Cisco E メール セキュリティ ソリューション v11 v1

最終更新日:2017 年 11 月 03 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
● ラップトップ	● Cisco AnyConnect®

このソリューションについて

Cisco E メール セキュリティ（旧称 Cisco IronPort E メール セキュリティ）は、電子メール送受信時に優れたクレンジングと制御を提供します。動的で変化が速く、今日の電子メールに影響を与える絶え間ない脅威に対し、お客様のニーズに応えられるさまざまなフォーム ファクタで可用性の高い電子メール保護を実現します。

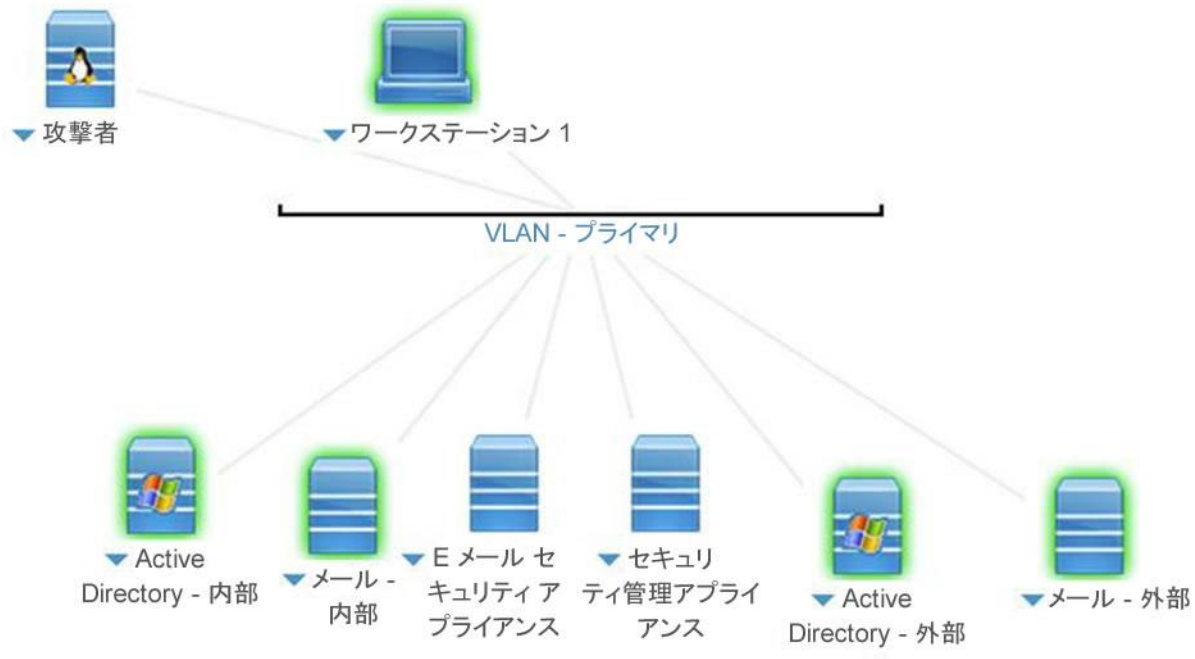
Cisco E メール セキュリティの機能と利点、利用可能なフォーム ファクタ、シスコの差別化要因などの詳細については、E メール セキュリティの概要をお読みください。

Cisco クラウド E メール セキュリティの詳細については、http://www.cisco.com/c/ja_jp/products/security/email-security/index.html を参照してください。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ（Topology）] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ

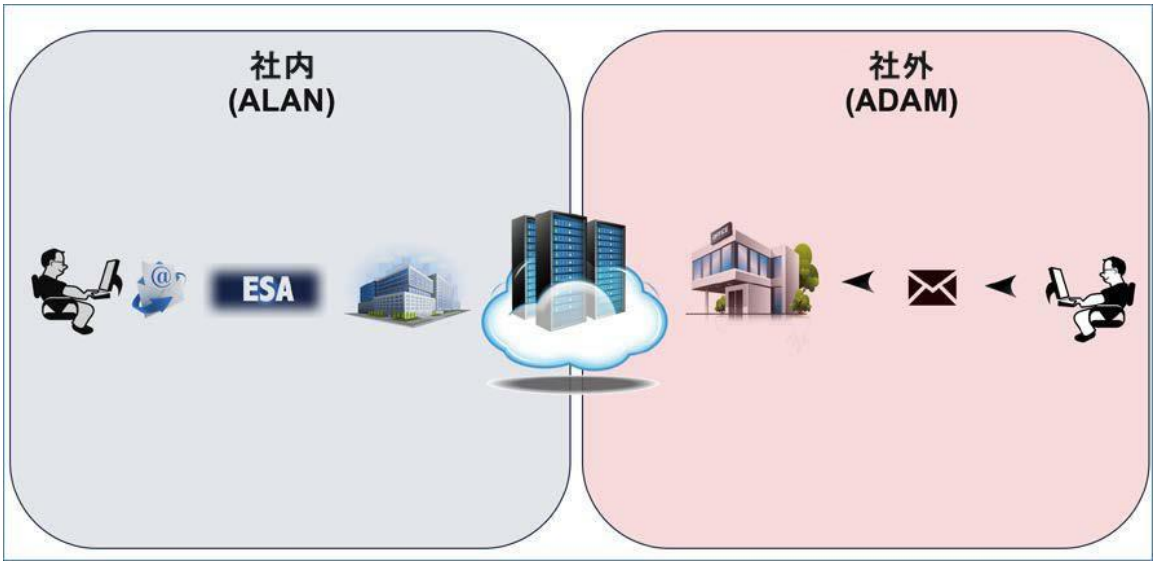


ラボのシナリオの論理トポロジはすべて、次の前提に基づいています。

「Alan」は、社内ユーザです。彼は Microsoft Outlook をメール クライアントとして使用しています。会社のメール サーバは Microsoft Exchange です。このサーバは、ポリシー制御と電子メールのウイルス予防のために、メッセージをルーティングする前に Cisco E メール セキュリティ ソリューションに転送します。

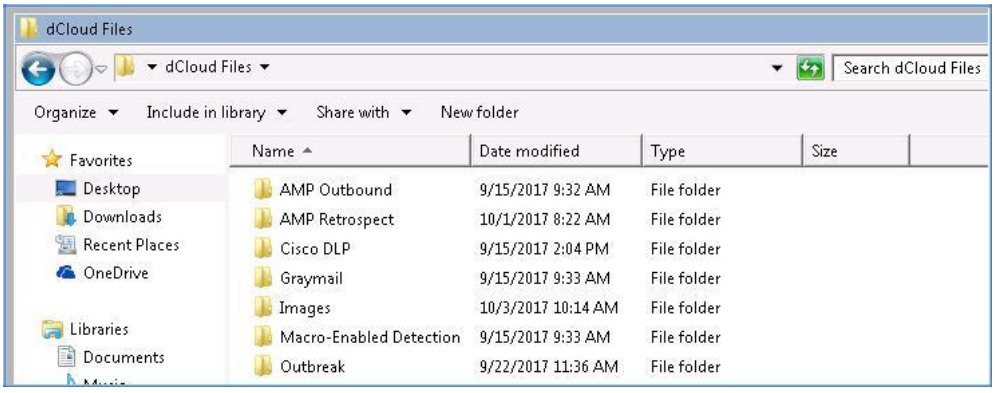
「Adam」は社外ユーザです。彼はメール ボックスの管理に Microsoft Outlook クライアントを使用していますが、彼が接続するメール サーバ プラットフォームの種類は、このラボでは問いません。

Alan - alan@dcloud.cisco.com　　Adam - adam@dcloud-out.cisco.com



補助ファイル

このラボでは、さまざまなシナリオで補助ファイルを使用します。これらはすべて、ワークステーションのデスクトップ上の dCloud Files フォルダにあります。



注:一部のシナリオでは、特定の補助ファイルを実行する際に注意を促すセキュリティ警告が表示されますが、これらは完全に安全です。「悪意のある」と分類されるすべてのファイルは、実際にはクリーンであり、どの環境にも悪影響を与えません。

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるためには、入念な準備が不可欠です。

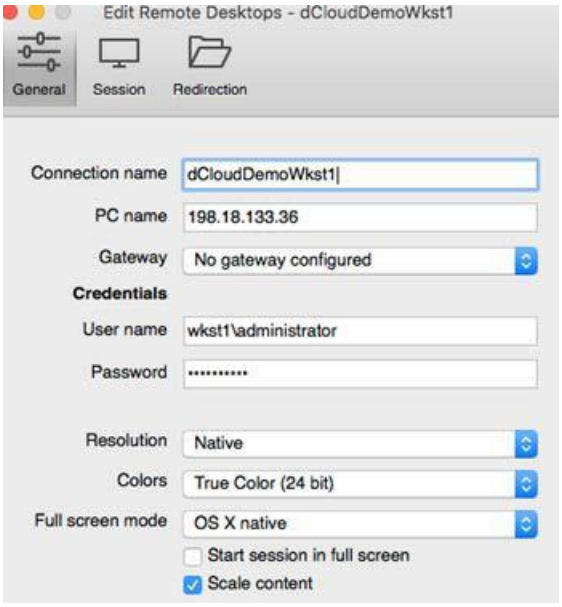
1. 次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。
2. dCloud セッションを開始します。[手順を見る]

注: セッションがアクティブになるまで最長で 10 分かかることがあります。

3. 最適なパフォーマンスを得るために、**Cisco AnyConnect VPN** [手順を見る] および**ラップトップのローカル RDP クライアント**[手順を見る] を使用してワークステーションに接続します。

ワークステーション 1:**198.18.133.36**、ユーザ名:**administrator**、パスワード:**C1sco12345**

注: Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [手順を見る] 。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法には、接続ができない場合や、パフォーマンスが悪い場合があります。



ケース スタディ

Voyage Corp

Voyage Corp 社は米国を本拠地とする企業であり、米国と欧州の小売業者や金融業者向けに IT 機器およびサービスを提供する大手サプライヤです。ビジネスの主要領域への多額の投資により、同社のグローバルな営業範囲は、アジアへと徐々に拡大しています。

同社のビジネス モデルは、主要な顧客およびサプライヤとの電子取引に依存しています。社内と社外の関係者の間の通信はすべて、原則として電子メールで行われます。

同社では電子メールの使用量が過去 2 年間で 20 % 以上増加しており、メール システムに対するランサムウェア攻撃やマルウェア攻撃の数も急増しています。最高技術責任者（CTO）に最近任命された Mark Valentino 氏は、戦略的通信システムをすべて再検討するように命じました。彼は特に電子メールを最重要視していたため、まず電子メールを再検討するように指示しました。

同社では、Gartner Magic Quadrant で報告されたセキュア E メール ゲートウェイのトップ企業に関する詳細なレビューを受けて、今日の高度な攻撃に対抗できる Cisco E メール セキュリティ ソリューションを電子メール保護プラットフォームとして採用しました。CTO の Valentino 氏の言葉を借りれば、シスコは長年にわたる比類ない製品革新の実績を有し、最先端かつ最高水準の E メール セキュリティを提供する業界リーダーです。

同社では、内外の電子メール トランザクションや通信を Microsoft Exchange で管理しています。オンプレミス運用を止めて Microsoft Exchange Online に移行することも検討しましたが、まだ決定には至っていません。

潜在的な脅威とセキュリティ上の懸念事項

Voyage Corp 社は、受信するメッセージを（可能であれば）認証された送信元に限定したいと考えています。また、個人情報等の保護法（HIPAA 法および PCI-DSS 法）が適用される社外関係者からの圧力を受けて、セキュリティ ポスチャを強化せざるを得なくなっています。

一部の部門では社外ネットワークから来るドキュメントの量が増えており、それらをより安全に受信したいと考えていました。ドキュメントは電子メールの添付ファイルとして届きますが、それらが引き起こす脆弱性について InfoSec チームが懸念しているためです。

セキュリティ ソリューション

同社は、既存の仮想プラットフォーム上で **Cisco E メール セキュリティ ソリューション**を稼動させることを選択し、セキュリティを維持するために次の Cisco E メール セキュリティ機能に投資します。

- 高度なマルウェア防御
- Sophos ウイルス対策
- McAfee ウイルス対策
- アウトブレイク フィルタ
- データ損失防止
- 画像アナライザ

目的

このラボでは、今日の高度な攻撃に対処するために必要なセキュリティ制御を実装する一連の演習を実行します。電子メールは依然として主要な攻撃ベクトルであり、Voyage Corp における電子メールの重要性を考えると、すべてのルートを十分に防御することが不可欠です。

厳密には必須ではありませんが、すべてのシナリオを順番に実行することをお勧めします。

シナリオ 1:　データ損失防止ポリシー（DLP）

使用例

Voyage Corp はビジネス パートナーのエコシステム内で作業してきましたが、パートナーとの間で交換する電子メールの量は徐々に増えています。一例として人事部（HR）は、すべてのスタッフが地域法を遵守して労働しているかを確認する目的で、郡の一部の自治体から大量に寄せられる従業員の個人情報に関する要求に、現在晒されています。頻繁に要求される情報の種類は、雇用履歴、マイナンバー番号、社会保障番号などです。

以前は、この情報を郵便で発送していました。しかし、すでに人員が削減されている HR 部としては、これらを印刷して発送用に梱包する負担が大きく、すでに問題になっています。さらに、これらの秘密書類用小包を送信するコストが 10 % 増加したことで、会計主任はコスト削減手段の導入を要求されています。

人事部長は、既存のテクノロジーを使用することによる多数の利点（速度やコストなど）を挙げ、情報を電子メールで送信するようにチームに指示しました。電子メールで送信する手段は、12 か月以上にわたって部門の負担を軽減するために役立ちます。しかし社内の情報セキュリティ（InfoSec）グループがポリシーを再検討した結果、その手段は社内セキュリティ ポリシーに大きく違反しており、停止するように通知されます。

InfoSec は、Cisco E メール セキュリティの管理者に、必要な措置を即座に実装するように指示します。

セキュリティ制御

Cisco E メール セキュリティ ソリューションは、メッセージと添付ファイルを検査し、禁止されている情報を Alan が実際に送信したかどうかを判定できます。これは、Voyage Corp が購入した Premium ライセンスに含まれる Cisco DLP 機能によって実現されます。

目的

このシナリオでは、今回のユースケース（社内ユーザの Alan から、社外ユーザの Adam に電子メールを送信する）に対処するために、エンドツーエンドのデータ損失防止（DLP）ポリシーを設定します。通常の環境下では、社内ユーザから社外ユーザへの電子メール トラフィックの交換はポリシーに違反しない通常のタスクとなりますが、今回のシナリオでは、組織のリスクとなるものを Alan が社外に送信することを確実に防止します。

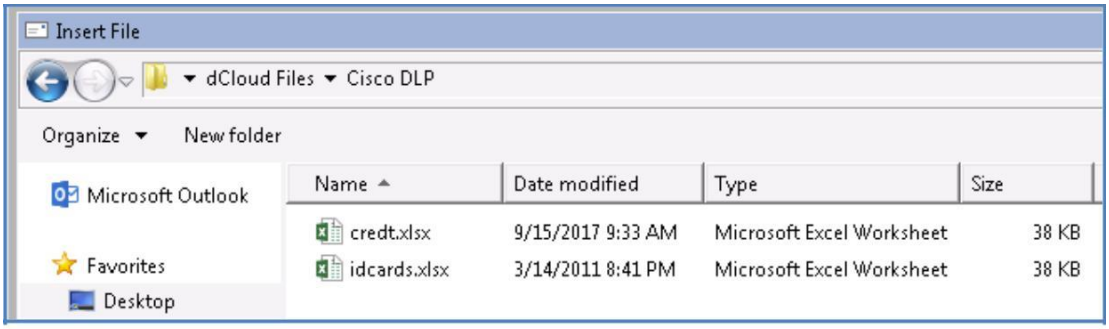
手順

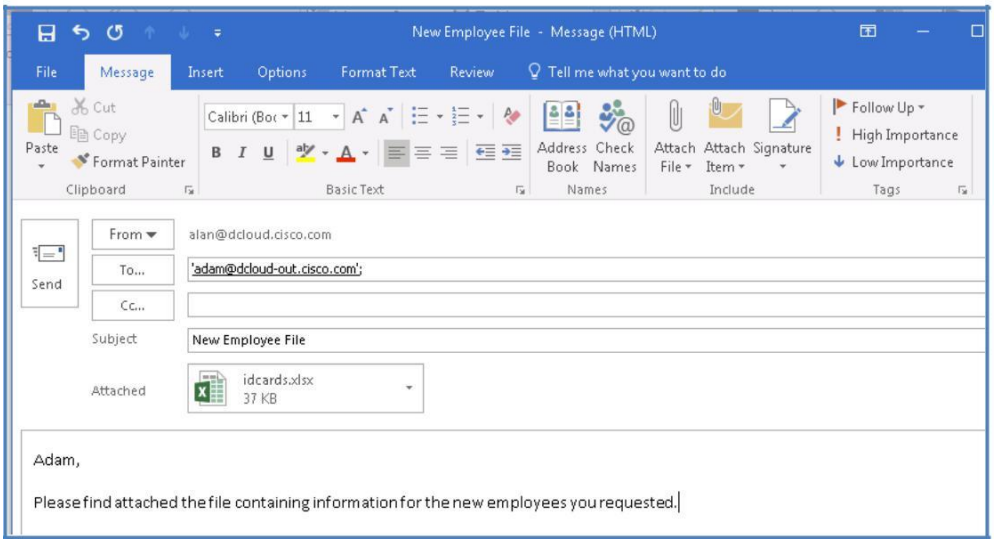
タスク：Cisco DLP が設定されていない状態で、ファイルが添付された電子メールを送信する（推定所要時間：5 分）

DLP ポリシーがトリガーされる基準と、その後に実行されるアクションを特定できれば、DLP ポリシーは比較的簡単に作成できます。

このシナリオのために、Cisco DLP ポリシーが設定された状態と設定されていない状態で、社会保障番号が含まれている Microsoft Excel ファイルを社内ユーザの Alan から社外の同業者（Adam）に送信し、最終結果に対する効果を確認します。

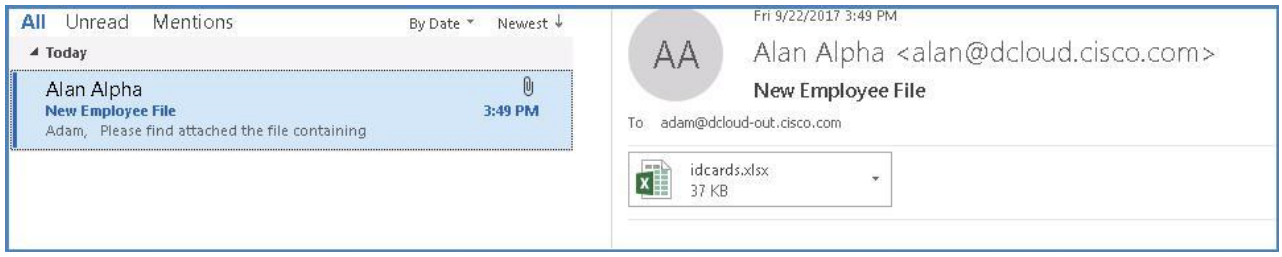
1. ワークステーション 1（以降、ワークステーションと呼ぶ）のタスク バーから Microsoft Outlook を起動し、次のパラメータで電子メールを準備します。
    - [差出人（From）]：alan@dcloud.cisco.com
    - [宛先（To）]：adam@dcloud-out.cisco.com
    - [件名（Subject）]：新入社員のファイル（New Employee File）
    - [本文（Body）]：Adam さん、依頼された新入社員の情報をファイルを送信いたします。ご査収ください。（Adam, Please find attached the file containing information for the new employees you requested.）
    - [添付ファイル（Attachment）]：IdCards.xlsx（保存先：デスクトップ上の Cisco DLP サブフォルダ内）





2. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。
3. Adam の受信トレイに移動し、[すべてのフォルダを送受信（Send/Receive All Folders）] をクリック、または **F9** キーを 2 ～ 3 回押して、メール クライアントを同期させます。

4. DLP ポリシーが存在しないため、ファイルが添付された電子メールは Adam のメール ボックスに配信されます。これは、予期される動作です。添付ファイルを開いて、Microsoft Excel ファイルのコンテンツを表示します。コンテンツが正常に表示され、電子メールのメッセージも変更されることはありません。



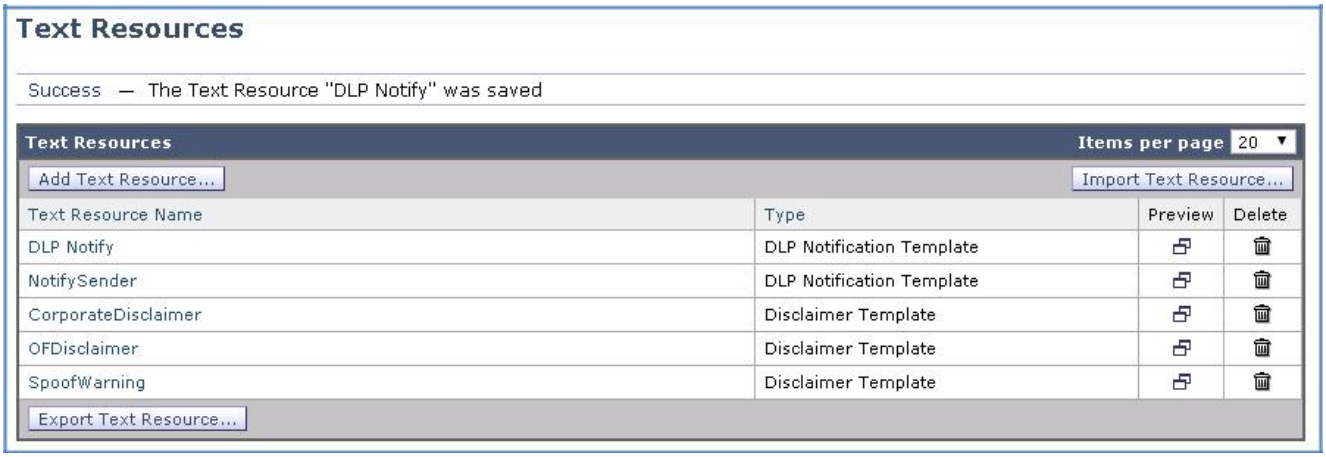
5. メッセージは意図された受信者に配信されていますが、意図した通り、Cisco E メール セキュリティ ソリューションの複数のエンジンによって処理されています。これらのエンジンのいずれかによって、メッセージまたは添付ファイルにリスク要因（ウイルスなど）が検出されると、定義されたアクションが実行されます。
6. 次のタスクでは、DLP 機能を備えた Cisco E メール セキュリティ ソリューションを設定して、秘密データが組織外に出ることを防ぐために必要な制御を実装します。

タスク：Cisco DLP テキスト リソースを設定する（推定所要時間：5 分）

DLP ポリシー設定の最初の手順は、（カスタム）テキスト リソースの作成です。テキスト リソースは、メッセージへの添付や、メッセージとしての送信が可能なテキスト テンプレートです。たとえば、設定されたポリシーに違反している電子メールに対してアクションが実行されたことを通知するテキスト リソースを作成できます。これにより、アクションが実行された理由、さらには次に実行すべきアクション（社内トレーニング、暗号化の活用など）に関する貴重なフィードバックが提供されます。
このシナリオでは、*DLP Notification*（DLP通知）テンプレートと *DLP Disclaimer*（DLP免責事項）テンプレートが作成されます。これらは今後も Cisco DLP ポリシー内で使用されます。

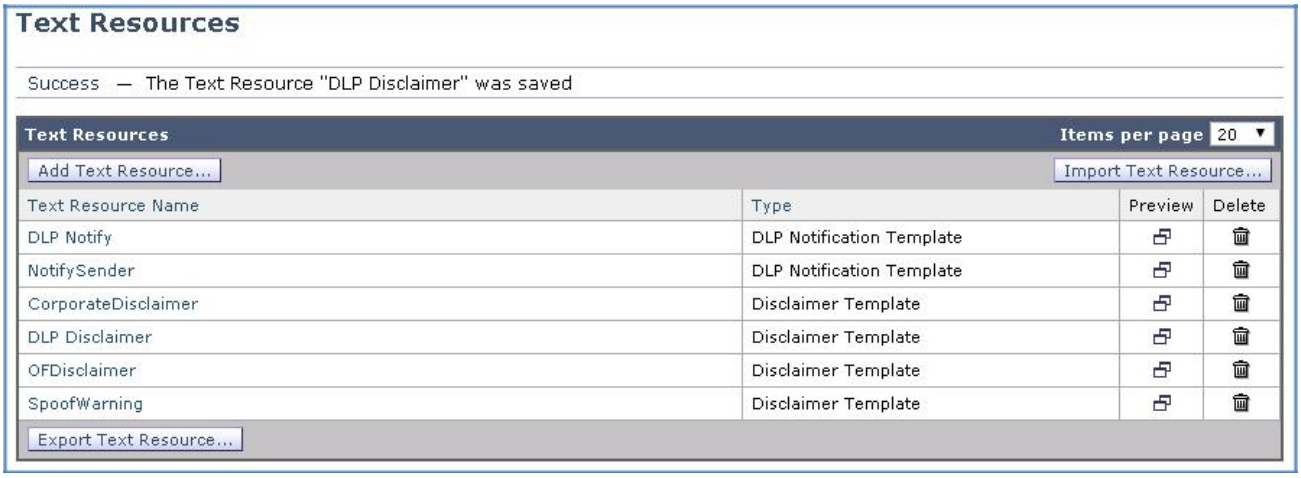
1. ワークステーションから Google Chrome を起動し、[詳細設定（Advanced）]、[esa.dcloud.cisco.com（安全ではない）に進む (Proceed to esa.dcloud.cisco.com (unsafe))] の順にクリックすると、デフォルト ページが自動的にロードされます。これが、Cisco E メール セキュリティの GUI ページになります。次のクレデンシャルでログインします。
    - **ユーザ名**：admin
    - **パスフレーズ**：C1sco12345
2. 認証に成功すると、Cisco E メール セキュリティのランディング ページ（[マイ ダッシュボード（My Dashboard）]）が表示されます。

3. [メール ポリシー（Mail Policies）] > [テキスト リソース（Text Resources）] に移動すると、デフォルト/設定済みテキスト リソースが表示されます。[テキスト リソースの追加（Add Text Resource）] ボタンをクリックし、次の情報を使用してカスタム通知テンプレートを作成します。
   - [名前（Name）]：DLP Notify（DLP 通知）
   - [タイプ（Type）]：DLP Notification Template（DLP 通知テンプレート）
   - [HTML]：企業ポリシーに違反する電子メールが送信されました（You have sent an email that is inconsistent with corporate policies on acceptable use）
4. [送信（Submit）] をクリックしてテキスト リソースを作成し、それが設定済みテキスト リソースのリストに追加されていることを確認します。

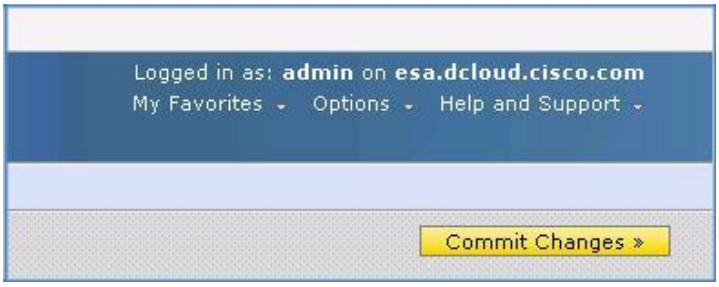


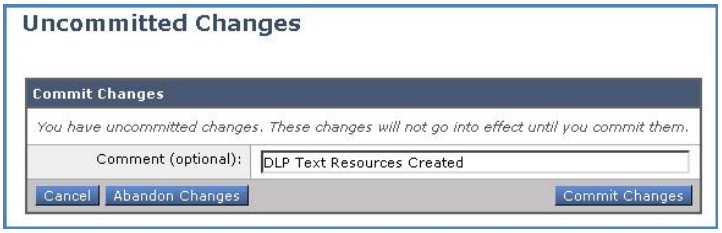
5. 他のテキスト リソースのために上記の手順を繰り返しますが、今回は [タイプ（Type）] を「Disclaimer Template」に変更します。
   - [名前（Name）]：DLP Disclaimer
   - [タイプ（Type）]：Disclaimer Template
   - [HTML]：この電子メールには、所定の受信者のみを対象とした秘密情報などが含まれている可能性があります。（This email may contain confidential and privileged material for the sole use of the intended recipient only.）

6. [送信（Submit）] をクリックしてテキスト リソースを作成します。



7. 完了したら画面の右上にある [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。



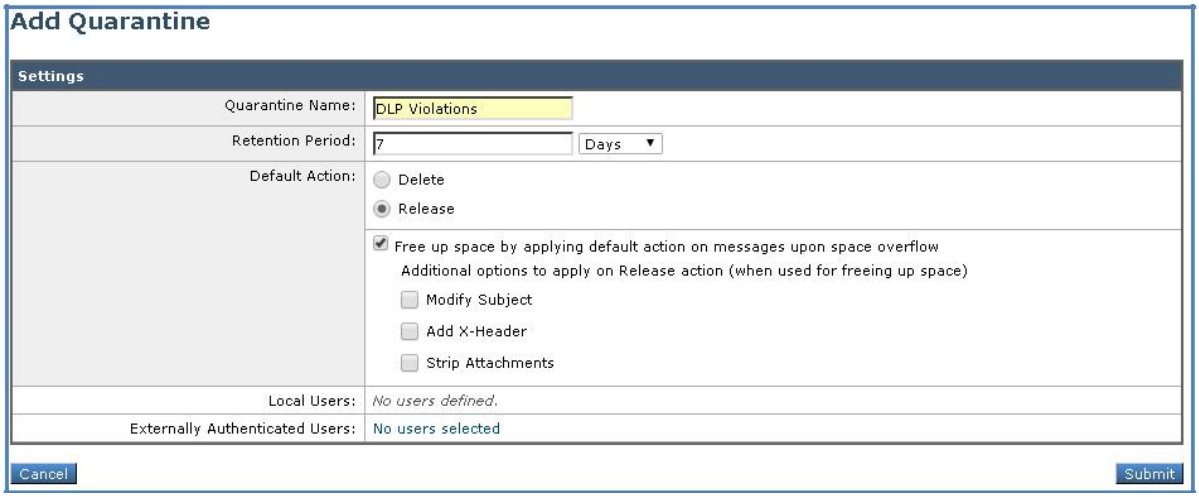


タスク：DLP 検疫エリアを設定する（推定所要時間：5 分）

Cisco E メール セキュリティ ソリューションは、受信/送信メッセージ内に疑わしいファイル（潜在的なマルウェアなど）やポリシー違反のコンテンツを検出すると、すぐに削除するのではなく、それらのメッセージを一旦検疫エリアに送信します。検疫エリアではそれらのメッセージが一定期間安全に保持されます。管理者はそれらのメッセージを再確認するか、またはメッセージの安全性をより正確に評価できる情報更新を待つことができます。

このタスクでは、Cisco DLP ポリシーに違反しているメッセージを保持する個別の検疫エリアを作成します。それらのメッセージは、このフォルダに送信された後に再確認され、意図した受信者に配信されるか、完全に削除されます。

1. [モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク検疫（Policy, Virus and Outbreak Quarantines）] に移動し、[ポリシー検疫の追加（Add Policy Quarantine）] ボタンを選択します。次の情報を使用して新しい検疫エリアを作成します。
   - [検疫エリア名（Quarantine Name）]：DLP Violations（DLP 違反）
   - [保持期間（Retention Period）]：7 Days（7 日）
   - [デフォルト アクション（Default Action）]：Release（解放）



2. [送信（Submit）] をクリックして検疫エリアを作成します。

3. 完了したら画面の右上にある [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

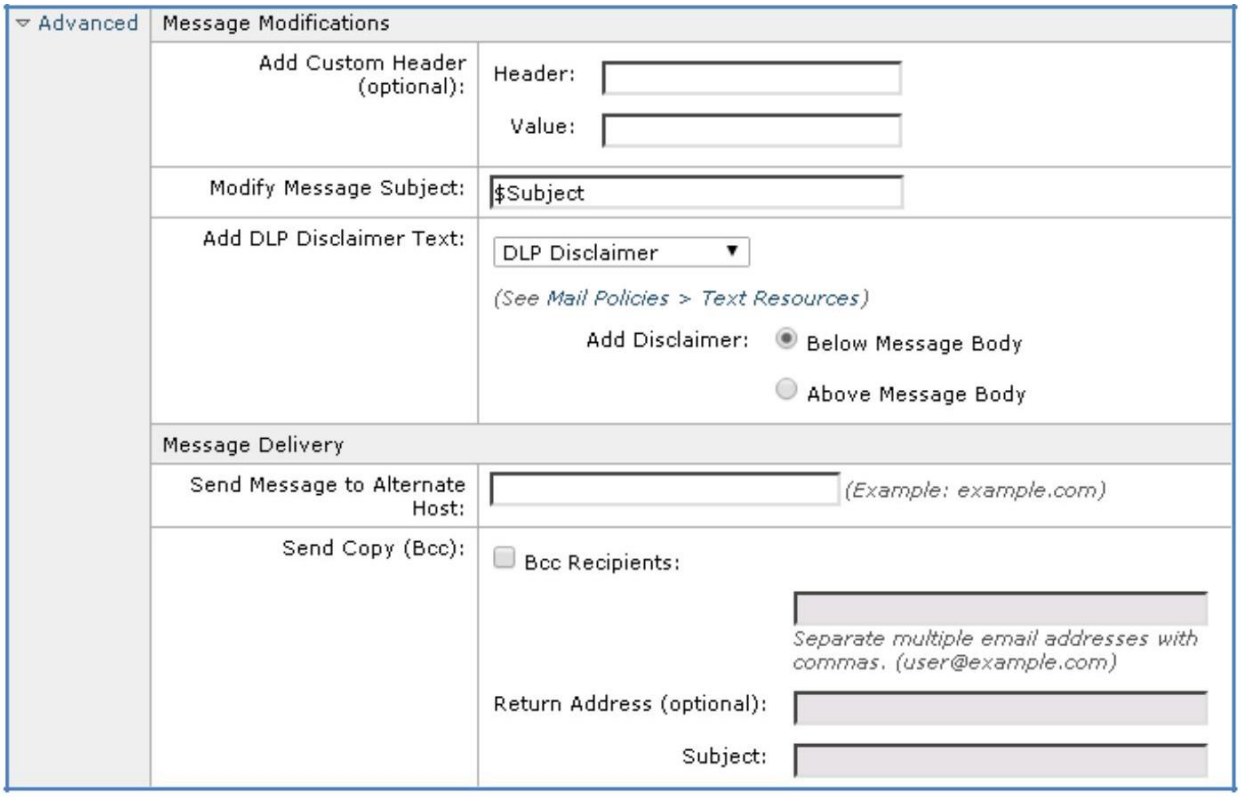
タスク：DLP ポリシー カスタマイズを設定する（推定所要時間：5 分）

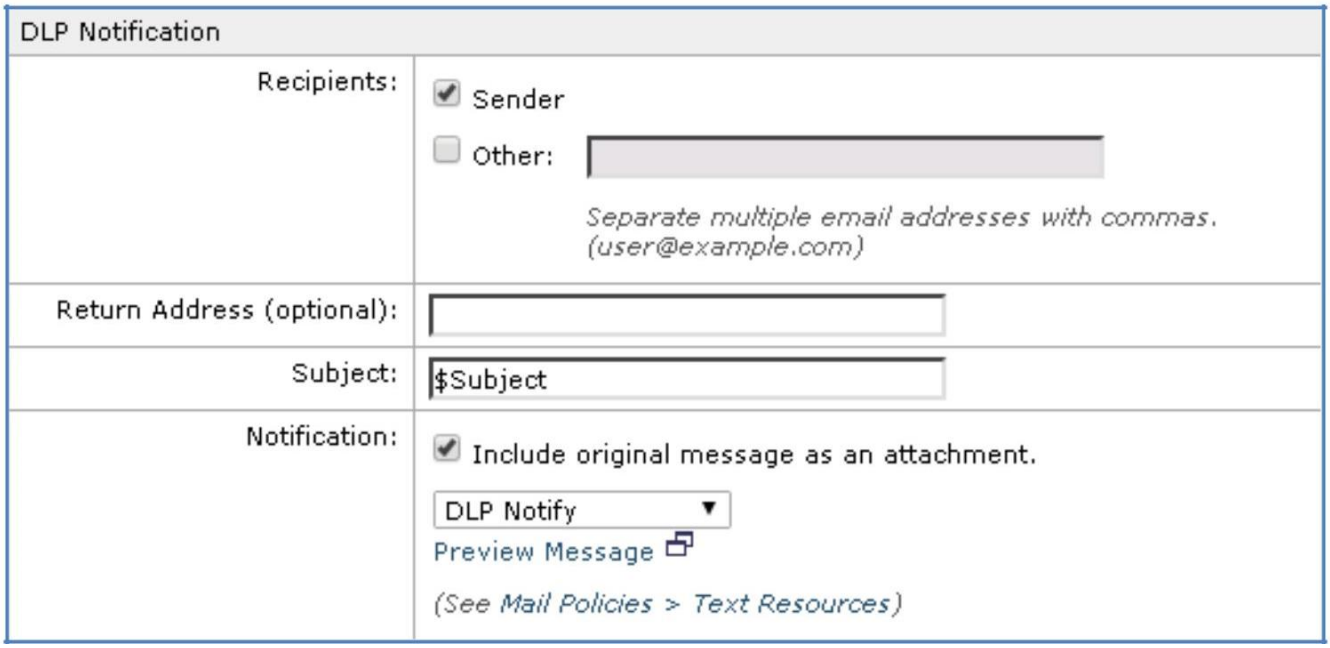
Cisco E メール セキュリティ ソリューションは、送信メッセージで DLP 違反の可能性を検出すると、プライマリ アクションおよびセカンダリ アクションを適用します。さまざまなアクションに対して、異なる違反タイプおよび重大度を割り当てることができます。

- [プライマリ アクションの選択肢（Primary actions include）]：配信、ドロップ、または検疫
- [セカンダリ アクションの選択肢（Secondary actions include）]：暗号化、件名ヘッダーの変更、または免責事項の追加

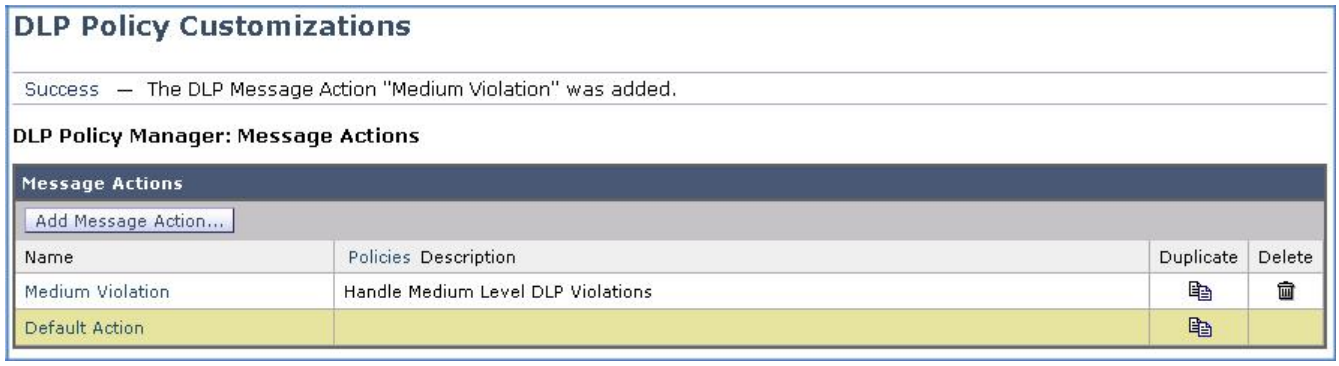
このタスクでは、ポリシー違反が発生したときに適用されるメッセージ アクションを作成します。

1. [メール ポリシー（Mail Policies）] > [DLP ポリシー カスタマイズ（DLP Policy Customizations）] に移動し、[メッセージ アクションの追加（Add Message Action）] ボタンを選択します。次の情報を使用して新しいメッセージ アクションを作成します。
   - [名前（Name）]：Medium Violation（中レベルの違反）
   - [説明（Description）]：Handle Medium Level DLP Violations（中レベルの DLP 違反の処理）
   - [メッセージ アクション（Message Action）]：Quarantine（検疫）
   - [ポリシー検疫（Policy Quarantine）]：DLP Violations（DLP 違反、前のタスクで作成。以降は、[詳細設定（Advanced）] で設定）
   - [メッセージの件名を修正（Modify Message Subject）]：$Subject
   - [ADLP 免責事項テキストを追加（Add DLP Disclaimer Text）]：DLP Disclaimer（DLP 免責事項）
   - [免責事項を追加（Add Disclaimer）]：[メッセージ本文の下（Below Message Body）] を選択
   - [DLP 通知（DLP Notification）]：[送信者（Sender）] を選択
   - [件名（Subject）]：$Subject
   - [通知（Notification）]：[元のメッセージを添付ファイルとして含む（Include original message as an attachment）] を選択し、[DLP 通知（DLP Notify）] を選択します。





2. [送信（Submit）] をクリックしてアクションを作成します。



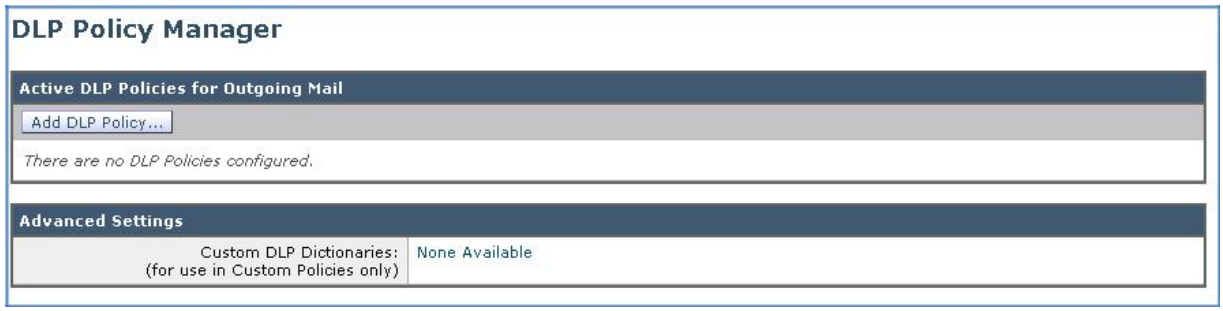
3. 完了したら画面の右上にある [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

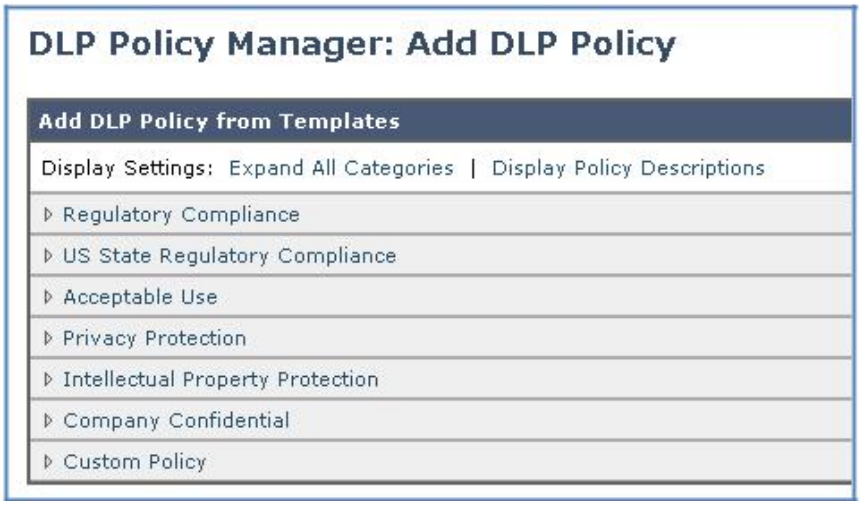
タスク：SSN を検出する DLP ポリシーを設定する（推定所要時間：5 分）

DLP ポリシーは、企業ポリシーに違反する可能性のある電子メール メッセージ内で何を検索するかを決定します。Cisco DLP エンジンには、一般に使用される事前設定済のポリシーが 100 件以上組み込まれています。さらに、ポリシーは大半の要件に合わせてカスタマイズできるため、きめ細かい制御を実現できます。

このタスクでは、事前設定されたテンプレートの 1 つを使用して社会保障番号（SSN）を特定し、前のタスクでカスタマイズした設定（Medium Violation）を使用して、実行するアクション（メッセージを検疫エリアに送信した後、この違反を送信者に通知する）を決定します。

1. [メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] に移動し、[DLP ポリシーの追加（Add DLP Policy）] ボタンを選択します。

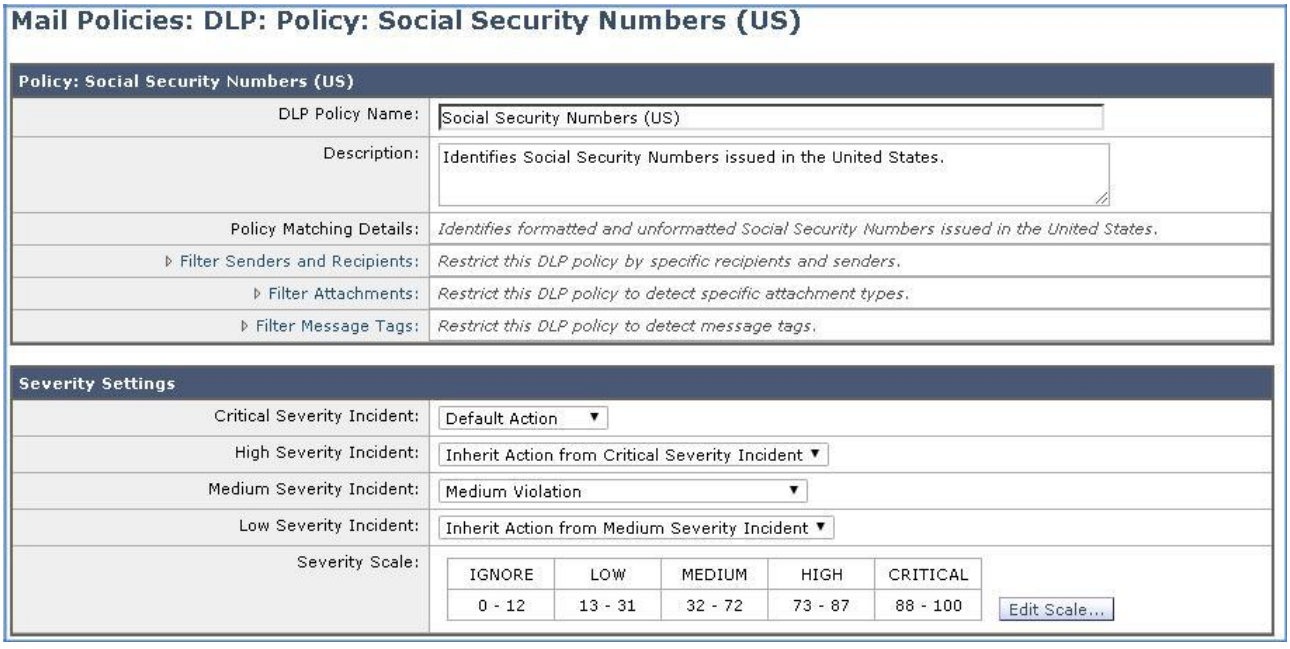




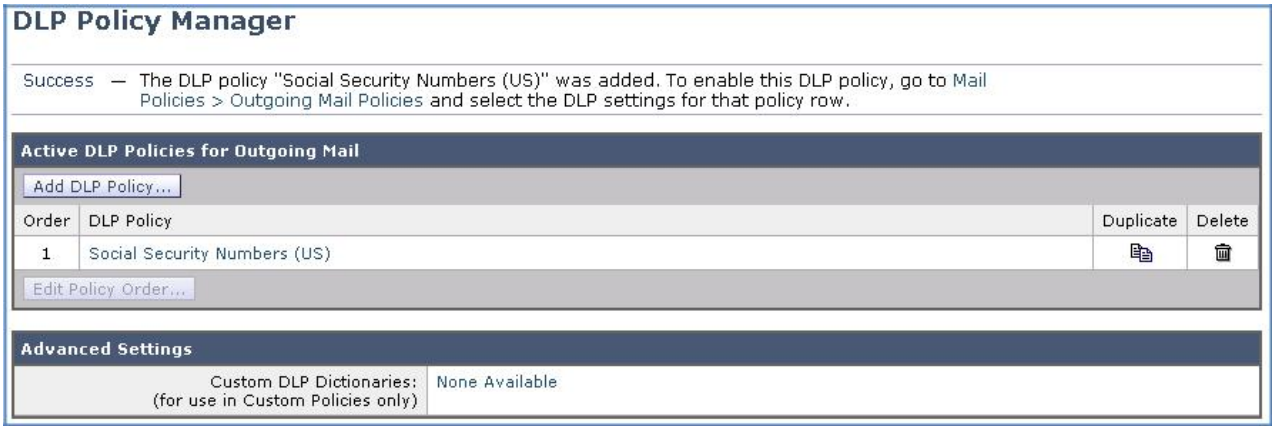
2. 「Privacy Protection」テンプレートを選択し、[社会保障番号（米国）（Social Security Numbers (US)）] までスクロールして、[追加（Add）] をクリックします。

