ESA CRES暗号化プロファイルのセキュリティ レベルの設定

内容

概要 <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>設定</u> <u>GUIからの設定</u> <u>GUIからの設定</u> <u>確認</u> <u>GUIからの検証</u> <u>CLIからの検証</u> <u>トラブルシュート</u> <u>最も一般的なエラー:</u> 関連情報

概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)内のCisco Registered Envelope Service Encryption(CRES)プロファイルの設定について、許可されるさまざまなセキュ リティレベルに重点を置いて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ESAの基本設定
- コンテンツフィルタ設定に基づく暗号化
- Cisco Registered Envelope Service

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

CRESプロファイルの作成は、ESAを介して暗号化サービスをアクティブ化および使用するため のコアタスクです。複数のプロファイルを作成する前に、CRESアカウントを作成してESAに対 して完全なアカウントがプロビジョニングされていることを確認します。

複数のプロファイルを設定でき、各プロファイルに異なるセキュリティレベルを設定できます。 これにより、ネットワークはドメイン、ユーザ、またはグループごとに異なるセキュリティレベ ルを維持できます。

設定

暗号化プロファイルを有効および設定するには、encryptionconfig CLIコマンドを使用するか、 GUIで[Security Services] > [Cisco IronPort Email Encryption]を選択します。

GUI からの設定

ESAから[Security Services] > [Cisco IronPort Email Encryption] > [Add Encryption Profile]に移動 します。

[Encryption Profile Settings]が表示されます。プロファイル名とその他の設定はカスタマイズ可能 で、組織の識別タグまたは方法によって異なります。

プロファイルごとにセキュリティレベルを定義する設定は、図に示すように[Envelope Settings]です。

		Exemple Envelope C
Envelope Heasope Security:	 Neph Security Recipient must enter a paraphrane to Security Reparaphrase worky required if notice No Perspheres Required The recipient date not used a paraphra 	gan the encrypted message, even if codestials are cached ("Remember Me" saincord). en contextual are cached ("Norwether Me" sanctor). See to apen the encrypted message.
Loge Link:	No link Define Defin	
Read Receipts:	2 C Dreble Raad Ressipts	
* Abascad	Chargeton Queue Timeset: @	14400 words
	Excellence of a state	Also 190 Also 190 Also 256
	Nonsee Attachment Decryption	Use becayption: Appliet Oraching thes setting will cause measure establishments to be decrypted at the key server. They will tasks longer to open, but they don't reactive a long obg-in.

注:プロファイル名には次のものが含まれることが推奨されます。コンテンツフィルタの作成と検証を迅速に識別するために、設定されたセキュリティレベルまたはプロファイルが関連付けられているグループの名前と一致させるため、「高」、「低」など。

ESAで許可されるセキュリティの3つのレベルは次のとおりです。

- 高セキュリティ:暗号化されたメッセージを開くには、受信者は常にパスフレーズを入力する必要があります。
- ・中セキュリティ:受信者の資格情報がキャッシュされている場合、受信者は資格情報を入力して暗号化されたメッセージを開く必要はありません。
- •パスフレーズは不要:これは、暗号化されたメッセージセキュリティの最低レベルです。受

信者は、暗号化されたメッセージを開くためにパスフレーズを入力する必要はありません。 パスフレーズで保護されていないエンベロープに対しては、開封確認、全員への返信、およ びメッセージ転送機能を有効にできます。

次のオブジェクトに対して、さまざまなレベルのセキュリティを設定できます。

エンベロープメッセージセキュリティ:

・高セキュリティ

- 中程度のセキュリティ
- パスフレーズは不要

ロゴリンク:ユーザが組織のURLを開けるようにするには、ロゴをクリックし、ロゴへのリンク を追加します。次のオプションから選択します。

- リンクなし、ライブリンクはメッセージエンベロープに追加されません。
- カスタムリンクURL。URLを入力して、メッセージエンベロープにライブリンクを追加します。

開封確認:このオプションを有効にすると、受信者がセキュリティで保護されたエンベロープを 開封したときに、送信者は受信確認を受け取ります。これはオプションの選択です。

[Advanced] :

暗号化キューのタイムアウト:メッセージがタイムアウトになるまでの時間(秒)を入力します 。メッセージがタイムアウトすると、アプライアンスはメッセージをバウンスし、送信者に通知 を送信します。

Encryption Algorithm(暗号化アルゴリズム):

- ARC4. ARC4は最も一般的な選択肢で、メッセージ受信者の復号遅延を最小限に抑えて強力 な暗号化を提供します。
- AES.AESは、より強力な暗号化を提供しますが、復号化に時間がかかり、受信者に遅延が生じます。AESは通常、政府および銀行のアプリケーションで使用されます。

メッセージ添付の復号化:復号化アプレットを有効または無効にします。このオプションを有効に すると、メッセージの添付ファイルがブラウザ環境で開かれます。このオプションを無効にする と、メッセージの添付ファイルがキーサーバで復号化されます。デフォルトでは、エンベロープ ではJavaアプレットは無効になっています。

注:セキュリティ上の理由により、最も使用されているブラウザではJavaアプレットが無 効になっています。

暗号化プロファイルが作成されたら、 イメージに示すように、プロビジョニングされていること を確認します。

Profile	Key Service	Provision Status
CRES_HIGH	Cisco Registered Envelope Service	Provisioned Re-provision

これらのプロファイルを適用するには、コンテンツフィルタを介して関連付ける必要があります 。

注意:コンテンツフィルタによってプロファイルが呼び出されない場合、暗号化設定は適用

ESAから、[Mail Policies] > [Outgoing Content Filters] > [Add a filter]に移動します

ユーザ、件名、グループ、送信者などの条件がフィルタ内で設定されたら、次の図に示すように 、発信フィルタの暗号化レベルを定義します。

Encrypt on Delivery

The message continues to the next st When all processing is complete, the i delivered.

