Clearswift SECURE Email Gateway (SEG) Lite
エクスプレス インストール ガイド

はじめに

このガイドでは、MIMEsweeper for SMTPと連携して、Clearswift SECURE Email Gateway (SEG) Liteを配置する方法を詳しく説明します。

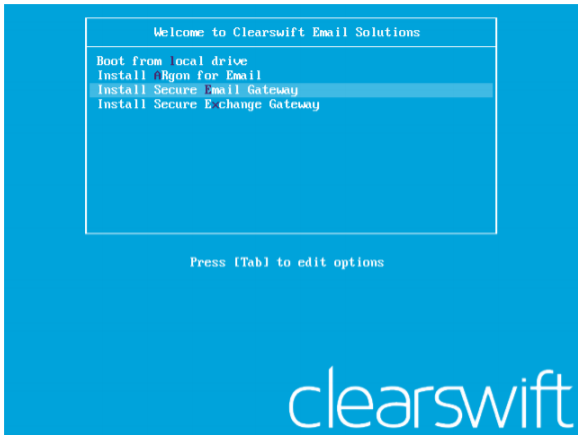
前提

このガイドでは、物理ハードウェアまたは vSphere や Hyper-V などの仮想プラットフォームにインストールすることを想定しています。 SEG Liteには、最低 4Gバイトの RAMと、少なくとも 120Gバイトのディスクスペースが必要です。最初にテストシステムを構築する場合は、より小さいディスクスペース (60Gバイト) で使用できます。

詳細な手順については、『Clearswift SECURE Email Gatewayインストールおよび入門ガイド』をこちらからダウンロードし参照してください。

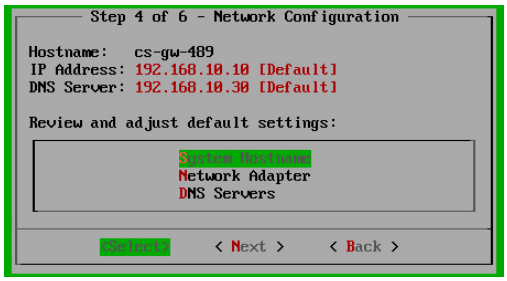
初期インストール

1. キットをこちら(http://download.clearswift.net/ISO/EMAIL_451_151.iso)からダウンロードします。
    a. 物理サーバーを構築する場合は、起動可能なDVDイメージを作成します。
2. 物理的なインストールでロードされたDVD、または仮想環境にインストールのために接続されたISOを使用して、インストールプロセスを開始します。次のような画面が表示されます。



3. [Install Secure Email Gateway]オプションを選択し、インストール処理を続行します。
4. 数分後、システムが再起動し、次のような画面が表示されます。

5. 「cs-admin」/「password」でログインし、System configurationを開始します。
6. 次の3つの画面で、システムロケール、キーボードとタイムゾーンを設定します。
7. 環境に合わせてホスト名、ネットワークアダプター、および DNSサーバーを設定します。



8. 3つの項目の入力が完了すると、「Next」ページに進むことができます。
9. ステップ5の画面で、「Online mode」を選択します。
10. ステップ6の画面で、cs-adminのコンソールログインのための強いパスワードを入力し、システム設定を適用します。

