegen.

Ontvangstbewijzen lezen: Als u deze optie inschakelt, ontvangt de afzender een ontvangstbewijs wanneer ontvangers de beveiligde envelop openen. Dit is een optionele selectie.

Gevorderd:

Time-out voor coderingswachtrij: Geef de tijdsduur (in seconden) op dat een bericht in de coderingswachtrij kan staan voordat het uitvalt. Zodra een bericht is verlopen, weerkaatst het toestel het bericht en stuurt het een melding naar de afzender.

Coderingsalgoritme:

- ARC4. ARC4 is de meest voorkomende keuze, het biedt sterke encryptie met minimale decoderingsvertragingen voor ontvangers van berichten.
- AES. AES zorgt voor een sterkere encryptie, maar het duurt ook langer om te decoderen, het introduceert vertragingen voor ontvangers. AES wordt meestal gebruikt in overheids- en banktoepassingen.

Berichtbijlage decoderen: de decodering-applet in- of uitschakelen. Nadat u deze optie hebt ingeschakeld, wordt de bijlage met het bericht geopend in de browseromgeving. Nadat u deze optie hebt uitgeschakeld, zorgt het ervoor dat de berichtbijlagen worden gedecodeerd op de sleutelserver. Standaard is Java Applet uitgeschakeld in de envelop.

Opmerking: De meest gebruikte browsers hebben Java Applet uitgeschakeld vanwege beveiligingsredenen.

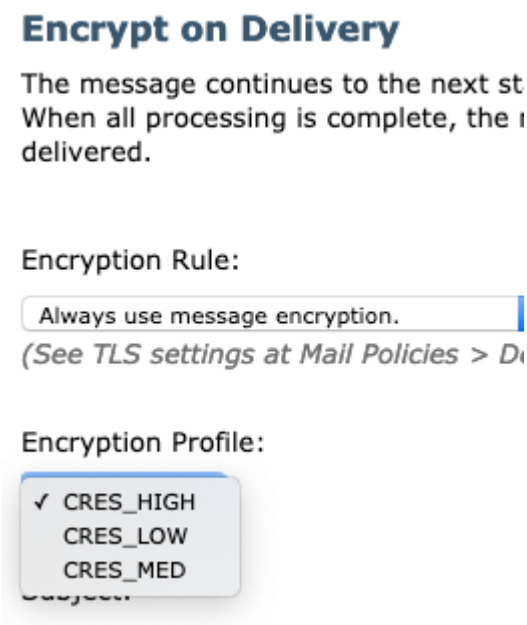
Nadat de coderingsprofielen zijn gemaakt. Zorg ervoor dat het wordt geleverd, zoals weergegeven in de afbeelding:

Elk van deze profielen moet worden gekoppeld via een inhoudsfilter om te kunnen worden toegepast.

⚠ Let op: als het profiel niet wordt aangeroepen door een inhoudsfilter, kunnen de coderingsinstellingen niet worden toegepast.

Navigeer vanuit ESA naar E-mailbeleid > Filters voor uitgaande inhoud > Een filter toevoegen

Nadat de conditie van gebruikers, onderwerp, groep, afzender, enz. in het filter is geconfigureerd, definieert u het coderingsniveau voor het uitgaande filter, zoals in de afbeelding wordt weergegeven:



⚠ Let op: Alle inhoudsfilters moeten worden gekoppeld aan het beleid voor uitgaande e-mail om goed te kunnen functioneren.

✎ Opmerking: u kunt meerdere coderingsprofielen configureren voor een gehoste sleutelservice. Als uw organisatie meerdere merken heeft, kunt u hiermee verwijzen naar verschillende logo's die zijn opgeslagen op de sleutelserver voor de PXE-enveloppen.

Configuratie vanuit CLI

Van ESA CLI type encryption config opdracht:

```
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):
[]>
```

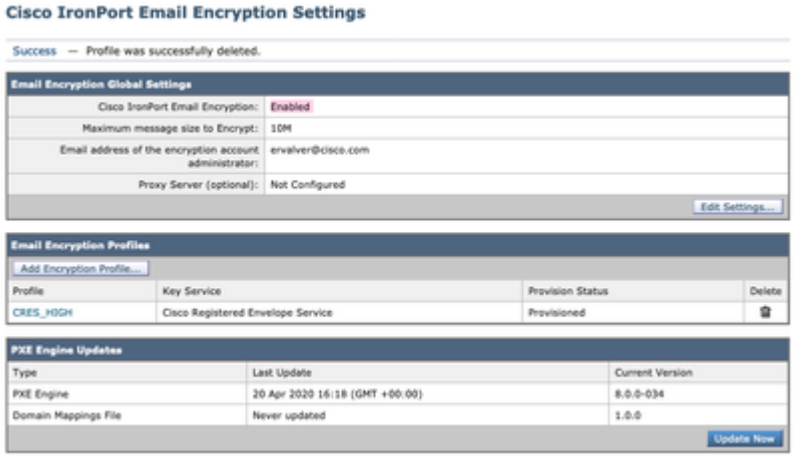
```
Would you like envelopes to be displayed in a language other than English ? [N]>

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
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Verificatie via GUI

Navigeer van ESA naar Beveiligingsservices > Cisco IronPort-e-mailcodering, zoals weergegeven in de afbeelding:



Opmerking: zorg ervoor dat de codering is ingeschakeld en dat het profiel is geconfigureerd. Zoals te zien is in de afbeelding.

Verificatie van CLI

Typ vanuit CLI de opdracht encryptconfig en typeprofielen.

```
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
```

Opmerking: zorg ervoor dat de codering is ingeschakeld en dat het profiel is geconfigureerd. Zoals te zien is in de afbeelding.

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Navigeer van ESA naar Systeembeheer > functietoetsen

Controleer of de functietoets is toegepast en actief is. De sleutel: IronPort e-mailcodering moet

actief zijn.

Navigeer van ESA naar Beveiligingsservices > Cisco IronPort-e-mailcodering

Controleer of de coderingsservice goed is ingeschakeld.

Controleer of het coderingsprofiel niet de status Niet geleverd heeft, zoals in de afbeelding wordt getoond:

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

Verifieer de laatste update van de engine, zoals weergegeven in de afbeelding:

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

Controleer in de details voor het bijhouden van berichten of er een fout wordt weergegeven.

Meest voorkomende fouten:

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

Oplossing: de service is momenteel niet beschikbaar of onbereikbaar. Controleer connectiviteits- en netwerkproblemen.

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

Oplossing: deze fout is gekoppeld aan:

- Licentieproblemen. Controleer de functietoetsen
- Het gebruikte profiel is niet voorzien. Identificeer aan de hand van het volgen van berichten het profiel dat is geconfigureerd voor inhoudfilter en -voorziening
- Er is geen profiel gekoppeld aan een inhoudsfilter. Soms worden de versleutelingsprofielen verwijderd, gewijzigd met verschillende namen, enz. Het geconfigureerde inhoudsfilter kan het gekoppelde profiel niet vinden

```
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.)
```

Oplossing: regelmatig wordt dit probleem veroorzaakt door de automatische invulling van het e-mailadres van de interne afzender (bijv. Outlook) van het e-mailadres van de ontvanger met een ongeldig "Van"/"Aan"-adres.

Meestal wordt dit veroorzaakt door aanhalingstekens rond het e-mailadres of andere illegale tekens in het e-mailadres.

Gerelateerde informatie

- Handleiding voor eindgebruikers
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.