3. [重大度の設定（Severity Settings）] を「**Medium Violation**」に変更することによってポリシーを編集します。これによって、以前にカスタマイズした違反設定（このポリシーに違反するメッセージの検疫エリアへの送信など）がポリシーで使用されるようになります。

    - [中レベルの重大度のインシデント（Medium Severity Incident）]：Medium Violation



4. [送信（Submit）] をクリックしてポリシーを作成します。

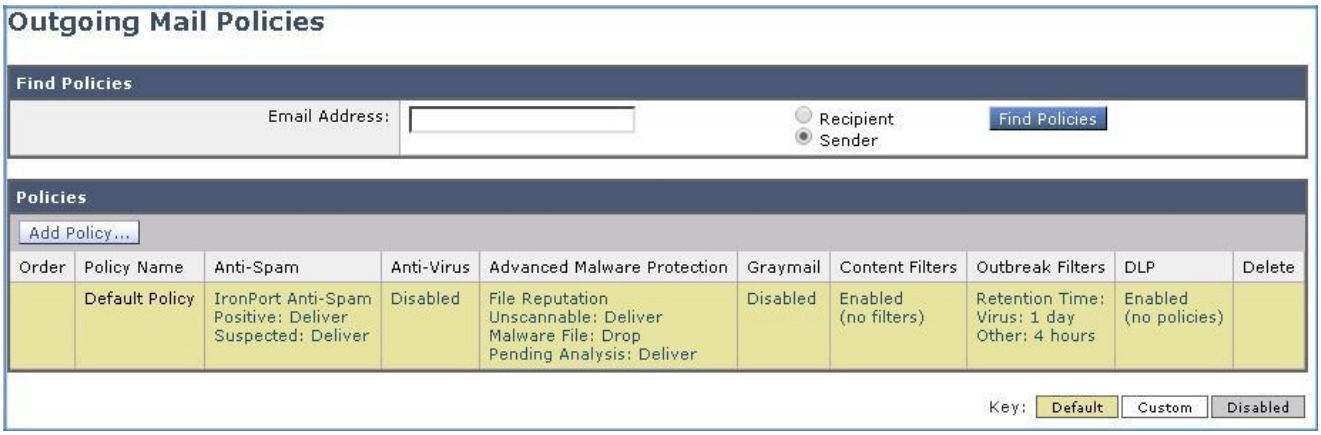


5. 完了したら画面の右上にある [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

タスク：送信メール ポリシーを設定する（推定所要時間：2 分）

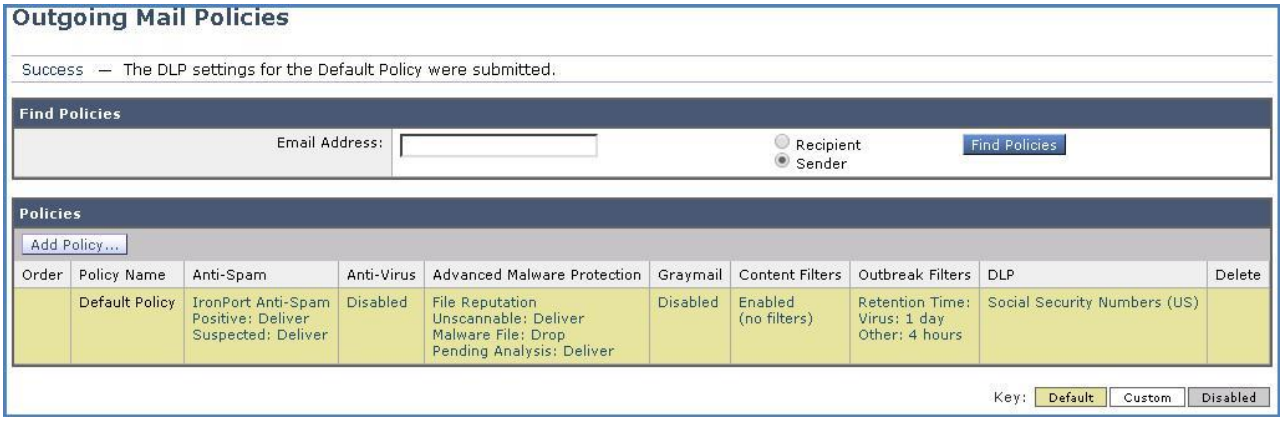
最後の手順では、送信メール ポリシーを設定して、以前に設定したすべてのコンポーネントを結合します。メール ポリシーは受信または送信のどちらでも作成できますが、データ損失防止などの一部の機能については、送信メッセージでのみ実行できます。

1. [メールポリシー（Mail Policies）] > [送信メール ポリシー（Outgoing Mail Policies）] に移動し、[DLP] 列の [有効（ポリシーなし）（Enabled (no policies)）] ハイパーリンクをクリックします。これにより、以前に定義したポリシーがデフォルト ポリシーに適用されます。



2. リスト内に 1 つだけあるポリシーにチェックマークを付け、[送信（Submit）] をクリックします。

3. DLP ポリシーが送信メール ポリシーの [DLP] セクションに追加されていることを確認します。

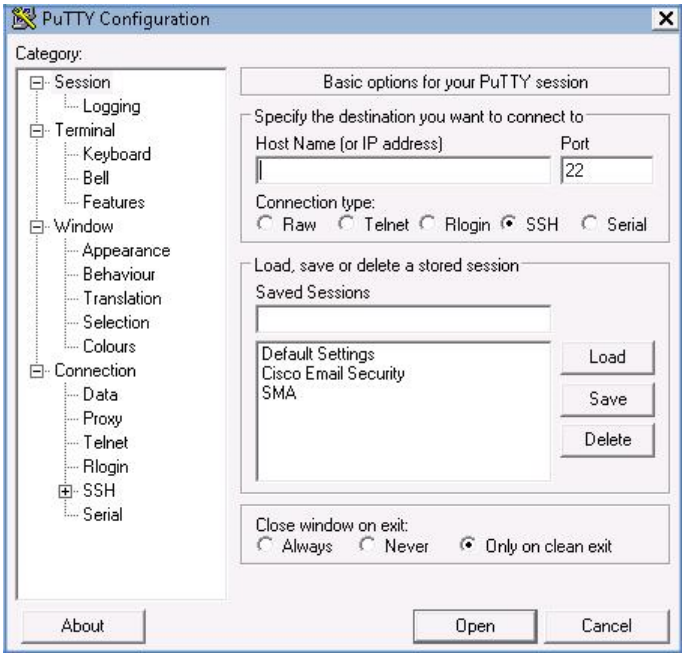


4. 最後に、[変更内容を確定（Commit Changes）] ボタンをクリックして、変更を適用します。必要に応じて任意のコメントを追加してください。

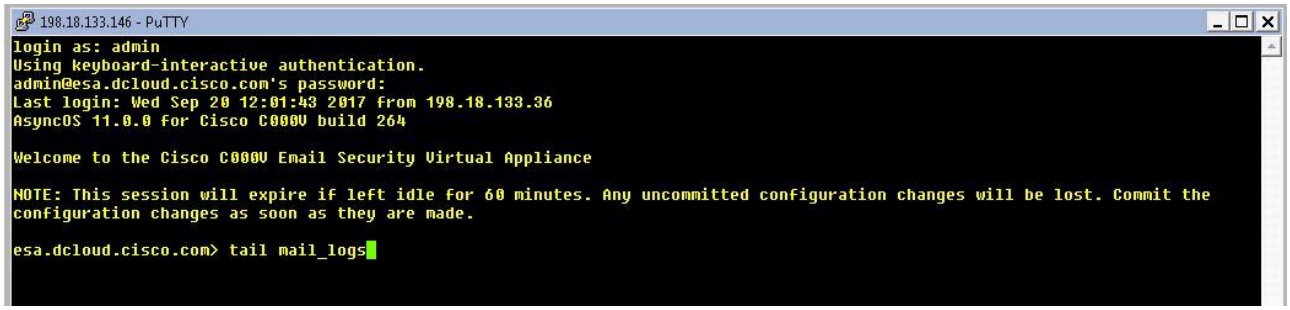
タスク：DLP ポリシーをテストする（推定所要時間：10 分）

必要なコンポーネントをすべて作成および設定したら、ポリシー内の Medium Violation がトリガーされるファイルが添付された電子メールを送信することによって、ポリシーをテストできます。CLI をモニタすることで、各メッセージに関するリアルタイム情報を確認できます。これは、Cisco E メール セキュリティ ソリューションによってメッセージがどのように処理されるか、またどのようなアクションが実行されるかを理解するために役立ちます。

1. ワークステーションから、タスクバーにある *PuTTY* を起動します。[保存済みセッション（Saved Sessions）] から「Cisco Email Security」を選択し、[開く（Open）] をクリックします。表示されるセキュリティ警告を確認します。

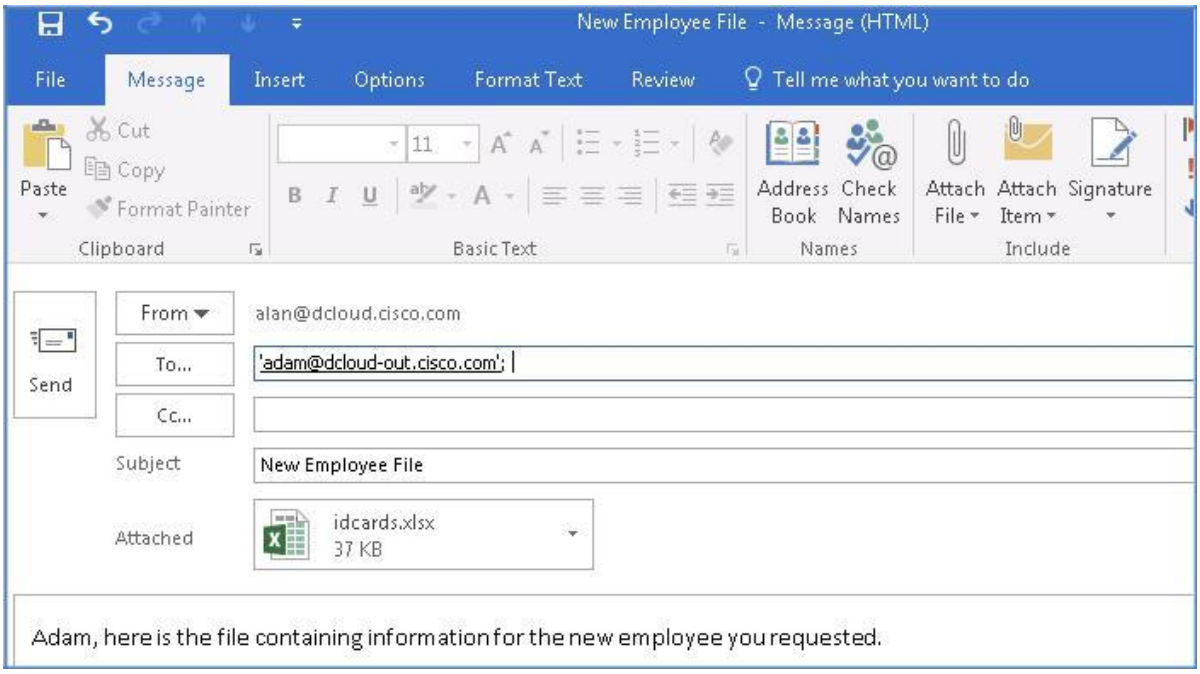


2. 前述のクレデンシャルを使用してログインします。ログインしたら、**tail mail_logs** コマンドを入力して Enter キーを押します。これをバックグラウンドで実行したまま、次の手順に進みます。

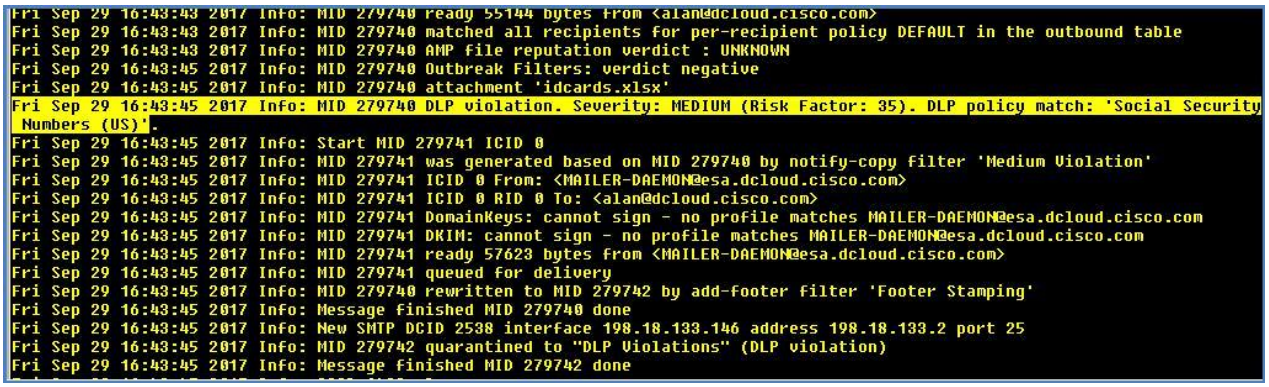


注:tail コマンドを使用すると、記録されるメール ログの最後の数行が端末に表示されます。これは、エラー メッセージまたはイベントが発生したときに、ログの最後の数行を参照してそれらを確認するために特に役立ちます。このコマンドは、Cisco E メール セキュリティ ソリューションで使用可能な 30 以上のログ ファイルのどれに対しても使用できます。目的のログ ファイルに関して tail コマンドを入力し、Enter キーを押すと、ログのリストが表示されます。

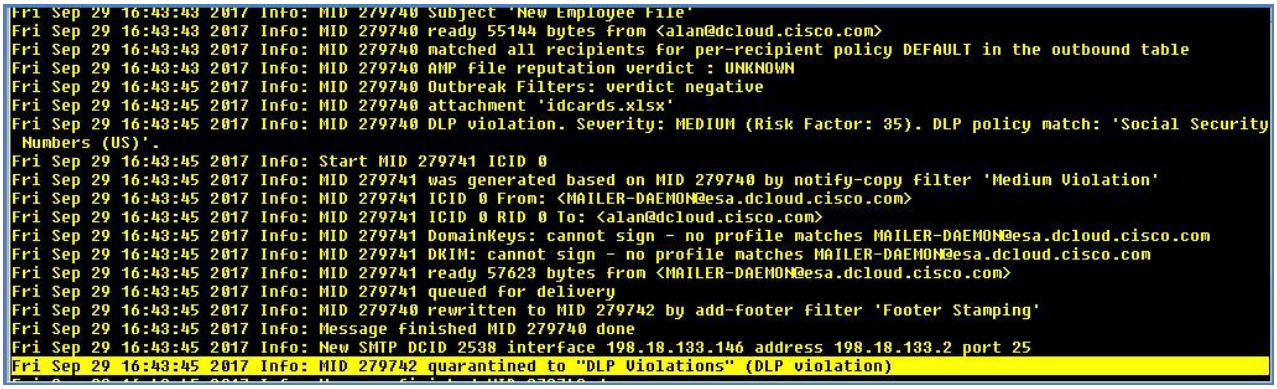
3. ワークステーションのタスク バーから Microsoft Outlook を起動し、次のパラメータで電子メールを準備します。
    - [差出人(From)]:alan@dcloud.cisco.com
    - [宛先(To)]:adam@dcloud-out.cisco.com
    - [件名(Subject)]:新入社員のファイル(New Employee File)
    - [本文(Body)]:Adam さん、依頼された新入社員の情報をファイルを送信いたします。ご査収ください。(Adam, Please find attached the file containing information for the new employees you requested.)
    - [添付ファイル(Attachment)]:IdCards.xlsx(保存先:デスクトップ上の Cisco DLP サブフォルダ内)



4. メールを送信します。[すべてのフォルダを送受信(Send/Receive Folder)] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。
5. 最初の手順で開いた CLI ウィンドウに戻ります。ログが表示されるまで数分かかる場合があります。
6. 最初の注目点は、メッセージに違反が含まれているという事実です。Social Security Numbers(社会保障番号)の場合は、リスク要因の 35 が Medium(中)レベルの違反の範囲内に入ります。



7. 次に、メッセージがカスタム DLP 検疫エリアにリダイレクトされたことに注目します。

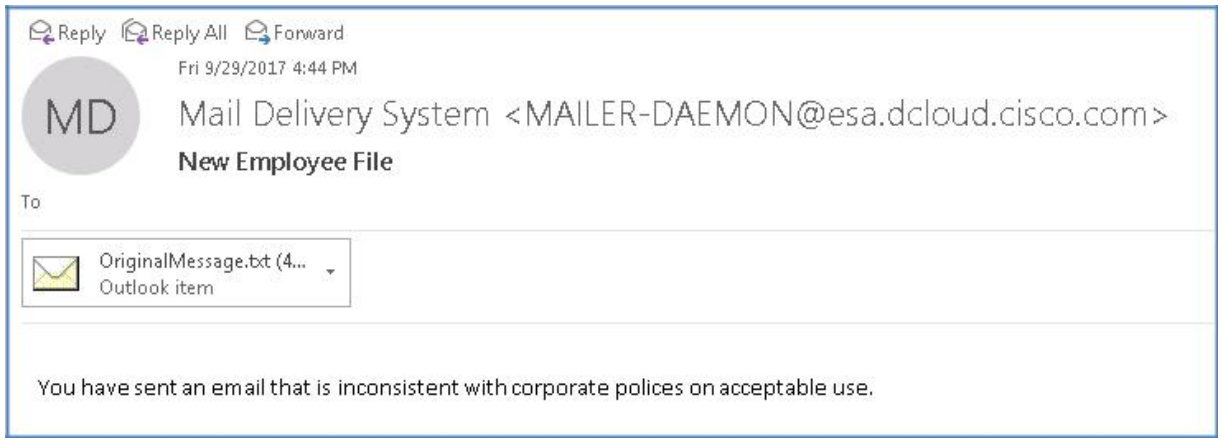


8. メッセージ ID（MID）を書き留めます。これは、後で相互に関連付けられます。

注：メッセージ ID（MID）は、ESA によって特定のメッセージに割り当てられている固有識別子です。MID は、シスコのアプライアンスによって受信されたすべてのメッセージに関連付けられており、メール ログで追跡できます。

注：異なるタイプの ID の詳細については、「What is a Message ID (MID), Injection Connection ID (ICID), or Delivery Connection ID (DCID)?」を参照してください。

9. Outlook クライアントに戻ると、この時点でメール ボックスが同期されています。同期されていない場合は、[すべてのフォルダを送受信（Send/Receive All Folders）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。
10. ここで、メッセージに関して実行されたアクションを確認できます。Alan に彼の違反を通知するカスタム メッセージ（以前に作成したもの）が適用され、Alan に配信されていることに注意してください。最も重要な点は、設定に従ってメッセージが検疫エリアにリダイレクトされたために、受信者には配信されていないことです。



タスク：DLP ポリシーをモニタする（推定所要時間：5 分）

[DLP インシデント（DLP Incidents）] ページには、送信メールで発生したデータ損失防止（DLP）ポリシー違反インシデントに関する情報が示されます。ソリューションでは、[送信メール ポリシー（Outgoing Mail Policies）] テーブルで有効にした DLP 電子メール ポリシーを使用して、ユーザが送信した秘密データが検出されます。

DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。DLP インシデント レポートを使用すると、次のような質問に答えることができます。

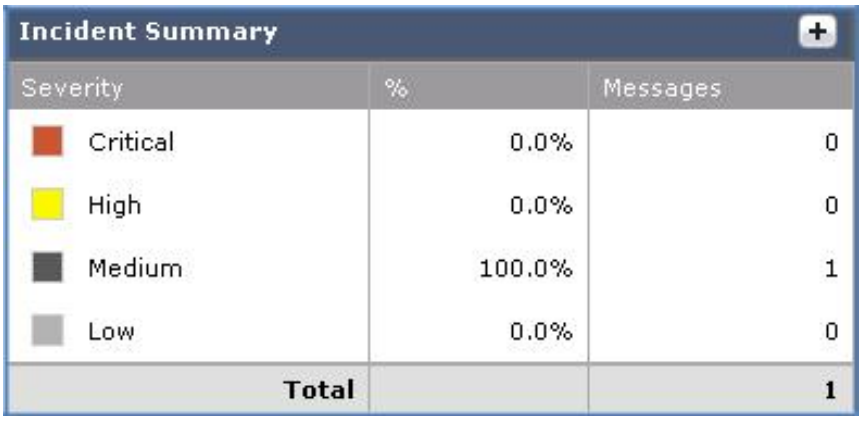
- ユーザが送信している秘密データのタイプ
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[DLP インシデント（DLP Incidents）] ページは、次の 2 つの主なセクションで構成されます。

- 重大度（[低（Low）]、[中（Medium）]、[高（High）]、[クリティカル（Critical）]）別の上位 DLP インシデントおよびポリシーの一致数を集約する DLP インシデントのトレンド グラフ
- [DLP インシデントの詳細（DLP Incidents Details）] リスト

このタスクでは、以前に発生した DLP インシデントについて、いくつかの分析を実行し、発生したことと発生した理由に関する詳細情報を取得します。

1. ワークステーションでの GUI セッションから、[モニタ（Monitor）] > [DLP インシデント（DLP Incidents）] レポートに移動すると、インシデント サマリーに Medium（中）レベルの違反が記録されています。

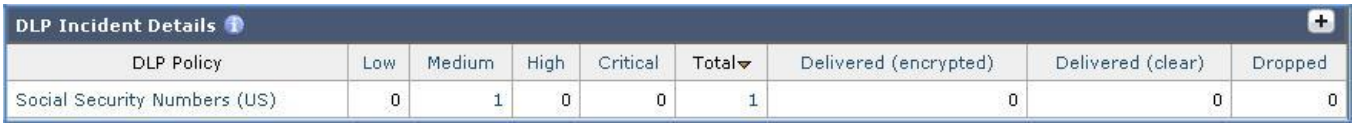


Incident Summary

Severity	%	Messages
Critical	0.0%	0
High	0.0%	0
Medium	100.0%	1
Low	0.0%	0
Total		**1**

注:場合によっては、違反を表示するためにウィンドウの表示を更新する必要があります。

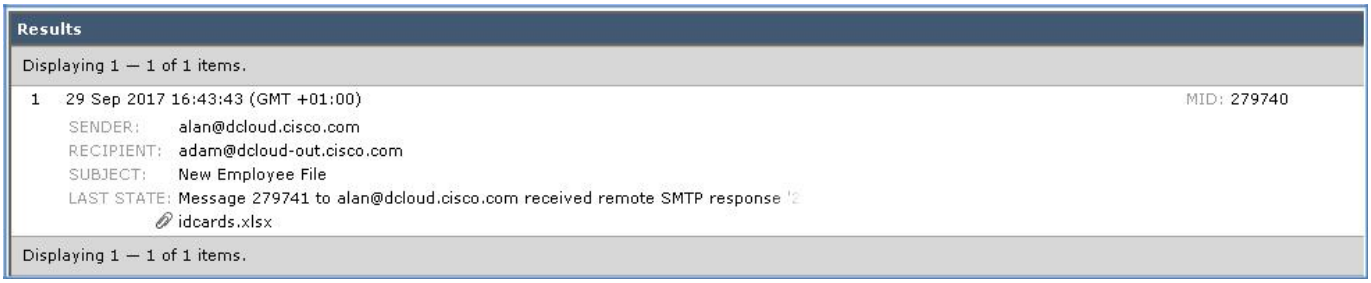
2. 画面の下部にスクロールして、インシデントの詳細を確認します。[中(Medium)] 列に違反が表示されます。



DLP Incident Details

DLP Policy	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
Social Security Numbers (US)	0	1	0	0	1	0	0	0

3. [中(Medium)] 列のインシデントをクリックすると、メッセージ トラッキング機能が起動し、メッセージ フローとそれに適用された各種アクションの詳細情報が表示されます。
4. メッセージ トラッキング ウィンドウから、[結果(Results)] セクションにスクロールし、以前のメッセージ ID(MID)と比較します。これは同じ値になります。



Results

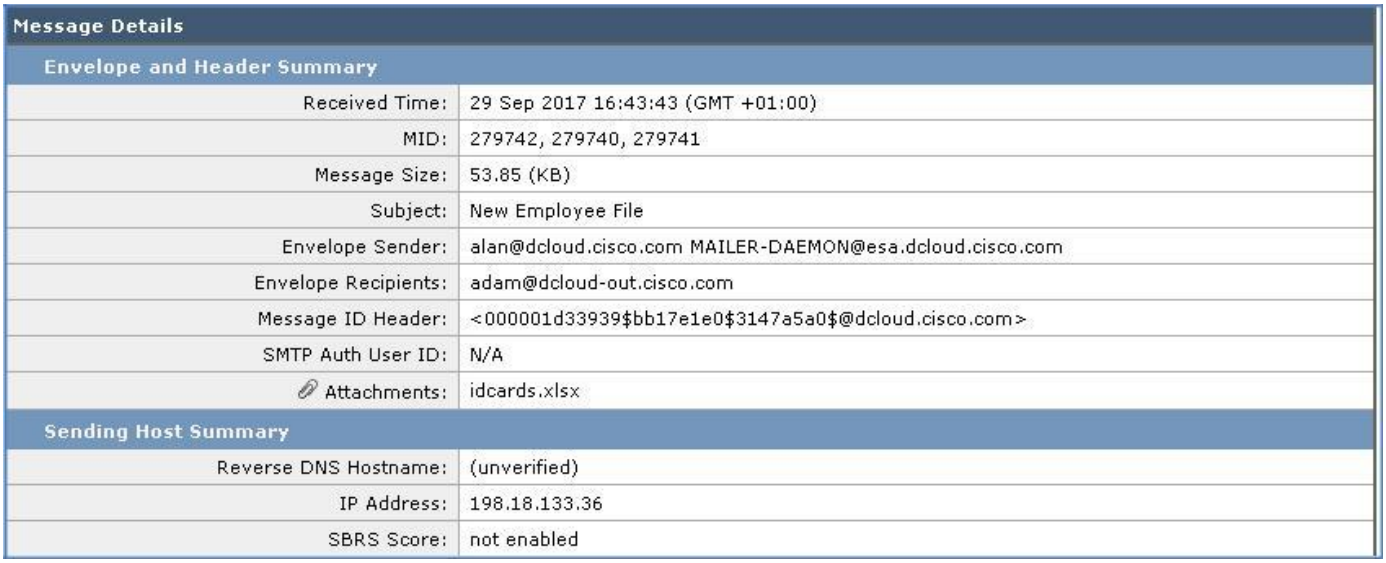
Displaying 1 — 1 of 1 items.

1 29 Sep 2017 16:43:43 (GMT +01:00) MID: 279740

SENDER: alan@dcloud.cisco.com
RECIPIENT: adam@dcloud-out.cisco.com
SUBJECT: New Employee File
LAST STATE: Message 279741 to alan@dcloud.cisco.com received remote SMTP response '2
idcards.xlsx

Displaying 1 — 1 of 1 items.

5. [詳細の表示（Show Details）] をクリックして、この特定のメッセージの詳細情報を表示します。



Message Details

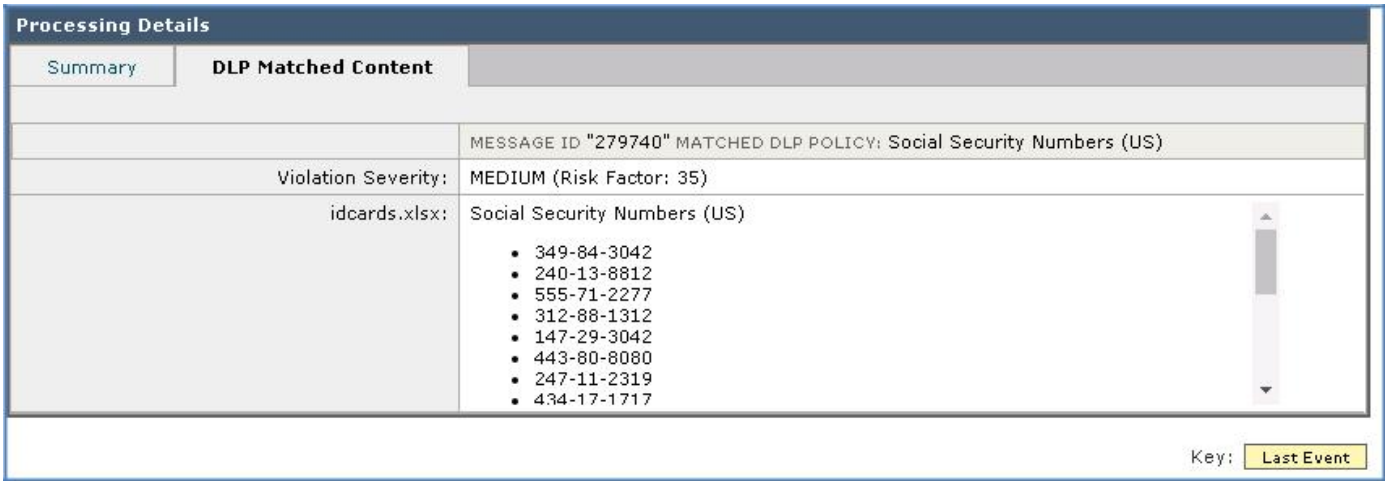
Envelope and Header Summary

Received Time:	29 Sep 2017 16:43:43 (GMT +01:00)
MID:	279742, 279740, 279741
Message Size:	53.85 (KB)
Subject:	New Employee File
Envelope Sender:	alan@dcloud.cisco.com MAILER-DAEMON@esa.dcloud.cisco.com
Envelope Recipients:	adam@dcloud-out.cisco.com
Message ID Header:	<000001d33939$bb17e1e0$3147a5a0$@dcloud.cisco.com>
SMTP Auth User ID:	N/A
Attachments:	idcards.xlsx

Sending Host Summary

Reverse DNS Hostname:	(unverified)
IP Address:	198.18.133.36
SBRS Score:	not enabled

6. [処理の詳細（Processing Details）] セクションで、[DLP と一致したコンテンツ（DLP Matched Content）] タブをクリックして、違反の原因となったコンテンツの正確な情報を確認します。



Processing Details

Summary | **DLP Matched Content**

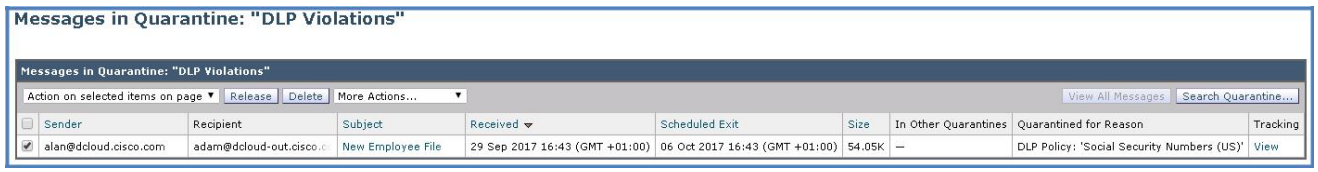
	MESSAGE ID "279740" MATCHED DLP POLICY: Social Security Numbers (US)
Violation Severity:	MEDIUM (Risk Factor: 35)
idcards.xlsx:	Social Security Numbers (US) • 349-84-3042 • 240-13-8812 • 555-71-2277 • 312-88-1312 • 147-29-3042 • 443-80-8080 • 247-11-2319 • 434-17-1717

Key: Last Event

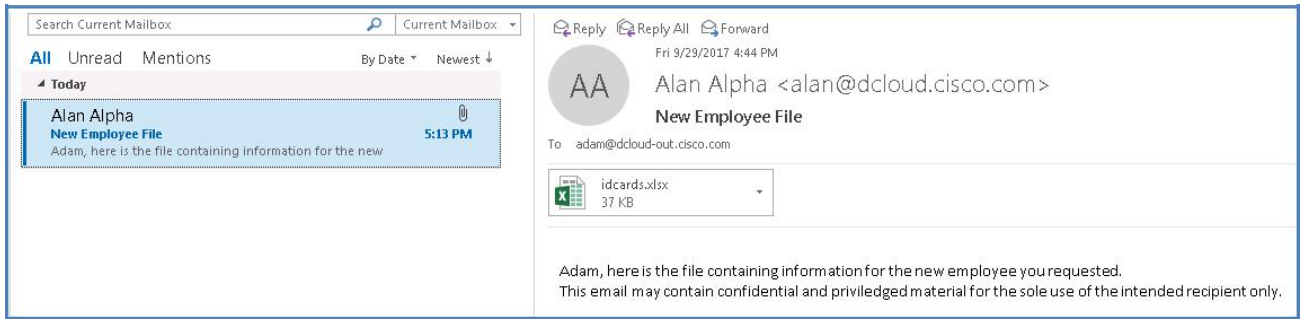
7. メッセージ トラッキング ウィンドウを閉じます。

8. [モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク検疫（Policy, Virus and Outbreak Quarantines）] > [DLP 違反（DLP Violations）] に移動すると、受信者の Adam に配信されないメッセージが、以前に作成した検疫エリアに格納されます。

9. [メッセージ（Messages）] 列の下の数字をクリックすると、メッセージの詳細情報が表示されます。メッセージを選択して [解放（Release）] ボタンをクリックし、メッセージが表示されたらアクションを確認します。



10. ワークステーションに戻ってメッセージをもう一度同期させると、メッセージが Adam のメール ボックスに表示されます。以前に設定した免責事項のテキストが追加されていることを確認できます。



11. 添付ファイルを開いて、コンテンツがもう一度表示されることを確認します。

注：通常、このような用途では、メッセージを送信する前に暗号化するか、メッセージを解放せずに検疫エリアに保持しておくことをお勧めします。

シナリオ 2:　疑わしい URL からの保護

使用例

Voyage Corp の広告部門では、製品の宣伝方法を改善するために、新しいキャンペーンに取り組むことを決定しました。これまでは、すべての広告を一般的な IT 誌に限って掲載してきました。広告業務担当のディレクタは、サービスによる収益が若干減少したことから、追加のリソースを投入し、製品とサービスに関する広告を家庭に確実に届けるようチームに依頼します。

IT 関係の Web サイトやブログを介した宣伝方法をよりよく理解するために、いくつかの広告代理店に相談しました。サンプル広告が複数のサイトに掲載され、それらの効果を確かめるため、毎週の統計情報が電子メールで広告マネージャに送信されることになりました。ある日の午後、広告マネージャは、一見無害なメッセージ内のリンクをクリックします。ブラウザは特定の Web サイトにリダイレクトされますが、重要なサービスを停止させる悪意のあるコードが（知らずとバックグラウンドで）ダウンロードされます。このことが社内サポート チームに報告されると、感染したマシンはすぐにネットワークから削除され、クレンジングとポスチャ アセスメントが実施されました。プロセス全体は完了まで数日を要しました。また、これによってアウトブレイク フィルタリング テクノロジーの導入が促されました。

セキュリティ制御

悪意のあるリンクや望ましくないリンクに対する制御と保護は、作業キュー内のスパム対策、アウトブレイク、コンテンツ、およびメッセージ フィルタリング プロセスに組み込まれます。これらの制御により、メッセージ内の悪意のある URL に対して保護効果が向上します。

URL フィルタリングはアウトブレイク フィルタリングに組み込まれます。こうして向上した保護効果は、侵入ポイントで脅威をブロックできるため、組織がすでに Web ベースの脅威からの保護（Cisco Web セキュリティ アプライアンスなど）を導入している場合でも有用です。

目的

このシナリオでは、Cisco セキュリティ プロキシ サービスを活用することで、マルウェアの感染源となっている可能性のある Web サイトへのアクセスをブロックし、電子メール内の悪意のある URL から保護します。

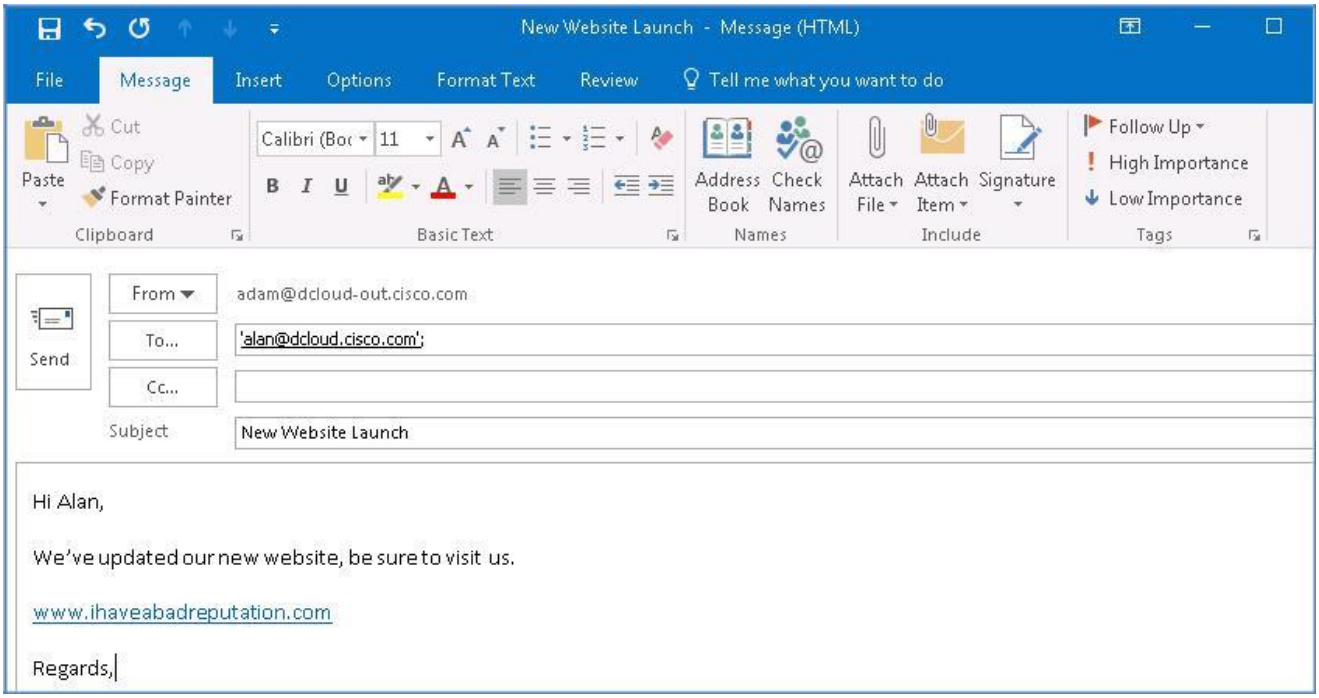
手順

タスク：メッセージ内の URL にアクセスする（推定所要時間：5 分）

1. 最初のタスクでは、メッセージ内の疑わしい URL を通知するメカニズムが導入されていない状況下で、電子メール内の潜在的に悪意のあるリンクによって何が起こるのかを示します。

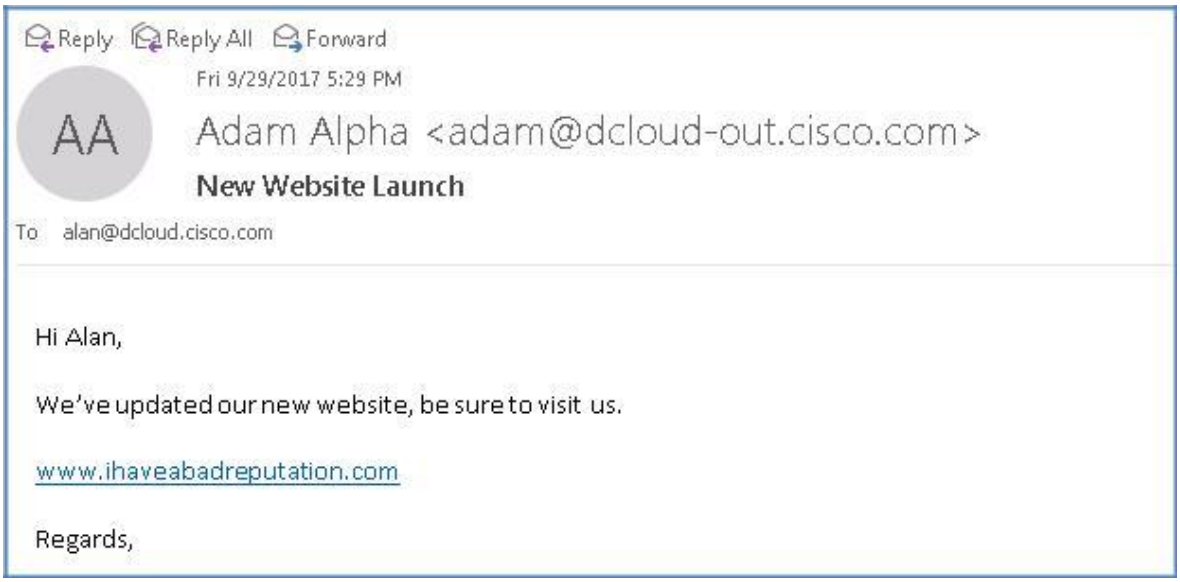
2. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。

   - [宛先(To)]:alan@dcloud.cisco.com
   - [件名(Subject)]:新しい Web サイトの立ち上げ(New Website Launch)
   - [本文(Body)]:Hi Alan,(Alan 様)
     Web サイトを更新しました。ぜひアクセスしてください。(We've updated our website, be sure to visit us.)
     www.ihaveabadreputation.com
     Regards,(よろしくお願いします。)

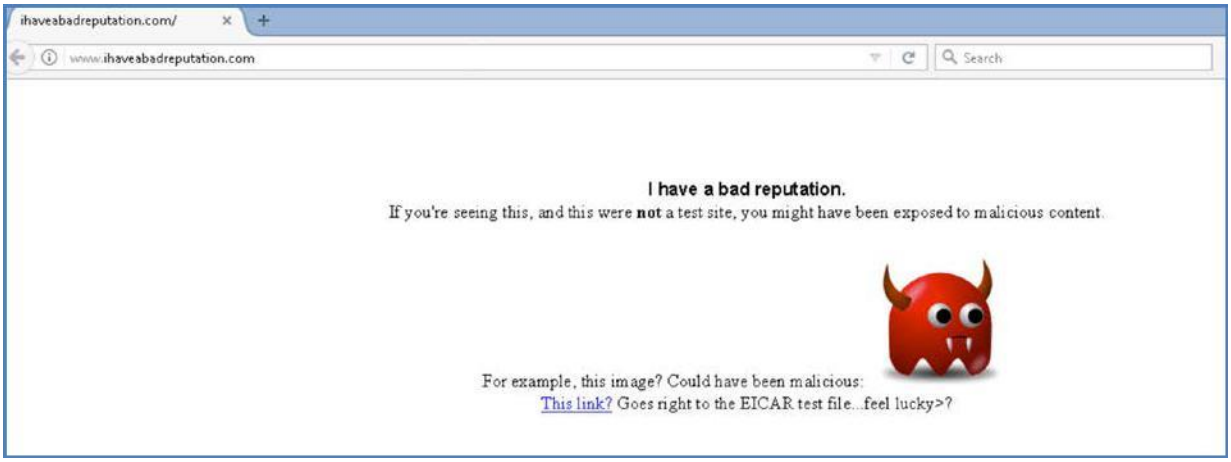


3. メールを送信します。[すべてのフォルダを送受信(Send/Receive Folder)] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

4. Alan の受信トレイを調べて、メッセージの受信を確認します。疑わしいハイパーリンクを含むメッセージが、そのままの状態で着信していることを確認できます。



5. メッセージ内のハイパーリンクを一度クリックすると、サイトにアクセス可能な状態でブラウザが起動します。これが悪意のあるコンテンツを含むサイトであれば、リンクをクリックしたエンド ユーザがリスクにさらされ、相互接続されたデバイス間で悪影響が迅速に広がる可能性があります。



6. ブラウザのウィンドウを閉じます。

タスク:コンテンツ フィルタを設定する(推定所要時間:3 分)

コンテンツ フィルタは、ウイルス対策スキャンや DLP などの他のコンテンツ セキュリティ機能による標準ルーチン処理以外のメッセージ処理をカスタマイズするために使用されます。

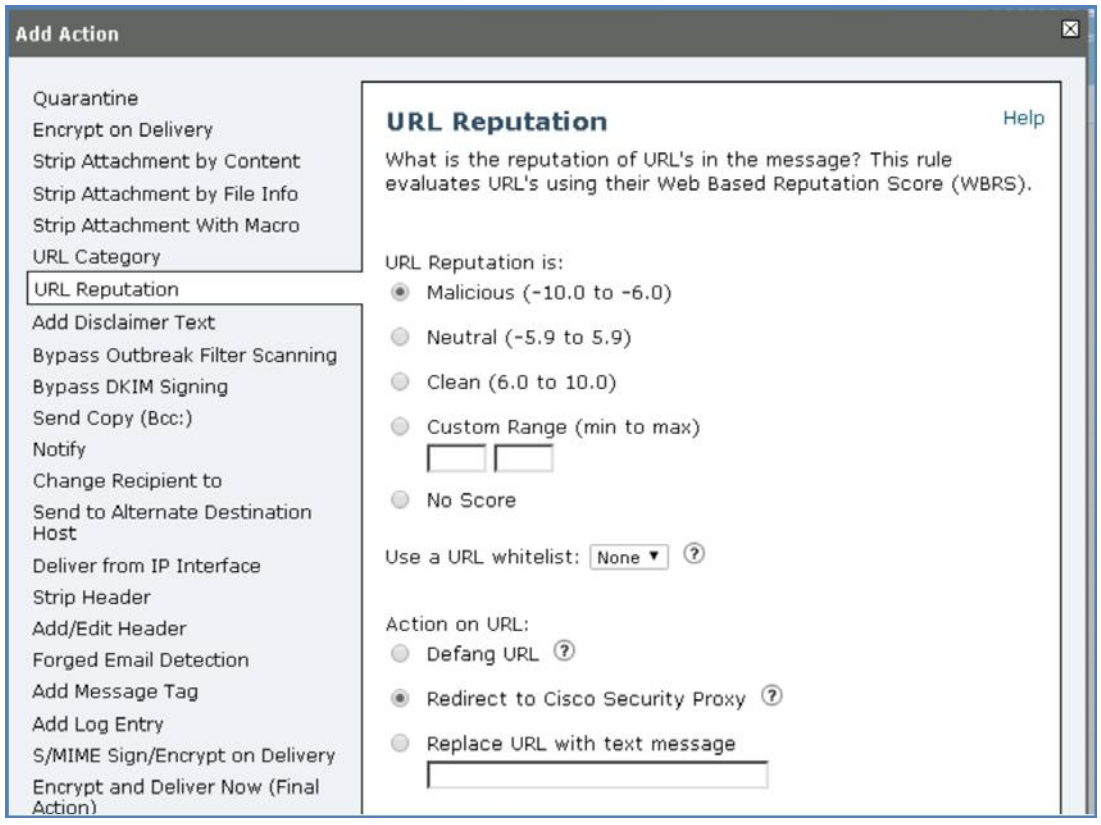
たとえば、後で検査するためにコンテンツを検疫する必要がある場合や、企業ポリシーのために特定のメッセージを配信前に暗号化する必要がある場合に、コンテンツ フィルタを使用できます。

