コンテンツ フィルタおよび DLP で暗号化をバイパスするにはどうすればいいですか。

目次

概要

このドキュメントでは、コンテンツ フィルタと DLP で暗号化をバイパスする方法について説明します。

コンテンツ フィルタおよび DLP で暗号化をバイパスするにはどうすればいいですか。

Cisco E メール セキュリティ アプライアンス (ESA) には、件名フィールドと DLP ポリシーに基づいて暗号化する必要のある環境が存在します。 メッセージの両方の暗号化トリガーをバイパスする必要があるインスタンスがあります。

1. 暗号化を行うフィルタより前に出力コンテンツ フィルタを作成します。 GUI で [Mail Policy] > [Outgoing Content Filters] > [Add Filters...] を選択します。
2. 条件は、件名で「[NOENCRYPT]」というキーワードを検索することです。 [Add Condition...] を選択し、[Subject Header] を選択して、[Contains] に「\[NOENCRYPT\]」と指定します。 ((「\」は「[」をリテラルに使用するためのものであるため、必ず入力してください。)
3. 最初のアクションは「メッセージタグの追加」であり、その値は「NOENCRYPTION」です。 ((これは DLP ポリシーの手順で後ほど使用されます。)
4. 最後のアクションは「残りのコンテンツ フィルタのスキップ (最終アクション) 」です。 ((このフィルタは順序リストで最後から 2 番目、暗号化フィルタは順序リストの最後にある必要があります。) つまり、次のようになります。

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	Subject Header	subject == "\\[NOENCRYPT\\]"	🗑

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Message Tag	tag-message ("NOENCRYPTION")	🗑
2	Skip Remaining Content Filters (Final Action)	skip-filters()	🗑

5. この時点で変更を送信し、保存します。
6. GUI で [Mail Policies] > [Outgoing Mail Policies] を選択し、コンテンツ フィルタをクリック

し（無効であった場合は有効にして）、新しいコンテンツ フィルタにチェックマークを付けて有効にします。
7. GUI で [Mail Policies] > [DLP Policy Manager] を選択し、暗号化を行う既存の DLP ポリシーをクリックします。
8. [Filter Message Tags] セクションが表示されるまで下にスクロールし、フィールドに NOENCRYPTION と入力し、その横にあるドロップダウンから [absent] を選択します。（つまり、この値が存在しない場合は暗号化を実行し、存在する場合は暗号化をスキップします。）
9. 変更を送信し、確定します。

関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems