反スパム、アンチウィルス、Graymail および発生フィルタ用の最良の方法 ガイド

目次

概要

メールを通して組織によって直面される大部分の脅威、不正侵入および迷惑はスパム、malware および混ぜられた不正侵入の形になります。 組織を入力する前に Cisco の E メール セキュリティ アプライアンス（ESA）はゲートウェイでこれらの脅威を断ち切るために複数の異なるテクノロジおよび機能が含まれています。 この資料は受信および送信 メール フローの反スパム、Graymail および発生フィルタをアンチウィルス、設定するために最良の方法アプローチを記述したものです。

スパム対策

反スパム 保護によってはスパムを含む既知脅威の全域が、phishing およびゾンビ不正侵入、またハードに検出 少量、「419"のような短命のメール脅威詐欺当たります。 さらに、反スパム 保護はダウンロード URL か実行可能モジュールによって悪意のあるコンテンツを配信するスパム不正侵入のような新しく、展開混ぜられた脅威を識別します。

Cisco E メール セキュリティは次の反スパム ソリューションを提供します:

- IronPort 反スパム フィルタリング（IPAS）
- Cisco インテリジェント な複数のスキャン フィルタリング（IMS）

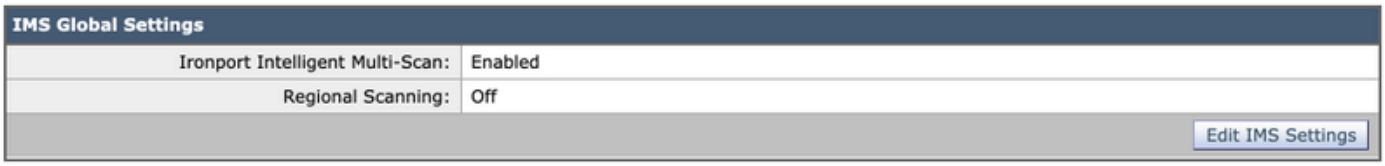
ESA の両方のソリューションを認可し、有効に することができましたり特定のメール ポリシーでしか 1 つを使用できません。 この最良の方法 資料が、私達 IMS 機能を使用する行っているの為。

フィーチャーキーを確認して下さい

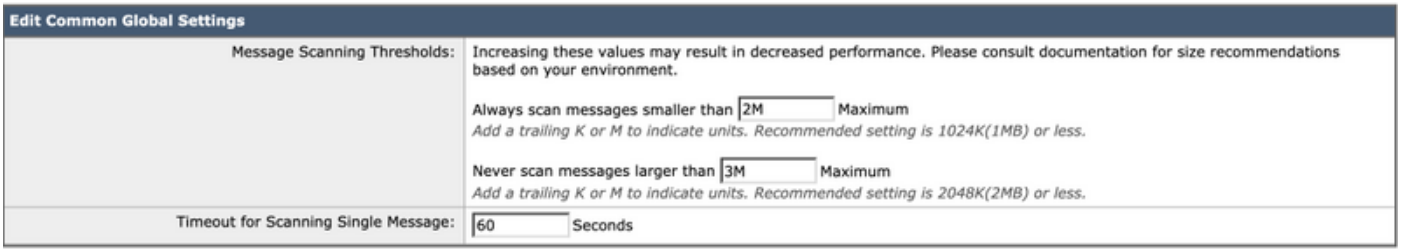
- ESA で、**システム 管理 > フィーチャーキー**にナビゲート して下さい
- インテリジェント な複数のスキャン ライセンスを探し、確かめて下さいアクティブであることを。

インテリジェント な複数のスキャン (IMS) をグローバルに 有効に して下さい

- ESA で、**セキュリティ サービス > IMS および Graymail** にナビゲート して下さい
- **IMS グローバルな設定の Enablebutton をクリックして下さい:**



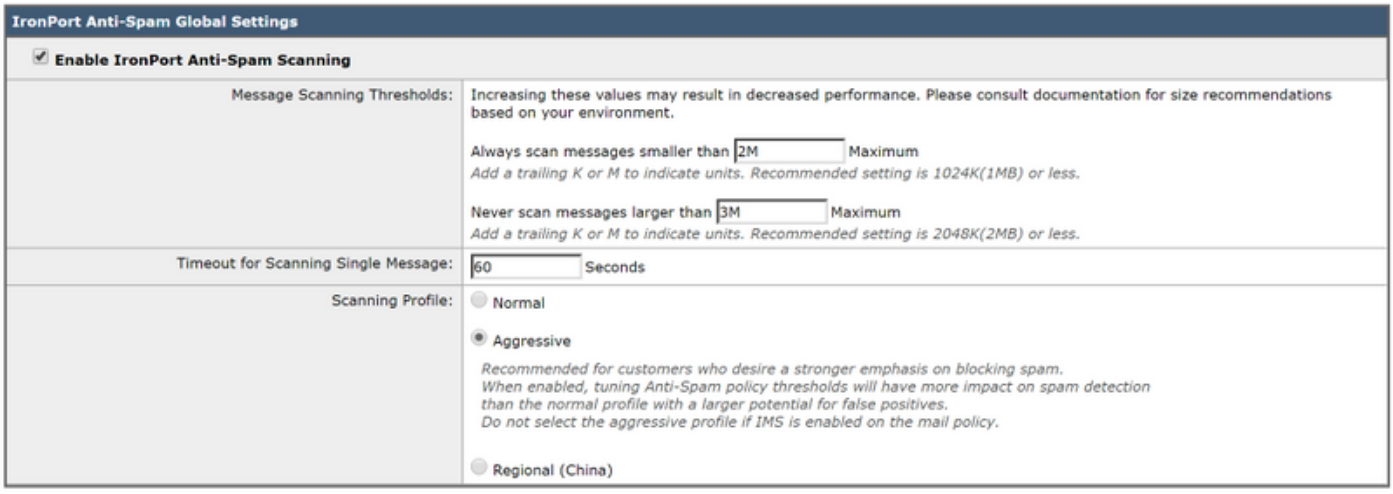
- **よくあるグローバルな設定を探し、グローバルな設定を『Edit』 をクリック して下さい**
- 複数の設定を行うことができます。 推奨 設定は下記のようにイメージで示されています:



- **Submitand を保存します変更を**クリックして下さい。

IMS ライセンス サブスクリプションを持たなければ:

- **セキュリティ サービス > IronPort 反スパムへのナビゲート**
- **IronPort 反スパム 概要の Enablebutton をクリックして下さい**
- [グローバル設定の編集 (Edit **Global Settings**)] をクリックします
- 複数の設定を行うことができます。 推奨 設定は下記のようにイメージで示されています:



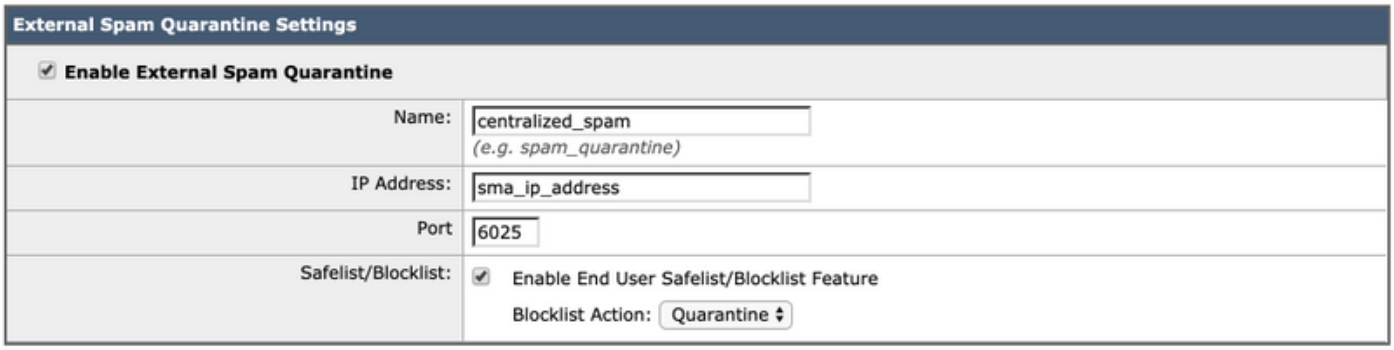
- Cisco はブロッキング スパムの強い重点を望む顧客向けに**積極的な**スキャン プロファイルを

選択することを推奨します。
- **Submitand を保存します変更を**クリックして下さい

中央集中型スパム検疫を有効に して下さい

反スパムに検疫するために送信 される オプションがあるのでスパム検疫が設定されるようにすることは重要です:

- **セキュリティ サービス > スパム検疫**へのナビゲート
- **Configurebutton をクリックして次のページに連れて行きます。**
- **enablebox のチェックによって検疫を有効に し、SMANAMEAND IP アドレス**で byfilling SecurityManagement アプライアンス（SMA）で中心になるべき検疫を指すことができます。 推奨 設定は下記のように示されています:



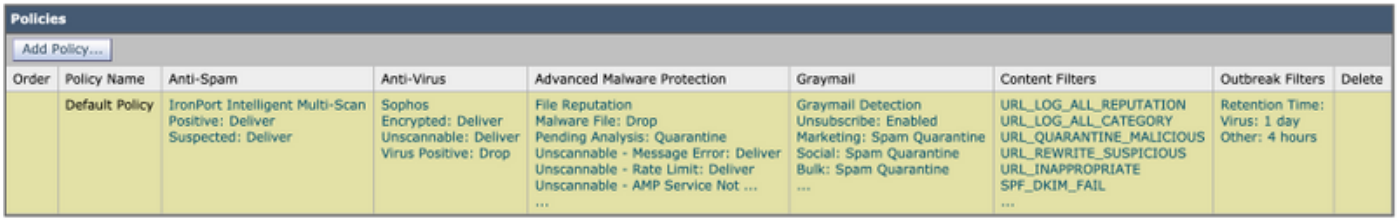
- **Submitand を保存します変更を**クリックして下さい

設定および中央集中型検疫に関する詳細については、最良の方法 資料を参照して下さい:
[ESA からの SMA への中央集中型ポリシーのための最良の方法、ウイルスおよび発生検疫セットアップおよび移行]

ポリシーの設定反スパム

インテリジェント な複数のスキャンがグローバルに設定されたら、今ポリシーを郵送するためにインテリジェント な複数のスキャンを適用できます:

- **ポリシー > 着信メール ポリシーを郵送する**ナビゲート
- 着信メール ポリシーは IronPort 反スパム設定をデフォルトで使用します。
- **反スパム**の下のブルー リンクをクリックすることはその特定のポリシーがカスタマイズされた反スパム設定を使用することができるように可能にします。
- あなたの下でカスタマイズされた反スパム設定を使用してデフォルトポリシーを示す例を参照します:

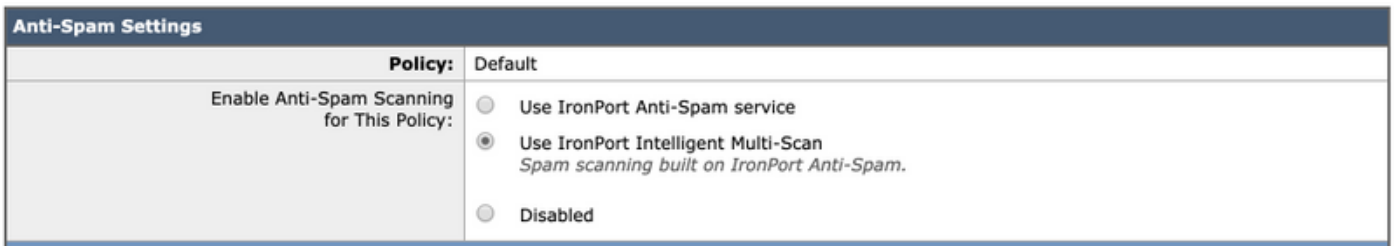


カスタマイズしたいポリシーのための反**スパム**の下のブルー リンクのクリックによる着信メールポリシーのカスタマイズ反スパム設定。

このポリシーのために有効に したい反スパム スキャン オプションを選択できます。

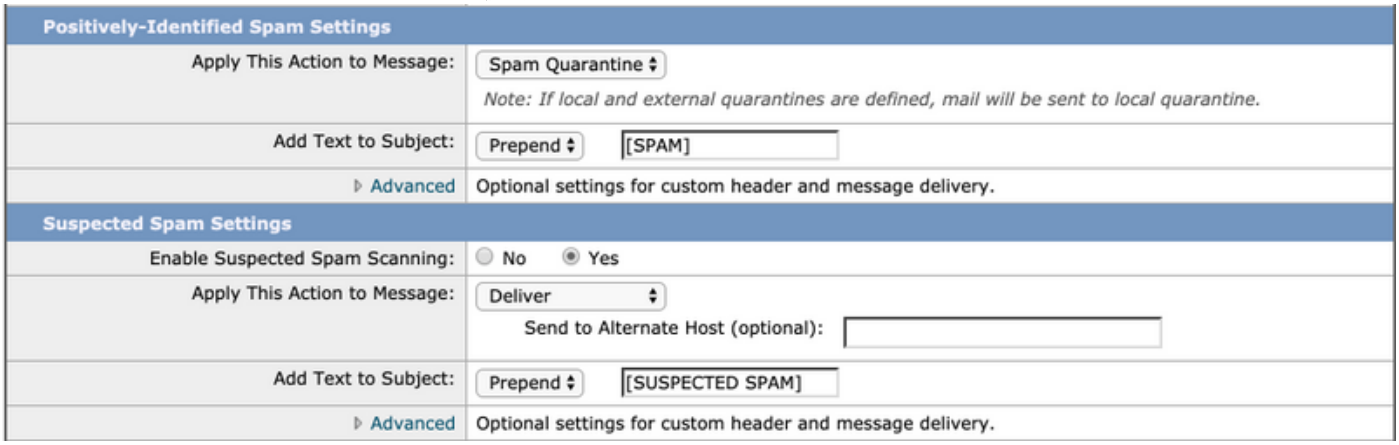
- この最良の方法 資料の目的で、使用 **IronPort インテリジェント な**複数のスキャンの隣で

Radio ボタンをクリックして下さい:

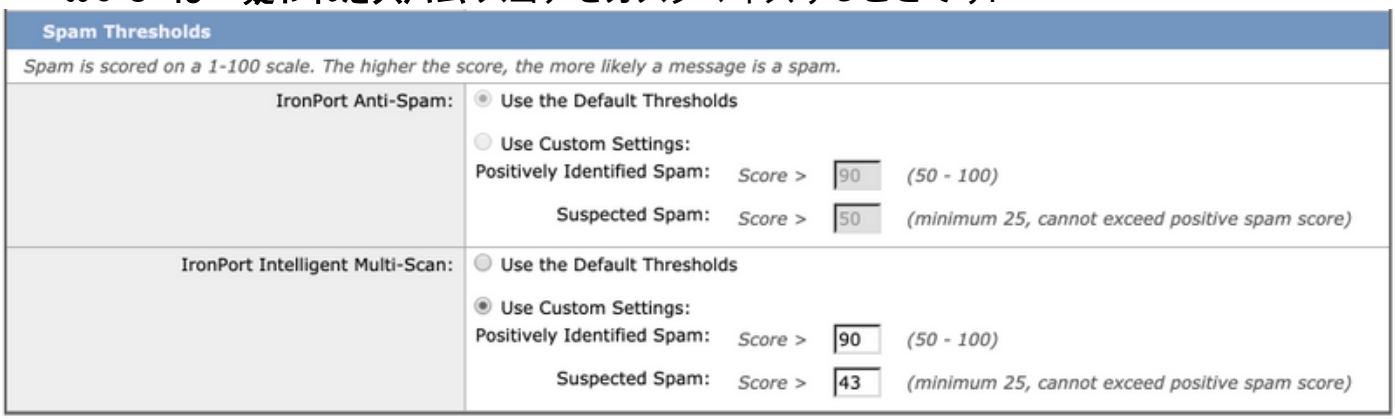


次の 2 つのセクションは肯定的**識別されたスパム設定**および**疑われたスパム設定が**含まれています:

- 推奨される最良の方法はサブジェクトに追加される付加されたテキスト**[スパム]**で肯定的**識別スパム**設定の**検疫**操作を設定することです;
- 付加されたテキスト**[疑われたスパム]**が付いている **Suspected スパム設定**のための操作がサブジェクトに追加したように**渡すために**適用して下さい:



- **スパム しきい値設定は**変更することができ推奨 設定は 90 へ肯定的**識別されたスパム** スコアおよび 43 へ**疑われたスパム** スコアをカスタマイズすることです:



- **Submitand を保存します変更を**クリックして下さい

ウイルス対策

アンチウィルス 保護は 2 つのサード パーティ エンジンを通して– Sophos および McAfee 提供されます。 これらのエンジンはすべての既知悪意のある脅威を、設定されるようにそれらをきれいにするか、または検疫する廃棄フィルタリングします。

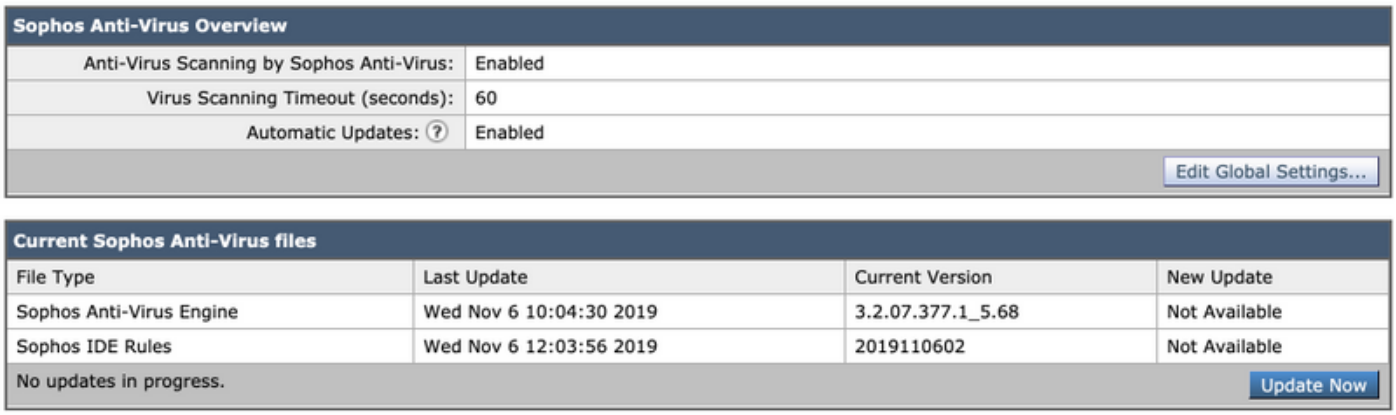
フィーチャーキーを確認して下さい

フィーチャーキーが両方ともおよびアクティブ 有効に なることを確認するため:

- **システム 管理 > フィーチャーキー**に行って下さい
- **Sophos がアンチウィルス**および **McAfee** ライセンス アクティブであることを確かめて下さい。

アンチウィルス スキャンを有効に して下さい

- **セキュリティ サービス**へのナビゲート > **アンチウィルス- Sophos**
- **Enablebutton をクリックして下さい。**
- **自動更新が有効に なり、Sophos アンチウィルス ファイル アップデートがうまく働いていることを確かめて下さい。 必要ならば、ファイル アップデートをすぐに始めるために『 Update now』 をクリック して下さい:**



- **Submitand を保存します変更を**クリックして下さい。

McAfee ライセンスが同様にアクティブである場合、> **アンチウィルス- McAfee はセキュリティ サービス**にナビゲート します

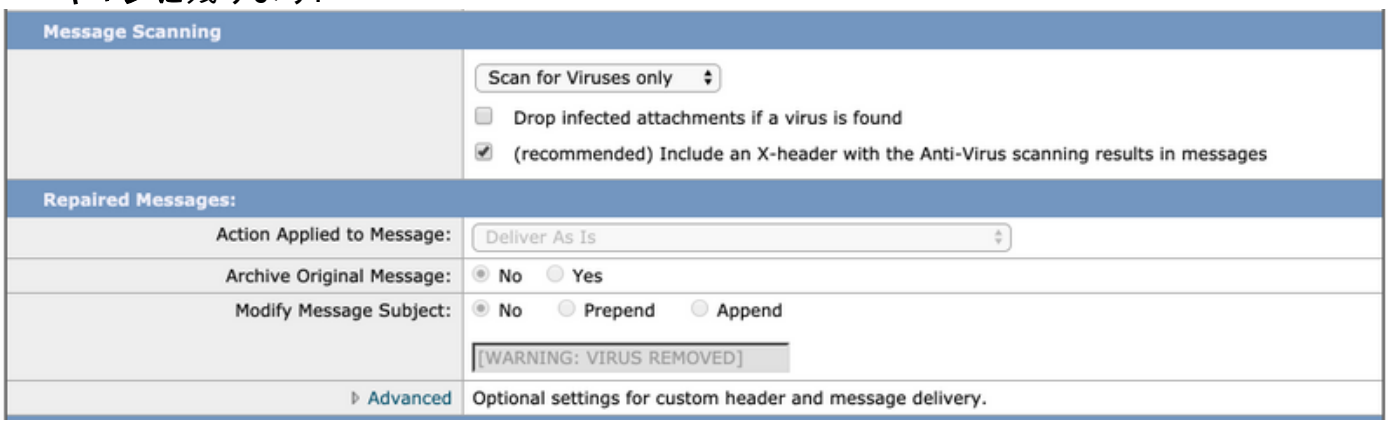
- **Enablebutton をクリックして下さい。**
- **自動更新が有効に なり、McAfee アンチウィルス ファイル アップデートがうまく働いていることを確かめて下さい。 必要ならば、ファイル アップデートをすぐに始めるために『 Update now』 をクリック して下さい。**
- **Submitand を保存します変更を**クリックして下さい

メール ポリシーのアンチウィルスを設定して下さい

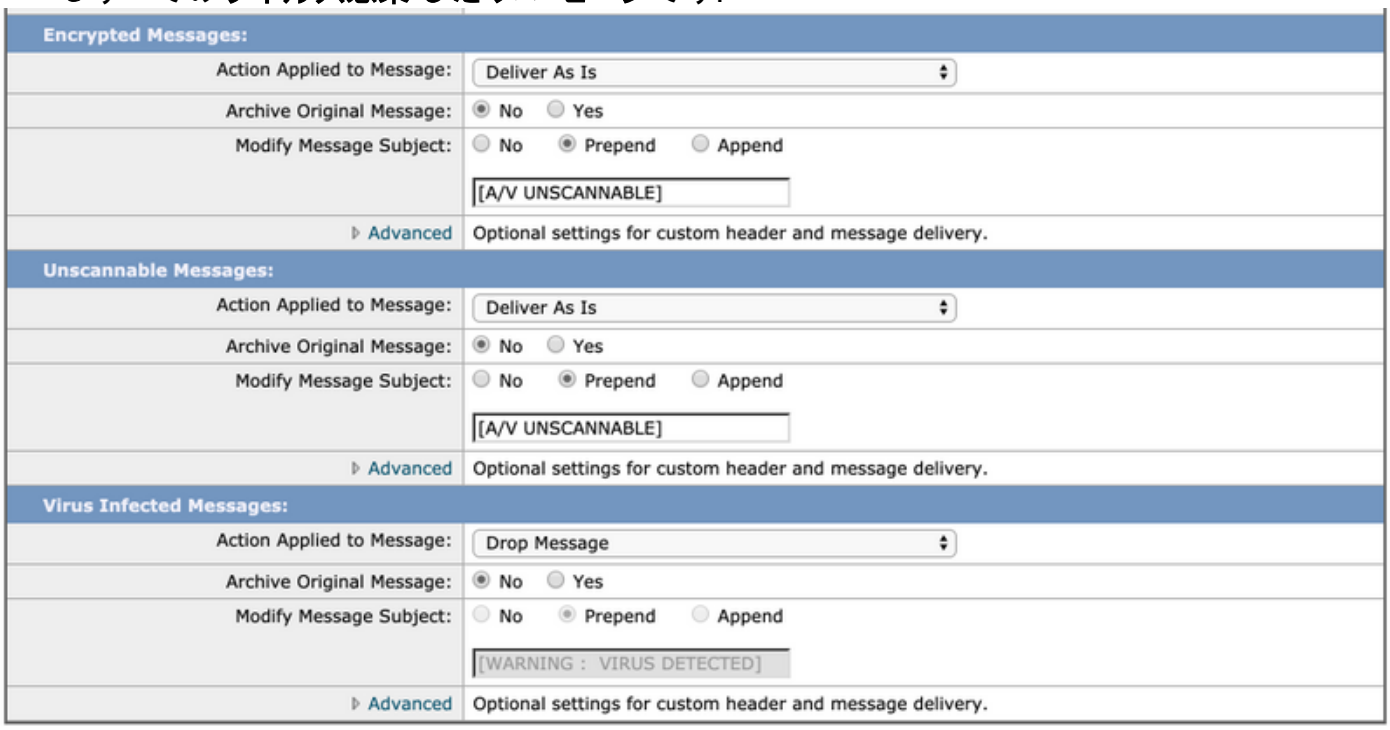
着信メール ポリシーで、以下は推奨されます:

- **ポリシー > 着信メール ポリシーを郵送する**ナビゲート
- カスタマイズしたいポリシーのためのアンチウィルスの下のブルー リンクのクリックによる着信メール ポリシーのカスタマイズ **アンチウィルス**設定。
- このポリシーのために有効に したいアンチウィルス スキャン オプションを選択できます。
- この最良の方法 資料の目的で、**アンチウィルス McAfee** および **Sophos を**両方選択して下さい:

- ファイルを修理するように試みません従ってメッセージ スキャンは**ウイルスのためのただスキャンに**残ります:



- **暗号化された**および **Unscannable メッセージ**のための推奨 処置は注意のための修正された件名との**現状のまま渡すこと**です。
- ウイルス対策のための推奨されるポリシーは下記のようにイメージに示すように**ドロップする**すべての**ウイルス感染 した メッセージ**です:



- **Submitand を保存します変更を**クリックして下さい

同じようなポリシーは発信 メール ポリシーのためにが推奨されます、送信 メールの件名を修正することを推奨しません。

グレイメール

E メール セキュリティ アプライアンスの graymail マネジメントソリューションは 2 つのコンポーネントで構成します: 統合された graymail スキャン エンジンおよびクラウド ベースはサービスの定期講読を解除します。 graymail マネジメントソリューションは組織が統合された graymail エンジンを使用して graymail を識別するようにし、適切なポリシー制御を加え、不必要なメッセージのを使用して定期講読を解除するためにエンドユーザ用の容易なメカニズムを提供することはサービスの定期講読を解除します。

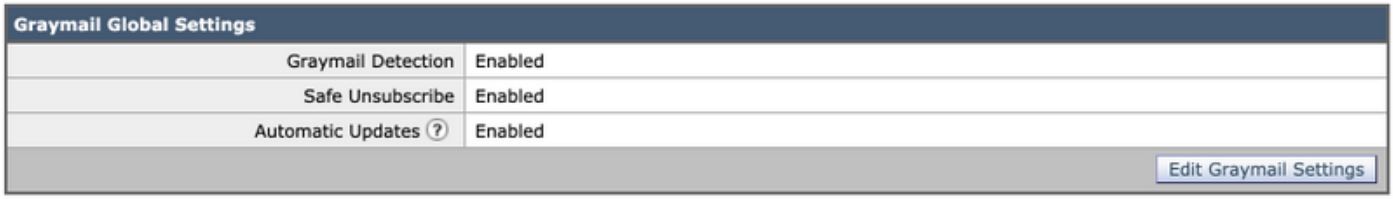
Graymail カテゴリーはマーケティング メール、社会的ネットワーク メールおよびバルク メールが含まれています。 詳細オプションはカスタム ヘッダーを付加すること、代替ホストへの送信およびメッセージをアーカイブすることが含まれています。 この最良の方法に関しては、Graymail のセーフを定期講読を解除しますデフォルト メール ポリシーのための機能の有効に します。

フィーチャーキーを確認して下さい

- ESA で、**システム 管理 > フィーチャーキー**にナビゲート して下さい
- **Graymail 安全な Unsubscription を**探し、確かめて下さいアクティブであることを。

Graymail を有効に すればセーフはサービスの定期講読を解除します

- **セキュリティ サービス** > IMS への ESA、ナビゲート**および Graymail**
- **Graymail グローバルな設定の編集 Graymail Settingsbutton をクリックして下さい**
- 選択して下さいすべてのオプション- **Graymail 検知を有効にして下さい、イネーブル セーフは自動更新の定期講読を解除し、有効に します**:



- **Submitand を保存します変更を**クリックして下さい

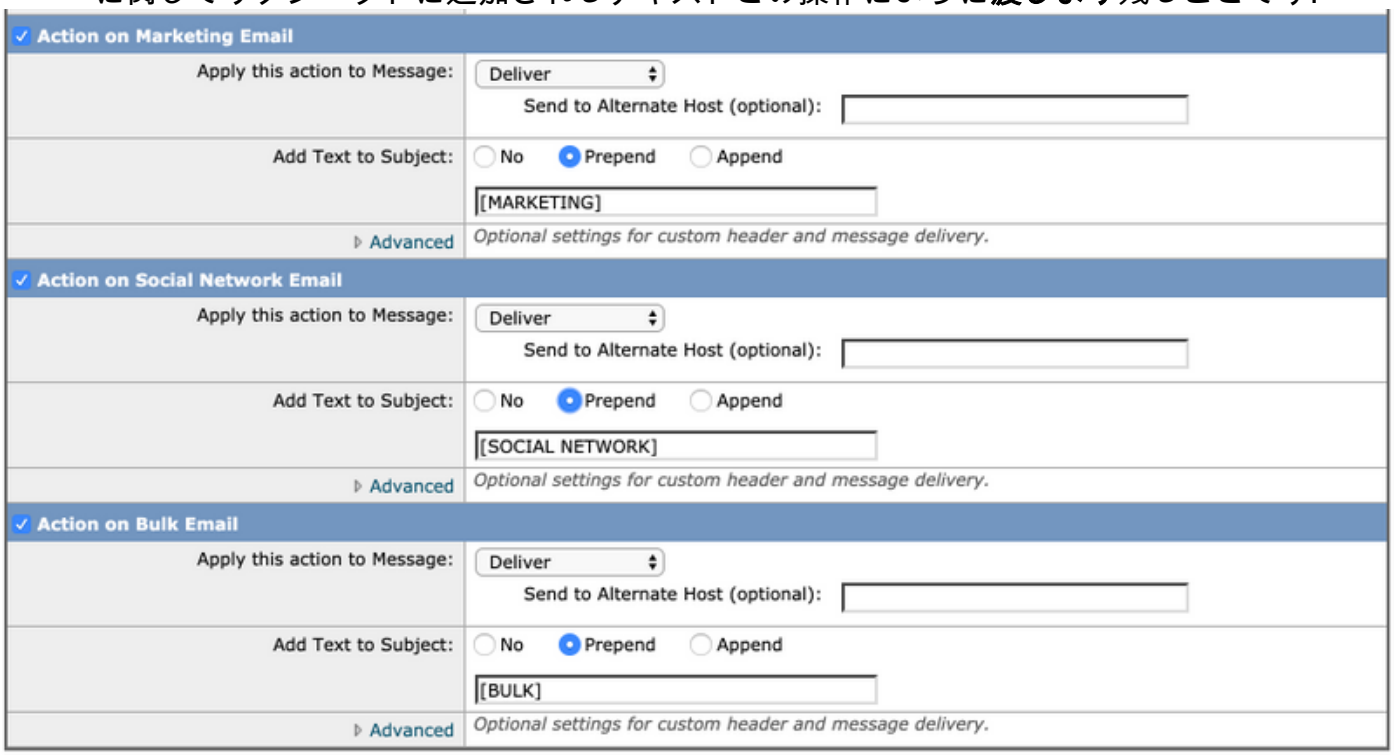
Graymail を設定すればセーフはポリシーで定期講読を解除します

Graymail およびセーフ Unsubscribe グローバルに設定されたら、今ポリシーを郵送するためにこれらのサービスを適用できます。

- **ポリシー** > **着信メール ポリシーを郵送する**ナビゲート
- **Graymail** の下のブルー リンクをクリックすることはその特定のポリシーが Graymail カスタマイズされた設定を使用することができるように可能にします。
- このポリシーのために有効に したい Graymailoptions を選択できます。
- この最良の方法 資料の目的で、Radio ボタンを**この**ポリシーのためのイネーブル Graymail 検出の隣でクリックし、**このポリシーのために定期講読を解除する Graymail を有効に して下さい**:

次の 3 つのセクションは**マーケティング メール設定の処理**、**社会的ネットワーク メール設定の処理**および**バルク メール設定の処理が**含まれています。

- 推奨される最良の方法はすべてを有効に し、付加されて下記に示されているようにカテゴリーに関してサブジェクトに追加されるテキストとの操作にように**渡します**残ることです:



- **Submitand を保存します変更を**クリックして下さい

発信 Mail ポリシーは **Graymail を無効**状態に残ってもらうはずです。

アウトブレイク フィルタ

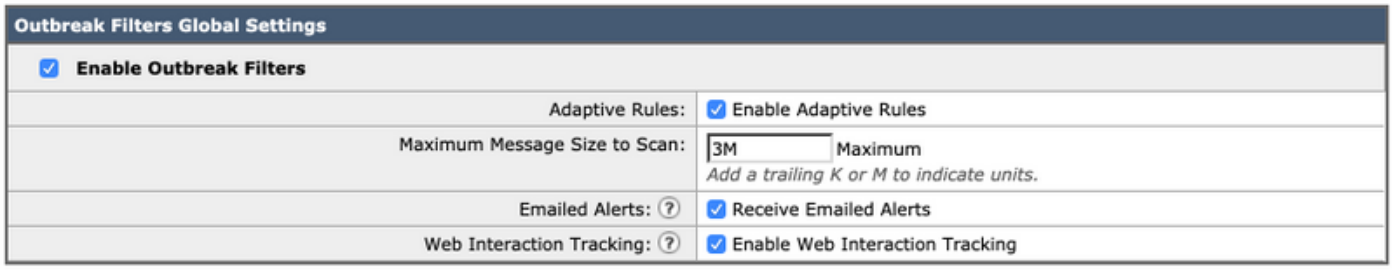
発生フィルタは正しく本当スパム カテゴリ–たとえば、phishing メールおよび詐欺メールの外部で落ち、ユーザ通知か検疫とそれらを適切に処理する項目をタグ付けするために反スパム エンジンのトリガーを、URL スキャンおよび検出 テクノロジー等々結合します。

フィーチャーキーを確認して下さい

- ESA で、**システム 管理 > フィーチャーキー**にナビゲート して下さい
- **発生フィルタを**探し、それがアクティブであることを確かめて下さい。

発生フィルタ サービスを有効に して下さい

- ESA で、**セキュリティ サービス > 発生フィルタ**にナビゲート して下さい
- **発生フィルタ 概要の Enablebutton をクリックして下さい**
- 複数の設定を行うことができます。 推奨 設定は下記のようにイメージで示されています:

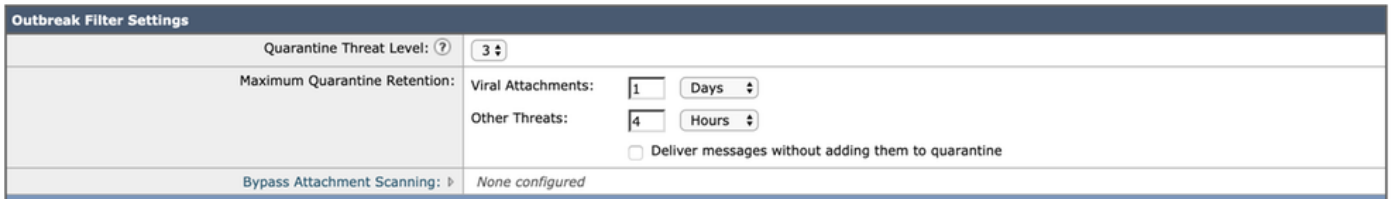


- **Submitand を保存します変更を**クリックして下さい。

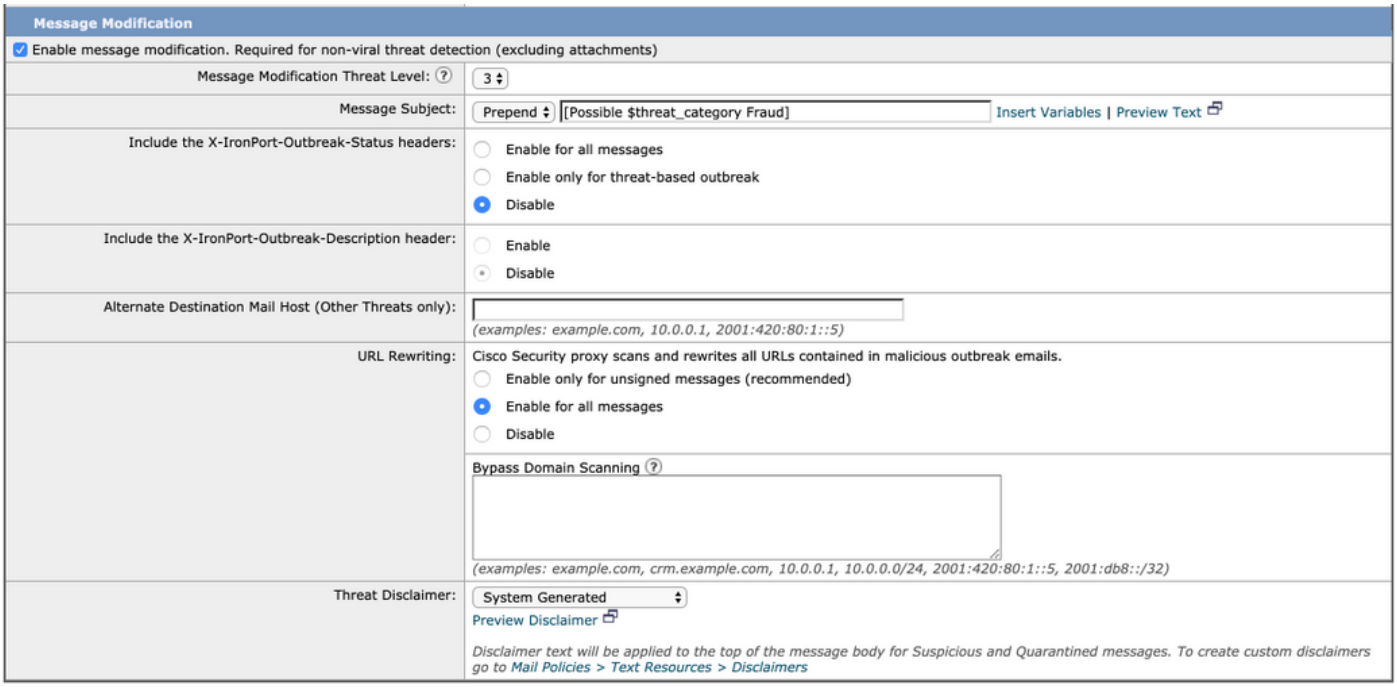
ポリシーの発生フィルタを設定して下さい

発生 Filtershas がグローバルに設定されて、今この機能 tomail ポリシーを適用できれば。

- **ポリシー > 着信メール ポリシーを郵送する**ナビゲート
- **発生フィルタ**の下のブルー リンクをクリックすることはその特定のポリシーがカスタマイズされた発生フィルタ設定を使用することができるように可能にします。
- この最良の方法 資料の目的で、デフォルト値を用いる発生フィルターの設定を保存します:



- 発生フィルタは悪意のある、疑わしいですかまたは phish 考えられる場合 URL を書き換えることができます。 URL によって基づく脅威を検出する、書き換えるために**メッセージ修正を**『Enable』 を選択 して下さい。
- **URL 書き換え**オプションが示されている続くことようにすべてのメッセージのための**イネーブル**あることを確かめて下さい:



- **Submitand を保存します変更を**クリックして下さい

発信 Mail ポリシーは**発生フィルタを無効**状態に残ってもらうはずです。

結論

この資料は E メール セキュリティ アプライアンス (ESA) で反スパム、アンチウィルスを、Graymail および発生フィルタ用のデフォルト、か最良の方法 コンフィギュレーション記述することを向けました。 これらのフィルターすべては受信および送信 メール ポリシーで利用可能であり、設定およびフィルタリングは両方で推奨されます–保護のバルクが受信のためである間、送信フローをフィルタリングすることは中継で送られたメールか内部 悪意のある不正侵入に対して保護を提供します。