コンテンツ フィルタには次のコンポーネントがあります。

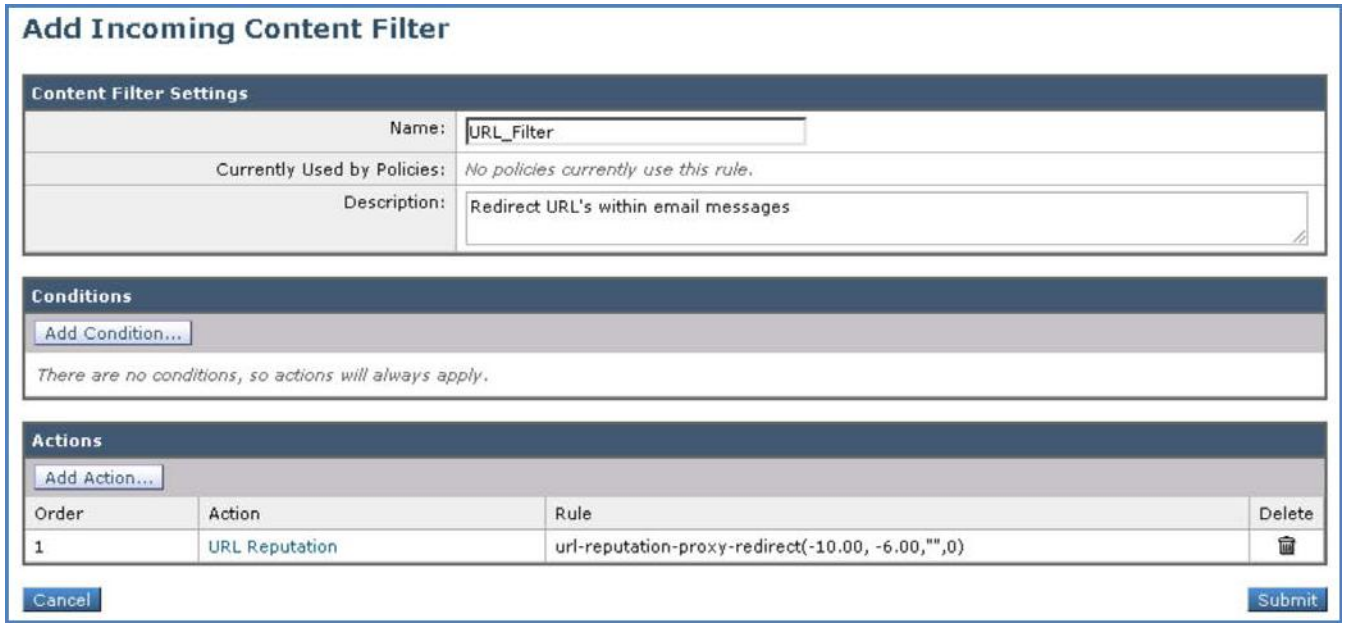
- ***条件***:ソリューションがコンテンツ フィルタを使用してメッセージをスキャンするタイミングを決定します(任意)。
- ***アクション***:メッセージに関してソリューションが実行します(必須)。

このタスクでは、電子メール メッセージ内で疑わしい URL を特定し、メッセージに対して適切なアクション(Cisco セキュリティ プロキシによってダイレクトし、その URL が実際に有害である可能性があるかどうかを判定する)を実行する新しいコンテンツ フィルタを作成します。

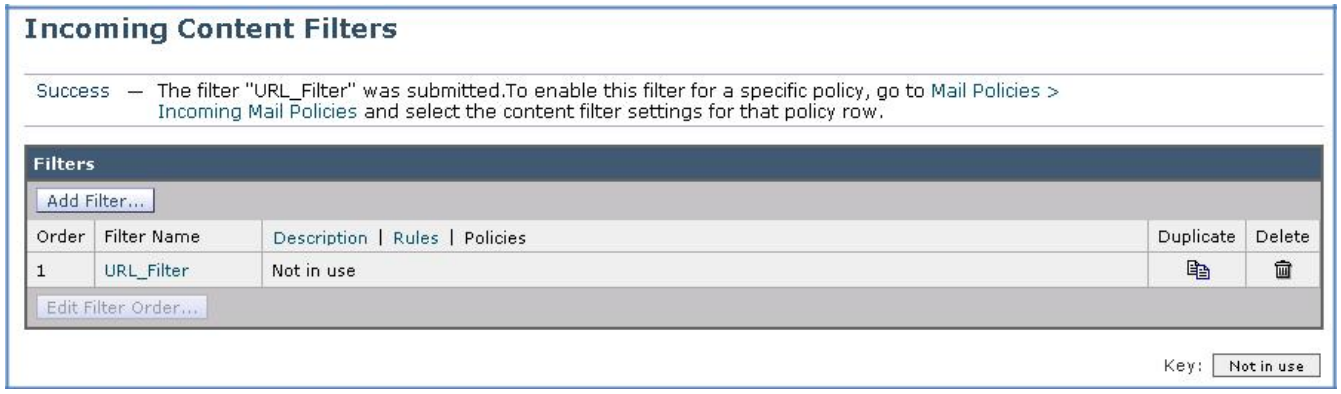
1. ワークステーションから GUI にアクセスし、[メール ポリシー(Mail Policy)] > [受信コンテンツ フィルタ(Incoming Content Filters)] に移動して、[フィルタの追加(Add Filter)] をクリックします。
2. 次の設定で*条件*と*アクション*を設定します。
   - [名前(Name)]:URL_Filter
   - [説明(Description)]:電子メール メッセージ内の URL をリダイレクトし(Redirect URLs within email messages)
   - [アクション(Action)] の 1:[URL レピュテーション(URL Reputation)] > [Cisco セキュリティ プロキシにリダイレクト(Redirect to Cisco Security Proxy)]



3. [OK] をクリックします。



4. [送信(Submit)] をクリックしてアクションを適用します。



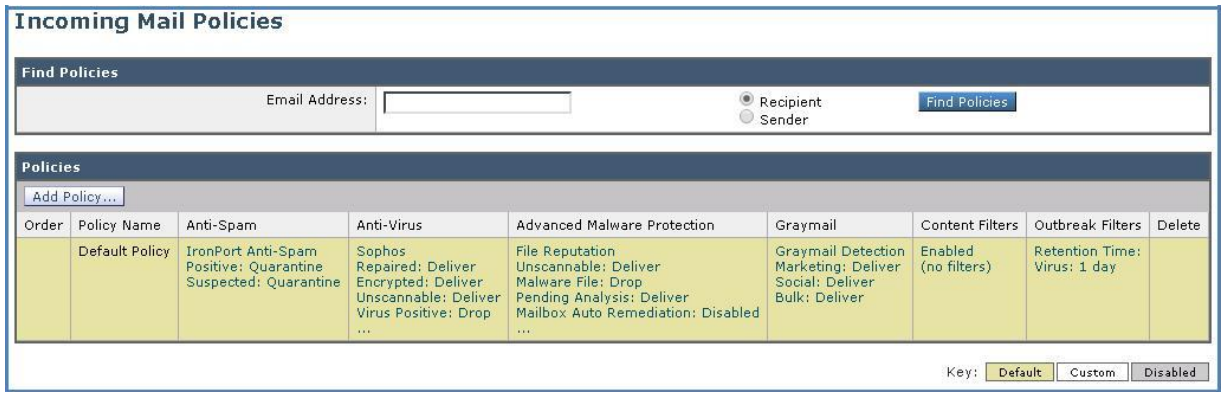
5. 完了したら [変更内容を確定(Commit Changes)] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

注:コンテンツ フィルタの動作とその柔軟性の詳細については、「Overview of Content Filters」を参照してください。

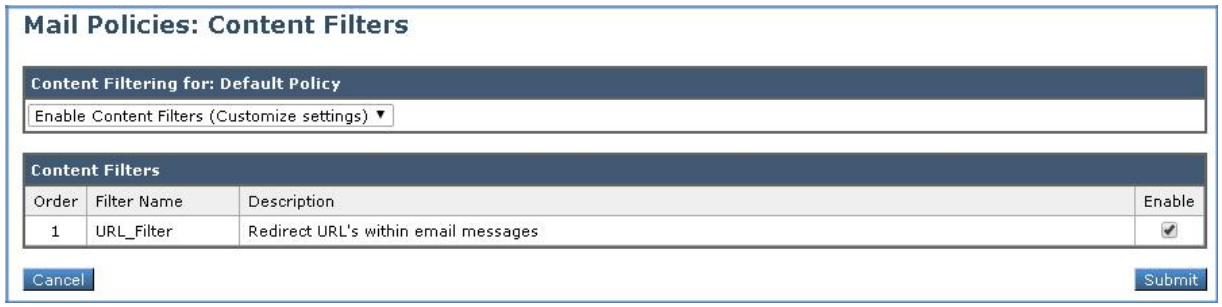
タスク:受信メール ポリシーを編集する(推定所要時間:1 分)

必要なコンテンツ フィルタを設定した後に使用するには、メール ポリシーに対して有効にする必要があります。

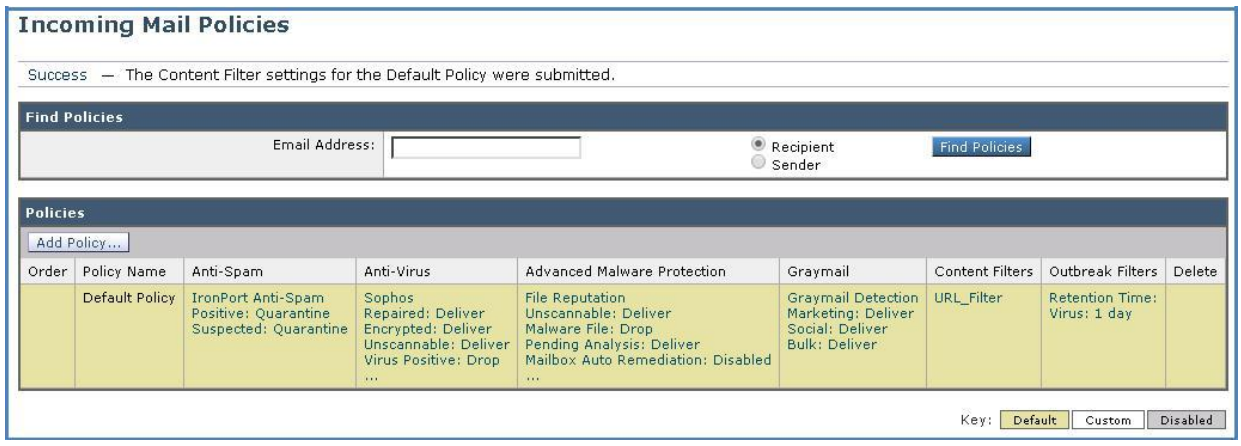
1. ワークステーションから GUI にアクセスし、[メール ポリシー(Mail Policy)] > [受信メール ポリシー(Incoming Mail Policies)] に移動して、[デフォルト ポリシー(Default Policy)] の [コンテンツ フィルタ(Content Filters)] ボックス内をクリックします。



2. 前の手順で作成した「**URL_Filter**」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。



3. [送信（Submit）] をクリックしてコンテンツ フィルタを作成し、ポリシーを確認します。



4. 完了したら画面の右上にある [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

注：メール ポリシーの詳細については、「Mail Policies」を参照してください。

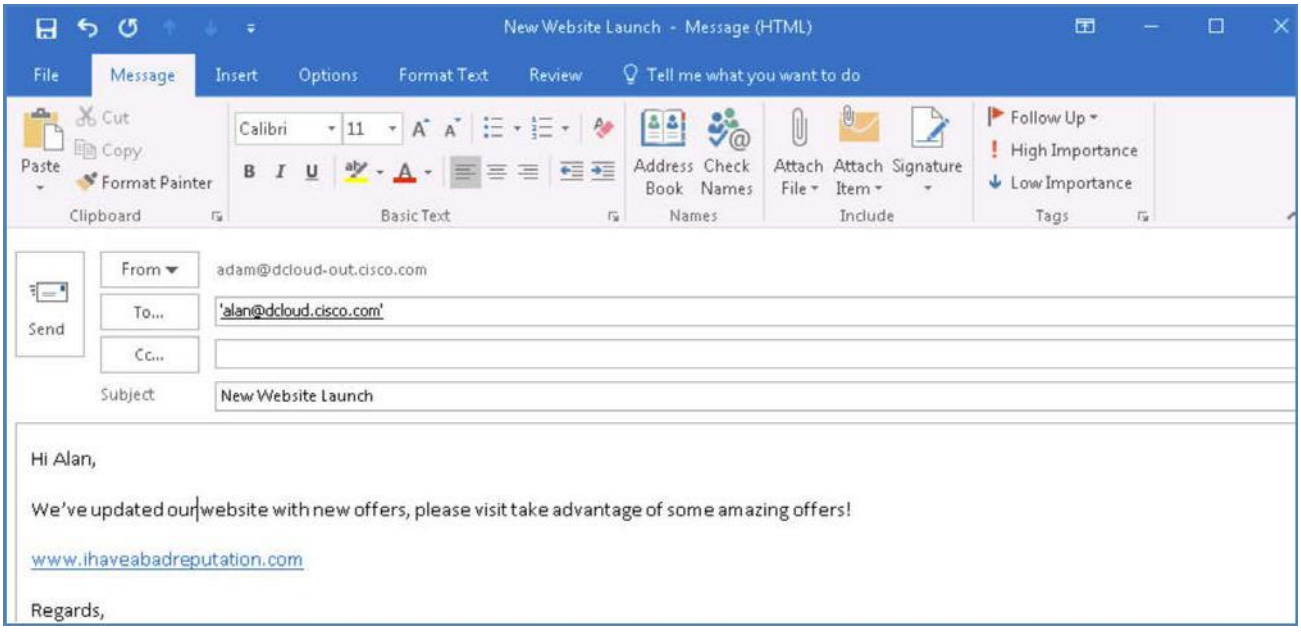
タスク：URL フィルタリングをテストする（推定所要時間：5 分）

前提条件となる構成が完了していれば、メッセージ本文に潜在的に悪意のある URL が記載された電子メールを社外ユーザの Adam から Alan に送信することによって、URL フィルタリング機能をテストできます。

CLI セッションの開始

メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。

1. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。
   - [宛先（To）]：alan@dcloud.cisco.com
   - [件名（Subject）]：新しい Web サイトの立ち上げ（New Website Site）
   - [本文（Body）]：Hi Alan,（Alan 様）
     Web サイトを更新して新しいオファーを紹介しています。ぜひアクセスして、いくつかの魅力的なオファーをご確認ください。（We've updated our website with new offers, please visit to take advantage of some amazing offers!）
     www.ihaveabadreputation.com
     Regards,（よろしくお願いします。）

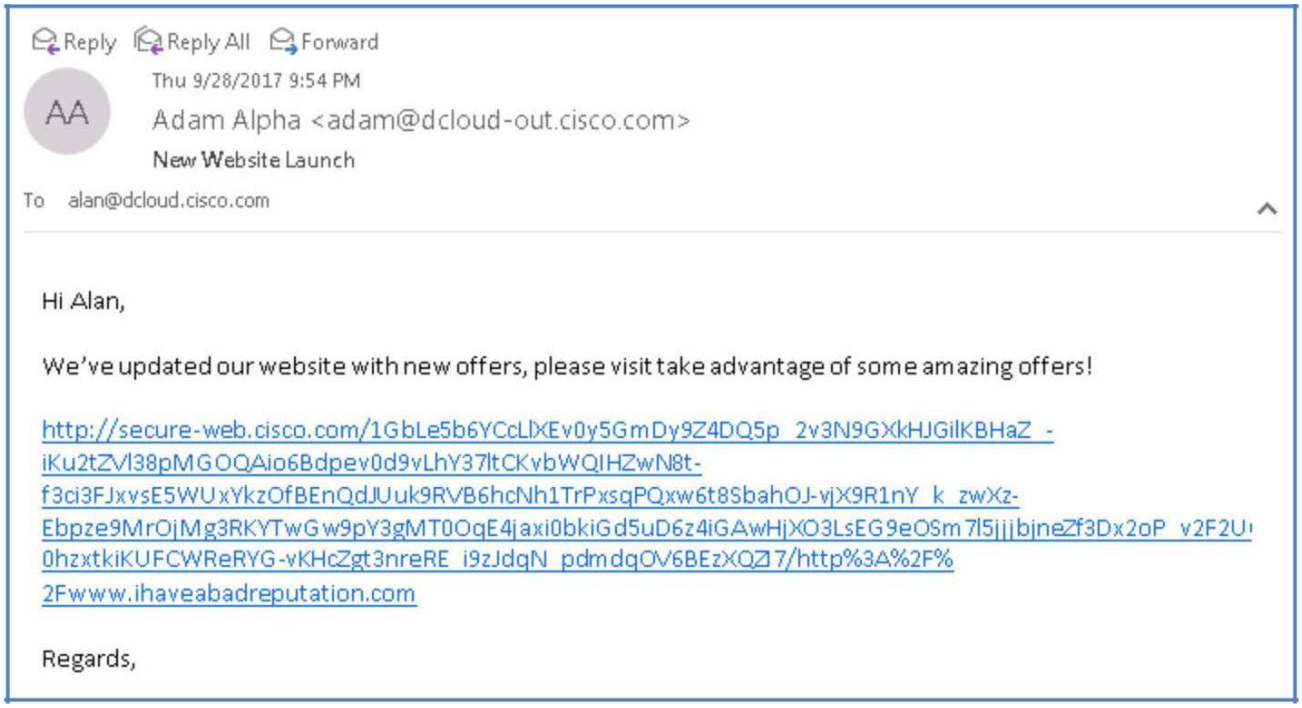


2. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

3. CLI に戻り、コンテンツ フィルタによってメッセージがどのように処理されたのかを確認します。メッセージは Cisco セキュリティ プロキシにリダイレクトされており、Web レピュテーションに基づいて、メッセージ内の URL が有害である可能性が判定されます。

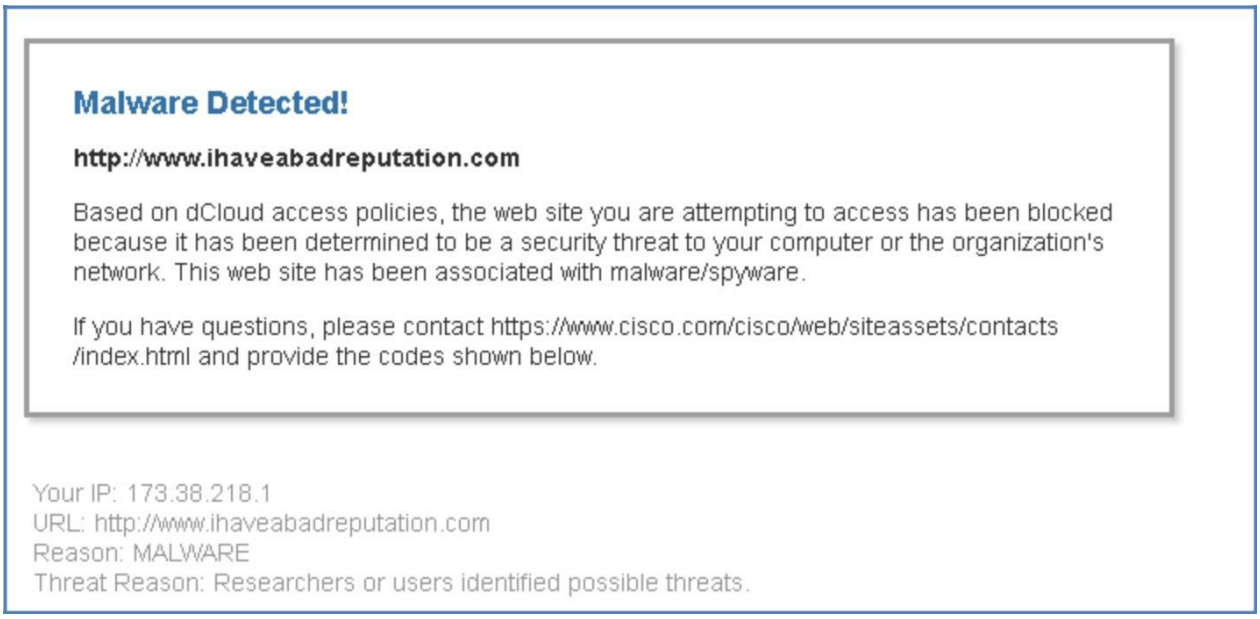
```
Fri Sep 29 17:38:05 2017 Info: Start MID 279747 ICID 6431
Fri Sep 29 17:38:05 2017 Info: MID 279747 ICID 6431 From: <adam@dcloud-out.cisco.com>
Fri Sep 29 17:38:05 2017 Info: MID 279747 ICID 6431 RID 0 To: <alan@dcloud.cisco.com>
Fri Sep 29 17:38:05 2017 Info: MID 279747 Message-ID '<002101d33941$5356c7d0$fa045770$@dcloud-out.cisco.com>'
Fri Sep 29 17:38:05 2017 Info: MID 279747 Subject 'New Website Launch'
Fri Sep 29 17:38:05 2017 Info: MID 279747 ready 3385 bytes from <adam@dcloud-out.cisco.com>
Fri Sep 29 17:38:05 2017 Info: MID 279747 matched all recipients for per-recipient policy DEFAULT in the inbound table
Fri Sep 29 17:38:05 2017 Info: MID 279747 interim verdict using engine: CASE spam negative
Fri Sep 29 17:38:05 2017 Info: MID 279747 using engine: CASE spam negative
Fri Sep 29 17:38:05 2017 Info: MID 279747 interim AV verdict using Sophos CLEAN
Fri Sep 29 17:38:05 2017 Info: MID 279747 antivirus negative
Fri Sep 29 17:38:05 2017 Info: MID 279747 AMP file reputation verdict : SKIPPED (no attachment in message)
Fri Sep 29 17:38:05 2017 Info: MID 279747 using engine: GRAYMAIL negative
Fri Sep 29 17:38:05 2017 Info: MID 279747 rewritten to MID 279748 by url-reputation-proxy-redirect-action filter 'URL_Filter'
Fri Sep 29 17:38:05 2017 Info: Message finished MID 279747 done
Fri Sep 29 17:38:05 2017 Info: MID 279748 Outbreak Filters: verdict negative
Fri Sep 29 17:38:05 2017 Info: MID 279748 queued for delivery
Fri Sep 29 17:38:05 2017 Info: New SMTP DCID 2543 interface 198.18.133.146 address 198.18.133.2 port 25
Fri Sep 29 17:38:05 2017 Info: Delivery start DCID 2543 MID 279748 to RID [0]
Fri Sep 29 17:38:06 2017 Info: Message done DCID 2543 MID 279748 to RID [0]
Fri Sep 29 17:38:06 2017 Info: MID 279748 RID [0] Response '2.6.0 <002101d33941$5356c7d0$fa045770$@dcloud-out.cisco.com> [Inter
nalId=4] Queued mail for delivery'
Fri Sep 29 17:38:06 2017 Info: Message finished MID 279748 done
Fri Sep 29 17:38:07 2017 Info: ICID 6431 close
Fri Sep 29 17:38:11 2017 Info: DCID 2543 close
```

4. Alan の受信トレイに戻り、この時点で URL がどのように変更されているかを確認します。ハイパーリンクは、Cisco セキュリティ プロキシへのリダイレクトが含まれているため、はるかに長くなっています。

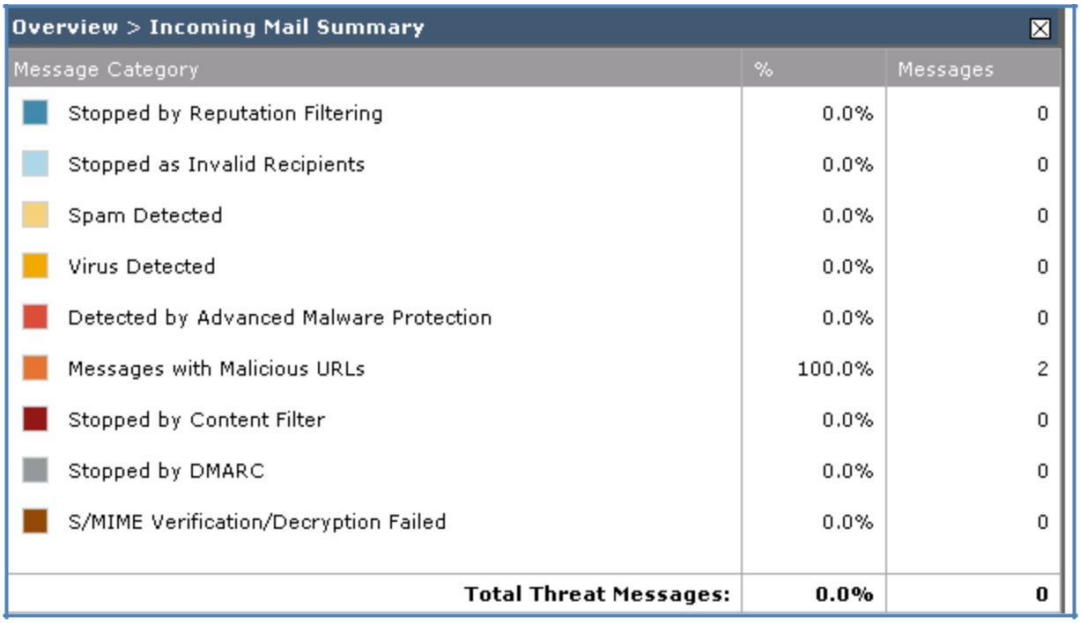


注:URL のレピュテーションとカテゴリは、クラウドベースの Cisco Web セキュリティ サービスによって提供されます。E メール セキュリティ ソリューションは、直接または Web プロキシを介して、Cisco Web セキュリティ サービスに接続します。その際は、「Firewall Information」で URL フィルタリング サービス用に指定されているポートが使用されます。通信は、相互証明書認証によって HTTPS を介して行われます。

5. URL を一度クリックしてブラウザでその URL にアクセスすることにより、以前に設定したポリシーに従い、レピュテーションに基づいて、その URL へのアクセスが厳格に禁止されていることを確認します。



6. [モニタ(Monitor)] > [マイダッシュボード(My Dashboard)] に移動し、発生したアクションが [悪意のある URL を含むメッセージ(Messages with Malicious URLs)] 項目に反映されていることを確認します。



Message Category	%	Messages
Stopped by Reputation Filtering	0.0%	0
Stopped as Invalid Recipients	0.0%	0
Spam Detected	0.0%	0
Virus Detected	0.0%	0
Detected by Advanced Malware Protection	0.0%	0
Messages with Malicious URLs	100.0%	2
Stopped by Content Filter	0.0%	0
Stopped by DMARC	0.0%	0
S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:	**0.0%**	**0**

注: 悪意のある URL または望ましくない URL からの保護の詳細については、「Protecting Against Malicious or Undesirable URLs」を参照してください。

シナリオ 3:　アウトブレイク フィルタ

使用例

Voyage Corp のサービス部門は最近、小売業界向けにカスタマイズされたサービスの新しいカタログを発表しました。このカタログにより、同社のサポート部門が提供するさまざまな IT 製品の調達、利用、およびサポートが容易になります。カタログの発表を後押しするため、電子メールを中心とする優れたマーケティング キャンペーンも開始されました。

マーケティング メールを配信するためにメーリング リストが使用されましたが、すべての返信は、キャンペーンに関する指標を収集するマーケティング コーディネータに送信されました。マーケティング コーディネータは、一見安全な添付ファイルと URL を含んだ電子メールを受け取りましたが、その URL をクリックすると、感染したペイロードが PC に持ち込まれました。社内では複数のウイルス対策エンジンが導入されていますが、いずれのエンジンもそのペイロードは検出できなかったのです。

セキュリティ制御

このシナリオでは、アウトブレイク フィルタが URL ベースの標的型の脅威からユーザをどのように保護するのかを示します。

標的型の脅威の量が少ない場合は、検出が難しくなることがあります。スパム対策の設定を高くしすぎると誤検出が増加し、ユーザは検疫エリアから正規のメッセージを探さなければならなくなります。これに対し、スパム対策の設定を低くしすぎると、受信する迷惑メールが増加します。

アウトブレイク フィルタは、疑わしい電子メールをさらにチェックします。これらのチェックによって不適切と判断されたメッセージを、ESA は URL を書き換えて検疫し、そのメッセージの解放後に再スキャンしてから配信します。配信前に検疫があることで、その時間内に新たに作成されたルールによって、検疫されたメッセージがスパムまたは悪意のあるメッセージかどうかを識別できる時間が ESA に与えられることになります。

目的

このシナリオでは、アウトブレイク フィルタにより、大規模なウイルス アウトブレイクやより小規模のウイルス以外の攻撃（フィッシング詐欺やマルウェア配信など）から組織がどのように保護されるのかを示します。データが収集されてソフトウェア アップデートが公開されるまでは新しいアウトブレイクを検出できない、大半のマルウェア対策セキュリティ ソフトウェアとは異なります。

注: このシナリオの前提条件タスクの一部は、これまでのシナリオで設定されています（免責事項など）。この演習の免責事項を作成する手順は、前のシナリオと同様です。

手順

タスク：アウトブレイク フィルタの免責事項を確認する（推定所要時間：2 分）

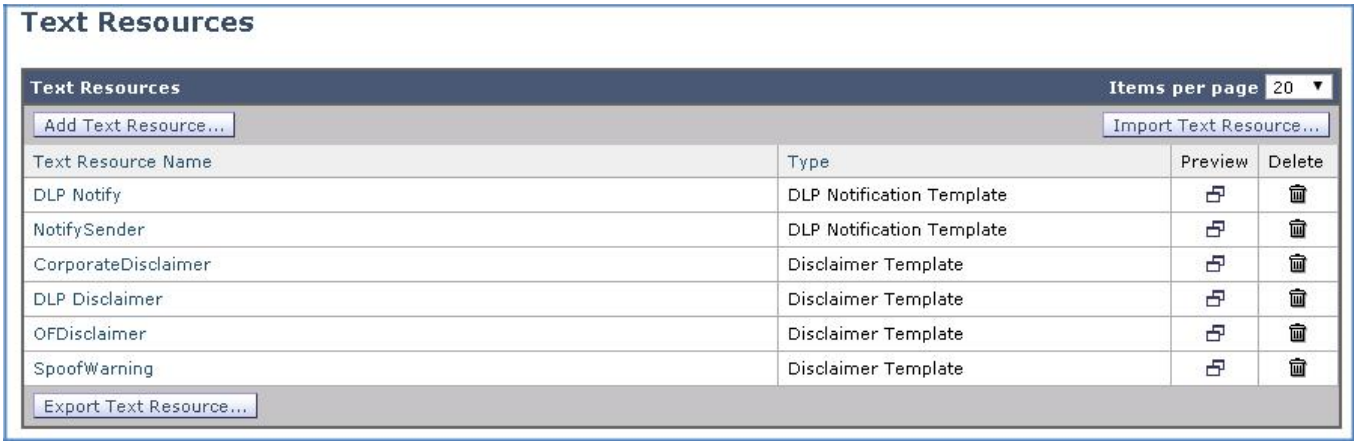
前のシナリオと同様に、Cisco E メール セキュリティ ソリューションでのポリシー設定では、テキスト リソースが重要な役割を果たします。アウトブレイク フィルタでは、悪意のあるアクションの完了を阻害するポリシーがソリューションによって適用される場合に、重要な情報とフィードバックをユーザに表示できます。

1. 免責条項内では、より詳細な情報を提供するためにアクション変数を使用できます。たとえば、アウトブレイク フィルタの利用時に、次のアクション変数を使用できます。

$threat_category	Replaced with the type of Outbreak Filters threat, such as phishing, virus, scam, or malware.
$threat_type	Replaced by a subcategory of the Outbreak Filters threat category. For example, can be a charity scam, a financial phishing attempt, a fake deal, etc.
$threat_description	Replaced by a description of the Outbreak Filters threat.
$threat_level	Replaced by the message's threat level (score 0 - 5).
$threat_verdict	Replaced by Yes or No, depending on the Message Modification Threat Level threshold. If the viral or non-viral threat level of a message is greater than or equal to the message modification threat level threshold, the value of this variable is set to Yes.

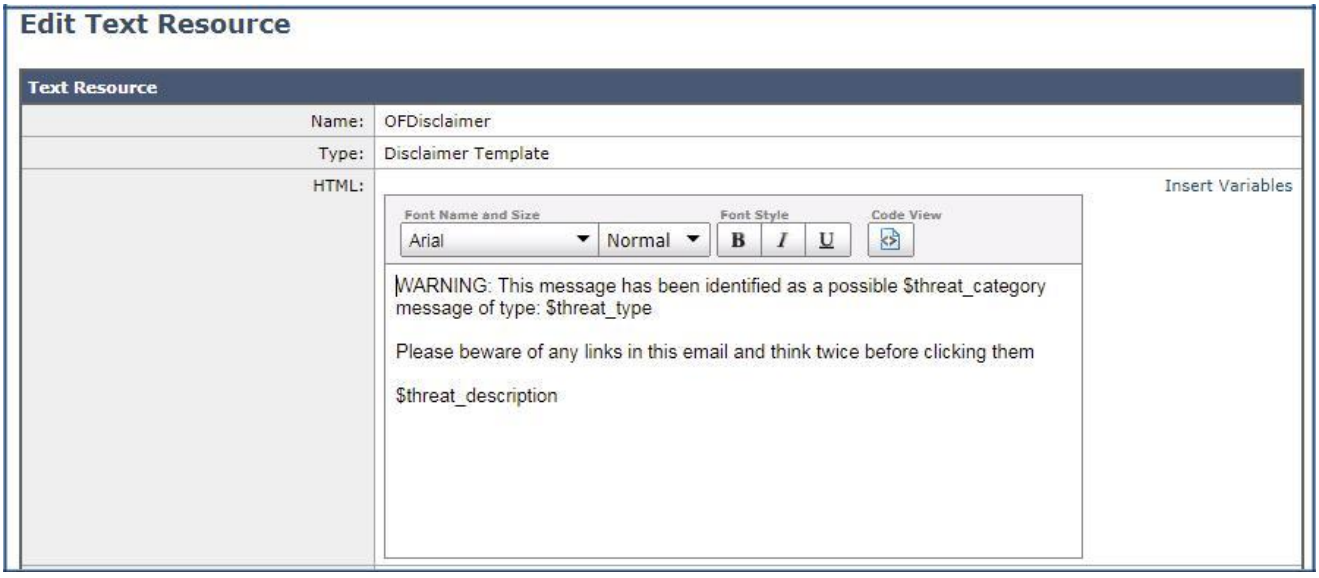
2. このタスクのために、事前設定されたアウトブレイク フィルタの免責事項を確認および検討します。

3. [メール ポリシー（Mail Policies）] > [テキスト リソース（Text Resources）] に移動し、テキスト リソースのリストから、事前設定された [OFDisclaimer] をクリックします。



4. このタイプの免責事項では、HTML テキストとアクション変数が使用されます。HTML ベースのメッセージとプレーン テキスト メッセージの両方を含むテキスト リソースが電子メール メッセージに適用された場合、HTML ベースのテキスト リソース メッセージは電子メール メッセージのテキストまたは HTML 部分に適用され、プレーン テキスト メッセージは電子メール メッセージのテキストまたはプレーン部分に適用されます。

5. HTML ベースのテキスト リソースを編集する場合は、HTML コードを手動で記述することなくリッチ テキストを入力できるリッチ テキスト編集機能を備えた GUI を使用できます。



6. [キャンセル(Cancel)] ボタンをクリックすると、前の画面に戻ります。変更は必要ありません。

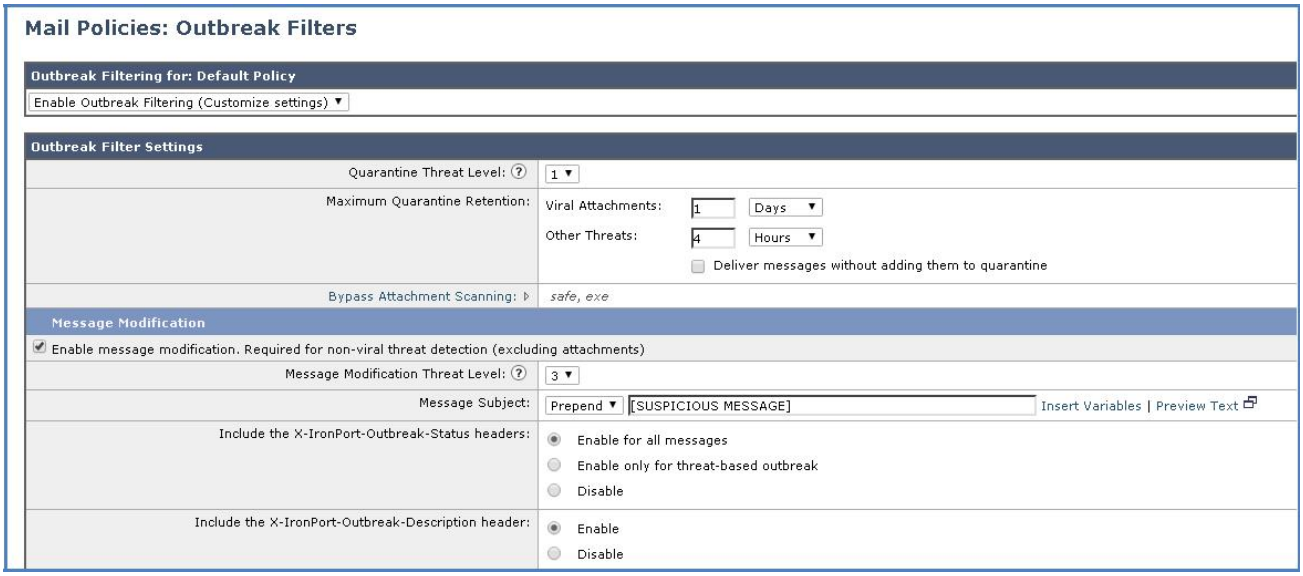
注:テキスト リソースとそのアプリケーションの詳細については、「Understanding Text Resources」を参照してください。

タスク:アウトブレイク フィルタを設定する(推定所要時間:2 分)

アウトブレイク フィルタ ルールは基本的に、電子メールのメッセージおよび添付ファイルの一連の特性(ファイル サイズ、ファイル タイプ、ファイル名、メッセージの内容など)に関連付けられた脅威レベル(例:4)です。たとえば、ファイル名に特定のキーワード(たとえば「hello」)が含まれており、.exe ファイル(サイズは 143 KB)が添付された疑わしい電子メール メッセージが増加していることを、Cisco SIO が通知したと想定します。この基準に一致するメッセージに対する脅威レベルを上げたアウトブレイク ルールが発行されます。Cisco E メール セキュリティ ソリューションは、新しく発行されたアウトブレイク ルールおよび適応型ルールを、デフォルトで 5 分ごとにチェックし、ダウンロードします。ソリューションでは、不審なメッセージを検疫するためのしきい値が設定されます。メッセージの脅威レベルが検疫のしきい値以上の場合、メッセージはアウトブレイク検疫エリアに送信されます。

1. アウトブレイク ポリシーを編集してメッセージを変更し、[アウトブレイク フィルタ(Outbreak Filters)] 列の下のリンク(**Retention Time: Virus 1 day**)をクリックして [アウトブレイク フィルタ(Outbreak Filters)] ページを開きます。

2. [メッセージの変更（Message Modification）] セクションで、[メッセージ変更を有効にする（Enable message modification）] にチェックマークを付けます。これはウイルス以外の脅威の検出（添付ファイルを除く）に必要です。[送信（Submit）] をクリックします。



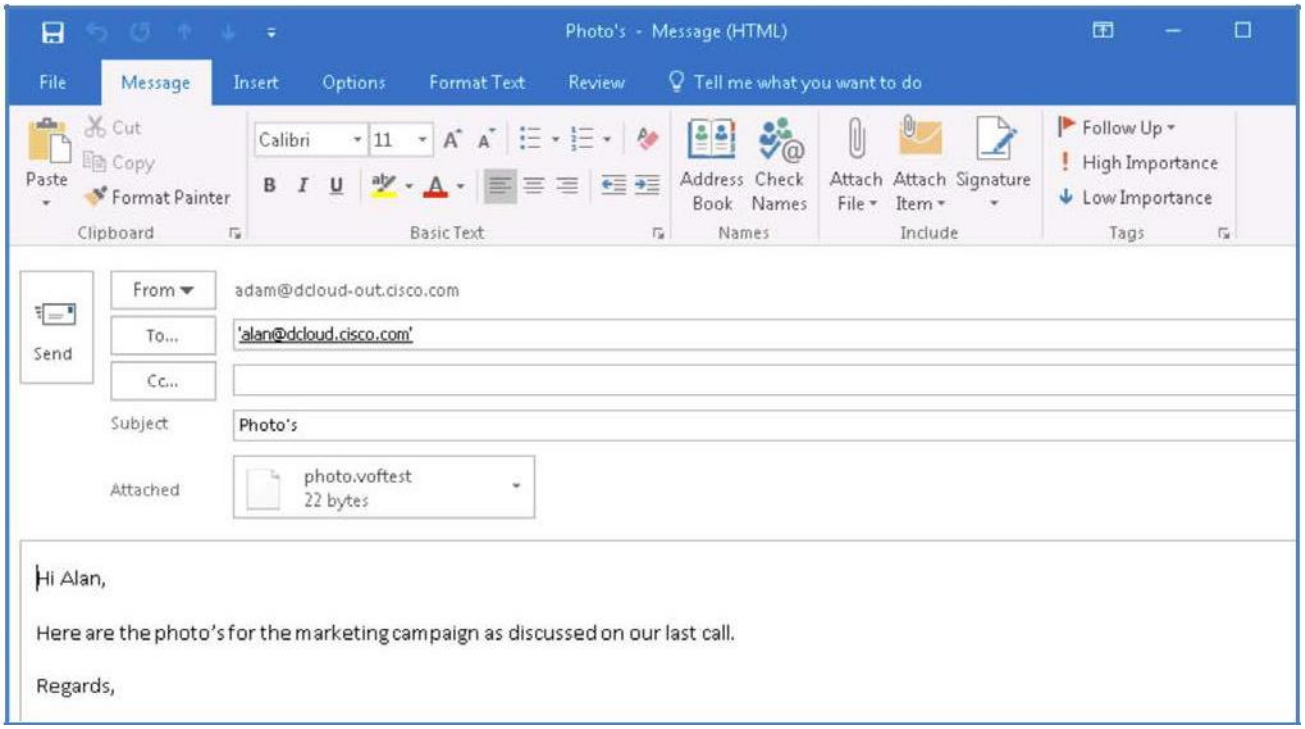
3. 完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

タスク：アウトブレイク フィルタをテストする（推定所要時間：5 分）

アウトブレイク フィルタの処理をデモンストレーションするには、Adam から Alan にメールを送信します。これは、前述のトポロジに従って社外ユーザから組織内に届くメッセージをシミュレートしています。

CLI セッションの開始

1. メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。
2. デスクトップから Outlook を起動し、Adam のメールボックスから、次のパラメータを使用して電子メールを作成します。
   - [宛先（To）]：alan@dcloud.cisco.com
   - [件名（Subject）]：写真（Photos）
   - [本文（Body）]：電話で話した新しい製品に関するデザインの写真です。（Here are the photos of the new product design mentioned on our call.）
   - [添付ファイル（Attach）]：デスクトップ上の Outbreak サブフォルダにある次の photo.voftest ファイルを添付します。



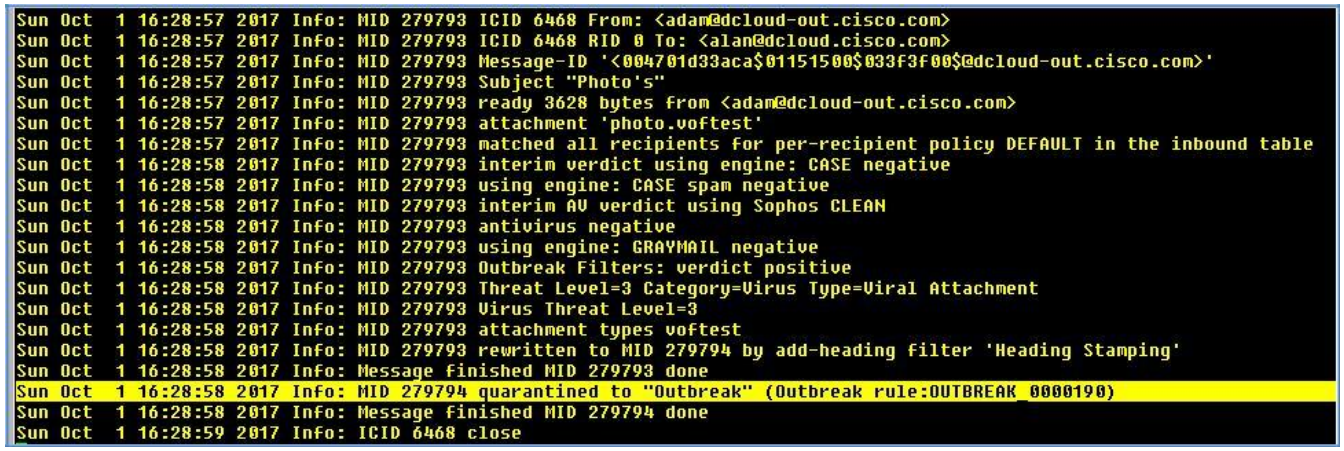
3. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

注：添付ファイルには、アウトブレイク ルール ID 190 に従って実際にシステム テストからアクションをトリガーするために十分な情報が含まれています。[セキュリティ サービス（Security Services）] > [アウトブレイク フィルタ（Outbreak Filters）] でこれを確認してください。

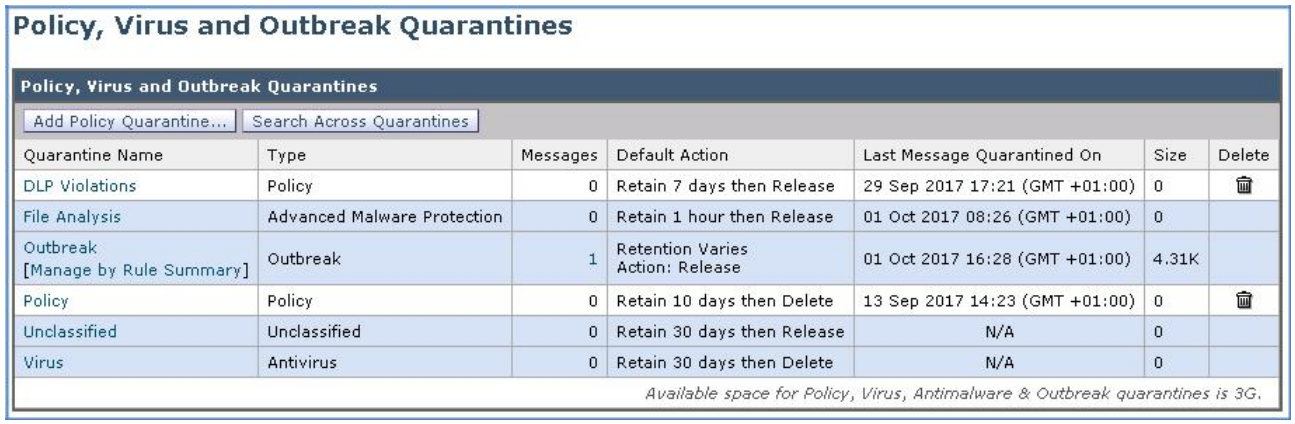
4. 開いたままにしておいた CLI シェルに移動し、メッセージが検疫された旨のログ メッセージを探します。Threat Level（脅威レベル）が 3 であることに注意してください。これは、メッセージが確認済みアウトブレイクの一部であるか、コンテンツが脅威となる中レベルのリスクがあることを示しています。また、ウイルス対策エンジンがどのようにしてクリーンな結果をもたらしたかにも注意してください。

```
Sun Oct  1 16:28:57 2017 Info: MID 279793 ICID 6468 From: <adam@dcloud-out.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 ICID 6468 RID 0 To: <alan@dcloud.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 Message-ID '<004701d33aca$01151500$033f3f00$@dcloud-out.cisco.com>'
Sun Oct  1 16:28:57 2017 Info: MID 279793 Subject "Photo's"
Sun Oct  1 16:28:57 2017 Info: MID 279793 ready 3628 bytes from <adam@dcloud-out.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 attachment 'photo.voftest'
Sun Oct  1 16:28:57 2017 Info: MID 279793 matched all recipients for per-recipient policy DEFAULT in the inbound table
Sun Oct  1 16:28:58 2017 Info: MID 279793 interim verdict using engine: CASE negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 using engine: CASE spam negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 interim AV verdict using Sophos CLEAN
Sun Oct  1 16:28:58 2017 Info: MID 279793 antivirus negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 using engine: GRAYMAIL negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 Outbreak Filters: verdict positive
Sun Oct  1 16:28:58 2017 Info: MID 279793 Threat Level=3 Category=Virus Type=Viral Attachment
Sun Oct  1 16:28:58 2017 Info: MID 279793 Virus Threat Level=3
Sun Oct  1 16:28:58 2017 Info: MID 279793 attachment types voftest
Sun Oct  1 16:28:58 2017 Info: MID 279793 rewritten to MID 279794 by add-heading filter 'Heading Stamping'
Sun Oct  1 16:28:58 2017 Info: Message finished MID 279793 done
Sun Oct  1 16:28:58 2017 Info: MID 279794 quarantined to "Outbreak" (Outbreak rule:OUTBREAK_0000190)
Sun Oct  1 16:28:58 2017 Info: Message finished MID 279794 done
Sun Oct  1 16:28:59 2017 Info: ICID 6468 close
```

5. MID を書き留め、メッセージに適用された最後のアクションが Quarantine（検疫）であることも書き留めておきます。

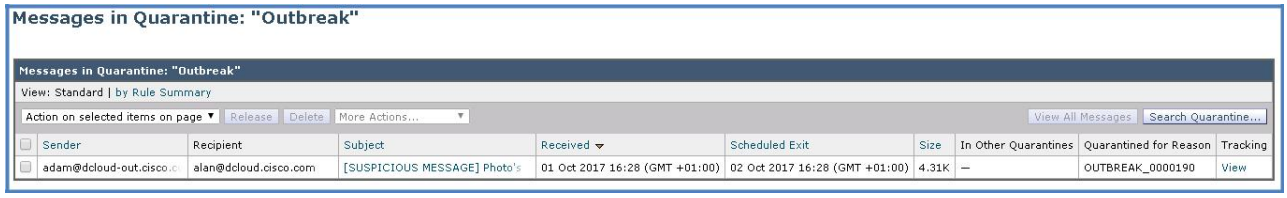


6. Outlook クライアントに戻り、Alan の受信トレイをクリックします。メッセージは、以前に作成したコンテンツ フィルタによって検疫されているため、表示されません。[モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク検疫（Policy, Virus and Outbreak Quarantines）] に移動し、この時点ではメッセージが *アウトブレイク* 検疫エリアに格納されていることに注意してください。

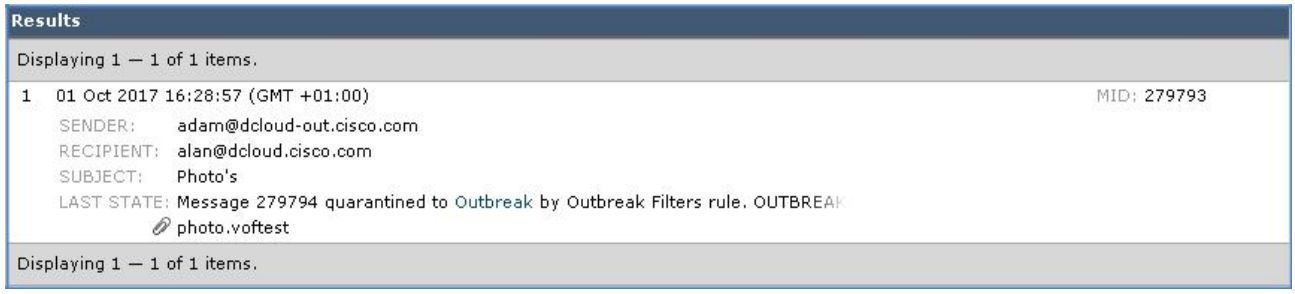


注：アウトブレイク脅威レベルの詳細については、「Outbreak Threat Levels」を参照してください。

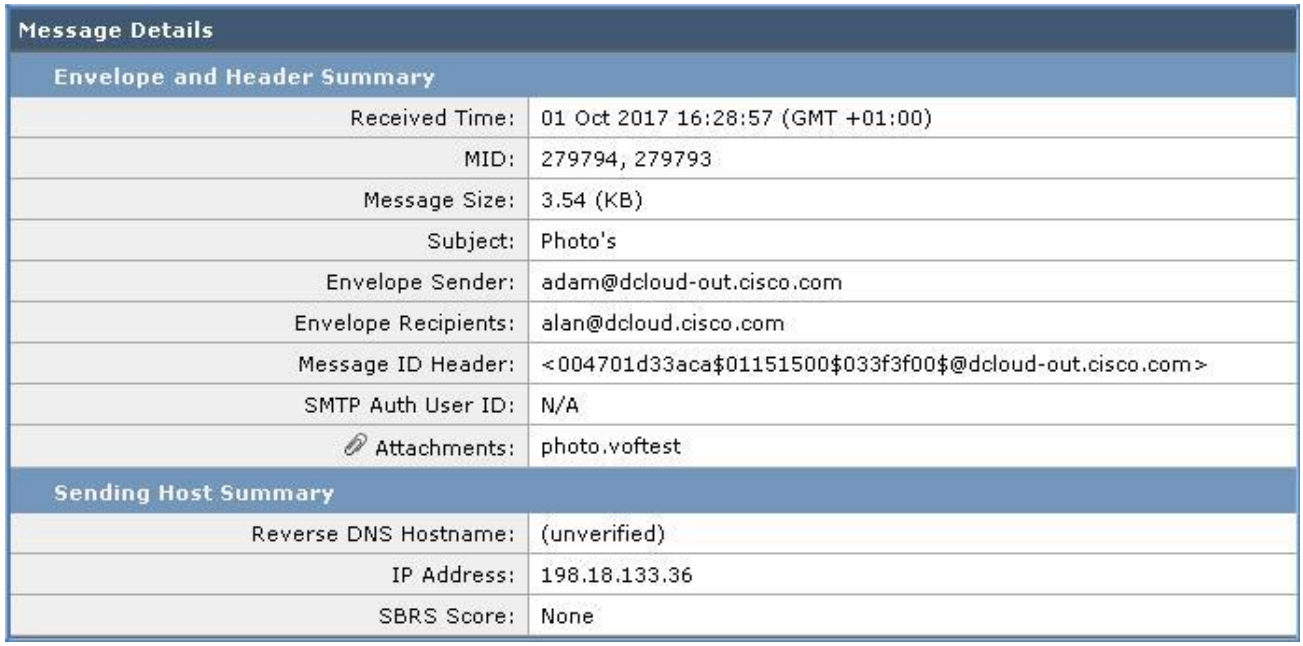
7. [メッセージ（Messages）] 列の値をクリックしてメッセージを表示し、メッセージが検疫された理由を確認します。



8. [トラッキング（Tracking）] の下の [表示（View）] をクリックして*メッセージ トラッキング*を起動し、[結果（Results）] セクションまでスクロールしてメッセージを表示します。MID は、前の手順で書き留めたものを参照している必要があります。



9. [詳細の表示（Show Details）] をクリックして、このメッセージが Cisco E メール セキュリティ ソリューションによって処理された方法と、さまざまなエンジンの影響についての詳細情報を取得します。最後に、アウトブレイク フィルタの判定と最後のアクション（検疫エリアに送信）を確認します。



Processing Details

	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: alan@dcloud.cisco.com
01 Oct 2017 16:28:57 (GMT +01:00)	Protocol SMTP interface Network (IP 198.18.133.146) on incoming connection (ICID 6468) from sender IP 198.18.133.36. Reverse DNS host None verified no.
01 Oct 2017 16:28:57 (GMT +01:00)	(ICID 6468) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS None country None
01 Oct 2017 16:28:57 (GMT +01:00)	Start message 279793 on incoming connection (ICID 6468).
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 enqueued on incoming connection (ICID 6468) from adam@dcloud-out.cisco.com.
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 on incoming connection (ICID 6468) added recipient (alan@dcloud.cisco.com).
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 contains message ID header '<004701d33aca$01151500$033f3f00$@dcloud-out.cisco.com>'.
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 original subject on injection: Photo's
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 (3628 bytes) from adam@dcloud-out.cisco.com ready.
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 contains attachment 'photo.voftest'.
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 matched per-recipient policy DEFAULT for inbound mail policies.
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Spam engine: CASE. Interim verdict: negative
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Spam engine: CASE. Final verdict: Negative
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Virus engine. Final verdict: Negative
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Outbreak Filters. Verdict: Positive
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 Virus Threat Level=3
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 contains attachment types voftest
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 rewritten as new message 279794 by add-heading Heading Stamping filter
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279794 quarantined to Outbreak by Outbreak Filters rule. OUTBREAK_0000190

10. ウィンドウを閉じてメッセージ トラッキング ウィンドウに戻ります。

11. [結果（Results）] セクションのすぐ下にある [検疫に戻る（Back to Quarantine）] ハイパーリンクをクリックします。

Results

Displaying 1 — 1 of 1 items.

1 01 Oct 2017 16:28:57 (GMT +01:00) MID: 279793

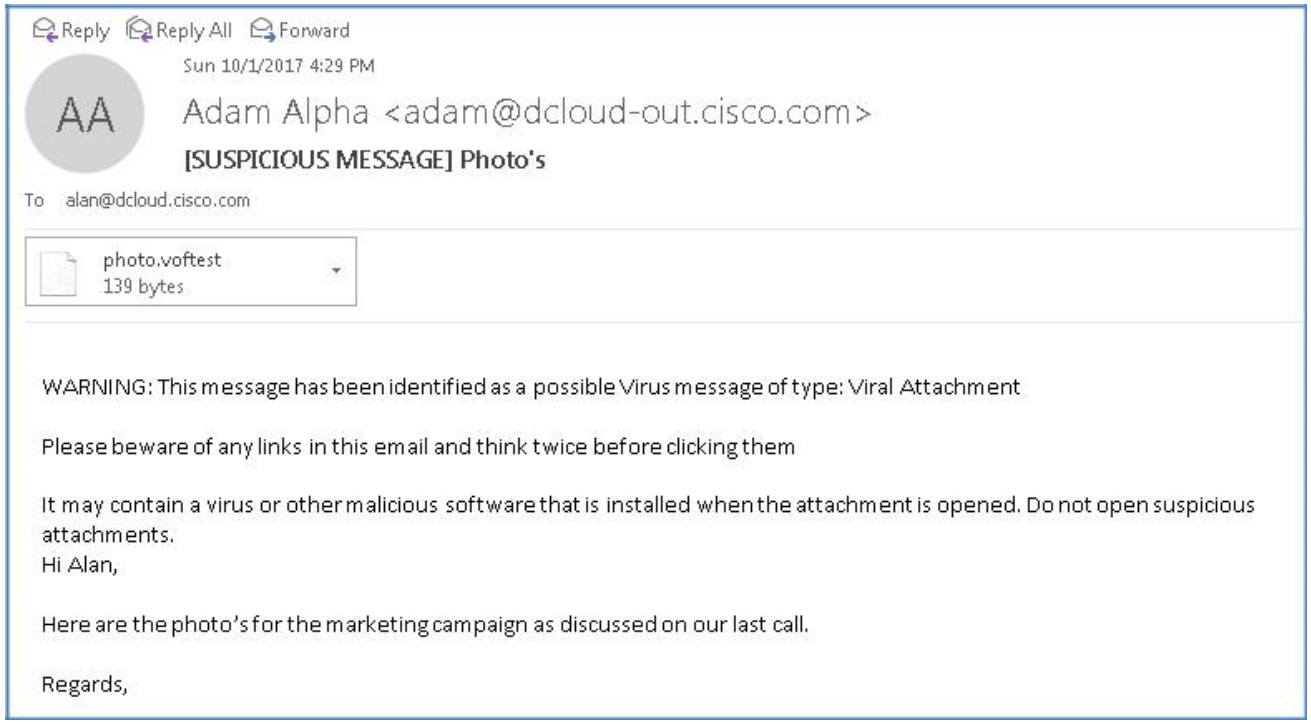
SENDER: adam@dcloud-out.cisco.com
RECIPIENT: alan@dcloud.cisco.com
SUBJECT: Photo's
LAST STATE: Message 279794 quarantined to Outbreak by Outbreak Filters rule. OUTBREA
photo.voftest

Displaying 1 — 1 of 1 items.

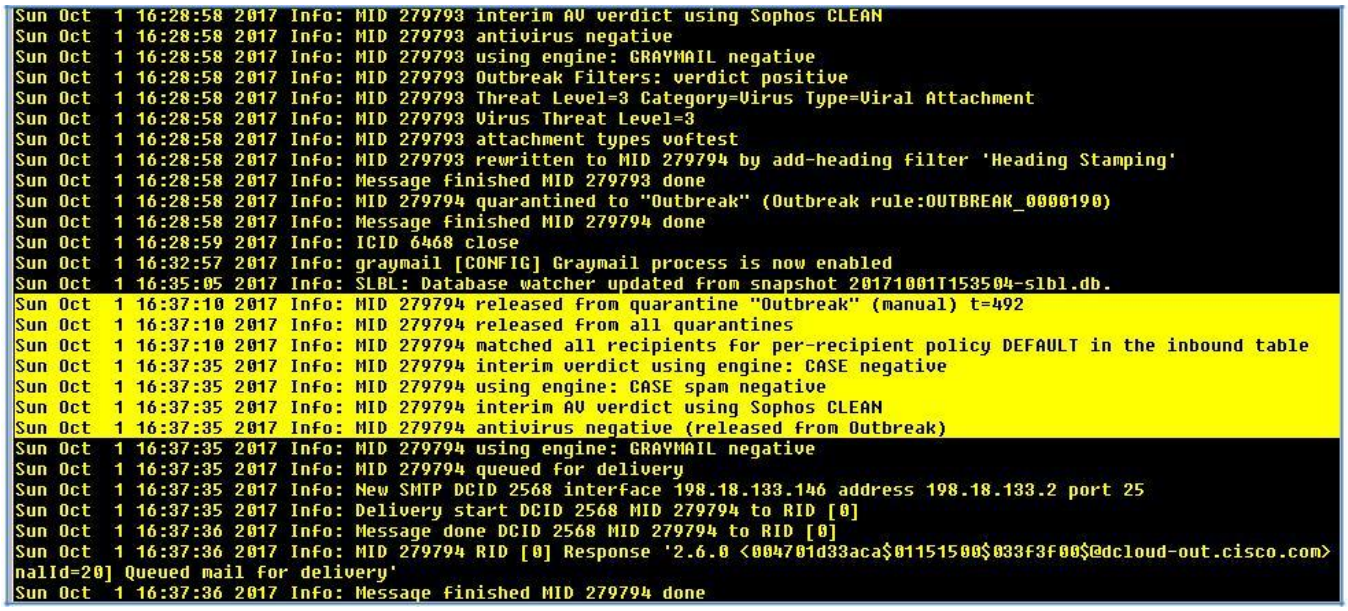
Back to Quarantine

12. [件名（Subject）] 見出しを確認して、メッセージにチェックマークを付け、[解放（Release）] ボタンをクリックして、メッセージが表示されたらアクションを確認します。

13. Outlook クライアントに戻り、メール ボックスを手動で同期させると、この時点ではメッセージが Alan の受信トレイに表示されます。件名ヘッダーにはポリシーに従った前文が付加され、ファイルの本文にも警告情報が適用されて、受信者の注意を喚起しています。



14. CLI ウィンドウに戻り、どのような手順でメッセージが検疫エリアから解放された後にエンジンによって再びメッセージがスキャンされ、受信者にメッセージが配信される前に判定が提供されるかを確認します。



注:電子メールが Cisco E メール セキュリティ ソリューションによって処理される際のフローの詳細については、「Understanding the Email Pipeline」を参照してください。

シナリオ 4:　偽装メールの検出

使用例

ビジネス リーダーが、ある会議を開催しました。この会議では、接続されるデバイスの急増や発生するセキュリティの上の課題について話し合われ、Voyage の顧客やそのパートナーが今後直面する可能性のある次世代の Internet of Things（IoT）に関する課題も議論されました。Voyage では、これを現行の製品でさらに市場シェアを獲得するための絶好の機会と見なし、ビジネス開発チームの主要メンバーに参加を義務付けました。何社かの市場調査企業が出席しましたが、重要な裏付け情報は会議後に電子メールで配信される予定でした。

会議から戻った業務担当ディレクタは、期日を過ぎた請求書の即時支払いを要求する電子メールを受信したと報告しました。その要求について詳しく調べたところ、その信憑性に関して追加の確認が必要になり、後に要求は正当なものではないことが判明しました。

セキュリティ制御

Cisco E メール セキュリティ ソリューションは、偽装された送信者アドレス *(From：ヘッダー)*を持つ不正なメッセージを検出し、そのようなメッセージに対して指定されたアクションを実行できます。

たとえば、偽装された送信者アドレスを持つメッセージを検出し、*From：*ヘッダーを隠された（スプーフィングされた）送信者に置き換えることができます。この場合、従業員には偽造された電子メール アドレスではなく、実際の送信者（攻撃者）の電子メール アドレスが表示されます。

目的

このシナリオでは、偽装メールの検出（FED）機能がどのようにして、選択したユーザやグループ（契約や財務などで権限を持つ大手企業の幹部など）をフィッシング攻撃から保護するのかが示されます。

標的型の脅威の量が少ない場合は、検出が難しくなることがあります。メールの偽装（スプーフィング）は簡単です。社内 LAN または外部環境から、トロイの木馬によって実行されます。偽装メールはスパムやフィッシング活動で頻繁に使用されます。

このシナリオは、差出人が従業員になりすまして企業内へ入りこんだスプーフィングの解決に重点を置きます。

注：このシナリオの基本的な前提条件の一部は、これまでのシナリオで設定されています（免責事項など）。この演習の免責事項を作成する手順は、前のシナリオと同様です。

注：偽造メールの検出の詳細については、「Forged Email Detection」を参照してください。

手順

タスク:なりすましメールを送信する(推定所要時間:3 分)

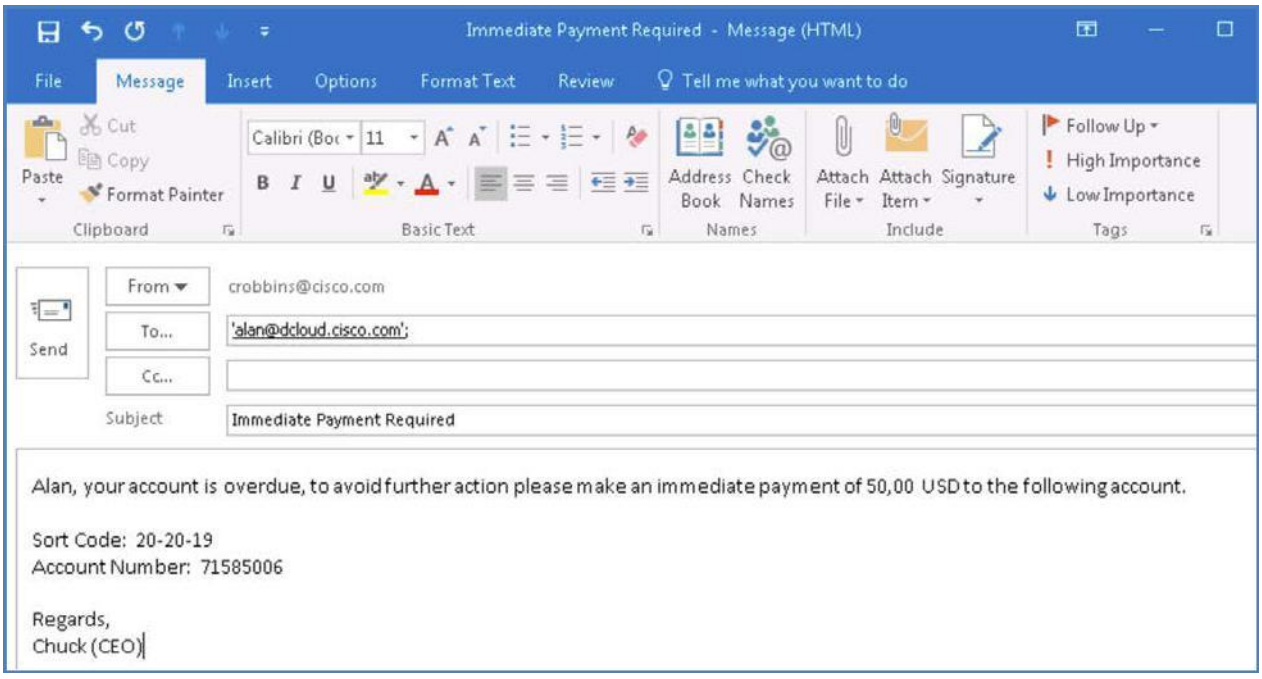
このタスクでは、偽造された可能性がある電子メールがどのように見えるか、またそれをいかに簡単に作成して送信できるかを示します。標的の受信トレイに届いたメッセージは、一見したところ、(スプーフィングされているため)正当な送信者から届いています。

1. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。

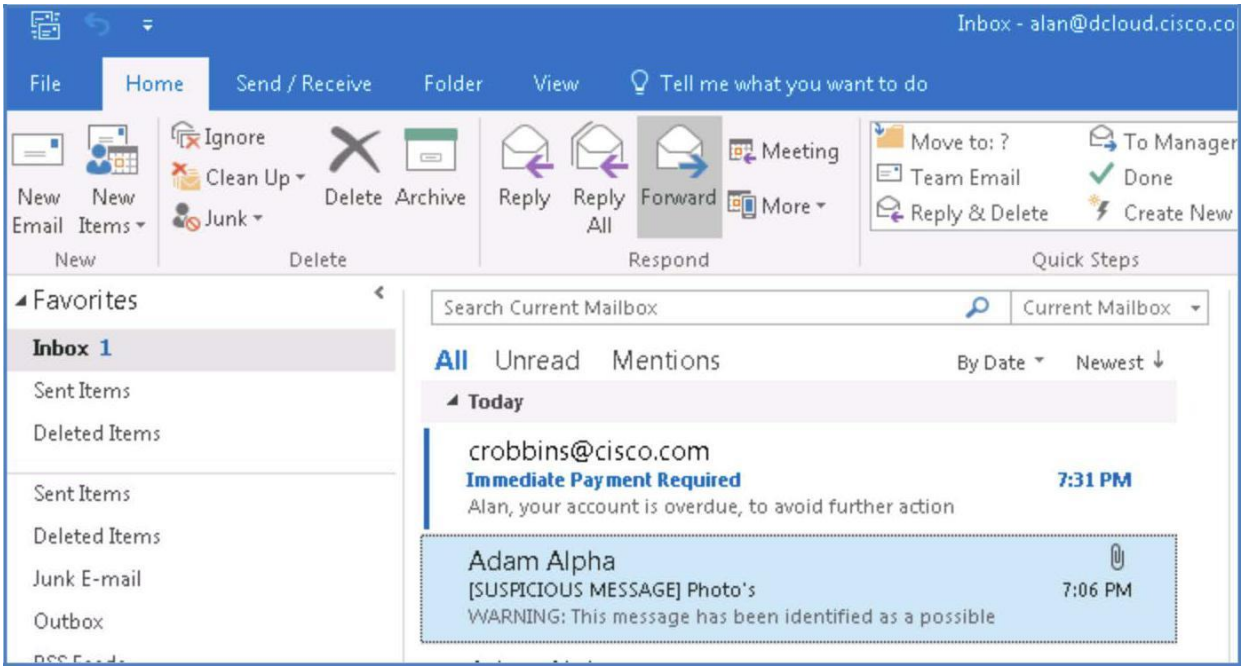
   - [差出人(From)]:crobbins@cisco.com
   - [宛先(To)]:alan@dcloud.cisco.com
   - [件名(Subject)]:Immediate Payment Required(至急お支払いください)
   - [本文(Body)]:Alan 様。お客様の口座の期限が切れています。停止措置を回避するために、次の口座に 50,000 ドルを即座にお振り込みください。(Alan, your account is overdue, to prevent further action please make an immediate payment of 50,000 USD to the following account:)

     Sort Code:20-20-19(支店コード:20-20-19)
     Account:71584006(口座番号:71584006)

     Regards,(よろしくお願いします。)
     Chuck(CEO)



2. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。
3. Alan の受信トレイを調べて、メッセージの受信を確認します。最初は *Chuck Robbins* から送信されたように見えます。



タスク：用語のコンテンツ ディクショナリを作成する

望ましくない動作に対処する最初のタスクは、この種の攻撃の対象となる可能性が高い、知名度の高い人物の名前を含むコンテンツ ディクショナリを作成することです。

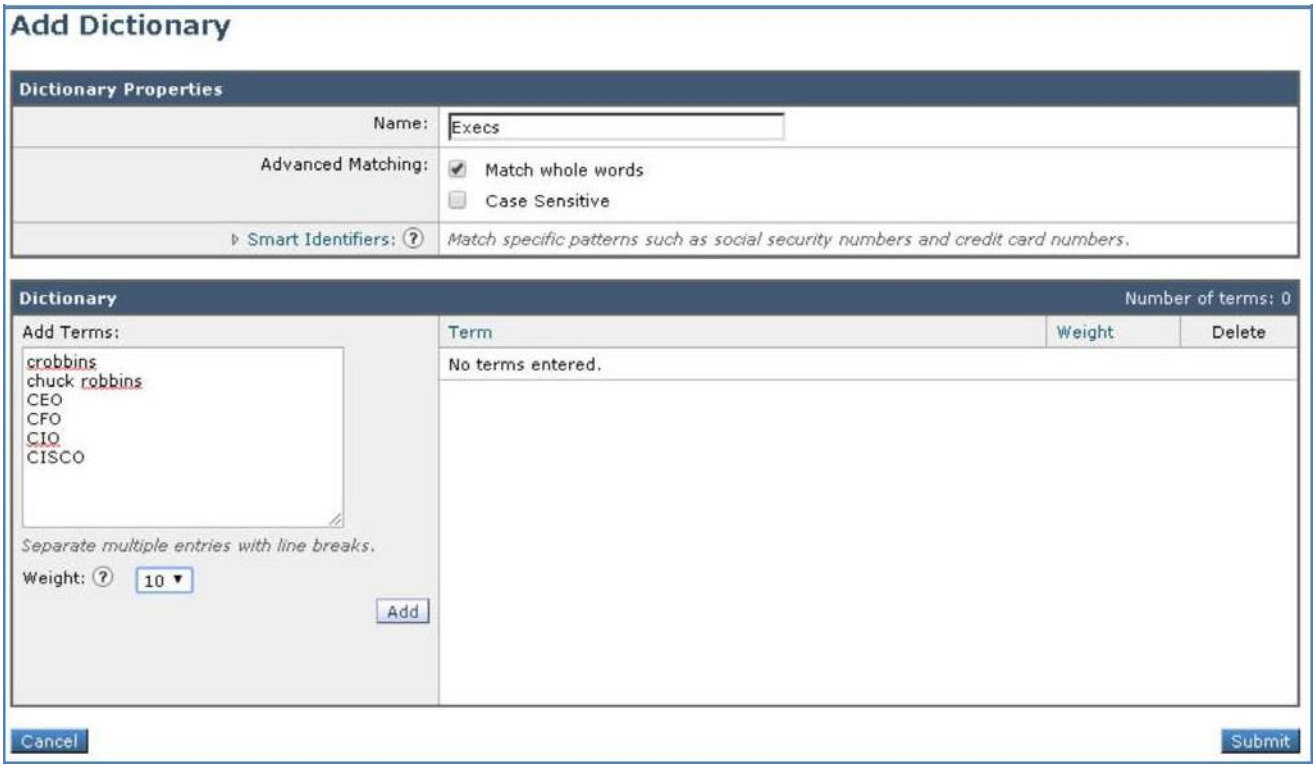
コンテンツ ディクショナリは、ソリューションの本文スキャン機能と連携して動作する単語またはエントリのグループであり、コンテンツ フィルタおよびメッセージ フィルタの両方に利用できます。定義したディクショナリを使用して、ディクショナリに含まれる単語に対してメッセージ、メッセージ ヘッダー、およびメッセージの添付ファイルをスキャンすることで、企業のポリシーに沿った適切なアクションを実行することもできます。このタスクでは、組織内の潜在的なターゲットの名前が一覧表示されるコンテンツ ディクショナリを作成します。

1. ワークステーションから GUI にアクセスし、[メール ポリシー（Mail Policy）] > [ディクショナリ（Dictionaries）] に移動して、表示されるウィンドウで [ディクショナリの追加（Add Dictionary）] をクリックします。これにより、特定されたユーザの名前でカスタム ディクショナリが作成されます。

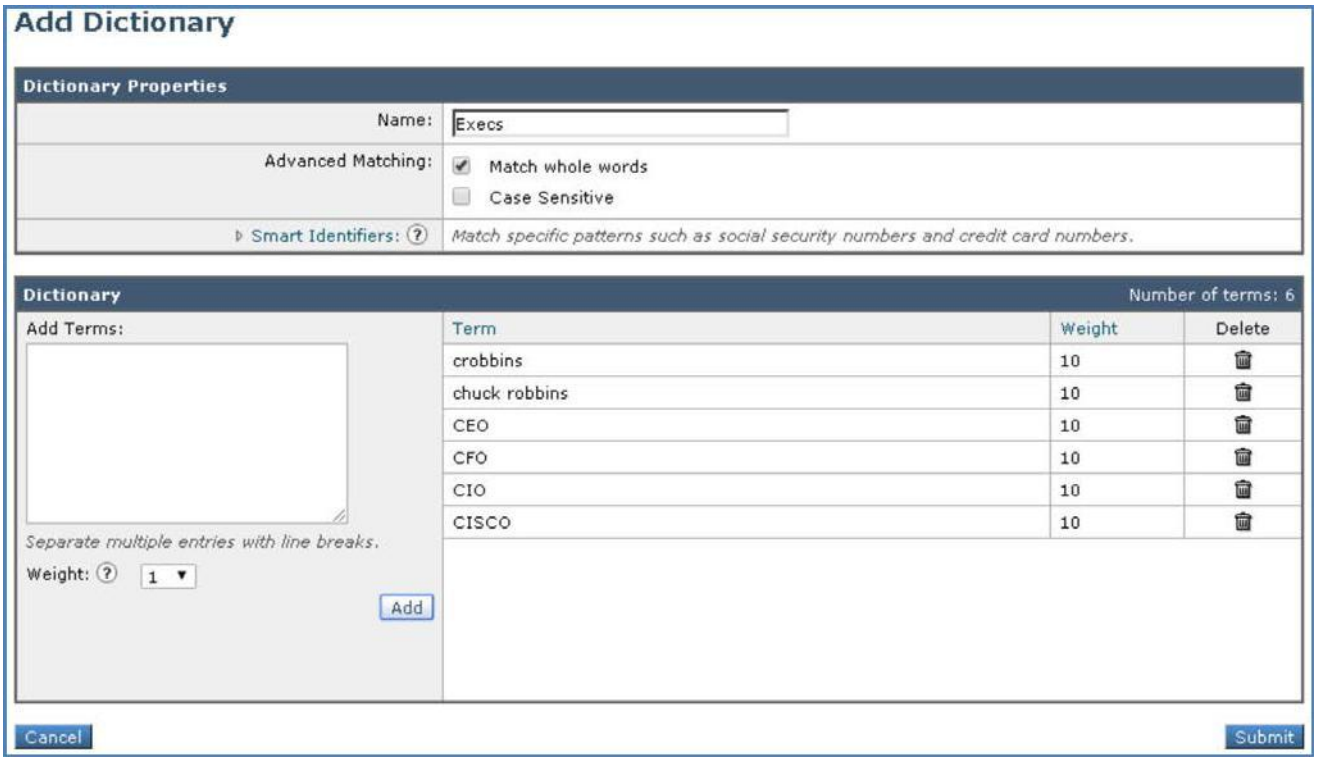
2. ディクショナリに次の情報を追加します。

   - [名前（Name）]：Execs（エグゼクティブ）
   - [用語の追加（Add Terms）]：crobbins
     chuck robbins
     CEO
     CFO
     CIO
     CISCO
   - [ウェイト（Weight）]：10

注：複数の用語を、各用語を改行で区切って一度にディクショナリに追加できます。



3. [追加（Add）] ボタンをクリックして、用語をディクショナリに追加します。



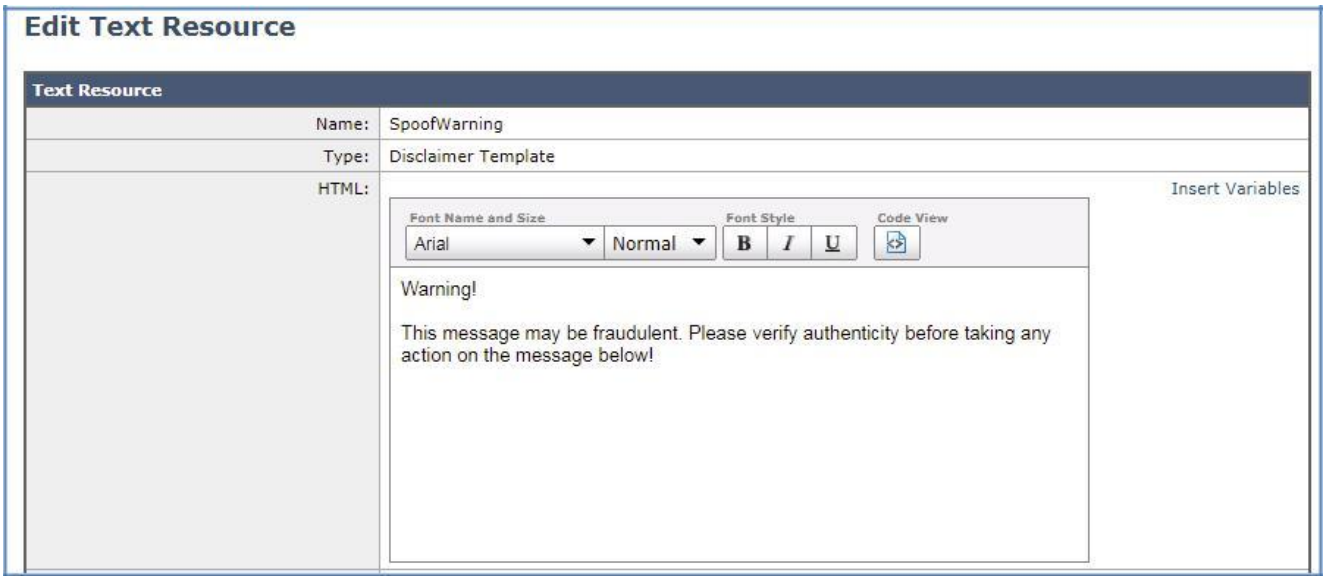
4. [送信（Submit）] をクリックしてディクショナリを作成します。

5. [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

タスク:免責事項テンプレートを確認する(推定所要時間:1 分)

このラボの前に、標的の電子メールに挿入されるカスタム免責条項を作成しました。このタスクでは、疑わしい電子メール メッセージを通知するカスタム通知がどのように受信者に表示されるかを確認します。

1. [メール ポリシー(Mail Policies)] > [テキスト リソース(Text Resources)] に移動し、事前設定テキスト リソースの [SpoofWarning] をクリックします。
2. 他の免責事項と同様に、このテキスト リソースは組織のニーズに合わせて HTML ベースで完全にカスタマイズできます。このメッセージの目的は、このメッセージを扱う受信者の注意を喚起することです。



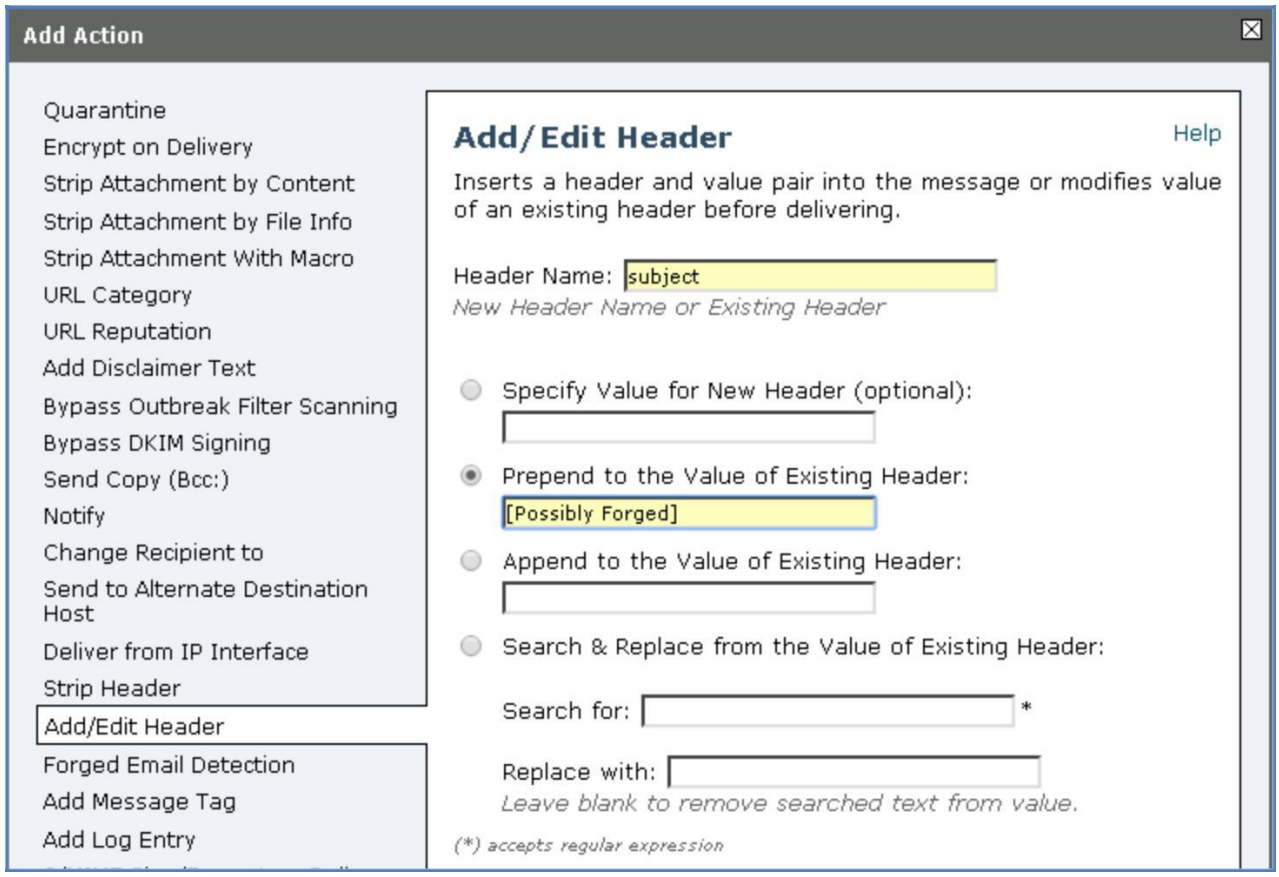
3. 必要に応じて警告を編集するか、[キャンセル(Cancel)] をクリックして画面を終了します。

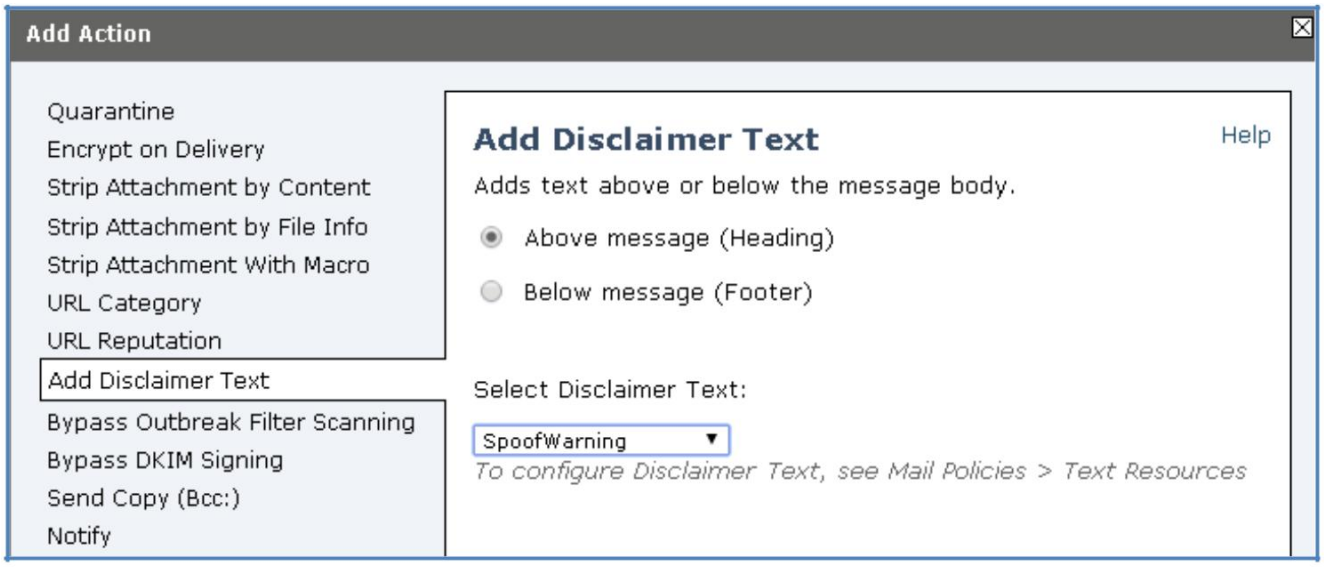
タスク:コンテンツ フィルタを設定する(推定所要時間:3 分)

前のシナリオのアウトブレイク フィルタと同様にコンテンツ フィルタを使用すると、ポリシーできめ細かくコンテンツを識別できます。このタスクでは新しいコンテンツ フィルタが作成され、前の手順で作成されたコンテンツ ディクショナリが使用されます。

1. ワークステーションから GUI にアクセスし、[メール ポリシー(Mail Policy)] > [受信コンテンツ フィルタ(Incoming Content Filters)] に移動して、[フィルタの追加(Add Filter)] をクリックします。次の設定で条件とアクションを設定します。
   - [名前(Name)]:FED_Spoof
   - [説明(Description)]:Identify Forged Email Messages(偽装メールのメッセージを識別します)
   - [条件(Conditions)]:[偽装メールの検出(Forged Email Detection)] > [コンテンツ ディクショナリ(Content Dictionary)]:Execs、類似性スコア 70

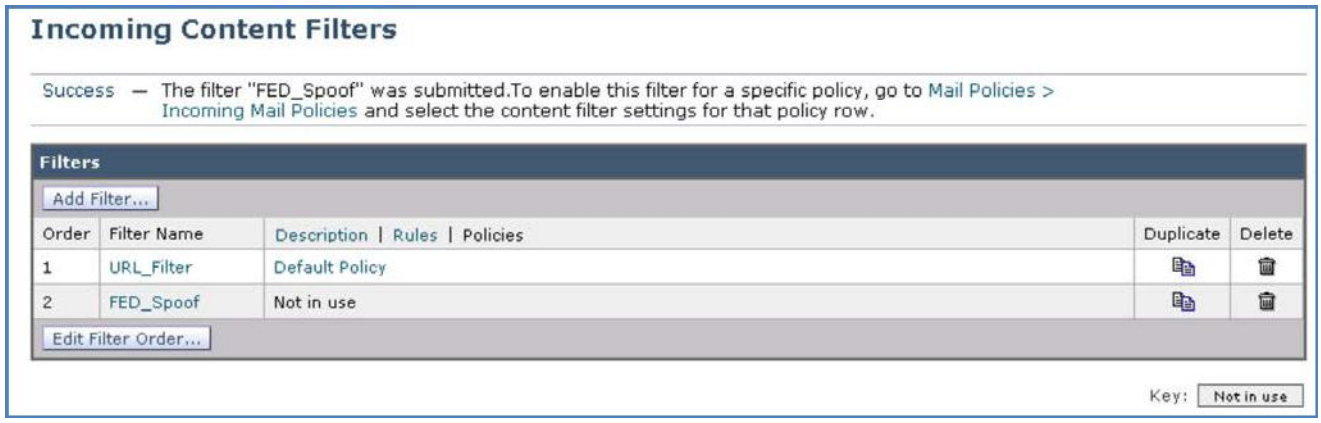
- [アクション（Action）] の 1：[ヘッダーの追加/編集（Add/Edit Header）] > [ヘッダー名（Header Name）]：subject
  [既存ヘッダーの値の前に追加（Prepend to the Value of Existing Header）]：[Possibly Forged]（[偽装の可能性あり]）
- [アクション（Action）] の 2：[免責事項テキストの追加（Add Disclaimer Text）] > [免責事項テキストの選択（Select Disclaimer Text）]：SpoofWarning



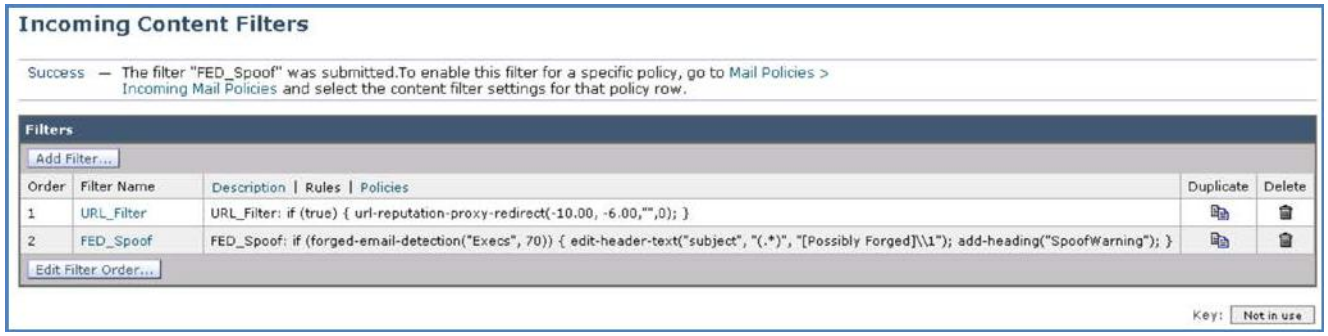


注:コンテンツ フィルタは通常、条件とアクションで構成されます。ここでの条件は、[エグゼクティブ(Execs)] ディクショナリと、偽装メールの可能性を特定するための類似性スコアを使用することです。スコアは 1 ～ 100 で表され、値が高いほどメールが偽装されている可能性が高くなります。

2. [送信（Submit）] をクリックしてコンテンツ フィルタを作成します。完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。



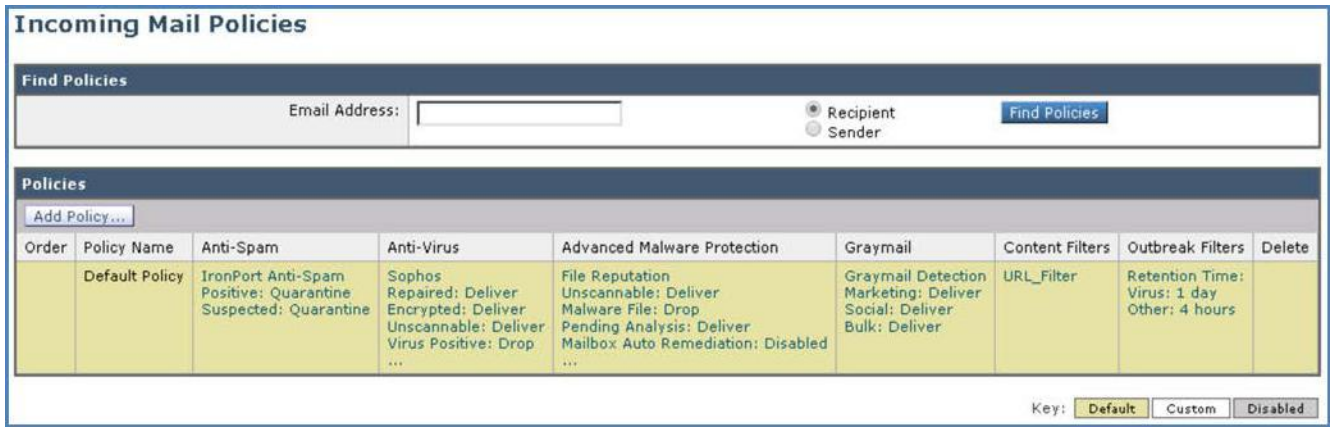
3. コンテンツ フィルタはまだ受信メール ポリシーに関連付けられていないため、使用されていません。
4. [ルール（Rules）] をクリックしてフィルタの構文を表示します。これは、コンテンツ フィルタではなくメッセージ フィルタの場合に入力する必要があったものとまったく同じです。



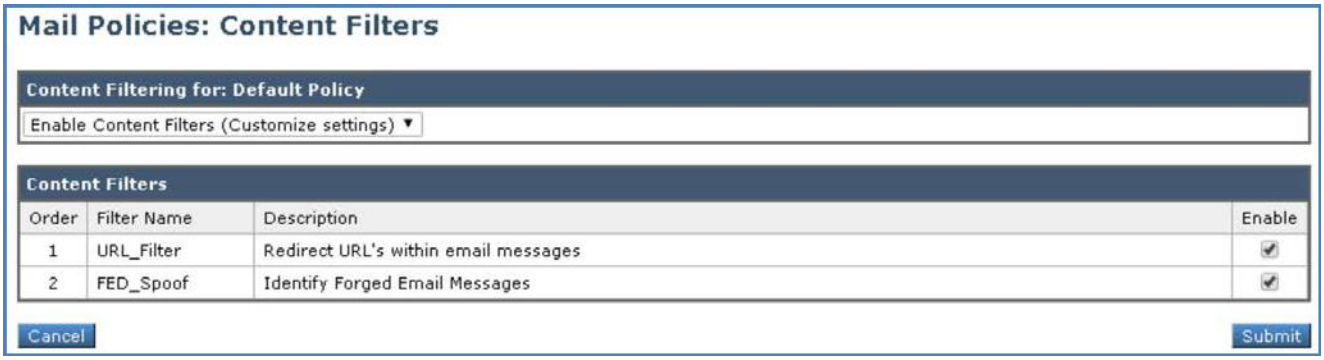
タスク：受信メール ポリシーを編集する（推定所要時間：1 分）

最後のタスクはデフォルトの受信メール ポリシーを変更して、コンテンツ フィルタを有効にすることです。

1. [メール ポリシー（Mail Policy）] > [受信メール ポリシー（Incoming Mail Policies）] に移動して、[デフォルト ポリシー（Default Policy）] の [コンテンツ フィルタ（Content Filters）] ボックス内をクリックします。

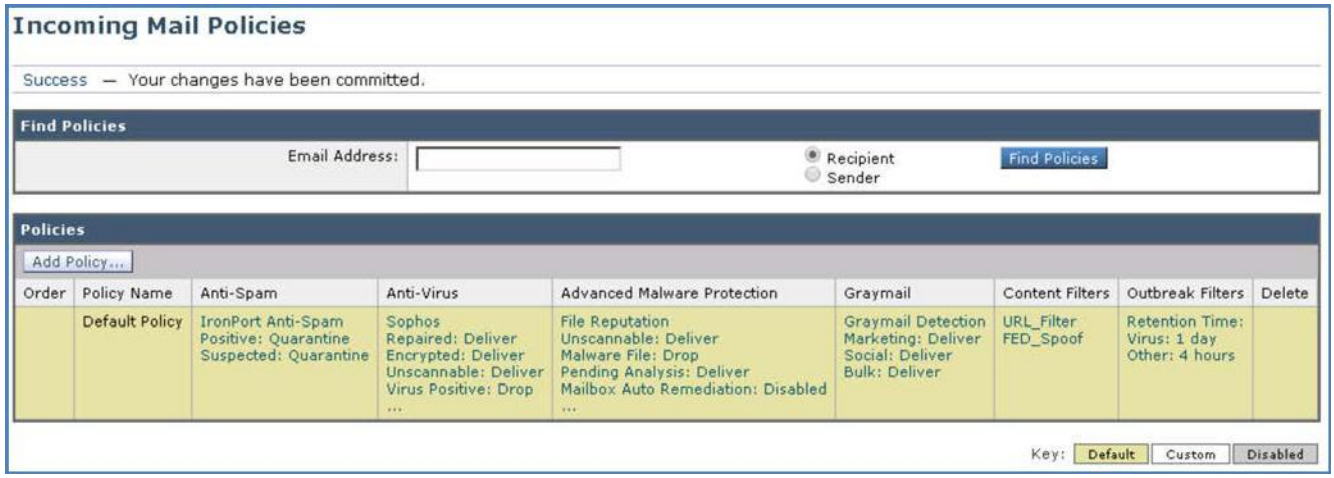


2. 前の手順で作成した「FED_Spoof」コンテンツ フィルタにチェックマークを付けて有効にします。



3. [送信（Submit）] をクリックしてコンテンツ フィルタを作成します。完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が有効になっていることを確認します。必要に応じて任意のコメントを追加してください。

4. 最後に デフォルト ポリシーに FED_Spoof が追加されていることを確認します。



タスク：偽装メールの検出をテストする（推定所要時間：5 分）

構成が完了していれば、このシナリオで実行した最初のタスクを繰り返して同じ文面のメッセージを再送信することで、偽装メール検出機能をテストできます。

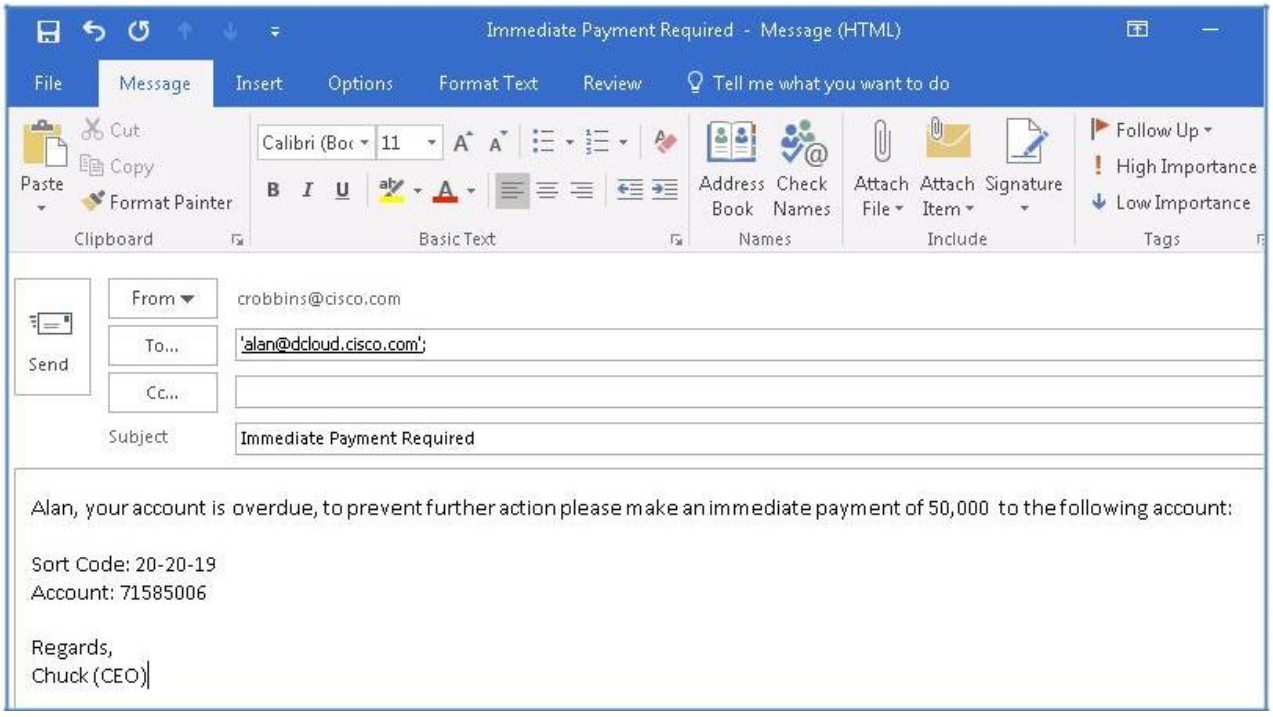
CLI セッションの開始

メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。

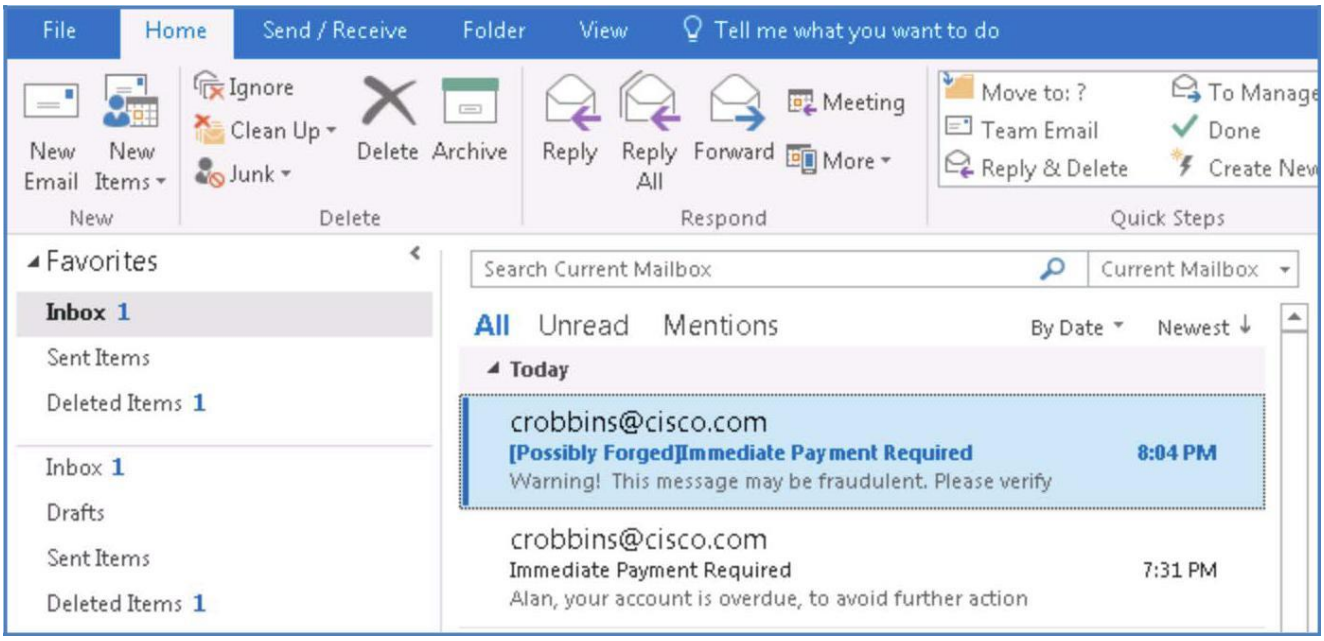
1. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。
   - [差出人（From）]：crobbins@cisco.com
   - [宛先（To）]：alan@dcloud.cisco.com
   - [件名（Subject）]：Immediate Payment Required（至急お支払いください）
   - [本文（Body）]：Alan 様。お客様の口座の期限が切れています。停止措置を回避するために、次の口座に 50,000 ドルを即座にお振り込みください。（Alan, your account is overdue, to prevent further action please make an immediate payment of 50,000 USD to the following account:）

     Sort Code：20-20-19（支店コード：20-20-19）
     Account：71584006（口座番号：71584006）

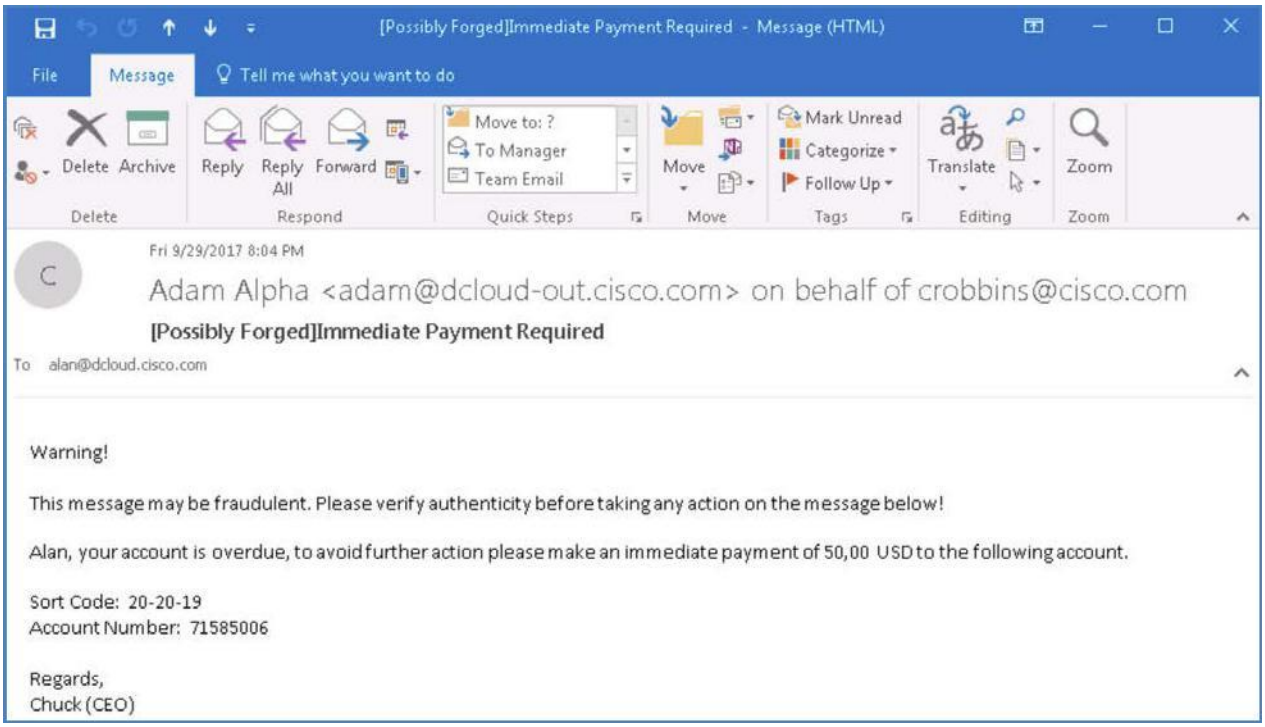
     Regards,（よろしくお願いします。）
     Chuck（CEO）



2. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。
3. Alan の受信トレイを調べて、メッセージの受信を確認します。一見すると *Chuck Robbins* から実際に送信されたようですが、最初のタスクで確認したものと比べて、今回はいくつかの変更点が明確に認められます。
4. まず、件名ヘッダーが修正されています。追加のカスタム テキストが前に付加されています。これによりメールの受信者は、受信メッセージに不審な点が少しでもあればすぐに気付きます。



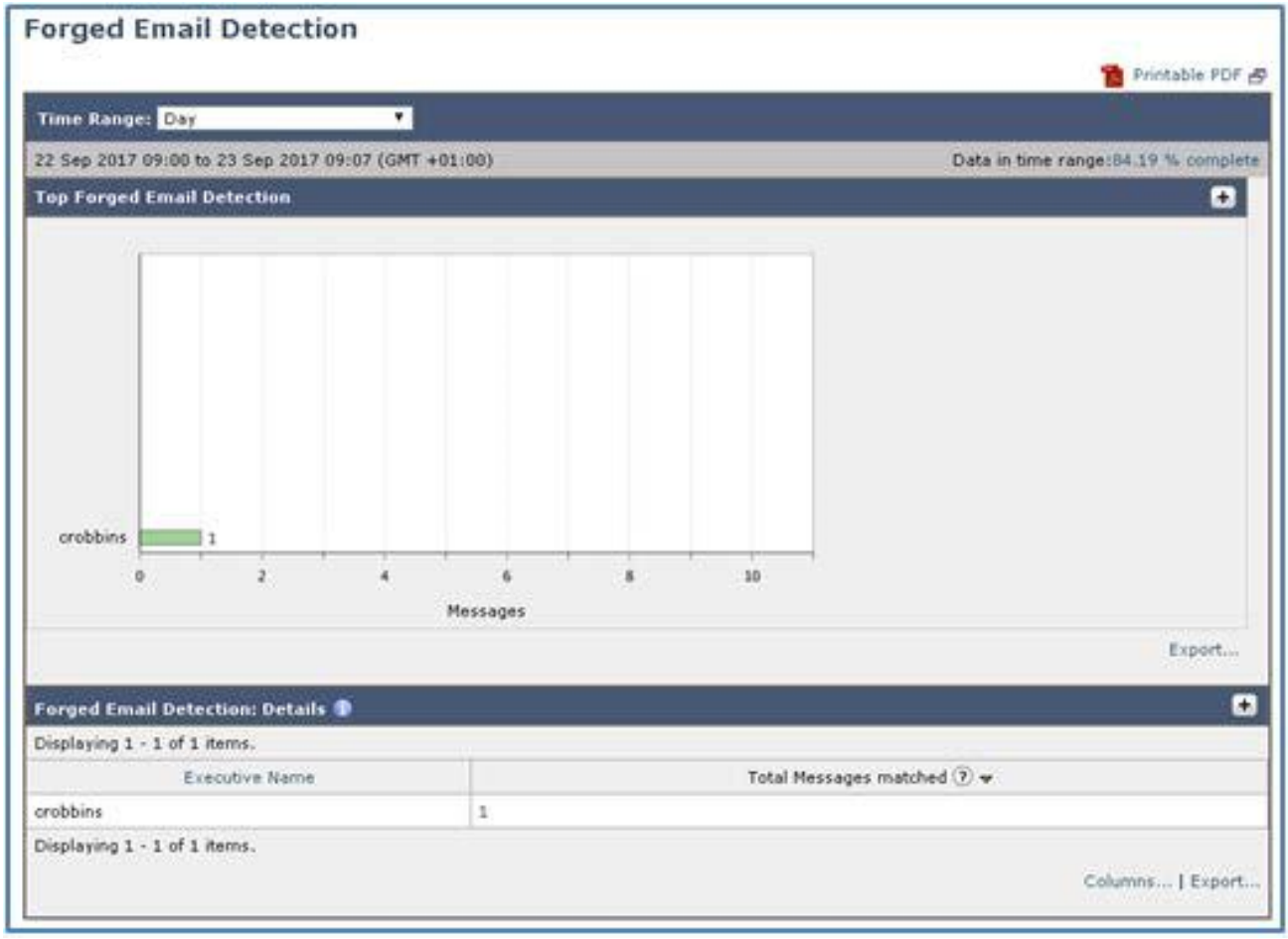
5. 次に、メッセージを開くと、メッセージに応答する際は注意するよう促す免責事項が追加されています。



6. CLI ウィンドウに戻り、このタイプのメッセージがエンジンによってどのように処理されるのかを確認します。

7. 最後にこれらのイベントに関する詳細情報を、GUI のモニタで確認できます。

8. ワークステーションから GUI にアクセスし、[メール ポリシー（Mail Policy）] > [偽装メールの検出（Forged Email Detection）] に移動して、レポートの内容を確認します。



シナリオ 5:　マクロの検出

使用例

Voyage Corp 社は最近、州政府が新たに創設した公共組織を新しい顧客として取引を開始しました。この組織は、今後重要な顧客となる可能性があるため、セールス チームは、すべての受注を迅速に処理することを主張します。以前の顧客では受注の処理に遅れが発生しサプライヤの切り替えを模索された経験もあったため、今回はその失態を防ぎたいと考えています。

新しい顧客の平均オンボーディング時間は 5 ～ 10 営業日です。これには、顧客をクレジット システムに登録し、（顧客のオンライン ポータル登録を行う前に必要となる）社内の法務チームによるデューデリジェンスを完了することが含まれます。

さらなる遅延によるビジネス損失を回避するため、地域顧客担当のディレクタは顧客の戦略的重要性を挙げてプロセスの迅速化を求め、当面の間はすべての受注を電子メールで受け取るように要請しました。最初の 2 日間は、受注アナリストに電子メールで送信された注文に問題はありませんでした。しかし 3 日目の午前中、Microsoft Excel ファイルが添付として届き、それを開いたところ直後にローカル ホストが不安定になりました。社内サポート チームによる詳細な調査の結果、問題のドキュメントには *TrojanDownloader:W97M/Adnel* に感染したマクロが隠されており、ドキュメントを開いたことで感染して迅速に拡散し、コンピュータが動作不能に陥ったことを突き止めました。ただちに、マクロが有効化されたファイルが添付されたメッセージは受け取らないことが決まります。

セキュリティ制御

マクロとは、タスクの実行を補助する自動実行型のコマンド群です。マクロコードは、Visual Basic for Applications（VBA）と呼ばれるプログラミング言語で記述された Office ドキュメントに組み込まれています。マクロは、マルウェアを侵入させたり、マルウェアをダウンロードさせたりするなどの不正用途で使用される可能性があります。悪意のあるマクロ ファイルの多くは Word ドキュメントや Excel スプレッドシートに含まれますが、他の形式も存在します。

Cisco E メール セキュリティ ソリューションにより、添付ファイルのフィルタ処理、高度なマルウェアの検出、添付ファイルに潜むマクロ ベースの脅威のスキャンが可能になります。マクロ検出機能は、コンテンツ フィルタやメッセージ フィルタを使用して、こうしたマクロを検出できるように設計されています。

目的

今回のシナリオでは、悪意のあるマクロが組み込まれている可能性のあるファイルを削除するために Cisco E メール セキュリティでマクロ検出機能を設定する一連の手順を実行します。

注: 添付ファイル内にマクロが隠されている危険性の詳細については、「Malicious Macros」を参照してください。

手順

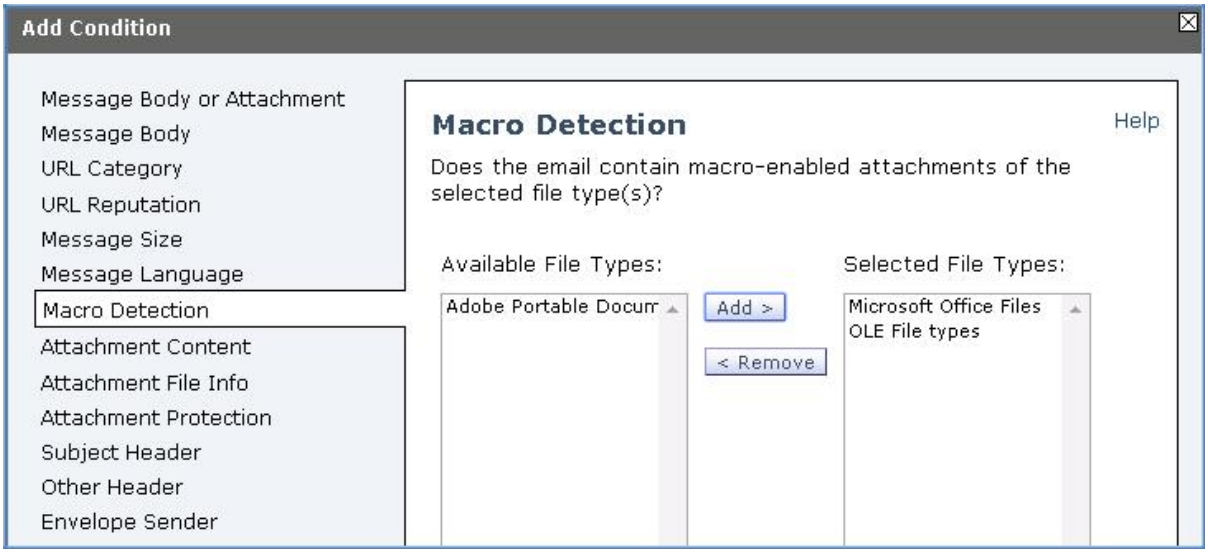
タスク:コンテンツ フィルタを設定する(推定所要時間:3 分)

前のシナリオの偽装メールの検出と同様に、コンテンツ フィルタはポリシーできめ細かくコンテンツを識別するために役立ちます。このタスクでは、ドキュメント内のマクロを識別して削除するための新しいコンテンツ フィルタを作成します。

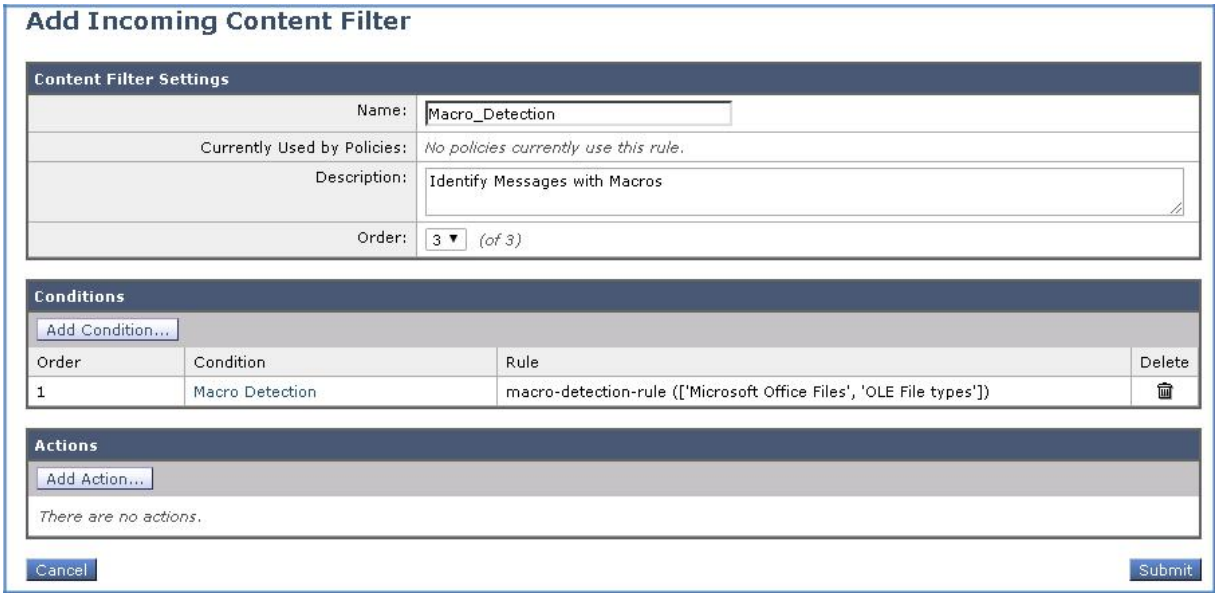
1. ワークステーションから GUI にアクセスし、[メール ポリシー(Mail Policy)] > [受信コンテンツ フィルタ(Incoming Content Filters)] に移動して、[フィルタの追加(Add Filter)] をクリックします。
2. 次の設定で*条件*と*アクション*を設定します。

   - [名前(Name)]:Macro_Detection
   - [説明(Description)]:Identify Messages with Macros(マクロを含むメッセージを識別します)
   - [条件(Conditions)]:[マクロの検出(Macro Detection)] > [利用可能なファイル タイプ(Available File Types)] > [Microsoft Office ファイル、OLE ファイル タイプ(Microsoft Office Files, OLE File Types)]
   - [アクション(Action)] の 1:[マクロを含む添付ファイルの削除(Strip Attachment with Macro)] > [利用可能なファイル タイプ(Available File Types)] > [Microsoft Office ファイル、OLE ファイル タイプ(Microsoft Office Files, OLE File Types)]

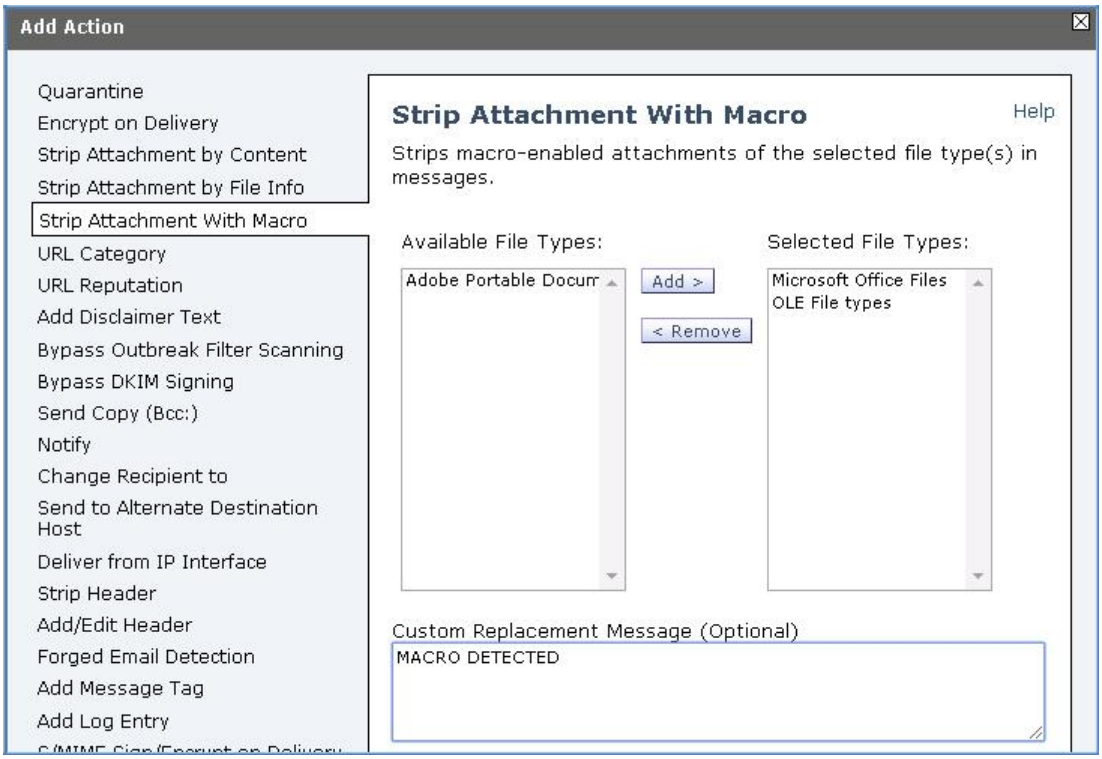
     [カスタム置換メッセージ(任意)(Custom Replacement Message (Optional))]:MACRO DETECTED(マクロが検出されました)



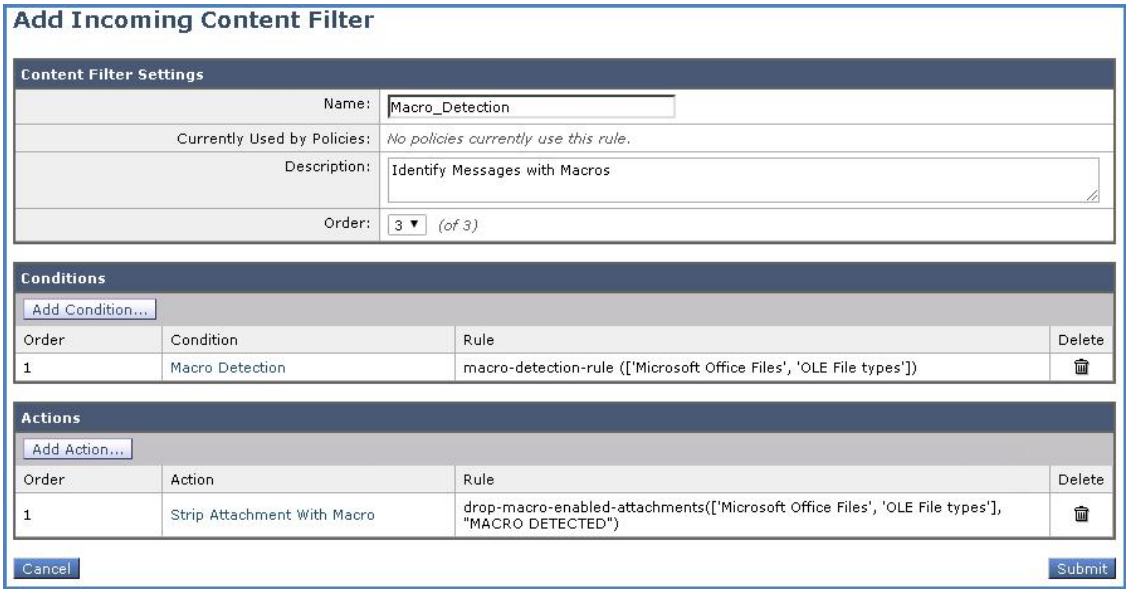
3. [OK] をクリックします



4. [アクションを追加（Add Action）] をクリックします。



5. [OK] をクリックします。

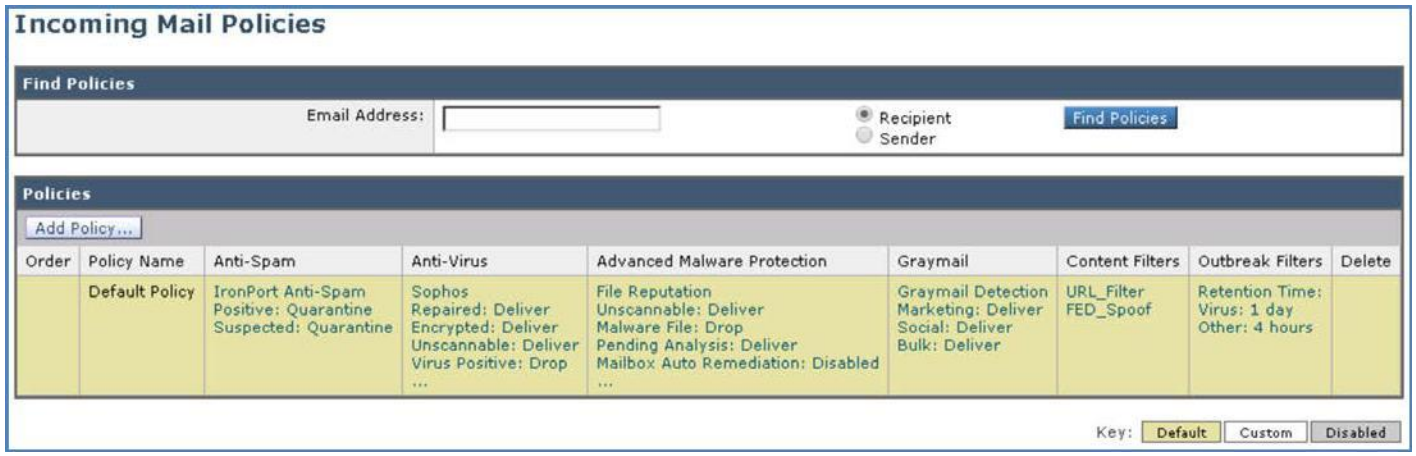


6. [送信(Submit)] をクリックしてコンテンツ フィルタを作成します。完了したら [変更内容を確定(Commit Changes)] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

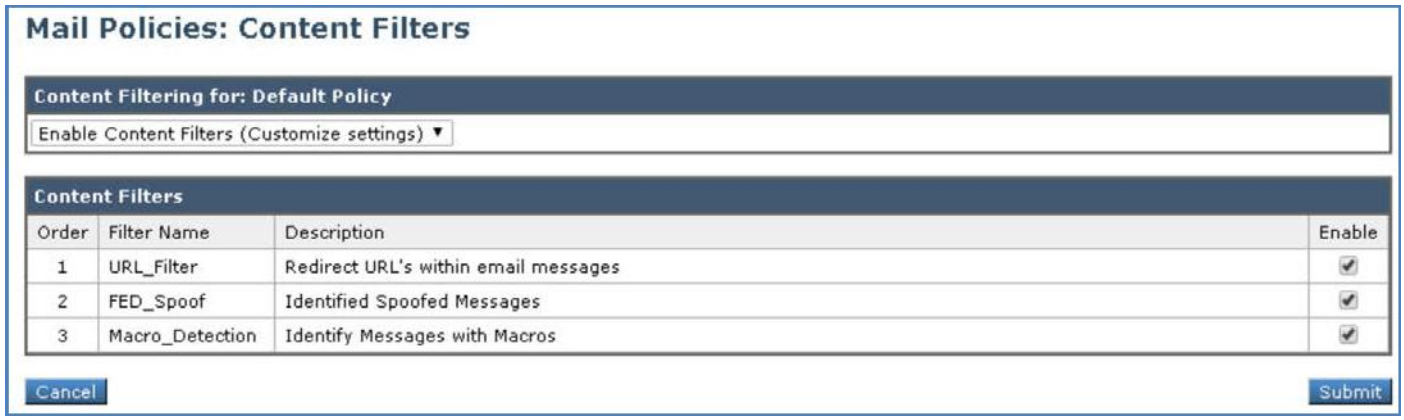
タスク:受信メール ポリシーを編集する(推定所要時間:1 分)

最後のタスクはデフォルトの受信メール ポリシーを変更して、コンテンツ フィルタを有効にすることです。

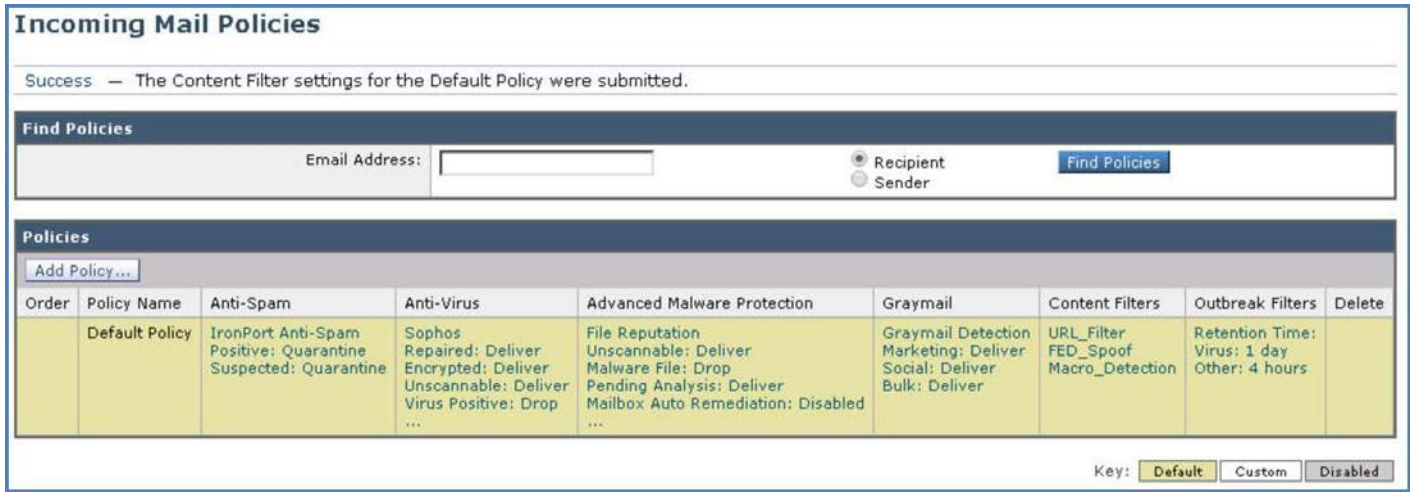
1. ワークステーションから GUI にアクセスし、[メール ポリシー(Mail Policy)] > [受信メール ポリシー(Incoming Mail Policies)] に移動して、[デフォルト ポリシー(Default Policy)] の [コンテンツ フィルタ(Content Filters)] ボックス内をクリックします。



2. 前の手順で作成した「Macro_Detection」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。



3. [送信（Submit）] をクリックしてコンテンツ フィルタを作成し、ポリシーを確認します。



4. 完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

タスク：マクロの検出をテストする（推定所要時間：5 分）

全体の構成が完了していれば、マクロが組み込まれたファイルを電子メールに添付して社外ユーザの Adam から Alan に送信することによって、マクロ検出機能をテストできます。

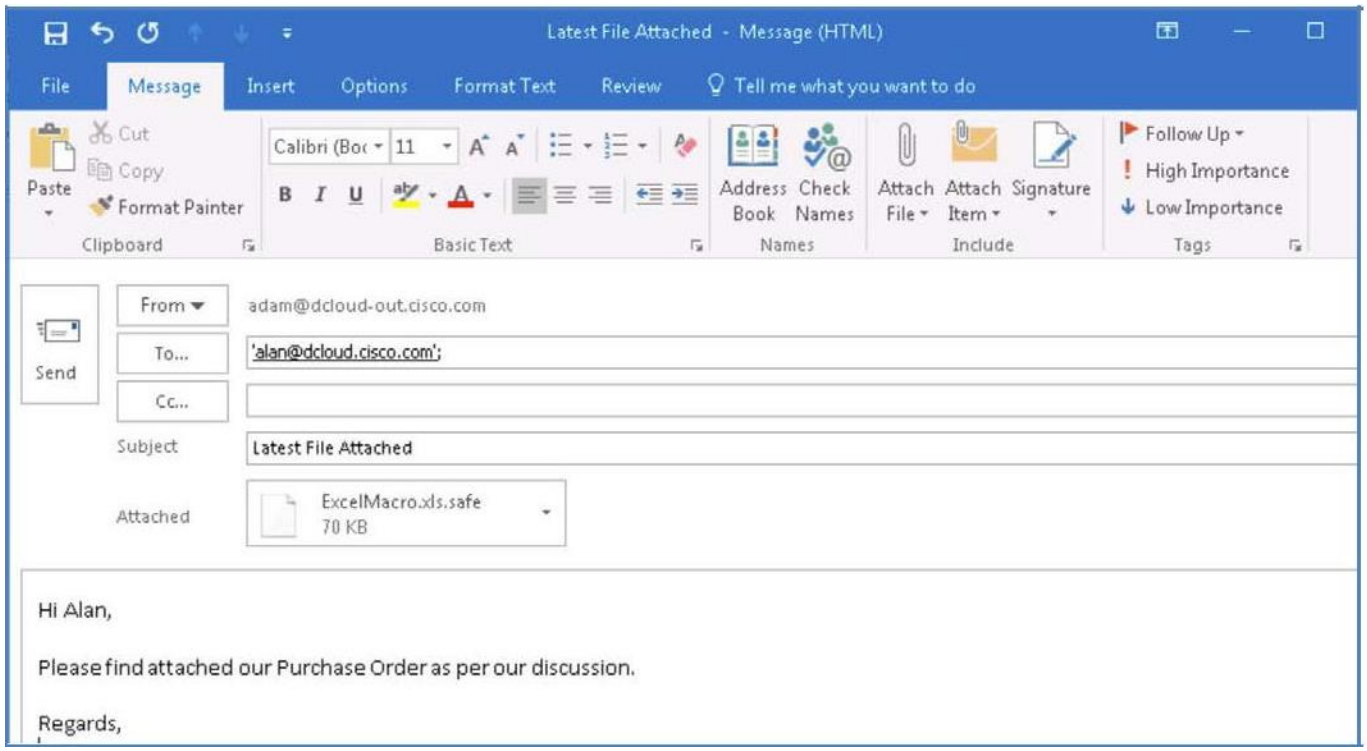
CLI セッションの開始

メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。

1. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。

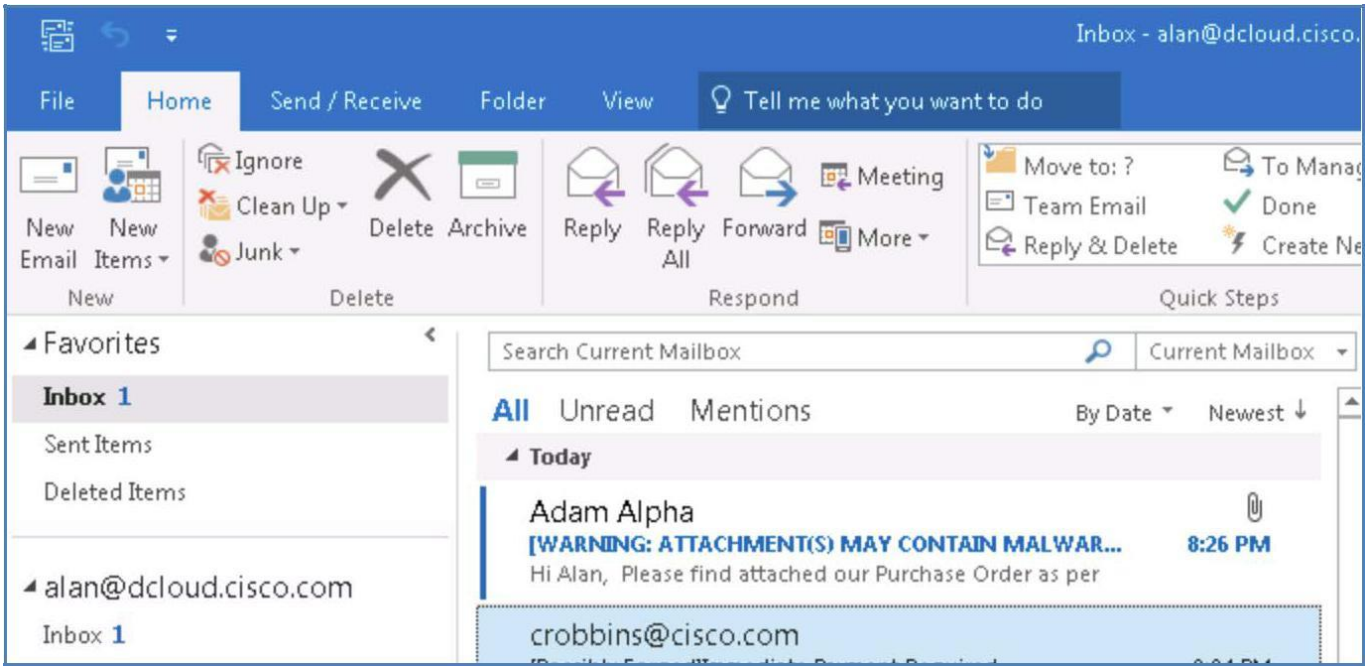
   - [宛先（To）]：alan@dcloud.cisco.com
   - [件名（Subject）]：最新ファイルを添付しています（Latest File Attached）
   - [本文（Body）]：お世話になります（Hi）

     前回の会議に沿って、ドキュメントを送信します。ご査収ください。（Please find attached document as per our discussion（）
   - [添付ファイル（Attachment）]：ExcelMacro.xls.safe（デスクトップ上の Macro-Enabled Detection サブフォルダに保存）

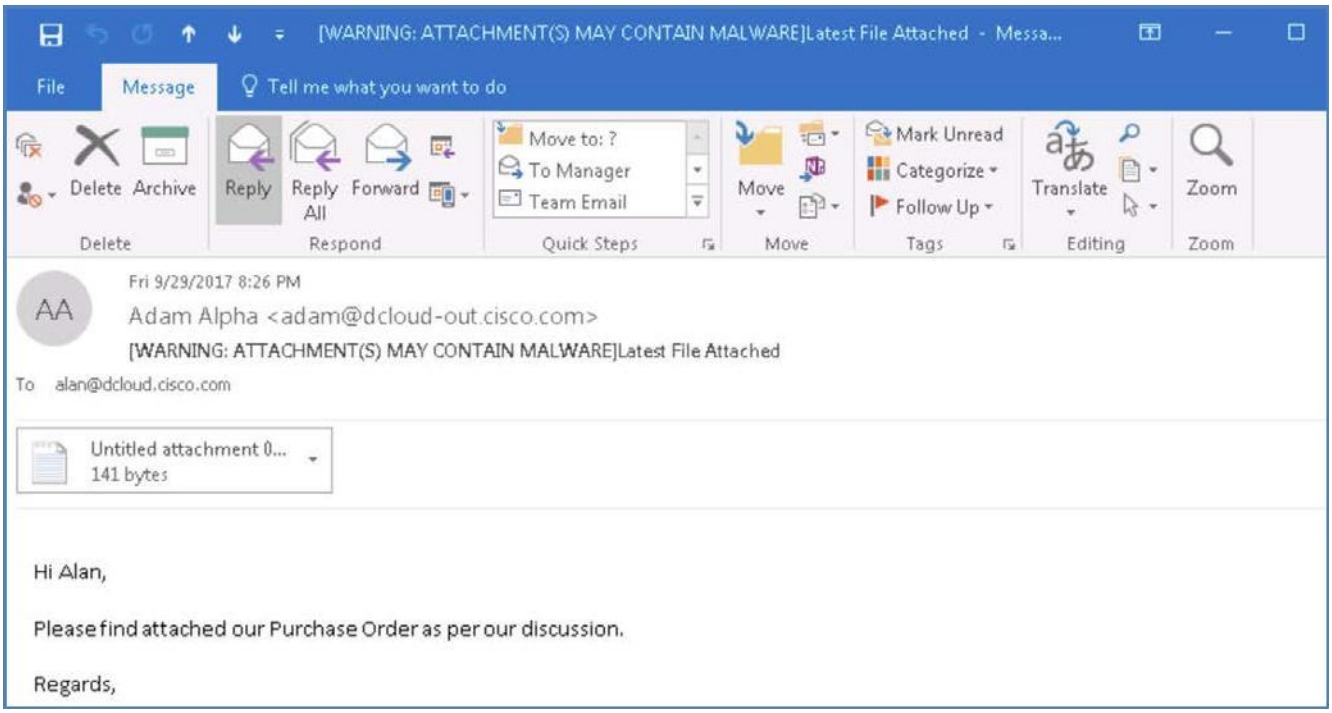


2. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

3. Alan はメッセージを受信します。受信者がすぐに気づくように件名ヘッダーが変更されていることを確認できます。



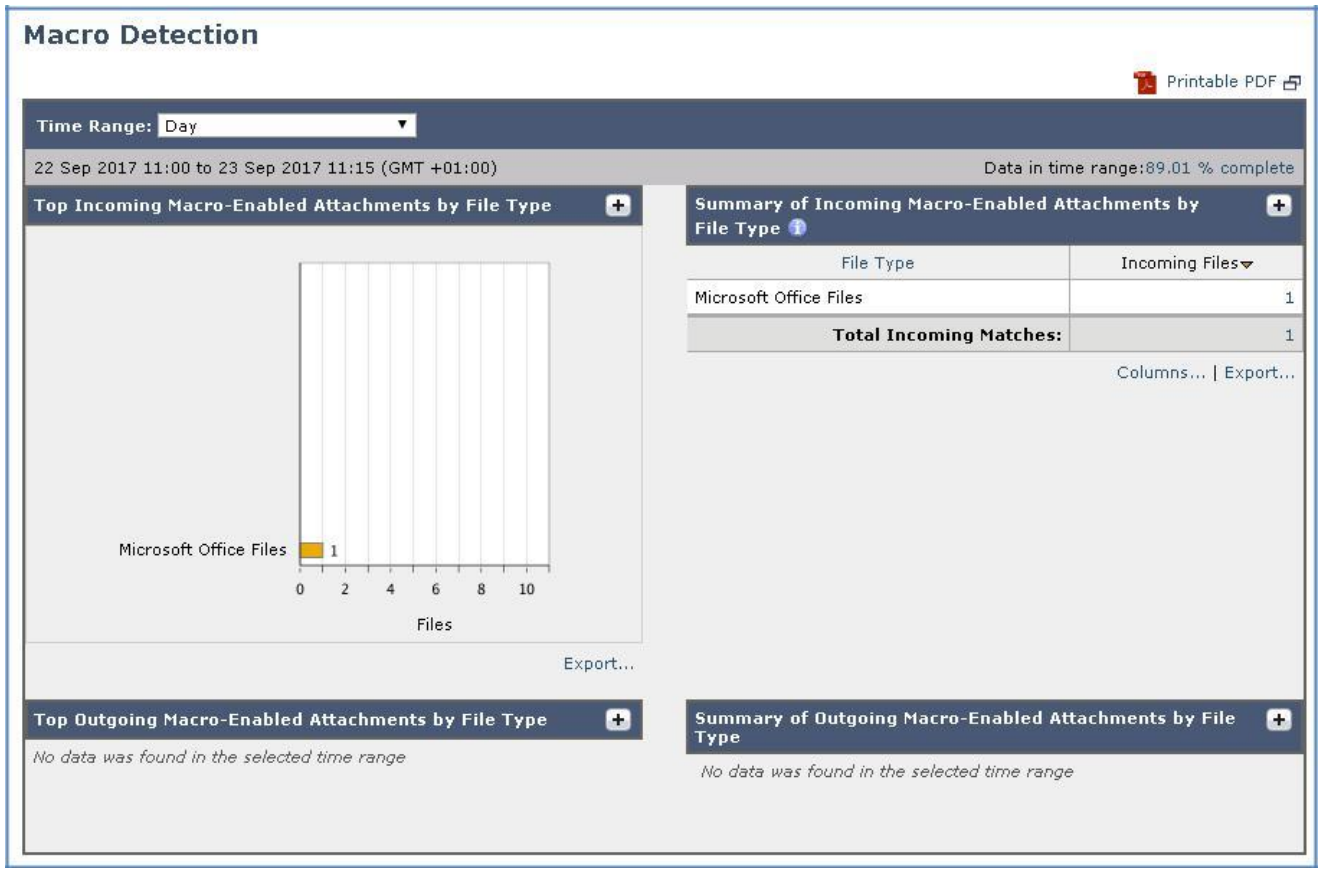
4. メッセージを開き、添付ファイルが削除されていることを確認します。



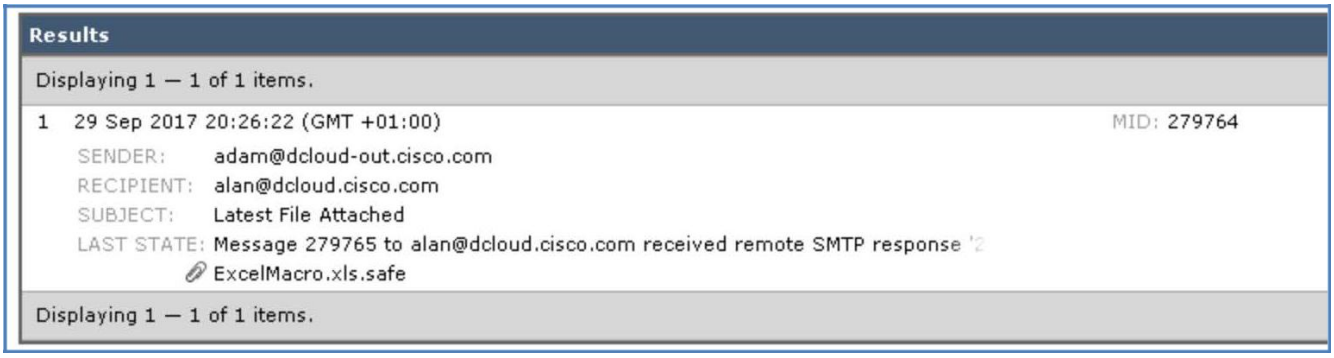
5. CLI に戻り、基盤となるメール処理が実行されていることと、そのファイルが削除された理由を確認します。MID を書き留めます。

```
Fri Sep 29 20:26:22 2017 Info: MID 279764 Subject 'Latest File Attached'
Fri Sep 29 20:26:22 2017 Info: MID 279764 ready 101506 bytes from <adam@dcloud-out.cisco.com>
Fri Sep 29 20:26:22 2017 Info: MID 279764 attachment 'ExcelMacro.xls.safe'
Fri Sep 29 20:26:22 2017 Info: MID 279764 matched all recipients for per-recipient policy DEFAULT in the inbound table
Fri Sep 29 20:26:22 2017 Info: MID 279764 interim verdict using engine: CASE spam negative
Fri Sep 29 20:26:22 2017 Info: MID 279764 using engine: CASE spam negative
Fri Sep 29 20:26:22 2017 Info: MID 279764 interim AV verdict using Sophos CLEAN
Fri Sep 29 20:26:22 2017 Info: MID 279764 antivirus negative
Fri Sep 29 20:26:23 2017 Info: MID 279764 AMP file reputation verdict : UNKNOWN(File analysis pending)
Fri Sep 29 20:26:23 2017 Info: MID 279764 SHA 30d9a3c2fe92d26c4dc85cdfe71b119bad15f9e78d778eee966c9346c1e4ab07 filename Excel
Macro.xls.safe queued for possible file analysis upload
Fri Sep 29 20:26:23 2017 Info: MID 279764 using engine: GRAYMAIL negative
Fri Sep 29 20:26:23 2017 Info: MID 279764 rewritten to MID 279765 by drop-macro-enabled-attachments filter 'Macro_Detection'
Fri Sep 29 20:26:23 2017 Info: Message finished MID 279764 done
Fri Sep 29 20:26:23 2017 Info: MID 279765 using engine: CASE using cached verdict
Fri Sep 29 20:26:23 2017 Info: CASE cache status: hits = 1, misses = 14, expires = 0, adds = 14, seconds saved = 0.69, total
seconds = 52.57
Fri Sep 29 20:26:23 2017 Info: MID 279765 Outbreak Filters: verdict negative
Fri Sep 29 20:26:23 2017 Info: MID 279765 queued for delivery
```

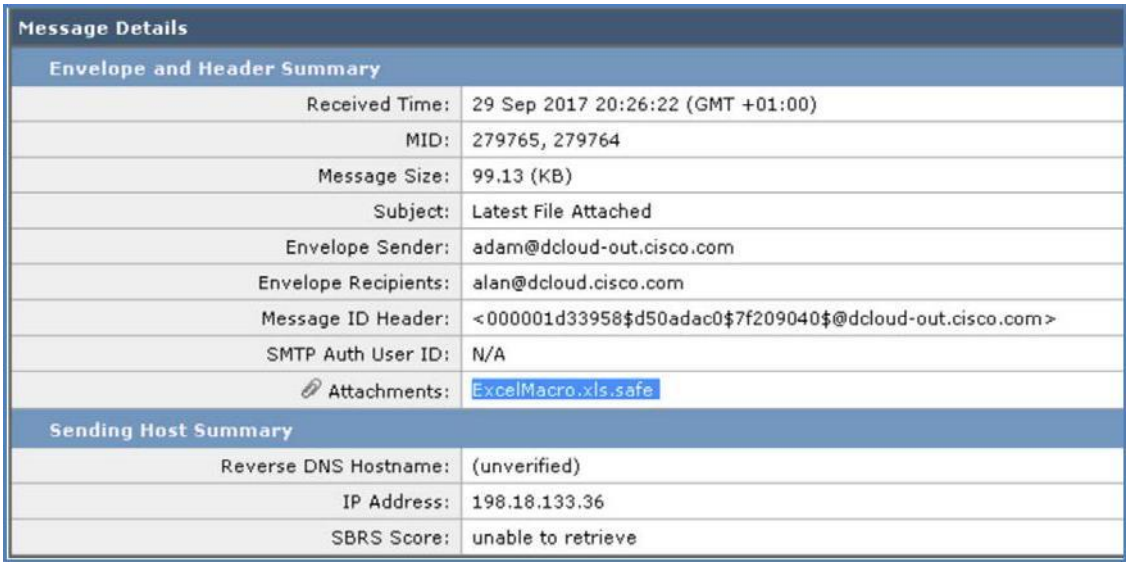
6. ワークステーションから GUI にアクセスし、[メール ポリシー（Mail Policy）] > [マクロの検出（Macro Detection）] に移動して、レポートの内容を確認します。



7. [受信ファイル（Incoming Files）] の下の値をクリックして、メッセージ トラッキングを起動します。トラッキングの情報が更新されるまでに数秒かかる場合があります。

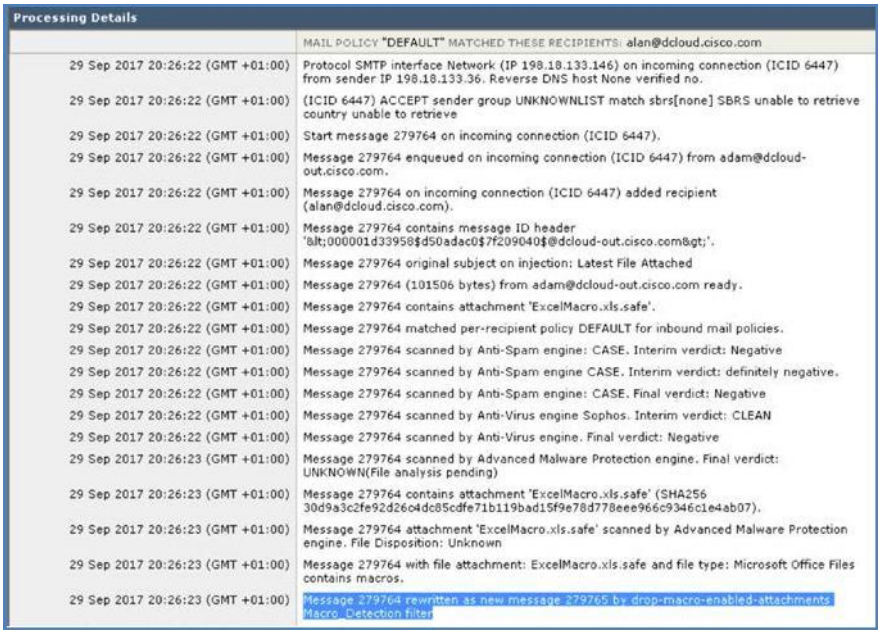


8. [詳細の表示（Show Details）] をクリックして、エンジンによってメッセージがどのように処理されたかと、ポリシー照合の結果として添付ファイルに適用されたアクションを確認します。



9. 処理セクションには、Cisco E メール セキュリティ ソリューションによるメッセージの一連の処理と有効になっているエンジンによって適用された、さまざまなアクションの詳細なタイムラインが示されます。

10. これは CLI セッションに表示されるものと同じ情報ですが、ここではスクロールされず CLI セッションが終了した後に確認できます。



Processing Details

	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: alan@dcloud.cisco.com
29 Sep 2017 20:26:22 (GMT +01:00)	Protocol SMTP interface Network (IP 198.18.133.146) on incoming connection (ICID 6447) from sender IP 198.18.133.36. Reverse DNS host None verified no.
29 Sep 2017 20:26:22 (GMT +01:00)	(ICID 6447) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS unable to retrieve country unable to retrieve
29 Sep 2017 20:26:22 (GMT +01:00)	Start message 279764 on incoming connection (ICID 6447).
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 enqueued on incoming connection (ICID 6447) from adam@dcloud-out.cisco.com.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 on incoming connection (ICID 6447) added recipient (alan@dcloud.cisco.com).
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 contains message ID header '<000001d33958$d50adac0$7f209040$@dcloud-out.cisco.com>'.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 original subject on injection: Latest File Attached
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 (101506 bytes) from adam@dcloud-out.cisco.com ready.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 contains attachment 'ExcelMacro.xls.safe'.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 matched per-recipient policy DEFAULT for inbound mail policies.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Spam engine: CASE. Final verdict: Negative
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Virus engine. Final verdict: Negative
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 scanned by Advanced Malware Protection engine. Final verdict: UNKNOWN(File analysis pending)
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 contains attachment 'ExcelMacro.xls.safe' (SHA256 30d9a3c2fe92d26c4dc85cdfe71b119bad15f9e78d778eee966c9346c1e4ab07).
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 attachment 'ExcelMacro.xls.safe' scanned by Advanced Malware Protection engine. File Disposition: Unknown
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 with file attachment: ExcelMacro.xls.safe and file type: Microsoft Office Files contains macros.
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 rewritten as new message 279765 by drop-macro-enabled-attachments Macro_Detection filter

11. 詳細なメッセージ トラッキングのウィンドウを閉じてメッセージ トラッキングのメイン画面に戻ります。

シナリオ 6:　地理位置情報ベースのフィルタリング

使用例

Voyage Corp 社は、2015 年に西ヨーロッパに事業を拡大しました。これは主に、英国（UK）、イタリア、フランス、スペイン、およびいくつかの小規模市場で重要顧客を増やすことで達成されました。ビジネスは堅調で前年比で 10 % の伸びを記録し、その後も劇的に成長すると思われました。しかし、UK が行った欧州連合（EU）からの離脱に関する決定により、上位 10 社の顧客の大半が影響を受けました。これらの顧客は法律に拘束されており、UK と EU の政治的結合が断たれた場合、UK との商取引を断念する必要がありました。

セキュリティ制御

Cisco E メール セキュリティは、特定の地理位置情報から着信メールの接続およびメッセージを処理し、適切なアクションを実行できます。たとえば、次のようなアクションを実行できます。

- 特定の地域から受信する電子メールよる脅威を防止します。
- 特定の地域からの電子メールの受信を許可または禁止します。

この機能は、次の方法で使用できます。

- 送信者グループによる SMTP 接続レベル
- コンテンツ フィルタ レベル

目的

このシナリオでは、選択した特定の国からの受信メッセージ（またはそれらの国への送信メッセージ）を処理するために、コンテンツ フィルタとホスト アクセス テーブルを使用して地理位置情報ベースのフィルタを設定する一連の手順を実行します。

注: 地理位置情報ベースのフィルタリングの詳細については、「Geolocation Based Filtering」を参照してください。

手順

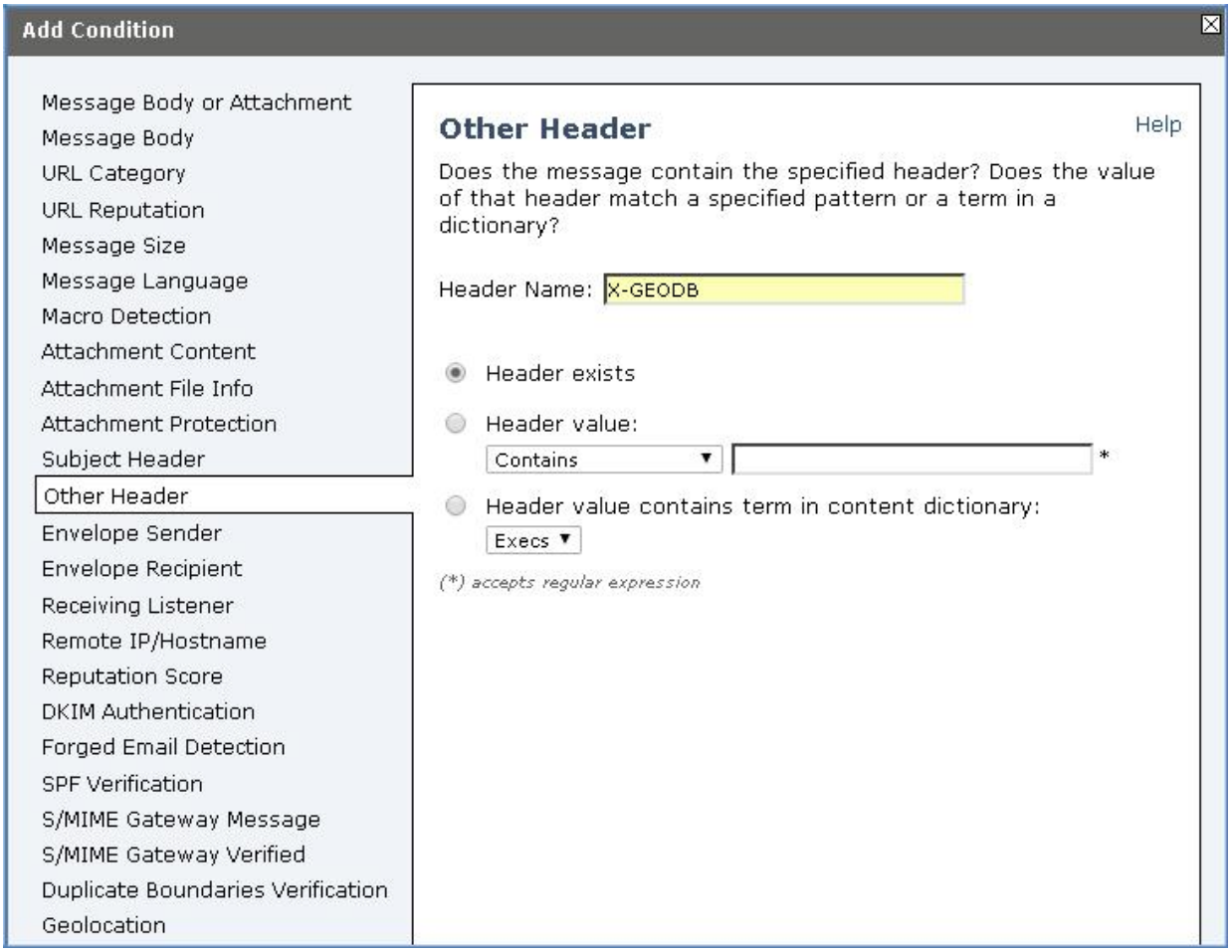
タスク:コンテンツ フィルタを設定する（推定所要時間:3 分）

前のシナリオと同様に、コンテンツ フィルタはポリシーできめ細かくコンテンツを識別するために役立ちます。このタスクでは、制御を禁止する国を指定するため、新しいコンテンツ フィルタを作成します。

1. ワークステーションから GUI にアクセスし、[メール ポリシー（Mail Policy）] > [受信コンテンツ フィルタ（Incoming Content Filters）] に移動して、[フィルタの追加（Add Filter）] をクリックします。

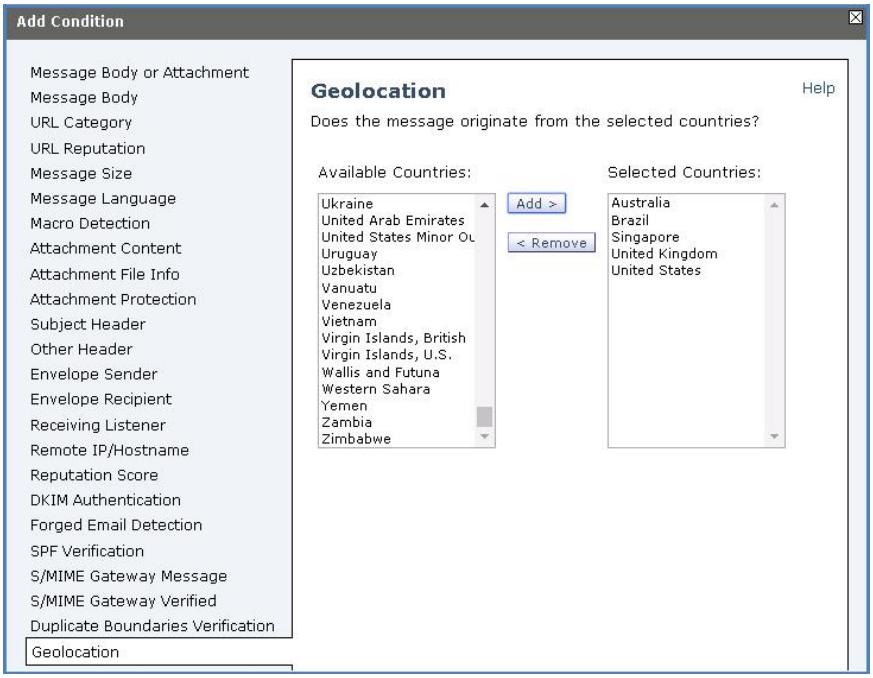
2. 次の設定で条件とアクションを設定します。

   - [名前(Name)]:Block_GeoDB
   - [説明(Description)]:位置ベースのフィルタリング(Location based Filtering)
   - [条件(Condition)] の 1:[その他のヘッダー(Other Header)] > [ヘッダー名(Header Name)]:X-GEODB
   - [条件(Condition)] の 2:[地理位置情報(Geolocation)] > [オーストラリア(Australia)]、[ブラジル(Brazil)]、[シンガポール(Singapore)]、[英国(United Kingdom)]、[米国(United States)]
   - [アクション(Action)] の 1:[ドロップ(最後のアクション)(Drop (Final Action))]



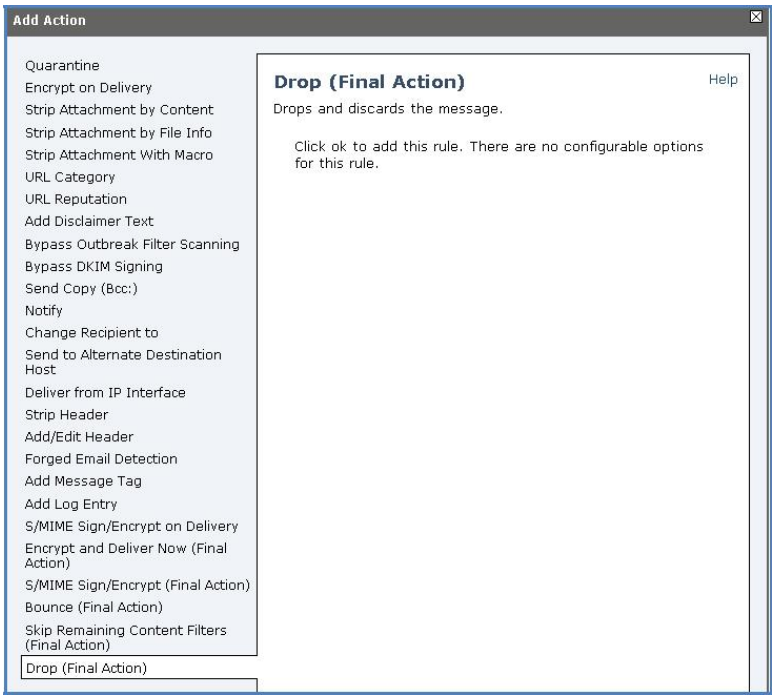
3. [OK] をクリックします

4. [条件を追加（Add Condition）] をクリックします。

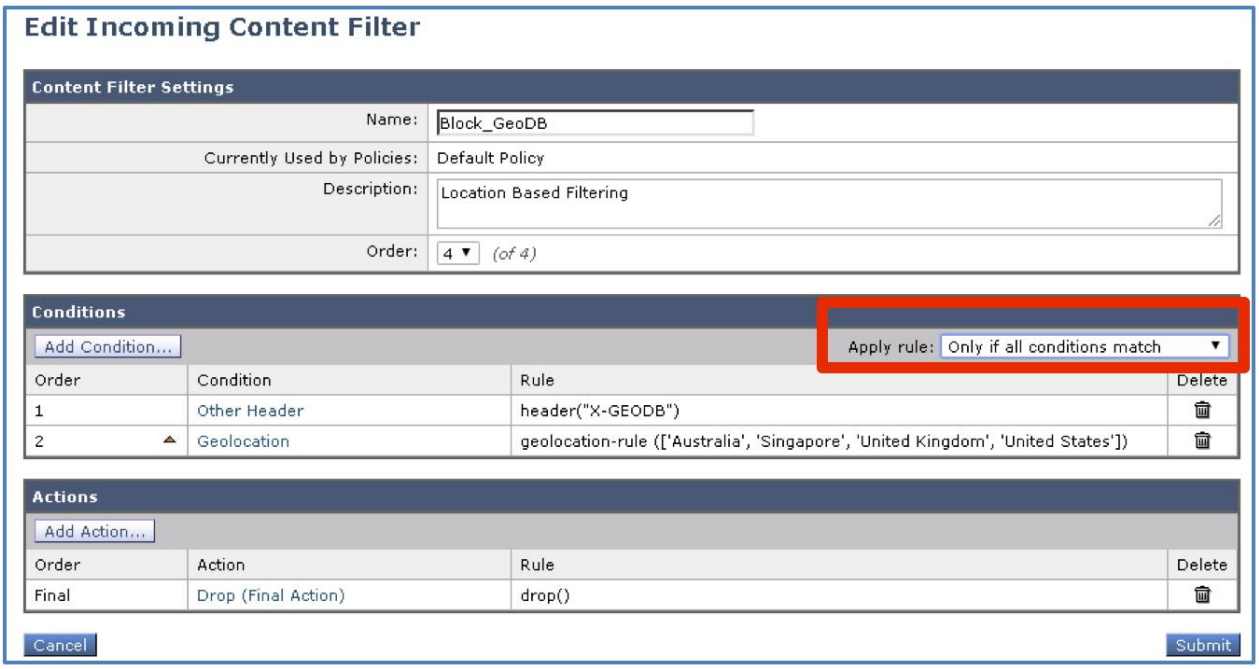


5. [OK] をクリックします。

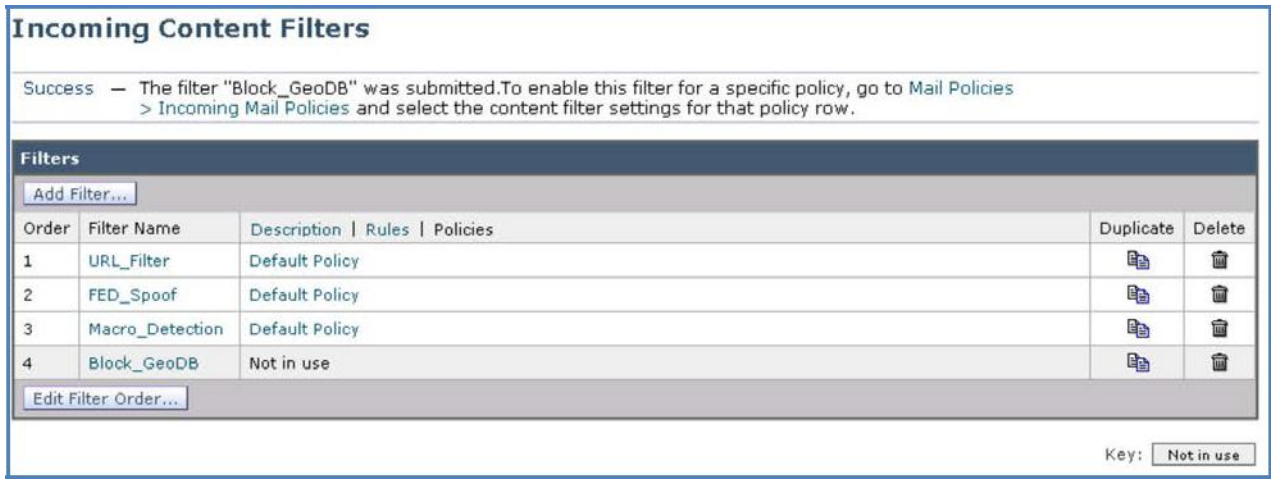
6. [アクションを追加（Add Action）] をクリックします。



7. 最後に [ルールの適用（Apply Rule）] ドロップダウン ボックスから [すべての条件が一致する場合のみ（Only if all conditions match）] を選択することにより、条件の動作を変更します。



8. [送信（Submit）] をクリックしてコンテンツ フィルタを作成します。

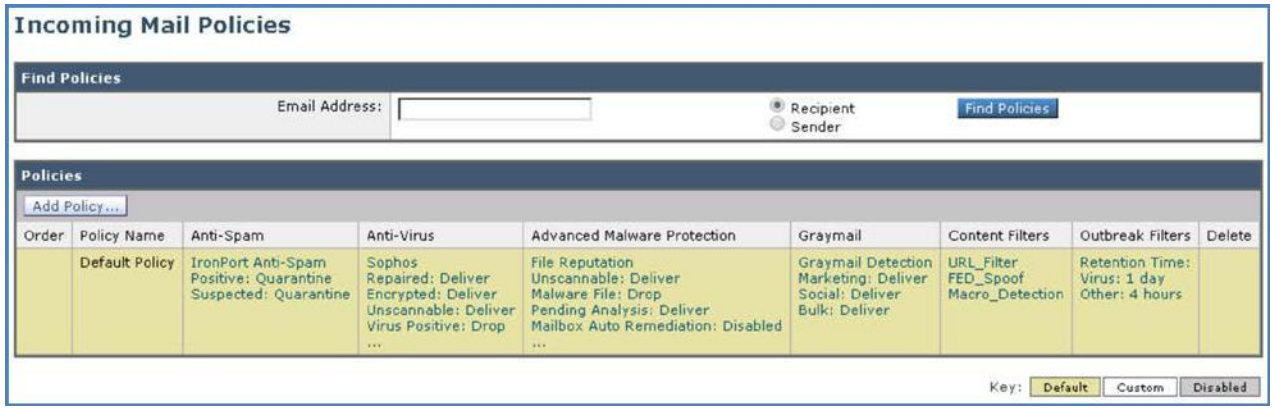


9. 完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

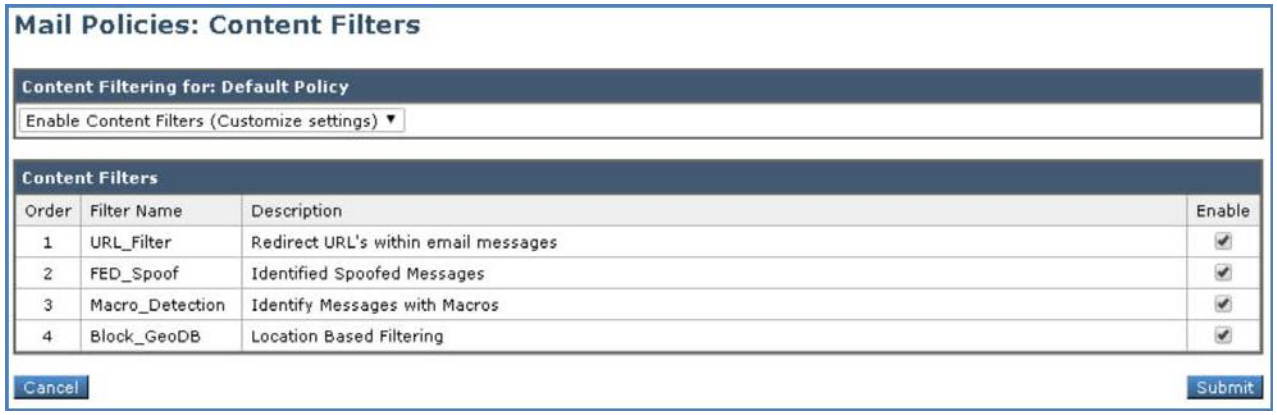
タスク:受信メール ポリシーを編集する(推定所要時間:1 分)

最後のタスクはデフォルトの受信メール ポリシーを変更して、コンテンツ フィルタを有効にすることです。

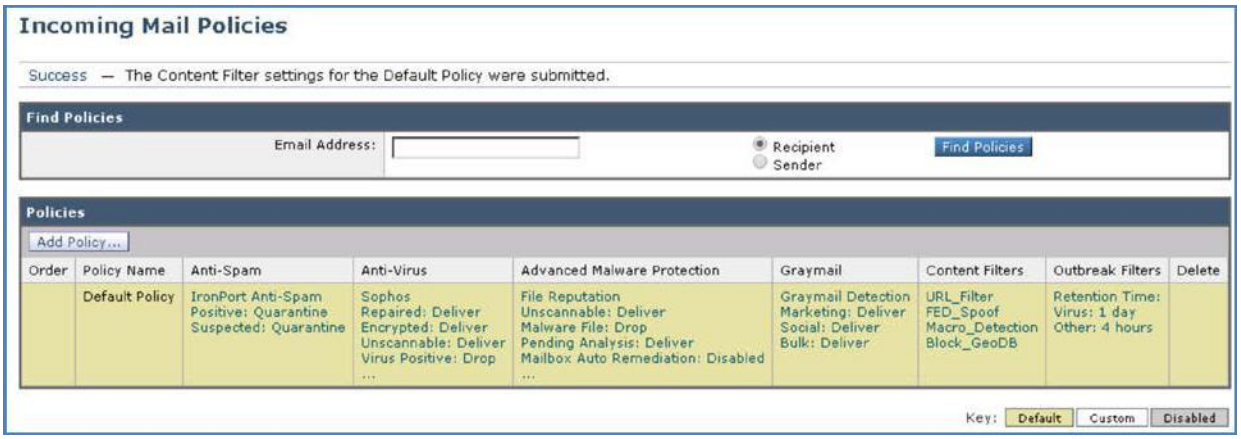
1. ワークステーションから GUI にアクセスし、[メール ポリシー(Mail Policy)] > [受信メール ポリシー(Incoming Mail Policies)] に移動して、[デフォルト ポリシー(Default Policy)] の [コンテンツ フィルタ(Content Filters)] ボックス内をクリックします。



2. 前の手順で作成した「Block_GeoDB」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。



3. [送信（Submit）] をクリックしてコンテンツ フィルタを作成し、ポリシーを確認します。



4. 完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

タスク：地理位置情報をテストする（推定所要時間：5 分）

全体の構成が完了していれば、社外ユーザの Adam（以前に指定した国をシミュレート）から Alan に電子メールを送信することによって地理位置情報機能をテストできます。

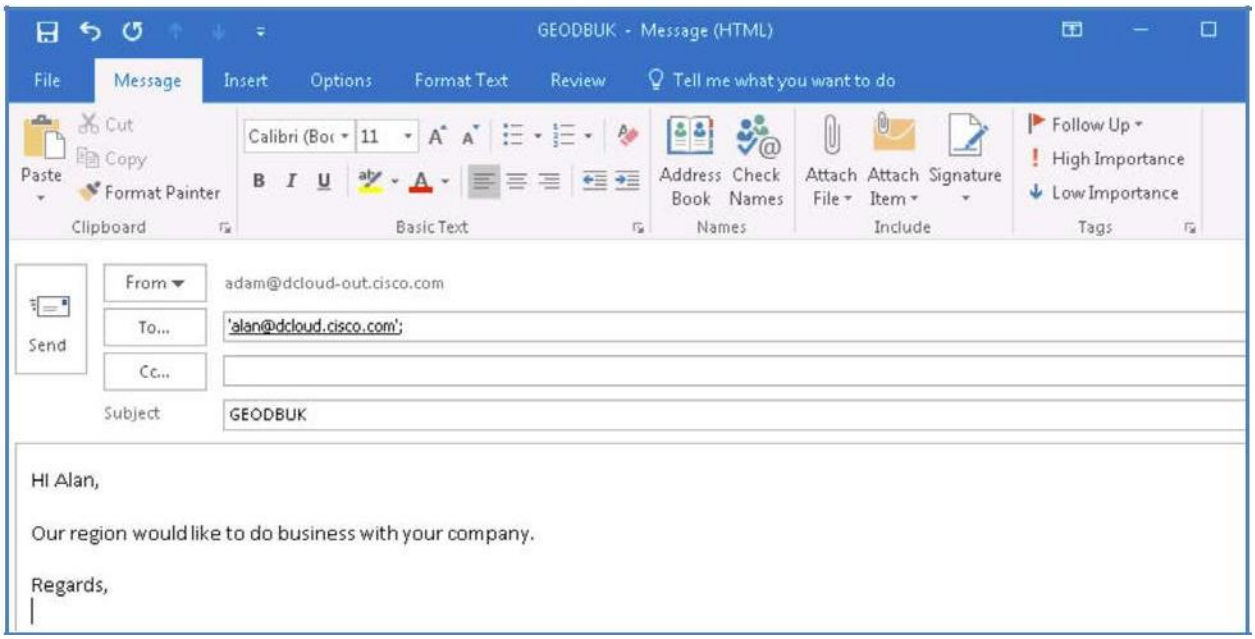
CLI セッションの開始

メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。

1. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。
   - [宛先（To）]：alan@dcloud.cisco.com
   - [件名（Subject）]：GEODBUK
   - [本文（Body）]：Hi Alan,（Alan 様）

     弊社では、御社との取引を希望しております。（Our region would like to do business with your company.）

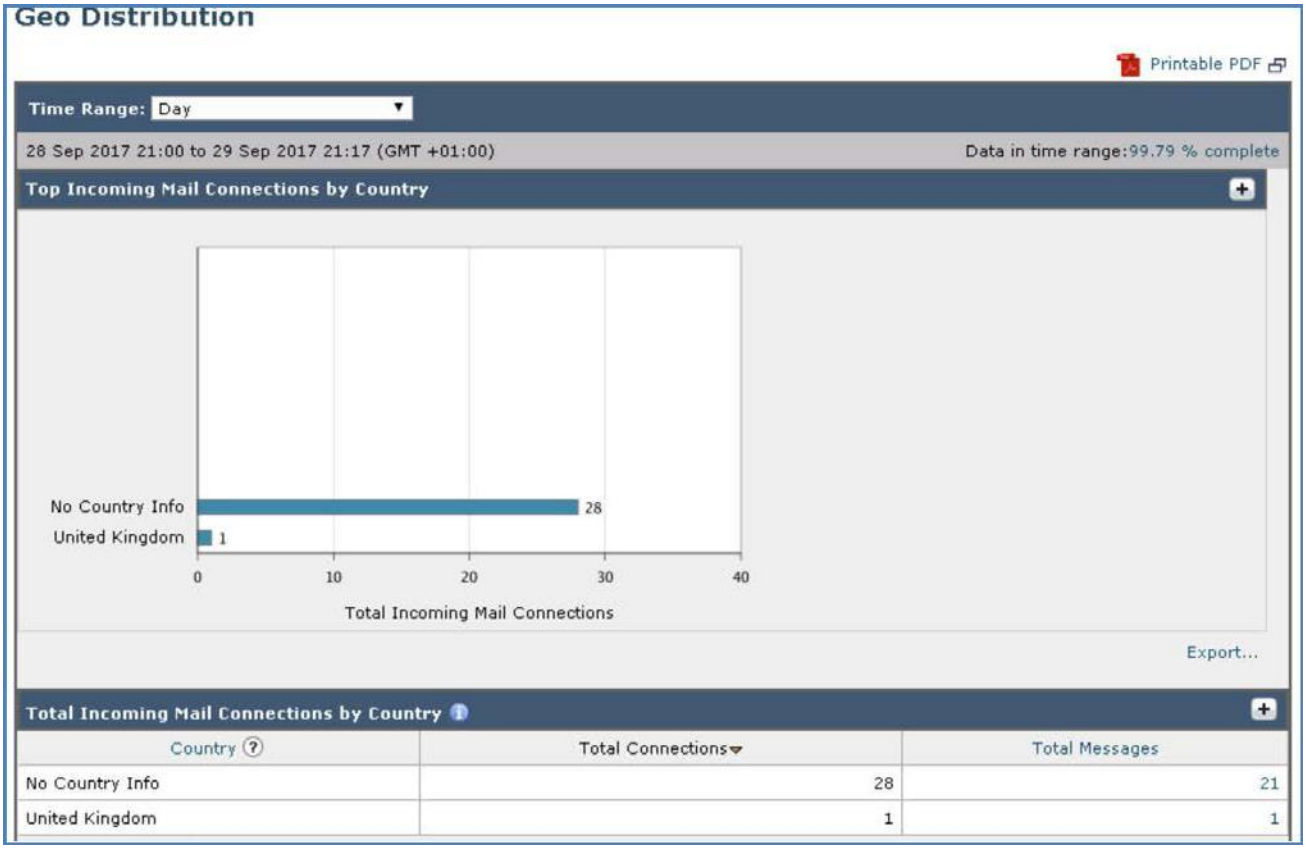
     Regards,（よろしくお願いします。）



2. メールを送信します。[すべてのフォルダを送受信（Send/Receive All Folders）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。
3. CLI に戻り、コンテンツ フィルタがどのようにメッセージを処理したかを確認します。

```
Fri Sep 29 21:17:21 2017 Info: ICID 6459 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country United Kingdom
Fri Sep 29 21:17:21 2017 Info: Delivery start DCID 2564 MID 279776 to RID [0]
Fri Sep 29 21:17:21 2017 Info: Start MID 279777 ICID 6459
Fri Sep 29 21:17:21 2017 Info: MID 279777 ICID 6459 From: <adam@dcloud-out.cisco.com>
Fri Sep 29 21:17:21 2017 Info: MID 279777 ICID 6459 RID 0 To: <alan@dcloud.cisco.com>
Fri Sep 29 21:17:21 2017 Info: MID 279777 Message-ID '<002e01d3395f$f3123750$d936a5f0$@dcloud-out.cisco.com>'
Fri Sep 29 21:17:21 2017 Info: MID 279777 Subject 'GEODBUK'
Fri Sep 29 21:17:21 2017 Info: MID 279777 ready 5395 bytes from <adam@dcloud-out.cisco.com>
Fri Sep 29 21:17:21 2017 Info: MID 279777 matched all recipients for per-recipient policy DEFAULT in the inbound table
Fri Sep 29 21:17:21 2017 Info: Message done DCID 2564 MID 279776 to RID [0] [('X-GEODB', 'YES')]
Fri Sep 29 21:17:21 2017 Info: MID 279776 RID [0] Response 'ok:  Message 279777 accepted'
Fri Sep 29 21:17:21 2017 Info: Message finished MID 279776 done
Fri Sep 29 21:17:21 2017 Info: Mail delivery client with DCID 2564 reached maximum messages-per-connection limit.
Fri Sep 29 21:17:21 2017 Info: ICID 6459 close
Fri Sep 29 21:17:21 2017 Info: DCID 2564 close
Fri Sep 29 21:17:21 2017 Info: MID 279777 interim verdict using engine: CASE spam negative
Fri Sep 29 21:17:21 2017 Info: MID 279777 using engine: CASE spam negative
Fri Sep 29 21:17:21 2017 Info: MID 279777 interim AV verdict using Sophos CLEAN
Fri Sep 29 21:17:21 2017 Info: MID 279777 antivirus negative
Fri Sep 29 21:17:21 2017 Info: MID 279777 AMP file reputation verdict : SKIPPED (no attachment in message)
Fri Sep 29 21:17:21 2017 Info: MID 279777 using engine: GRAYMAIL negative
Fri Sep 29 21:17:21 2017 Info: Message aborted MID 279777 Dropped by content filter 'Block_GeoDB' in the inbound table
Fri Sep 29 21:17:21 2017 Info: Message finished MID 279777 done
```

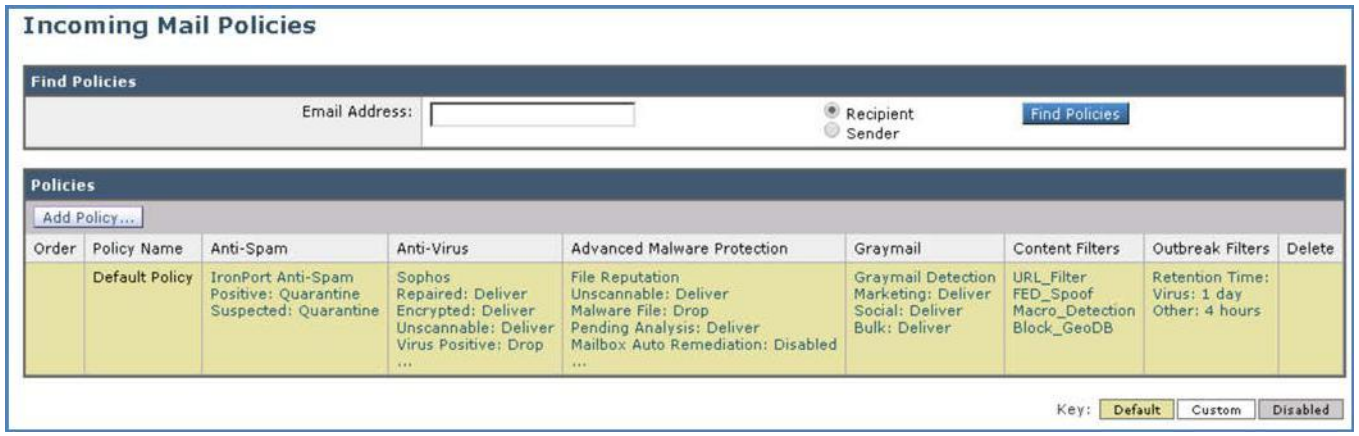
4. ワークステーションから GUI にアクセスし、[メール ポリシー（Mail Policy）] > [地理的区分（Geo Distribution）] に移動して、レポートの内容を確認します。



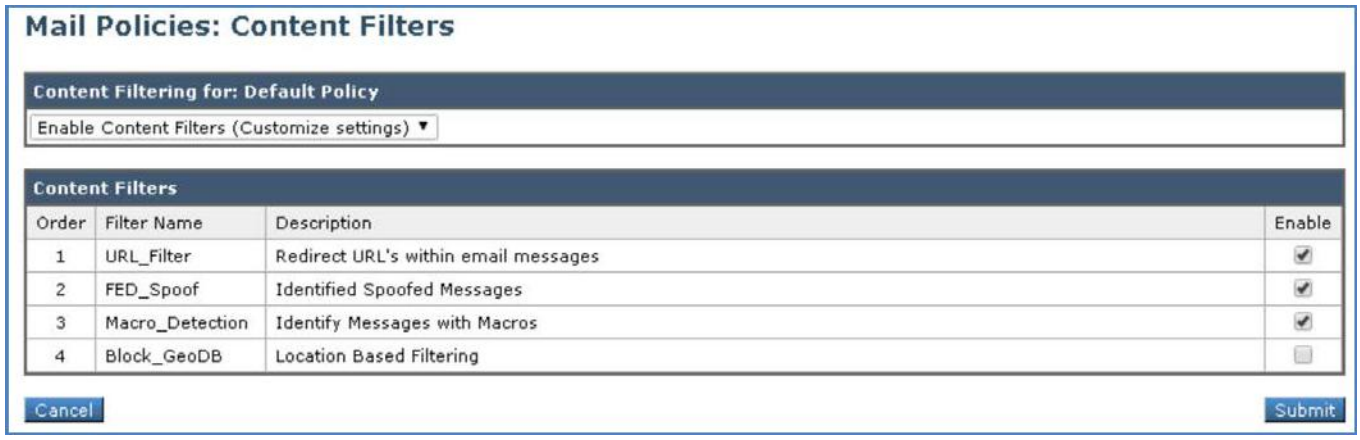
タスク：接続レベルで地理位置情報ベースのフィルタリングを実行する（推定所要時間：5 分）

地理位置情報ベースのフィルタリングは、ホスト アクセス テーブル（HAT）に適用される接続レベルでも実行できます。HAT はリモート ホストからの着信接続を制御するリスナー用のルール セットを保持しています。すべての設定済みリスナーには独自の HAT があり、通常はパブリック リスナーとプライベート リスナーが存在します。その名前が示すようにパブリックは外部向きのリスナーであり、プライベートは内部向きのリスナーです。

1. まず、前のタスクで追加されたデフォルト メール ポリシーからコンテンツ フィルタを削除します。厳密には、コンテンツ フィルタは後で電子メール パイプラインで処理されるためここで削除する必要はありませんが、ベスト プラクティスに従って削除しておきます。
2. ワークステーションから GUI にアクセスし、[メール ポリシー（Mail Policy）] > [受信メール ポリシー（Incoming Mail Policies）] に移動して、[デフォルト ポリシー（Default Policy）] の [コンテンツ フィルタ（Content Filters）] ボックス内をクリックします。



3. 前の手順で作成した「Block_GeoDB」コンテンツ フィルタのチェックマークを外して無効にします。

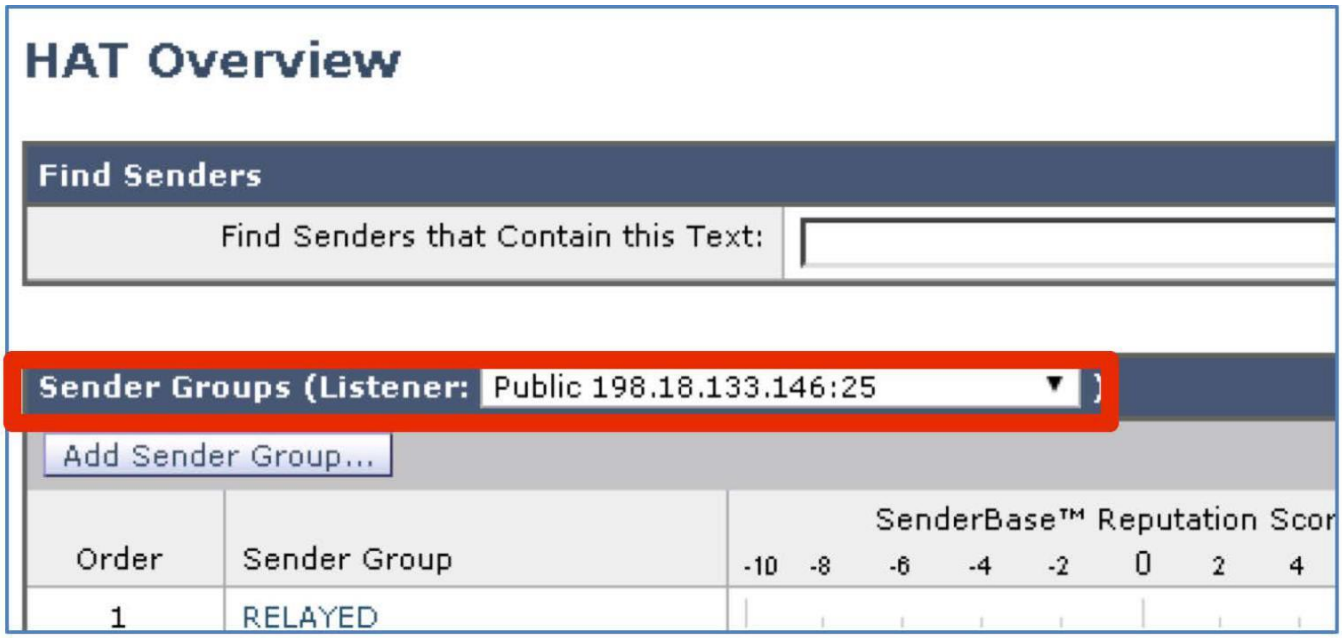


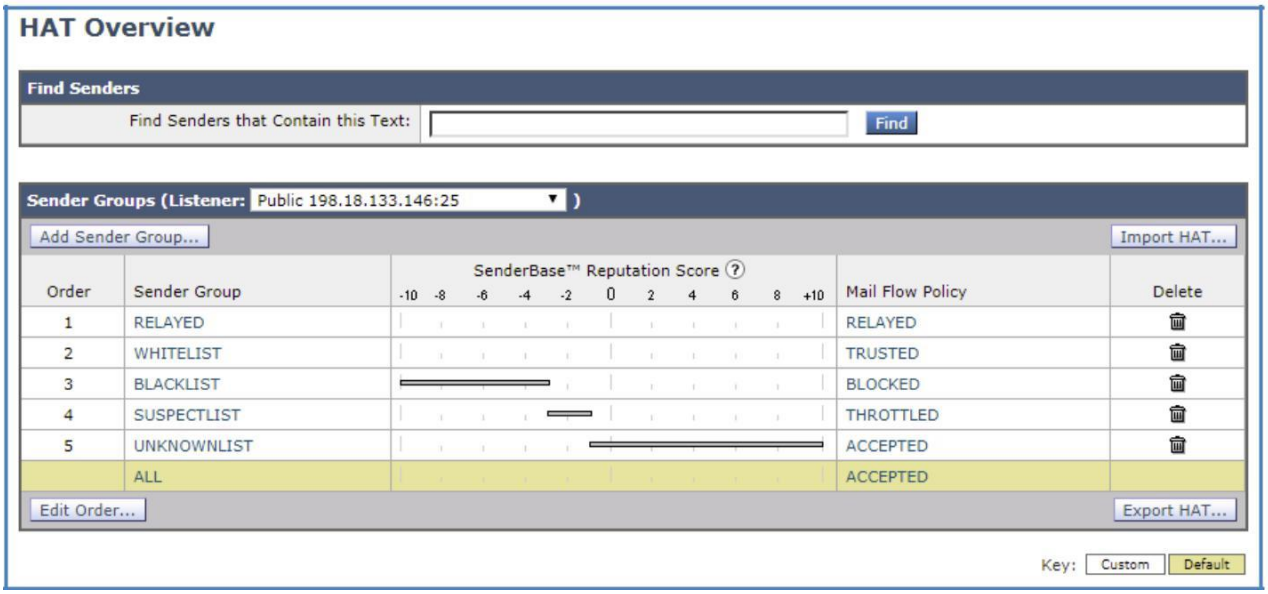
4. [送信（Submit）] をクリックしてアクションを適用します。完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

注：ホスト アクセス テーブルの詳細については、「Host Access Table」を参照してください。

5. [メール ポリシー（Mail Policies）] > [HAT の概要（HAT Overview）] に移動し、表示される画面で [送信者グループの追加（Add Sender Group）] をクリックします。

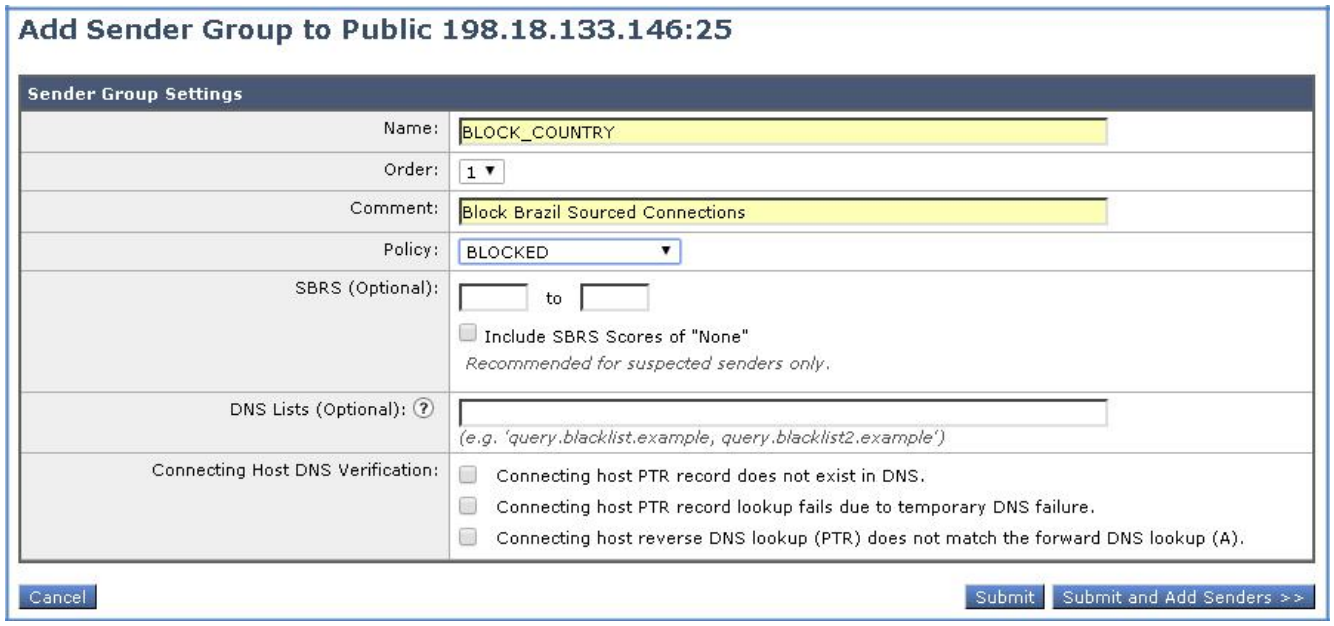
6. リスナーのリストから [送信者グループ（リスナー）パブリック（Sender Groups (Listener) Public）] が選択されていることを確認します。



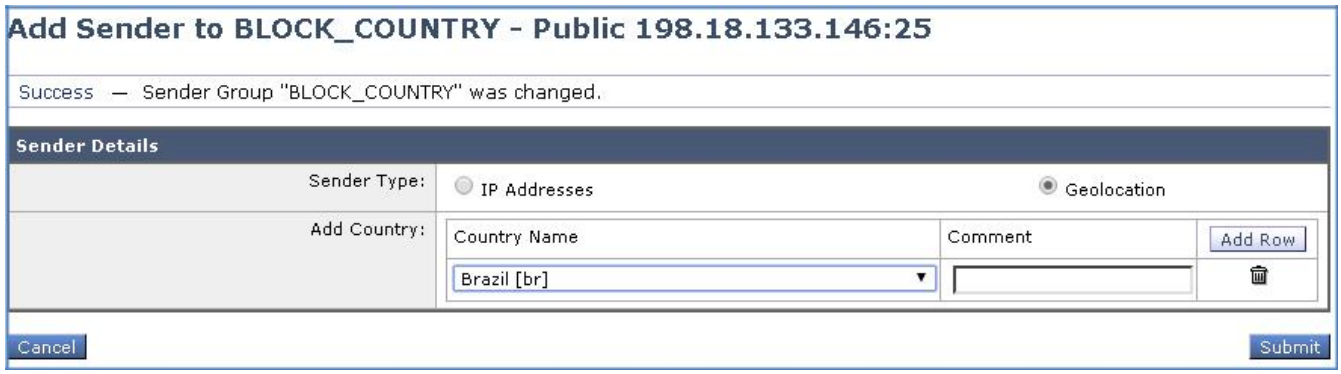


7. 次の設定を使用して新しい送信者グループを作成します（指定されていない場合はデフォルト設定を使用）。

- [名前（Name）]：BLOCK_COUNTRY
- [順序（Order）]：1
- [コメント（Comment）]：Block Brazil Sourced Connections（ブラジルを送信元とする接続をブロックします）
- メール フロー [ポリシー（Policy）]：BLOCKED（ブロック）



8. [Submit and Add Senders（送信と送信者の追加）] ボタンをクリックします。
9. 表示される画面で、[地理位置情報（Geolocation）] ラジオ ボタンを選択します。これにより、事前設定されたリストから国を選択できるようになります。

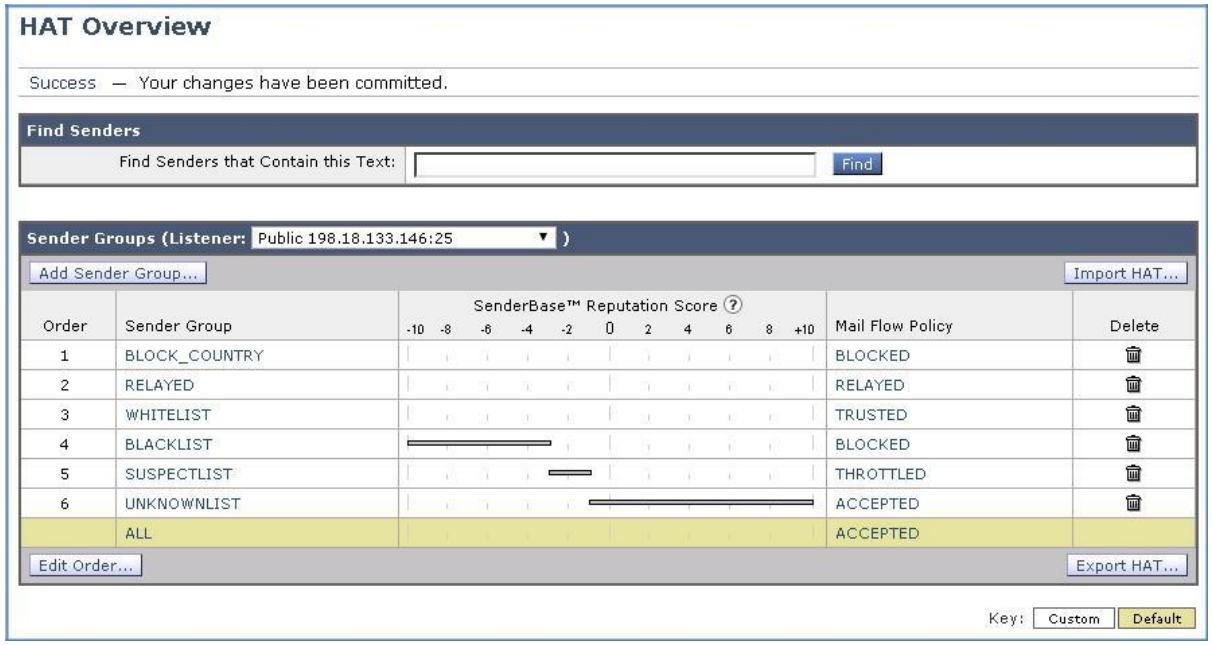


注：[地理位置情報（Geolocation）] ラジオ ボタンがない場合は、前の手順に戻って、[送信者グループ（Sender Groups）] からパブリック インターフェイスが選択されていることを確認してください。

10. ドロップダウンを使用して [ブラジル（Brazil）] を選択し、必要に応じてコメントを追加して、[送信（Submit）] ボタンをクリックします。

11. [ブラジル（Brazil）] が正常に追加されたことを確認してから [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

12. [HAT の概要（HAT Overview）] のリストの順序で、前の手順で作成した*送信者グループ*が一番上になっていることを確認します。



タスク：地理位置情報ベースのフィルタリングをテストする（推定所要時間：5 分）

全体の構成が完了していれば、社外ユーザ（接続が制限されるべき国からの接続をシミュレート）から Alan に宛てて電子メールを送信することにより、地理位置情報機能をテストできます。

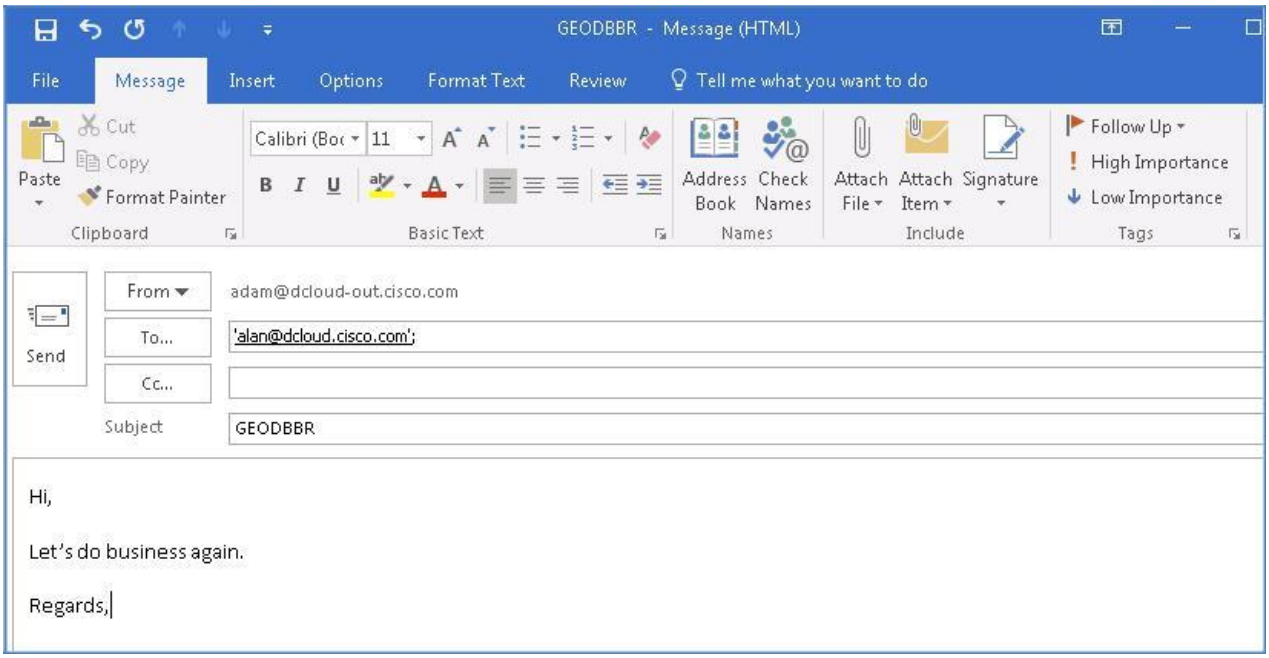
CLI セッションの開始

メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。

1. [モニタ（Monitor）] > [地理的区分（Geo Distribution）] に移動して、ブラジルからの接続がログに記録されていないことを確認します。いかなる種類の接続についても、この位置からは試みられたことがないかシミュレートされていないため、その国の統計情報はリストに示されません。
2. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。
   - [宛先（To）]：alan@dcloud.cisco.com
   - [件名（Subject）]：GEODBBR
   - [本文（Body）]：Hi Alan,（Alan 様）

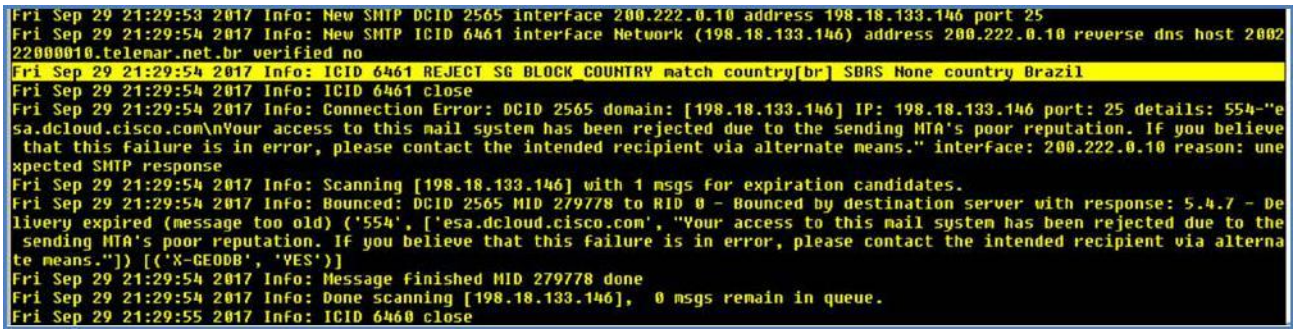
     弊社では、御社との取引を希望しております。（Our region would like to do business with your company.）

     Regards,（よろしくお願いします。）

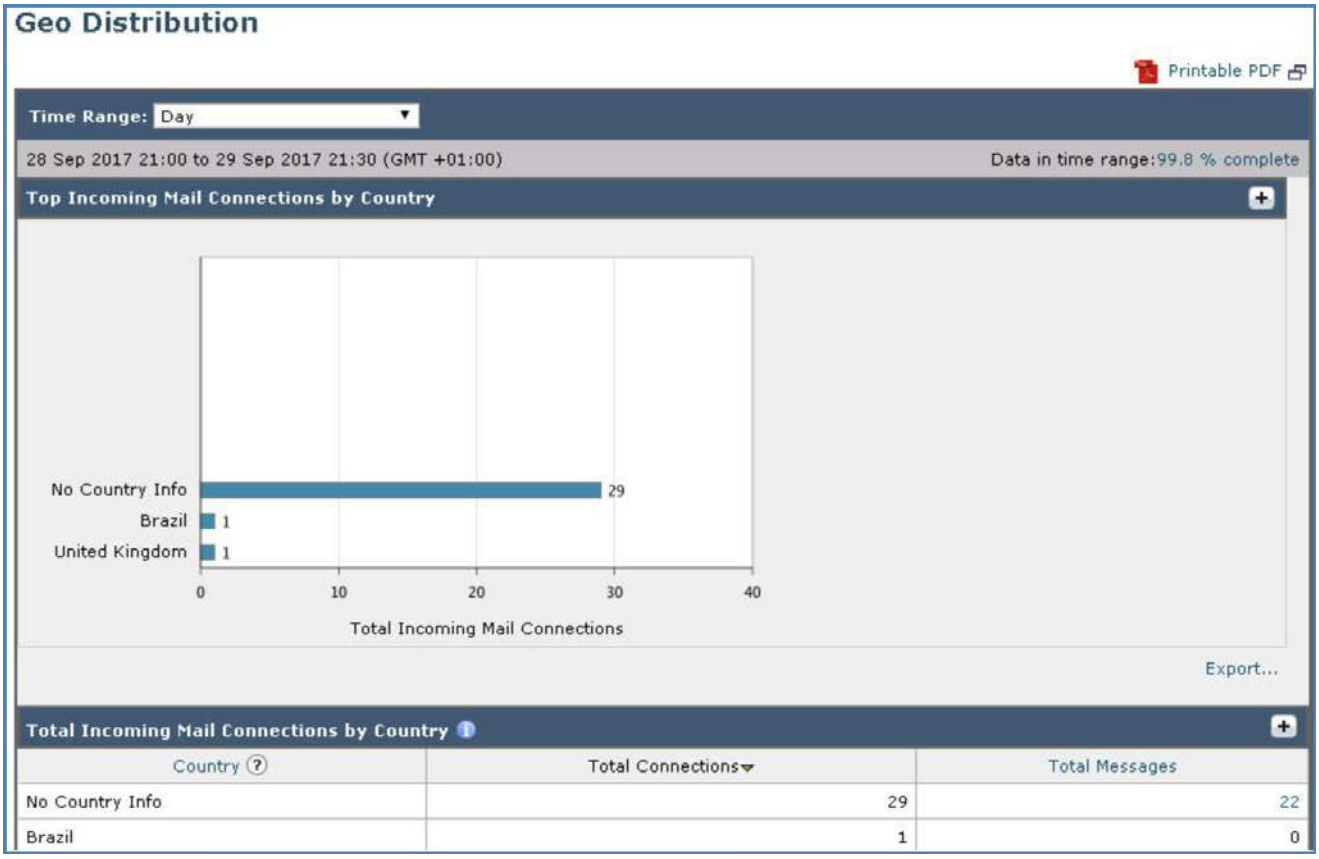


3. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

4. CLI セッションに戻り、ログをスクロールして、国が一致したためにその後に接続が拒否されたことを通知するログ エントリを探します。この時点で処理が停止するため、スパム対策エンジンやウイルス対策エンジンはこのメッセージに関して処理を実行する必要がなく、貴重な演算リソースを節約できます。



5. 最後に [モニタ（Monitor）] > [地理的区分（Geo Distribution）] に移動し、必要に応じて画面の表示を更新して、この時点では国の情報が追加されていることを確認します。ブラジルは [総接続数（Total Connections）] 列に示され、[総メッセージ数（Total Messages）] 列は値が 0 であることを確認してください。これは、地理位置情報機能によって接続レベルでブロックされており、それを超えてメッセージが処理されることがないためです。



シナリオ 7:　高度なマルウェア防御

使用例

最近、あるサードパーティ金融会社が、次世代データセンター機器に投資したいと考えている州内の企業向けに、利率を優遇したクレジットを提供するキャンペーンを開始しました。キャンペーンの電子メールは、過去 12 か月間の支払い総額が大きいエコパートナーすべてに送信されました。Voyage Corp もこの中に含まれています。マーケティング アシスタンスは、キャンペーン メールの 1 通を受信しますが、悪意のあるペイロードが含まれていることには気付きません。彼女の PC はそれに感染し、一時的に動作しなくなります。インストールされているウイルス対策ソリューションは適切に設定されており、シグネチャの更新もソフトウェア開発者の推奨に従って行われていました。防御層は従来型とは言え強固でしたが、脅威のすり抜けを許してしまいます。

セキュリティ制御

ほとんどのウイルス対策ベンダーはシグネチャベースの検出のみを実行するため、ウイルス対策ベンダーにまだ知られていない悪意のあるファイルは、対応できないソリューションによって簡単に見逃される可能性があります。高度な攻撃、さらには標的型の攻撃から効果的に保護するには、ポイント インタイムの検出と再解析による継続的な分析を組み合わせること、つまり AMP for Email を追加の防御層として機能させることを検討してください。最近の調査では、Cisco E メール セキュリティで AMP ファイル レピュテーション スキャンを有効にすると、電子メール トラフィックにおけるマルウェア全体の検出率が最大 50 % 向上することが判明しています。

目的

このシナリオでは、AMP のファイル レピュテーション機能とファイル解析機能を示します。ファイルのレピュテーションを確認した後、それをファイル解析のために Cisco AMP クラウドに送信して判定します。判定結果を得るためにファイルが送信されている間、受信者への電子メール メッセージは検疫エリアに保持されます。

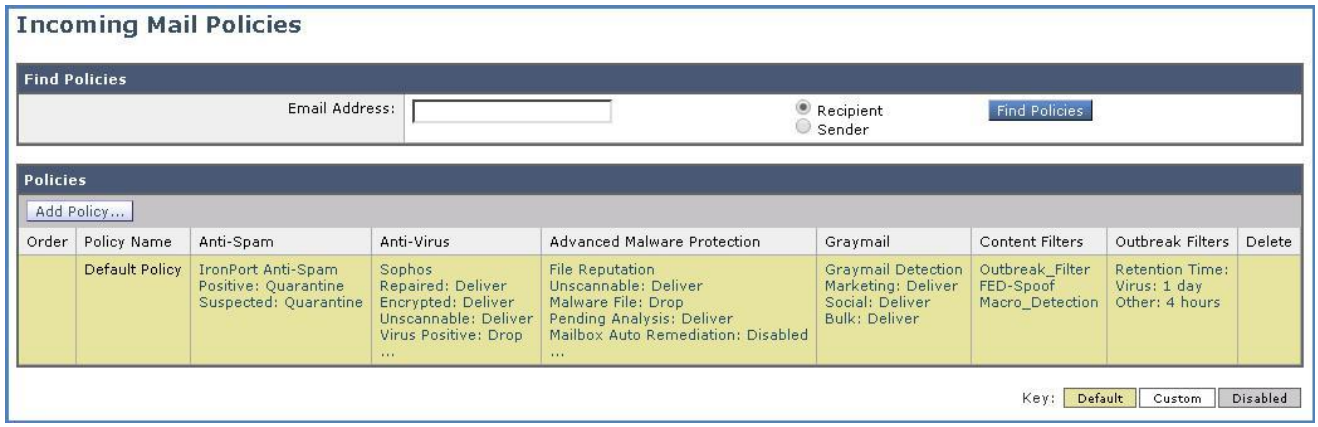
注: AMP の詳細については、「AMP on Cisco Email Security」を参照してください。

手順

タスク:AMP ポリシーを編集する(推定所要時間:1 分)

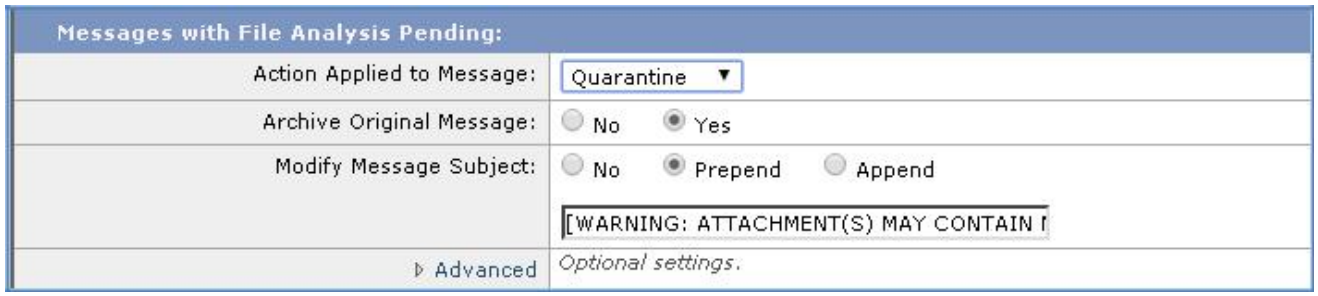
1. 最初にデフォルト ポリシーを編集します。Cisco AMP クラウドに分析目的で送信されたファイルが添付されていた元のメッセージに適用されるアクションを変更します。

2. ワークステーションから GUI にアクセスし、[メール ポリシー（Mail Policy）] > [受信メール ポリシー（Incoming Mail Policies）] に移動して、[デフォルト ポリシー（Default Policy）] の [高度なマルウェア防御（Advanced Malware Protection）] セクション内をクリックします。



3. [ファイル解析を有効にする（Enable File Analysis）] にチェックマークが付いていることを確認します。これにより、判定結果が未知の適格ファイルは、エキスパート分析および判定のために Cisco ThreatGrid サンドボックスにリダイレクトされます。

4. [ファイル分析が保留中のメッセージ（Message with File Analysis Pending）] セクションまでスクロールし、[メッセージに適用されるアクション（Action Applied to Message）] を [検疫（Quarantine）] に変更します。

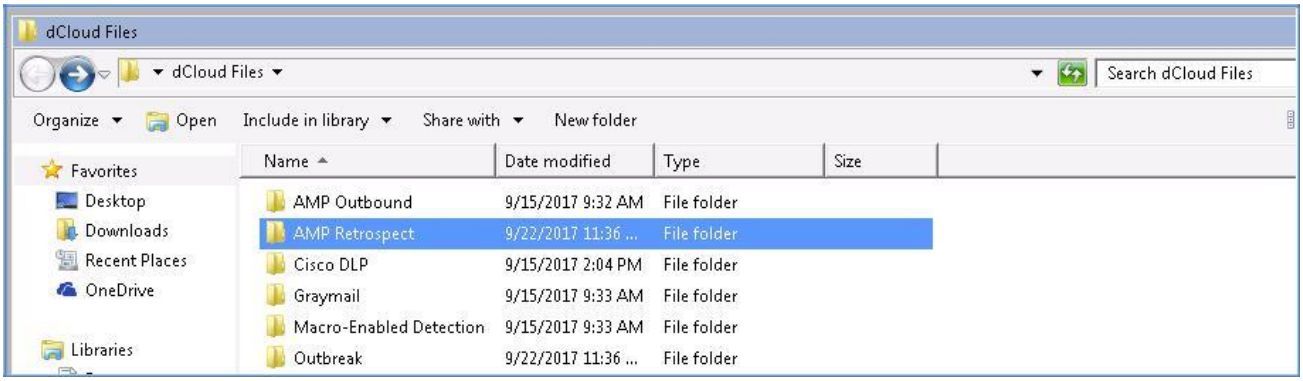


5. [送信（Submit）] をクリックしてアクションを適用し、変更内容を確定します。

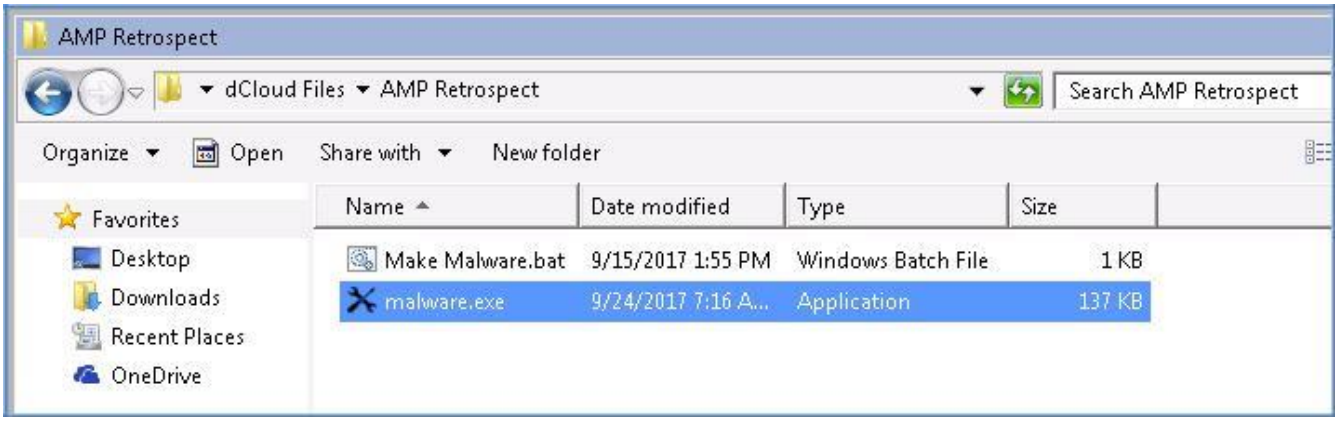
タスク：悪意のあるファイルを作成する（推定所要時間：1 分）

このタイプの分析をシミュレートするためにクリーン ファイルを生成し、組織に着信するメール内で使用します。このファイル自体には悪影響を与える機能はありませんが、Cisco AMP ファイルは、この悪意のあるテスト ファイルを処理し、悪意のあるペイロードを含んでいる場合と同じアクションを実行します。

1. ワークステーションのデスクトップに移動し、「dCloud Files」というフォルダを見つけて開いた後、フォルダの中にある「AMP Retrospect」というサブフォルダを開きます。



2. Malware.bat ファイルをダブルクリックし、メッセージが表示されたら [実行（Run）] ボタンを押すことで確認して、そのファイルを開きます。正常に実行されると、malware.exe という 2 つ目のファイルが生成されます。



タスク：悪意のある可能性のあるファイルが添付されたメッセージを送信する（推定所要時間：1 分）

悪意のあるペイロードを含むファイルによってファイルが生成された時点で、生成されたファイルを添付ファイルとして Adam から Alan にメッセージを送信します。これは、AMP エンジンをトリガーして必要な判定結果を提供させるために十分なアクションです。

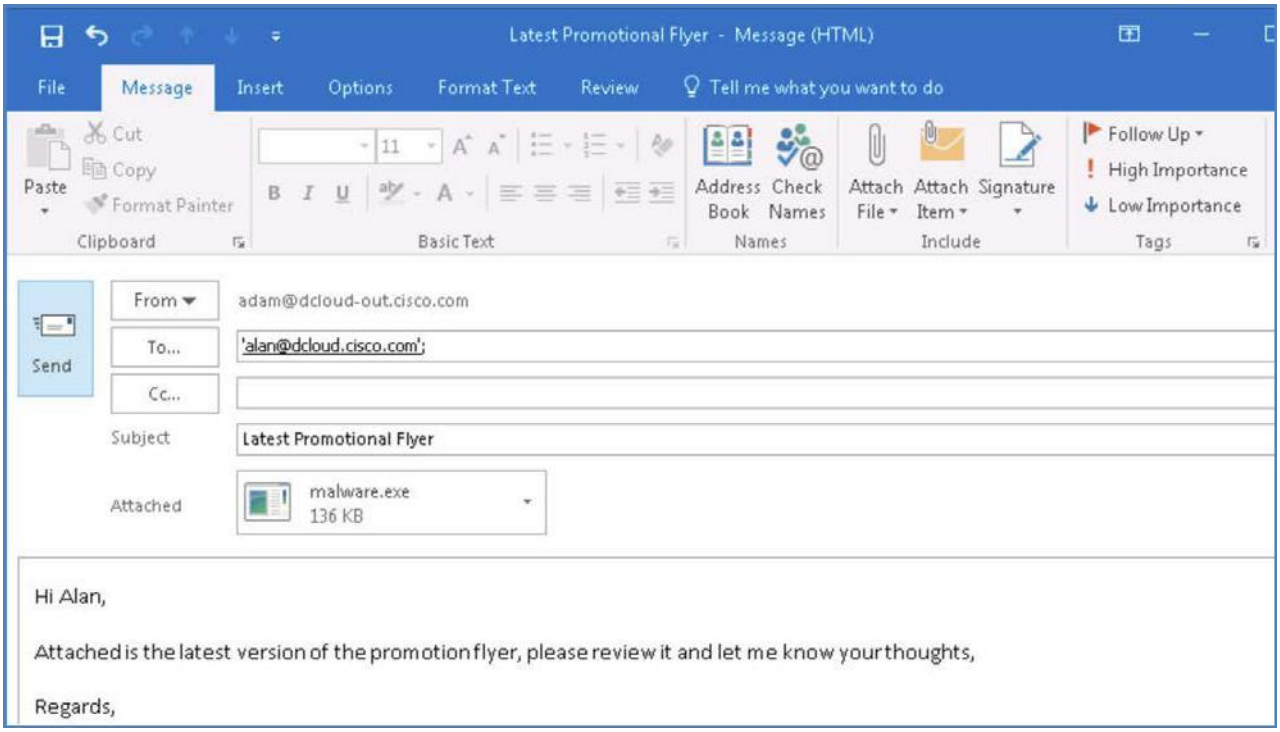
CLI セッションの開始

メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。

1. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。
   - [宛先（To）]：alan@dcloud.cisco.com
   - [件名（Subject）]：最新の販促チラシ（Latest Promotional Flyer）
   - [本文（Body）]：Hi Alan,（Alan 様）

     最新バージョンの販促チラシを添付しました。確認して、意見を聞かせてください。（Attached is the latest version of the promotional flyer, please review it and let me know your thoughts.）

     Regards,（よろしくお願いします。）
   - [添付ファイル（Attachment）]：前の手順で作成したファイル（Malware.exe ファイル）を添付します。

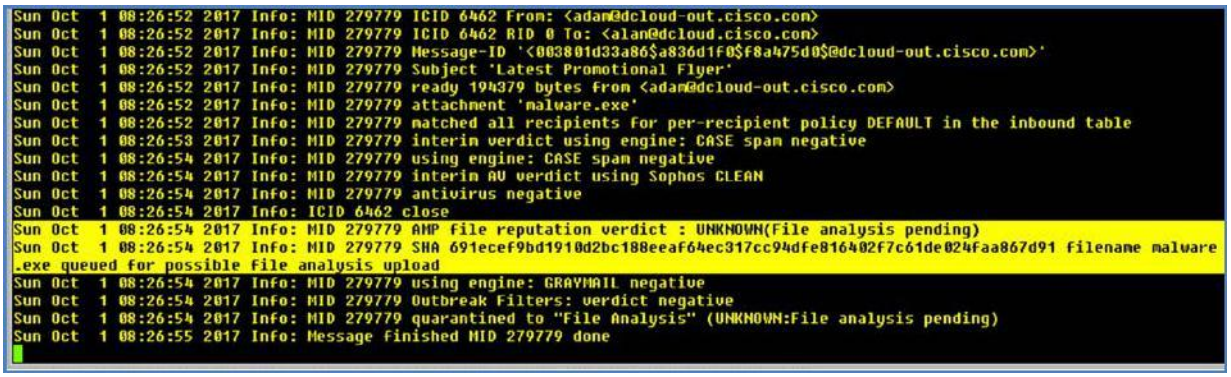


2. メッセージを送信します。Microsoft Outlook によって、安全ではないファイルに関する警告が表示されるので、[はい（Yes）] をクリックしてこの警告を無視します。
3. [すべてのフォルダを送受信（Send/Receive All Folders）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

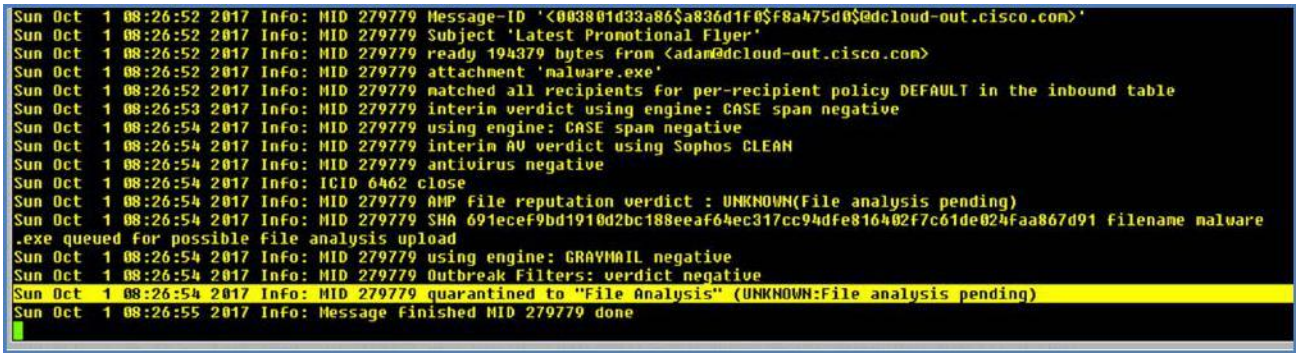
タスク：AMP をモニタする（推定所要時間：10 分）

このタスクでは、Cisco E メール セキュリティ ソリューションと、特に AMP エンジンによって、悪意のある可能性があるファイルがどのように処理されるのかが示されます。

1. CLI セッションに移動し、ログがスクロールするまで待ちます。新しいアクティビティによって画面の表示が更新されるまでにしばらく時間がかかる場合があります。ここで最初に注目すべき点は、スパム対策エンジンとウイルス対策エンジンが判定を下すと何が起こるのかです。
2. 次のログの強調表示された行およびそれ以前の行は、ファイル レピュテーションの判定を示しています。判定が UNKNOWN（未知）であるため、ファイルはさらなる分析のために送信されます。またこのとき、SHA256 が割り当てられていることにも注意してください。
3. MID を書き留めます。



4. 次に注目すべき点は、最終的な判定が返される間にファイルに何が起こるのかです。



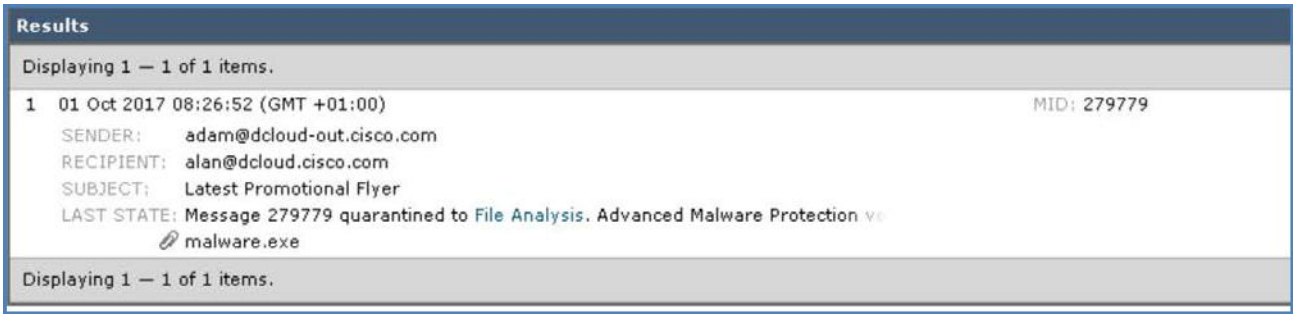
注：判定が返されるまでに数分かかる場合があります。CLI ウィンドウを実行したまま次の手順に進むか、休憩を取ってください。