Encryption Rule:

Always use message encryption. (See TLS settings at Mail Policies > De

Encryption Profile:

✓ CRES_HIGH CRES_LOW CRES_MED

> **注意**:正常に機能するには、すべてのコンテンツフィルタを発信メールポリシーに関連付け る必要があります。

> 注:ホステッドキーサービスに複数の暗号化プロファイルを設定できます。組織に複数のブ ランドがある場合は、PXEエンベロープのキーサーバに保存されている別のロゴを参照でき ます。

CLI からの設定

ESA CLIでencryptionconfigコマンドを入力します。

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

Proxy: Not Configured

Profile Name Key Service Proxied Provision Status _____ _____ _____ _____ Hosted Service No HIGH-CRES 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 are cached ("Remember Me" selected).) 2. Medium Security (No passphrase entry required if recipient credentials are cached ("Remember Me" selected).) 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. Delays could be caused by key server outages or resource limitations: [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.

 Commit this configuration change before continuing.
 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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

GUIからの検証

図に示すように、ESAから[Security Services] > [Cisco IronPort Email Encryption]に移動します。

Cisco IronPort Email Encryption Settings

Ca	ce IrenPert Email Encryption:	Enabled			
Haxin	rum message size to Encrypt:	104			
Email addr	ess of the encryption account administrator:	ervelver@class.com			
	Proxy Server (optional):	Not Configured			
				Det	Settings
sail Encrystian I	hafiles				
all Encryption P	hofiles				
all Encryption P dd Encryption Pe	volies				
nail Encryption P Idd Encryption Pe offic	Key Service		Provision St.	atua	Delete
vall Encryption P Idd Encryption Pro office ES_HIGOH	Nofiles Stig Key Service Cace Registered Em	velope Service	Provision St. Provisioned	aha	Delete
nali Encryption P Idd Encryption Pr Min IES_MIGH	Nofiles Star Key Service Caco Registered Em	velope Service	Provision St. Provisioned	etus	Delete
all Encryption P Idd Encryption Pr Ifin E5_HIGH E Engline Update	Nofiles Star Key Service Cisco Registered Dr	velope Service	Provision St. Provisioned	atus	Dalata B
all Encryption A dd Encryption Av Alla E5_1024 E Engine Update M	Nofiles Stig Key Service Cisco Registered En es	velope Service est Update	Provision Sk Provisioned	etus Current Version	Delete
sail Encryption P Idd Encryption Pr offic IES_HIGH IE Engline Update PR E Engline	Nofiles Slip Key Service Cisco Registered Em es La 26	velope Service est Update 0 Apr 2020 16:18 (GMT +00:00)	Provision Sk Provisioned	current Version 8.0.0-034	Delete B

注:暗号化が有効になっており、設定されているプロファイルがプロビジョニングされてい ることを確認します。図に示すように。

CLIからの検証

CLIからencryptconfigとtype profilesコマンドを入力します。

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

注:暗号化が有効になっており、設定されているプロファイルがプロビジョニングされていることを確認します。図に示すように。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ESAから、[System Administration] > [feature keys]に移動します

機能キーが適用され、アクティブであることを確認します。キー:IronPort Email Encryptionがア クティブになっている必要があります。

ESAから[Security Services] > [Cisco IronPort Email Encryption]に移動します

暗号化サービスが正しく有効になっていることを確認します。

次の図に示すように、暗号化プロファイルが[Not Provisioned]ステータスになっていないことを 確認します。

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

図に示すように、エンジンの最後のアップデートを確認します。

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

[Message Tracking details]で、エラーが表示されているかどうかを確認します。

最も一般的なエラー:

5.x.3 - Temporary PXE Encryption failure

ソリューション:サービスは現在利用できないか、到達不能です。接続とネットワークの問題を 確認します。

5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration issue. Please contact your administrator

ソリューション:このエラーは次のエラーに関連しています。

- ライセンスの問題機能キーを確認してください
- ・使用されたプロファイルはプロビジョニングされません。コンテンツフィルタおよびプロビジョニングで設定されたプロファイルをメッセージトラッキングから特定する
- コンテンツフィルタに関連付けられたプロファイルはありません。暗号化プロファイルが削除されたり、異なる名前で変更されたりすることがあります。設定されたコンテンツフィルタで、関連付けられたプロファイルが見つかりません

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.) ソリューション:定期的に、この問題は、内部送信者の電子メールクライアント(Outlookなど)が、無効な「From」/「To」アドレスを含む受信者の電子メールアドレスを自動的に入力することによって発生します。

これは通常、電子メールアドレスの引用符や、電子メールアドレスの他の不正な文字が原因で発 生します。

関連情報

- ・<u>CRES管理ガイド</u>
- ・<u>エンドユーザガイド</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>