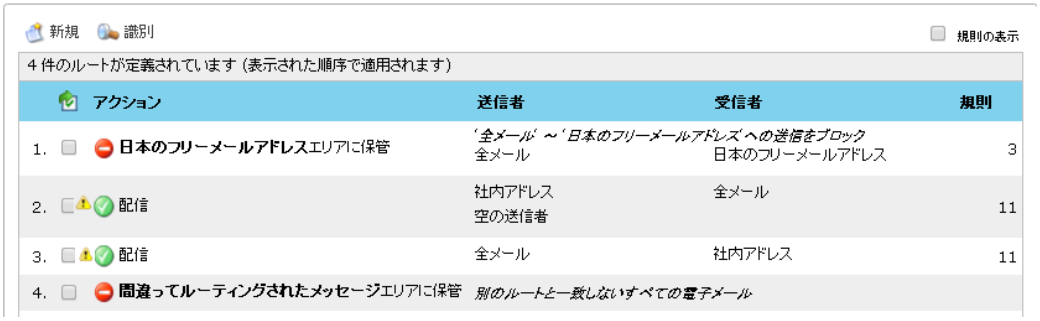
システムの設定

システムの設定の次のフェーズは、ブラウザーを使用して実行します。

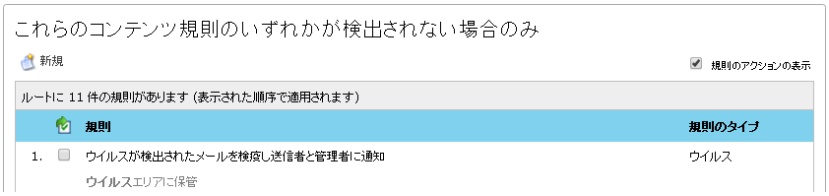
11. ステップ7で定義したIPアドレスを使用して、次のように入力します。
    https : // <ip address>
12. 事前に要求したSEG Liteライセンスキーを入力し、ライセンス契約に同意する必要があります。（ライセンス契約をお読みください。）
13. [社内ドメイン]ページで、システムがメールを処理する電子メールドメインを8つまで入力します。（ドメインが8つ以上ある場合は後で追加できます。）
14. 〔社内メールサーバー]ページで、ダウンストリーム サーバーのホスト名またはIPアドレスを入力します。この場合は、MIMEsweeper for SMTPサーバーである必要があります。
15. 会社の設定から出るメールのルーティングで、組織からメールを送信する上流のメールホストを入力します。
16. システムアラートに使用するシステムメールアドレスを定義し、最後にWebUI管理者アカウントのパスワードを入力します。これには、cs-adminアカウントと同じパスワードまたは異なるパスワードにすることができます。
17. [次へ]をクリックしてFIPSサポートを無効にし、[完了]を押してシステム設定ウィザードを終了します。数分後、ブラウザーウィンドウが更新されるか、または手動でページを更新するとログインページが表示されます。

製品の設定

18. 管理者アカウントでログインし、[ポリシー]〉[メールポリシールート]を選択してルートペインに移動します。

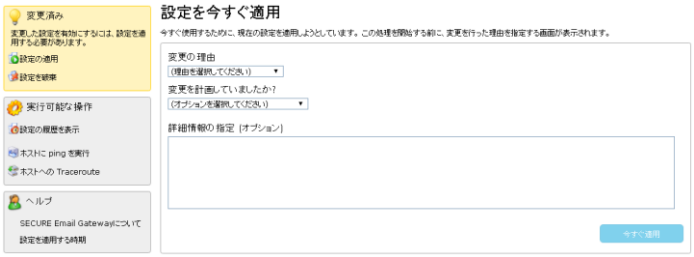


19. 黄色の三角形の警告マークは、そのルートのルールの1つにエラーがあることを示しています。SEG Liteはウイルス対策スキャナー（購入可能）を備えていないため、ルート内のウイルス対策規則はライセンスされていないので、削除する必要があります。
20. DNS ルートを選択して、[編集] を押します。
21. ポリシールートページが開き、適用する規則が表示されます。
22. 三角形の警告マークが表示されている規則を選択し、削除します。（規則はルートから削除されますが、設定を適用するまで実際には削除されません。）



23. ルート2で行った作業をルート３でもう一度繰り返し、三角形の警告マークが残っていないことを確認します。

24. これでウイルス対策の警告メッセージは表示されなくなりますが、プロセスを完了するために、設定を適用してください。この手順は、システムを再設定した後に必要です。



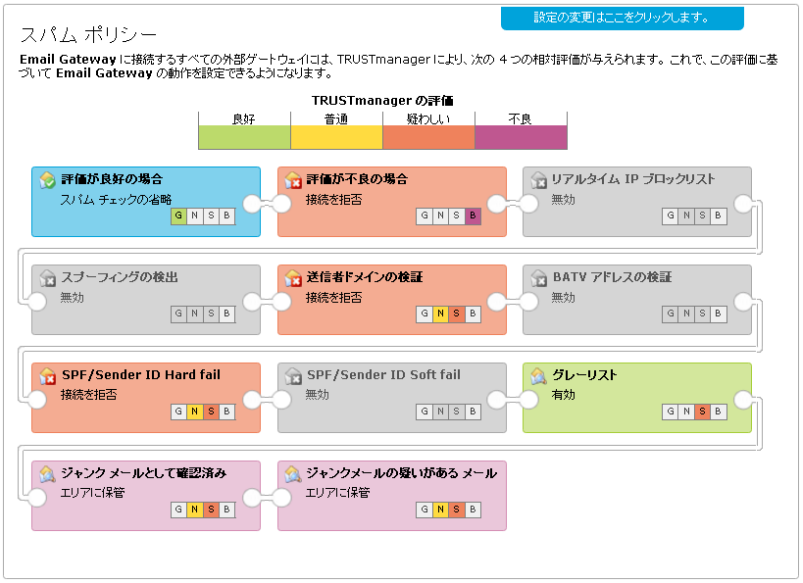
25. 受信ルートと送信ルートの両方で提供されている他のサンプルのコンテンツ規則を確認し、必要に応じて削除または修正してください。

スパムをブロックするように設定する

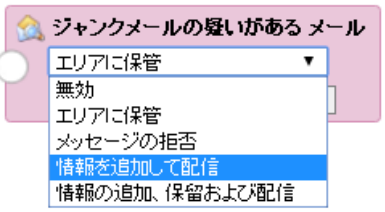
SEG Liteは、組織に届くスパムをブロックするために使用します。良好なメッセージは処理され、MIMEsweeperサーバー（MSW）に配信されます。明白なスパムメールは拒否されるか SEG に保持されますが、疑わしいメッセージ（「Greymail」と呼ばれることもあります）を SEG Liteで保留して管理するか、MSWに渡してメッセージを保留して管理するかを決定する必要があります。

26. 保留されたメッセージを SEG Liteに保留する場合は、次をお読みください。
    a. システムは、デフォルトで明白なスパムメールを拒否し、ジャンクメールの疑いのあるメールをスパム検疫エリアに保持し、システム管理者が手動で確認するように構成されています。
    b. 時間が経つと上記の作業が管理者の負担になる可能性があるため、エンドユーザーが独自のメッセージを解放できるようにシステムを構成することができます。SEG LiteでPMMメッセージの管理を有効にするための必要な手順については、 こちら(Gateway の設定および管理 > Gateway の設定 > PMM の設定 > PMM の設定 > PMM モードについて ）を参照してください。

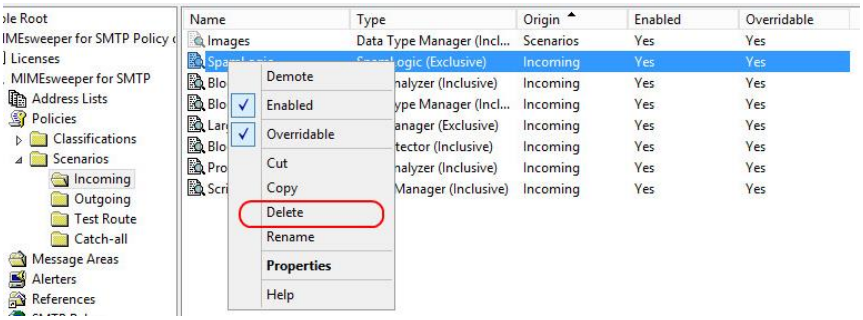
27. 保留するメッセージを MSW で保存する場合は、次をお読みください。
    a. SEG Liteシステムでは、疑わしいスパムメッセージを MSW ホストに渡すために、デフォルト設定を変更する必要があります。これを行うためには、[ポリシー] > [SpamLogicの設定]ページに移動し、[スパムポリシー] セクションの [設定の変更はここをクリックします]ボタンをクリックします。



    b. ジャンクメールの疑いのあるメールのバブルで、アクションを「情報を追加して配信」に変更し、ポリシーを適用します。

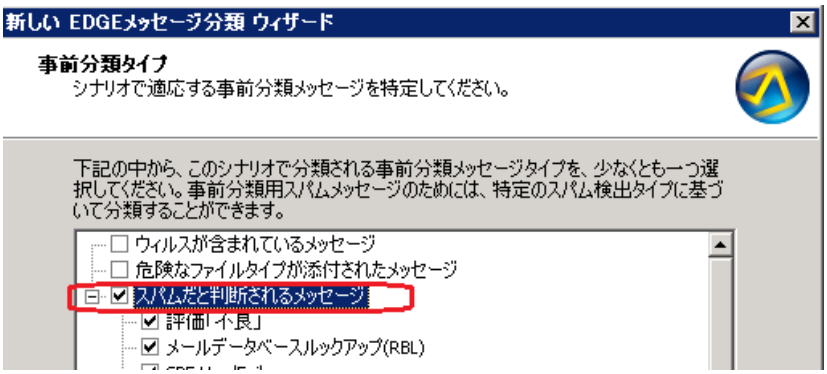


c. MSWホストでは、2つの作業が必要です。 最初に、既存のSpamLogicシナリオを削除します。



d. ここで、新しい[Edgeメッセージ分類] 規則を受信シナリオフォルダーに追加します。

e. SEG Liteで ″スパム″と識別されたメッセージを選択します。

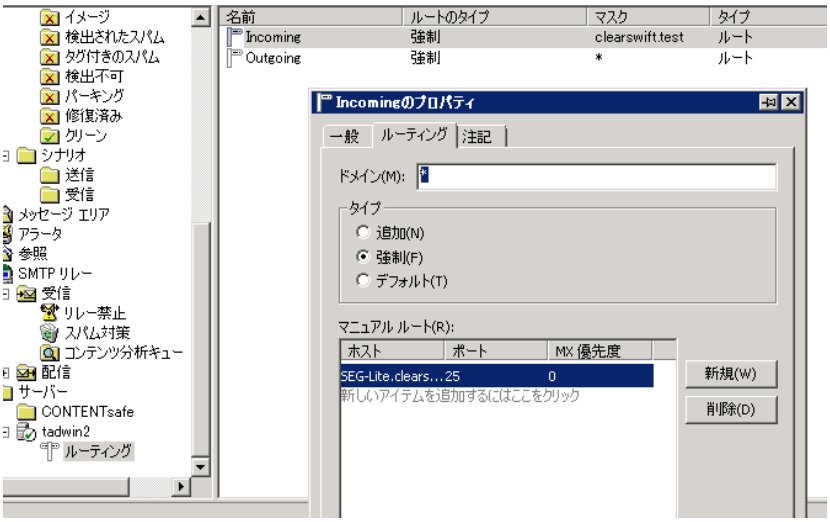


f. 次に、スパムメッセージの分類を指定します。

g. 最後にポリシーを保存して適用します。

28. スパムの検出をテストし、システムが期待どおりに機能することを保証するには、メッセージ本文にGTUBEスパムテストパターン(https://ja.wikipedia.org/wiki/GTUBE)を使用します。これは SEG Liteで「ジャンク メールとして確認済み」フィルターによって検出されるため、SEG Liteでこれらをブロックしている場合は、スパムメールの保留エリアにメッセージが表示されます。SEG Liteで「情報を追加して配信」オプションを使用してMSWに配信する場合には、「Edgeメッセージ分類」がスパムを検出すると、メッセージはMSWホストに保持されます。

29. テストが終了したら、次の作業を行ってください：
    a. 受信メールが MSW ホストではなくSEG Liteに最初に配信されるようにしてください。
    b. SEG Liteが送信メールをスキャンするには、SEG Liteにメールを送信するためにワイルドカードのルーティングエントリーを設定する必要があります。これは、SEG の製品軍に統合されたTLSで電子メールを送信されたい場合に特に便利です。



技術サポート

弊社の専用テクニカルサポートチームは、このプロセスの支援が必要な場合にのみ、電話または Eメールで対応しております。インストール設定以外のサポートが必要な場合、または完全な移行プロジェクトについてご相談が必要な場合は、プロフェッショナルサービスチームにてオプションを検討させていただきます。