注：AMP SHA の詳細については、「SHA-2」を参照してください。

5. [モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク検疫（Policy, Virus and Outbreak Quarantines）] に移動します。この時点では AMP ファイル レピュテーション サービスから判定結果が返されるまで、設定済みの AMP ポリシーに従ってメッセージが検疫されます。

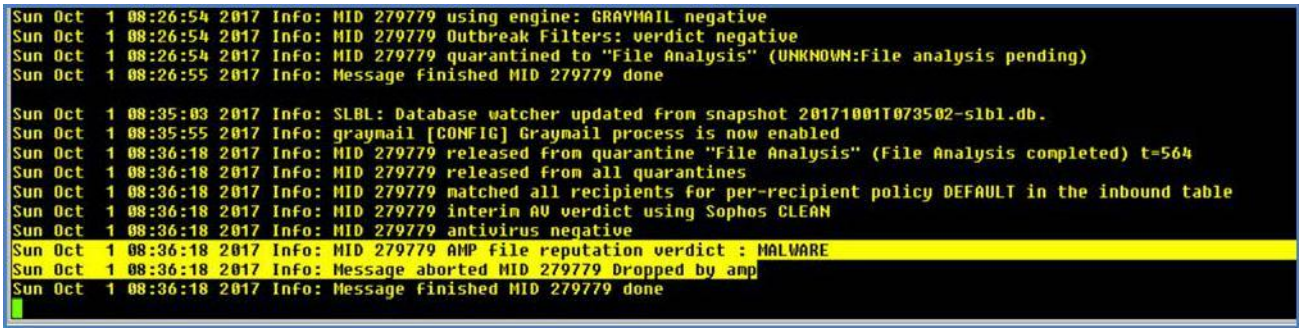
6. [モニタ（Monitor）] > [AMP ファイル分析（AMP File Analysis）] に移動して、[中間判定（Interim Disposition）] に示されているように、ファイルがまだ分析されていないことに注意してください。

7. [詳細（Details）] をクリックしてメッセージ トラッキングを起動し、[結果（Results）] セクションまでスクロールするとメッセージが一覧表示されます。やはり MID が、以前に CLI 内で確認したものと一致することを確認してください。

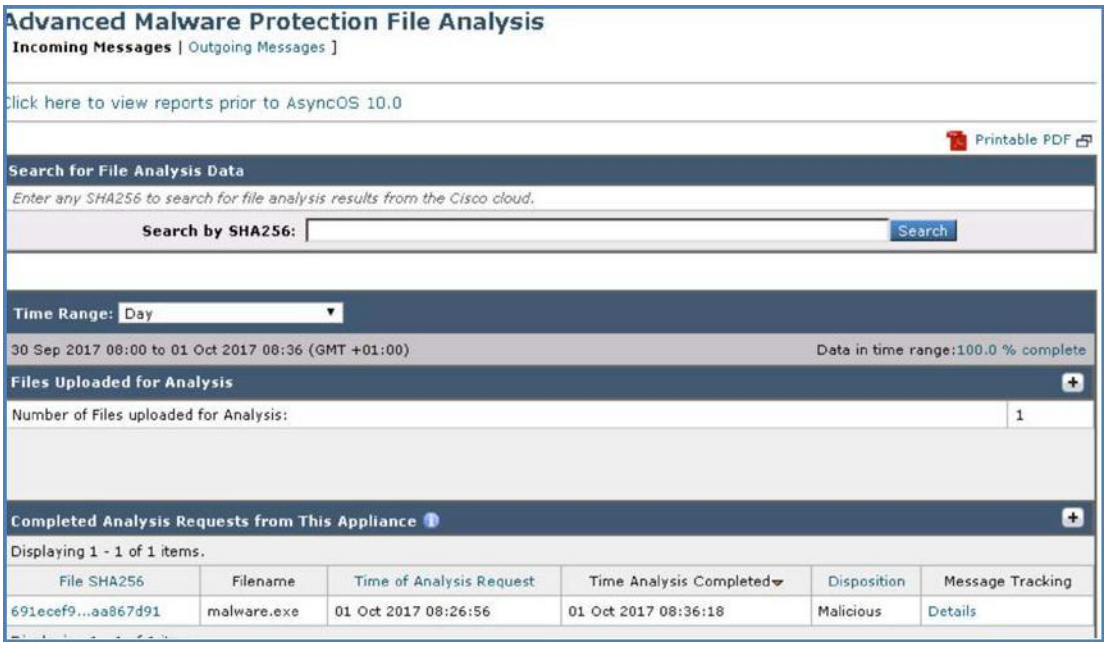


注：AMP の詳細については、「Advanced Malware Protection (AMP)」を参照してください。

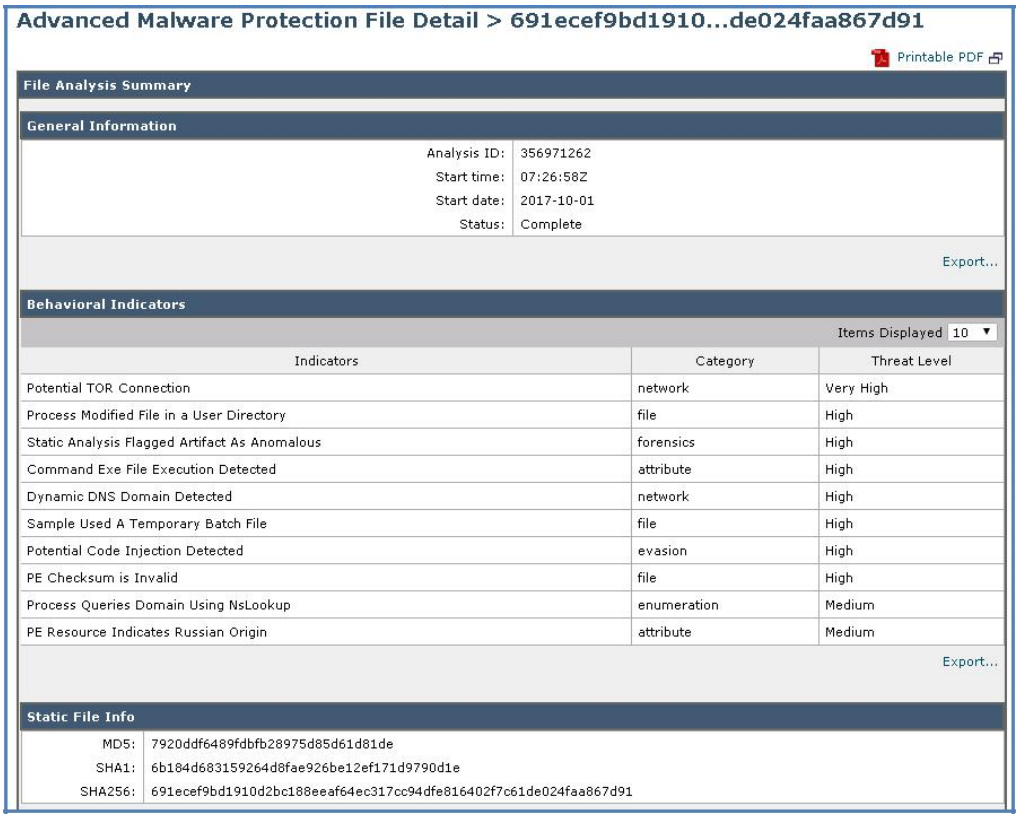
8. CLI セッションに戻り数分待つと、判定が返されます。分析のためにファイルが送信されてから判定が返され、最後に最終アクションが実行されるまでの時間を書き留めます。



9. GUI に戻り、[モニタ（Monitor）] > [AMP ファイル分析（AMP File analysis）] に移動します。この時点では、ここにも判定が表示されます。



10. [SHA] をクリックすると、認識された脅威の詳細情報とファイルに割り当てられているさまざまな脅威レベルが表示されます。



Advanced Malware Protection File Detail > 691ecef9bd1910...de024faa867d91

Printable PDF

File Analysis Summary

General Information

Analysis ID:	356971262
Start time:	07:26:58Z
Start date:	2017-10-01
Status:	Complete

Export...

Behavioral Indicators

Items Displayed 10

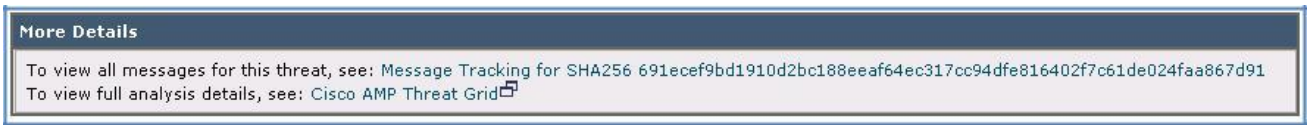
Indicators	Category	Threat Level
Potential TOR Connection	network	Very High
Process Modified File in a User Directory	file	High
Static Analysis Flagged Artifact As Anomalous	forensics	High
Command Exe File Execution Detected	attribute	High
Dynamic DNS Domain Detected	network	High
Sample Used A Temporary Batch File	file	High
Potential Code Injection Detected	evasion	High
PE Checksum is Invalid	file	High
Process Queries Domain Using NsLookup	enumeration	Medium
PE Resource Indicates Russian Origin	attribute	Medium

Export...

Static File Info

MD5:	7920ddf6489fdbfb28975d85d61d81de
SHA1:	6b184d683159264d8fae926be12ef171d9790d1e
SHA256:	691ecef9bd1910d2bc188eeaf64ec317cc94dfe816402f7c61de024faa867d91

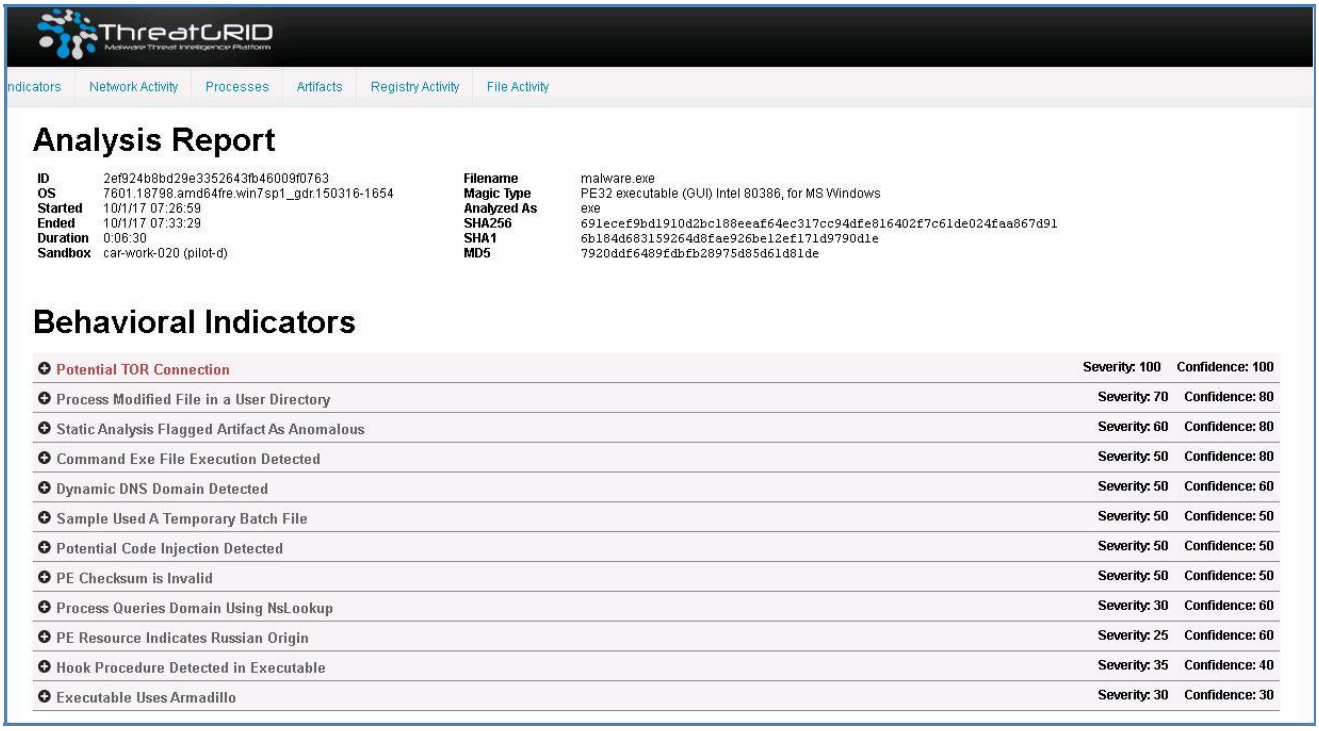
11. 最後に **Cisco AMP Threat Grid** へのリンクをクリックして、完全な分析の詳細情報を入手します。



More Details

To view all messages for this threat, see: Message Tracking for SHA256 691ecef9bd1910d2bc188eeaf64ec317cc94dfe816402f7c61de024faa867d91
To view full analysis details, see: Cisco AMP Threat Grid

12. これによって Cisco AMP Threat Grid ポータルにリダイレクトされ、このファイルが悪意のあるものである原因の詳細な分析を確認できます。



13. Threat Grid のウィンドウを閉じて [モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク検疫（Policy, Virus and Outbreak Quarantines）] に移動し、この時点でキューが空になっていることを確認します。これは、ファイルに関して悪意があるという判定が返され、検疫エリアから削除されたためです。

シナリオ 8:　グレイメールの検出

使用例

Voyage Corp では、Cisco E メール セキュリティ ソリューションに投資したことによってスパムとして分類されるメッセージの量が著しく減少し、最近のユーザ満足度調査で大半のユーザにより高い満足度が報告されています。複数のセキュリティ エンジンの実装後、電子メール メッセージ内の脅威の制御が大幅に改善され、報告されるインシデントも急減しました。

しかし、サインアップした企業 Web サイトからメッセージを受け取っているユーザの一部が不満を持つようになりました。たとえば、ある企業顧客担当マネージャには Netflix から電子メールが定期的に届いています。当初は望んだものの、現在では完全に受け取らないか、少なくとも受信トレイ内で適切に分類されるようにし、常に大量に届く電子メールを容易に整理できるようにしたいと考えています。

セキュリティ制御

「グレイメール」メッセージとは、ニュースレター、メーリング リスト購読、ソーシャル メディア通知といった、スパムの定義に適合しないメッセージです。これらのメッセージは、ある時点では有用であったものの、その後にエンドユーザがメッセージの受信を望まなくなるまで価値が低下しています。

グレイメールとスパムの違いですが、スパムはエンドユーザがサインアップしていないメッセージであるのに対して、グレイメールはどこかの時点で自らサインアップしています（エンドユーザがニュース レター配信に登録した、会議で連絡先の詳細情報を提供した、など）。

目的

このシナリオでは、Cisco E メール セキュリティ ソリューションによってグレイメールがどのように分類および処理されるかを、シミュレーションを通じて示します。

注: E メール セキュリティ アプライアンスのグレイメール管理ソリューションは、統合グレイメール スキャン エンジンとクラウドベースの購読解除サービスの 2 つのコンポーネントで構成されます。グレイメール スキャン エンジンはベース オペレーティング システムの一部ですが、購読解約サービスを使用するには追加のライセンスが必要です。

手順

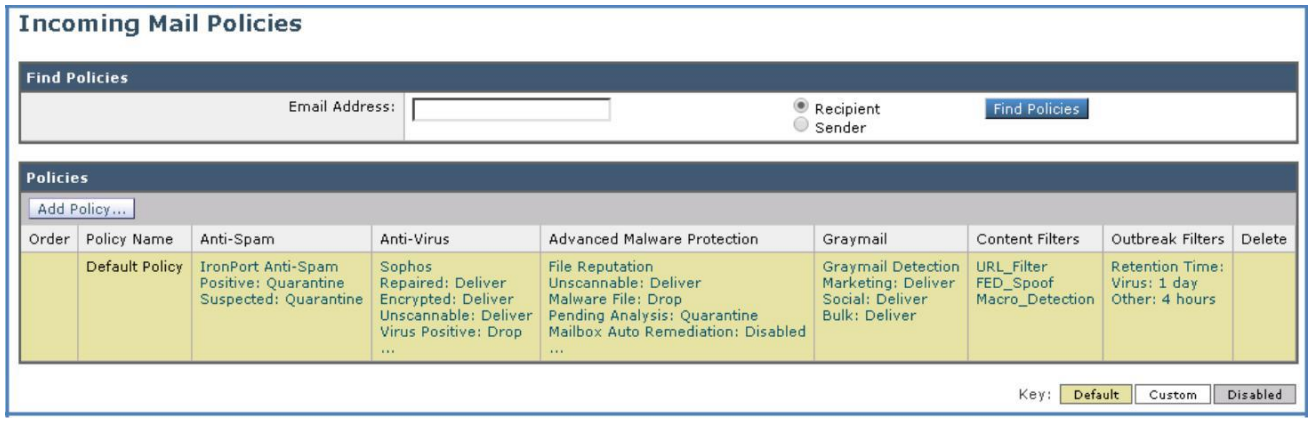
タスク: グレイメールの分類をカスタマイズする（推定所要時間: 2 分）

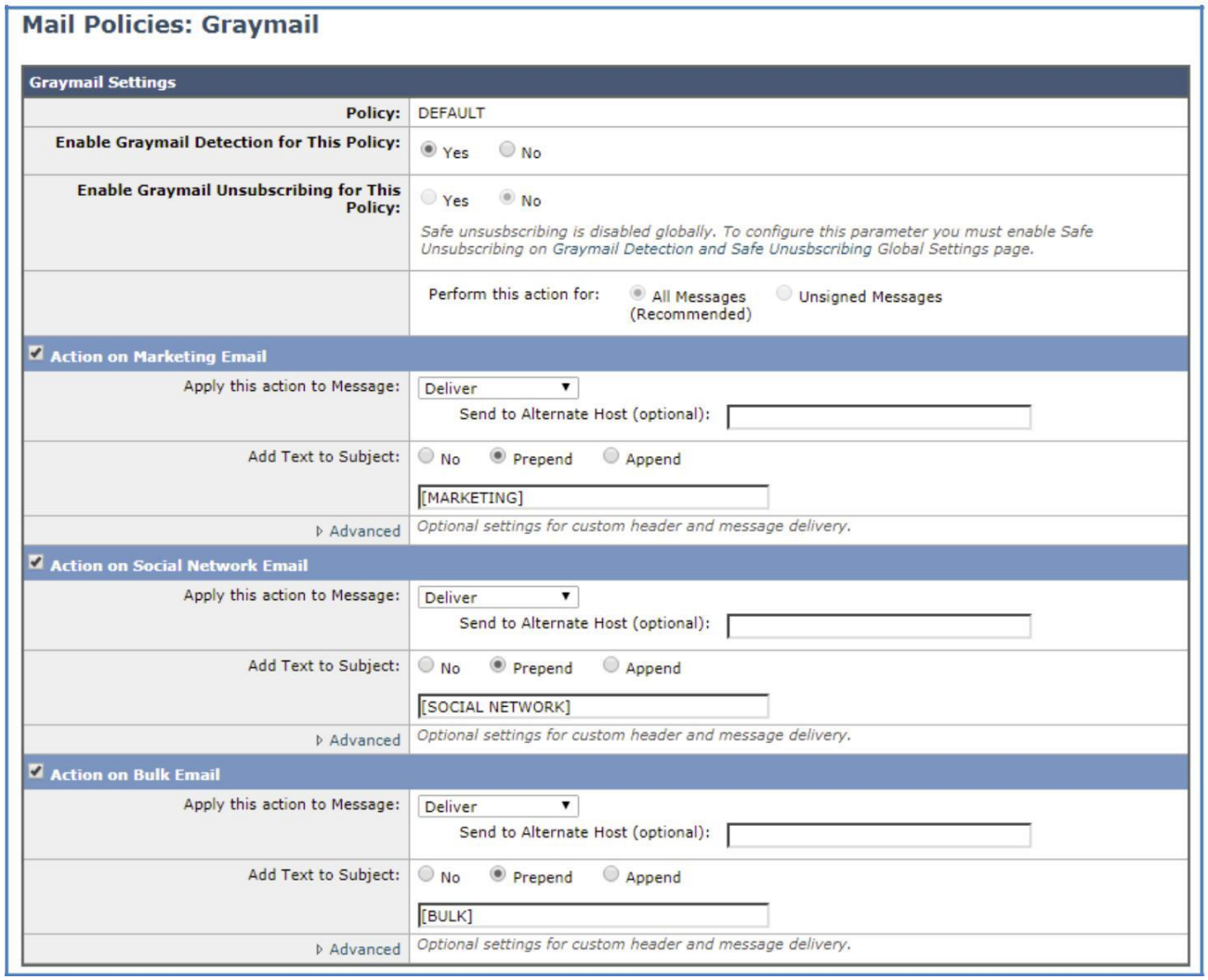
グレイメール エンジンにより、各グレイメールが次のカテゴリのいずれかに分類されます。

- **マーケティング電子メール:** 専門マーケティング グループから送信される広告メッセージ。
- **ソーシャル ネットワーク電子メール:** ソーシャル ネットワーク、出会い系 Web サイト、フォーラムなどから送信される通知メッセージ。
- **バルク電子メール:** 認知度の低いマーケティング グループから送信される広告メッセージ（例: テクノロジー メディア会社からのニュースレターなど）。

このタスクではこれらを確認し、わずかに変更を加えます。

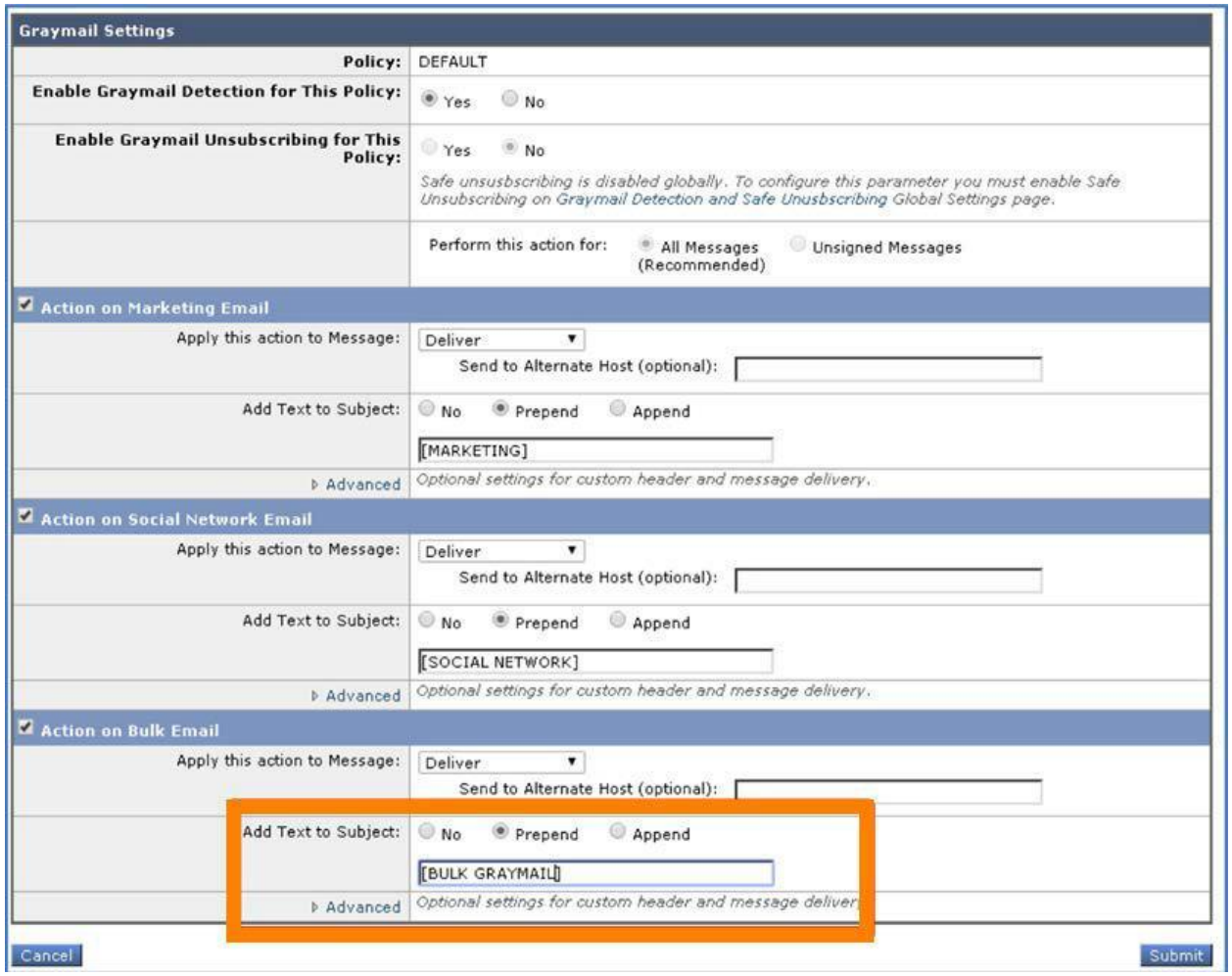
1. ワークステーションから GUI にアクセスし [メール ポリシー（Mail Policy）] > [受信メール ポリシー（Incoming Mail Policies）] に移動して、[デフォルト ポリシー（Default Policy）] の [グレイメール（Graymail）] ボックス内をクリックすることにより、[グレイメール設定（Graymail Settings）] を起動します。



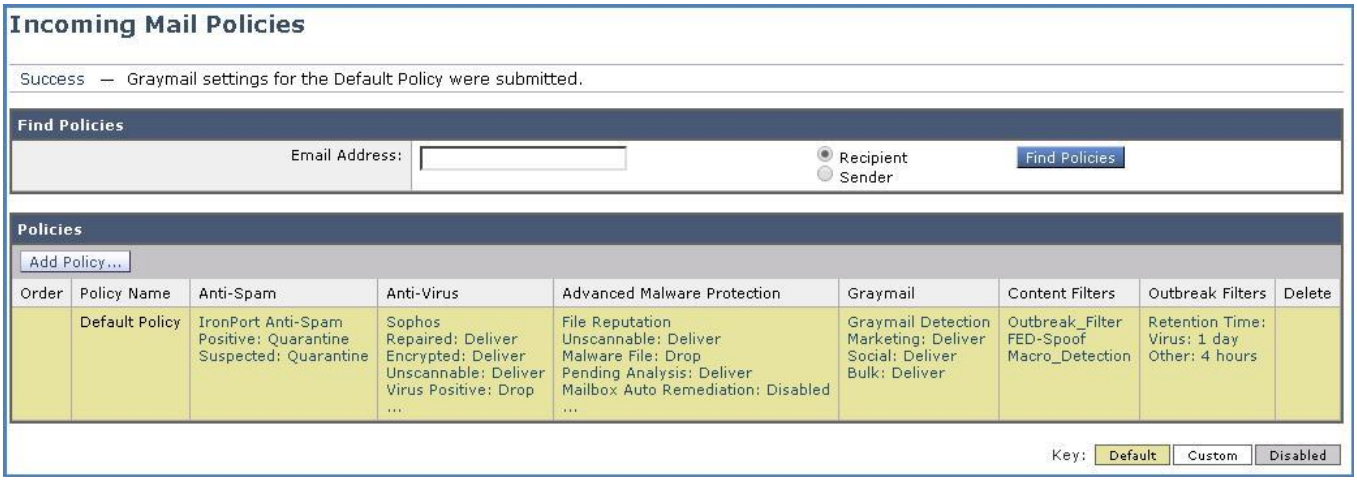


2. [バルク電子メールに関するアクション（Action for Bulk Email）] で、[件名へのテキストの追加（Add Text to Subject）] のデフォルト設定を編集して、別のテキストが表示されるようにします。

3. デフォルトのテキストを「**BULK GRAYMAIL**」（バルク グレイメール）に変更します。



4. [送信（Submit）] をクリックして変更を適用します。



5. 完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

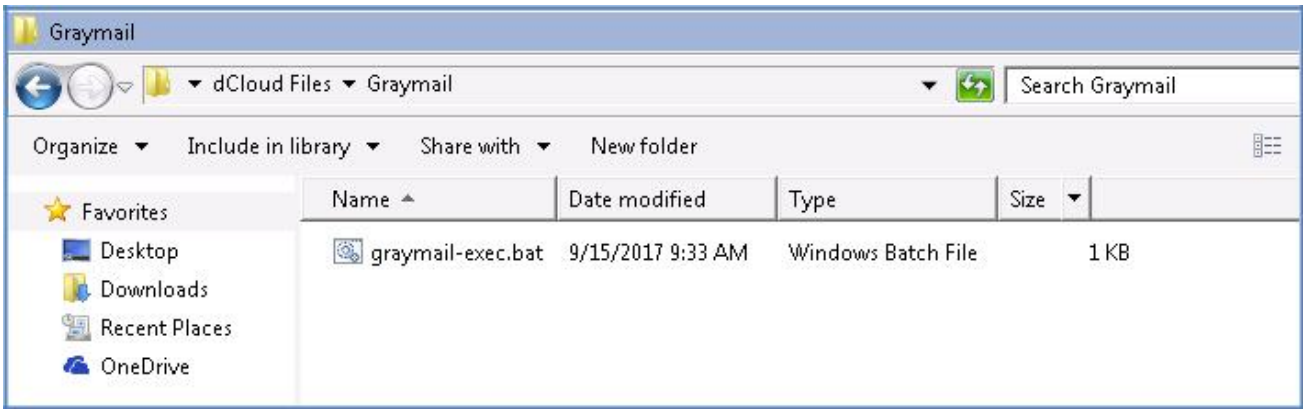
タスク：グレイメールをシミュレートする（推定所要時間：5 分）

グレイメール エンジンの効果を確認するために、このタスクでは、エンジンによってバルク電子メールに分類される Netflix メッセージの送信と処理をシミュレートします。

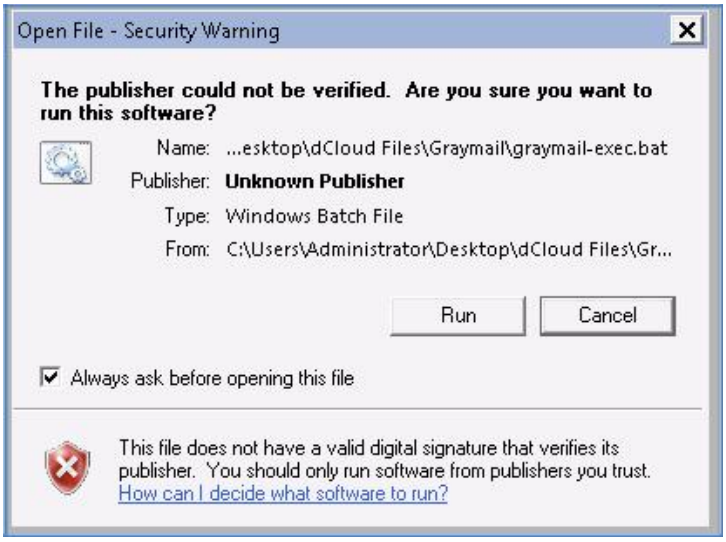
CLI セッションの開始

メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。

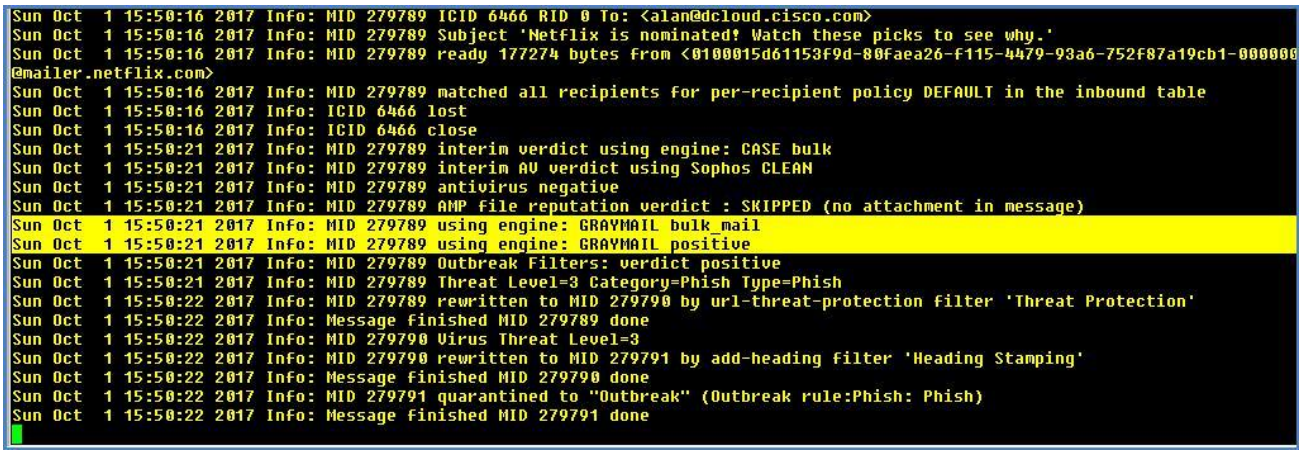
1. デスクトップ上の dCloud File フォルダ内の Graymail サブフォルダを開き、graymail-exec.bat ファイルがあることを確認します。



2. そのファイルをダブルクリックして実行します。この環境では安全であるため、セキュリティ警告メッセージに同意します。



3. CLI に移動し、グレイメール エンジンがこのタイプのメッセージをどのように分類するのかを確認します。



4. また、アウトブレイク フィルタ エンジンが判定を出し、メッセージ対するアクション（メッセージを検疫エリアに送信）を実行したことも確認してください。

```
Sun Oct  1 15:50:16 2017 Info: MID 279789 ICID 6466 RID 0 To: <alan@dcloud.cisco.com>
Sun Oct  1 15:50:16 2017 Info: MID 279789 Subject 'Netflix is nominated! Watch these picks to see why.'
Sun Oct  1 15:50:16 2017 Info: MID 279789 ready 177274 bytes from <0100015d61153f9d-80faea26-f115-4479-93a6-752f87a19cb1-000000
@mailer.netflix.com>
Sun Oct  1 15:50:16 2017 Info: MID 279789 matched all recipients for per-recipient policy DEFAULT in the inbound table
Sun Oct  1 15:50:16 2017 Info: ICID 6466 lost
Sun Oct  1 15:50:16 2017 Info: ICID 6466 close
Sun Oct  1 15:50:21 2017 Info: MID 279789 interim verdict using engine: CASE bulk
Sun Oct  1 15:50:21 2017 Info: MID 279789 interim AV verdict using Sophos CLEAN
Sun Oct  1 15:50:21 2017 Info: MID 279789 antivirus negative
Sun Oct  1 15:50:21 2017 Info: MID 279789 AMP file reputation verdict : SKIPPED (no attachment in message)
Sun Oct  1 15:50:21 2017 Info: MID 279789 using engine: GRAYMAIL bulk_mail
Sun Oct  1 15:50:21 2017 Info: MID 279789 using engine: GRAYMAIL positive
Sun Oct  1 15:50:21 2017 Info: MID 279789 Outbreak Filters: verdict positive
Sun Oct  1 15:50:21 2017 Info: MID 279789 Threat Level=3 Category=Phish Type=Phish
Sun Oct  1 15:50:22 2017 Info: MID 279789 rewritten to MID 279790 by url-threat-protection filter 'Threat Protection'
Sun Oct  1 15:50:22 2017 Info: Message finished MID 279789 done
Sun Oct  1 15:50:22 2017 Info: MID 279790 Virus Threat Level=3
Sun Oct  1 15:50:22 2017 Info: MID 279790 rewritten to MID 279791 by add-heading filter 'Heading Stamping'
Sun Oct  1 15:50:22 2017 Info: Message finished MID 279790 done
Sun Oct  1 15:50:22 2017 Info: MID 279791 quarantined to "Outbreak" (Outbreak rule:Phish: Phish)
Sun Oct  1 15:50:22 2017 Info: Message finished MID 279791 done
```

5. [モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク検疫（Policy, Virus and Outbreak Quarantines）] に移動し、この時点でキューが空になっていることを確認します。これは、ファイルに関して悪意があるという判定が返され、検疫エリアから削除されたためです。

Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines

Add Policy Quarantine... | Search Across Quarantines

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
DLP Violations	Policy	0	Retain 7 days then Release	29 Sep 2017 17:21 (GMT +01:00)	0	🗑
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	01 Oct 2017 08:26 (GMT +01:00)	0	
Outbreak [Manage by Rule Summary]	Outbreak	1	Retention Varies Action: Release	01 Oct 2017 15:50 (GMT +01:00)	236.8K	
Policy	Policy	0	Retain 10 days then Delete	13 Sep 2017 14:23 (GMT +01:00)	0	🗑
Unclassified	Unclassified	0	Retain 30 days then Release	N/A	0	
Virus	Antivirus	0	Retain 30 days then Delete	N/A	0	

Available space for Policy, Virus, Antimalware & Outbreak quarantines is 3G.

6. [メッセージ（Messages）] 列の下の数字をクリックしてメッセージを表示し、メッセージの横にチェックマークを付け、[解放（Release）] ボタンを押してファイルを転送します。

Messages in Quarantine: "Outbreak"

Messages in Quarantine: "Outbreak"

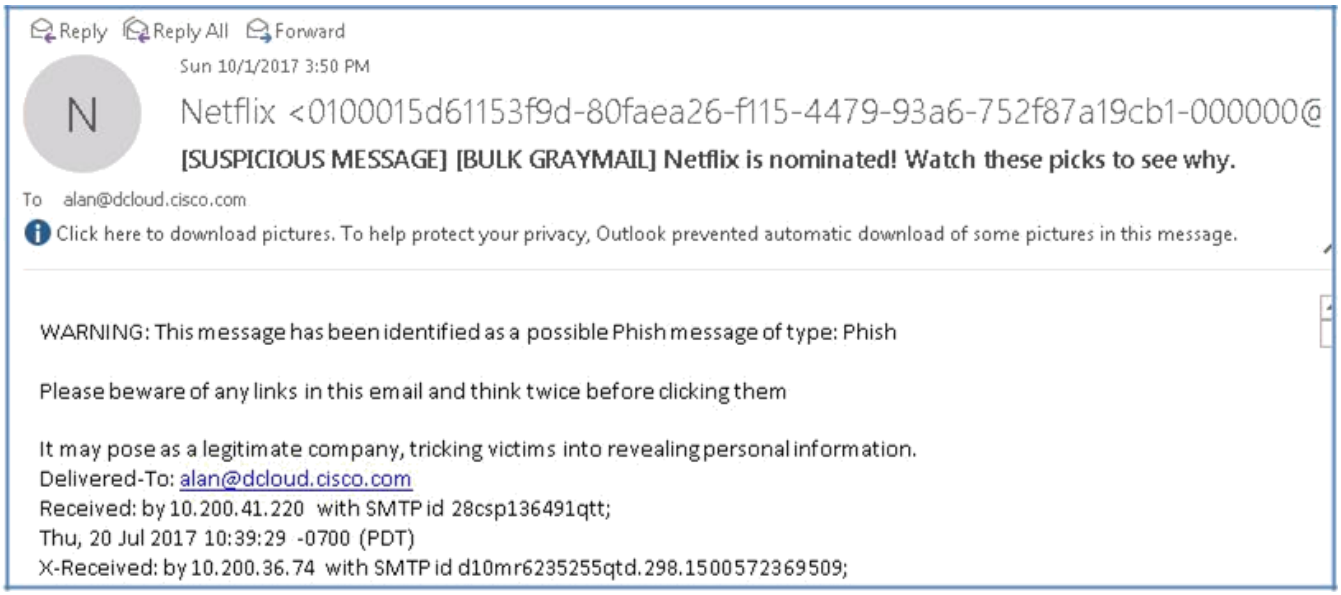
View: Standard | by Rule Summary

Action on selected items on page ▼ | Release | Delete | More Actions... ▼

Sender	Recipient	Subject	Received ▼	Scheduled Exit	Size
☑ 0100015d61153f9d-80fae	alan@dcloud.cisco.com	[SUSPICIOUS MESSAGE] [BULK C	01 Oct 2017 15:50 (GMT +01:00)	01 Oct 2017 16:40 (GMT +01:00)	236.8K

< Back to Quarantine List

7. デスクトップから Outlook クライアントに戻り、メールボックスを同期させます。この時点では、Netflix からのメッセージが Alan の受信トレイに表示されます。前のタスクに従って件名ヘッダーが変更されていることに注意してください。



注:この機能の第 2 の部分は購読解約です。この機能により、エンドユーザは購読解約サービスを使用して不要なメッセージの購読を容易に解除できます。これらの機能の詳細については、「Graymail and Safe Unsubscribe」を参照してください。

シナリオ 9:　画像分析

使用例

Voyage Corp では、地元のカレッジからのインターン生を事務所で定期的に受け入れ、学生が卒業前に貴重な就労経験を得られるよう支援しています。その見返りとして、採用プロセスを経ることなく臨時労力を得ています。インターン期間は人事部とカレッジ間の合意に基づいて、1 ～ 4 週間の範囲で設定されます。

最近、インターン生を新たに受け入れましたが、実習期間は 1 週間だけで、電子メールや Web システムの正しい使用方法や注意について社内で決められたトレーニングを受ける時間がほとんどありませんでした。そうした中でインターン生が受け取ったものは、職場には不適切であろうコンテンツが含まれる電子メールでした。その結果、インターン生とその同僚は不必要に恥ずかしい思いをすることになりました。

セキュリティ制御

メッセージによっては画像を含むため、それらのコンテンツをスキャンして適切性を判断する必要が生じます。画像分析エンジンを活用すれば、電子メール内の不適切なコンテンツを検出できます。画像分析は、ウイルス対策やスパム対策のスキャン エンジンを補完ないし代用できません。その目的は、電子メールに含まれる不適切なコンテンツを検出しポリシーを適用することにあります。画像分析スキャン エンジンを使用すれば、電子メールを分析して検疫し、傾向を検出することによって、より適切なポリシーを適用しエンドユーザを教育できます。

目的

このシナリオでは、Cisco E メール セキュリティ ソリューションの画像分析エンジンによって電子メール本文内の不適切なコンテンツがどのように識別され、企業ポリシーが定めたアクションがどのように実行されるのかを示します。

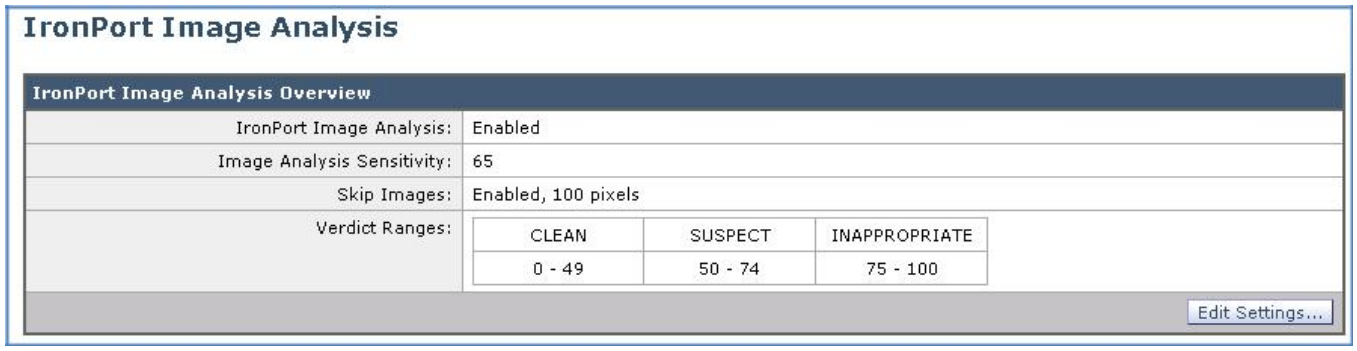
注: 画像分析の利点の詳細については、「画像分析」を参照してください。

手順

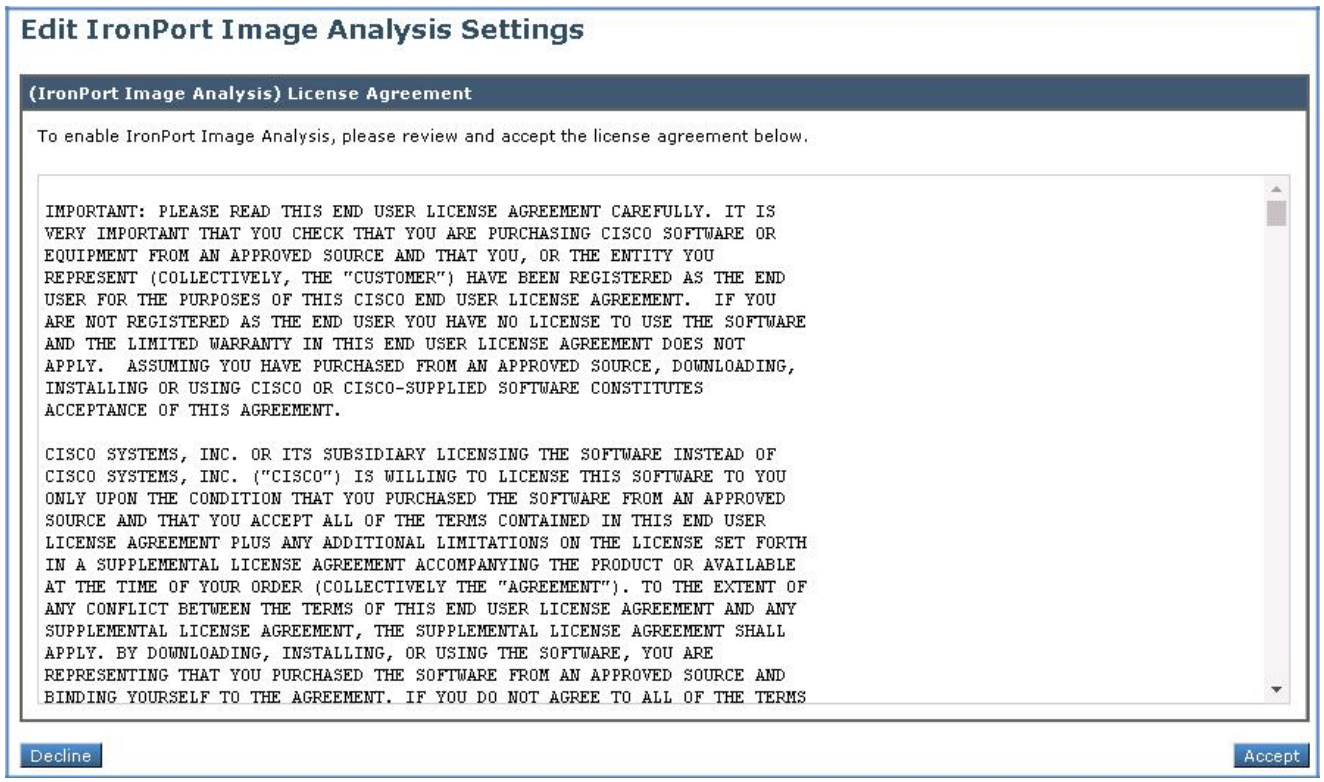
タスク:画像分析機能を有効にする(推定所要時間:5 分)

画像分析機能は追加ライセンスで使用でき、実働環境の要件に合わせて調整できます。

1. [セキュリティ サービス(Security Services)] > [IronPort 画像分析(IronPort Image Analysis)] に移動し、表示される画面で [設定の編集(Edit Settings)] をクリックします。



2. ライセンス契約を確認し、[同意する(Accept)] をクリックします。

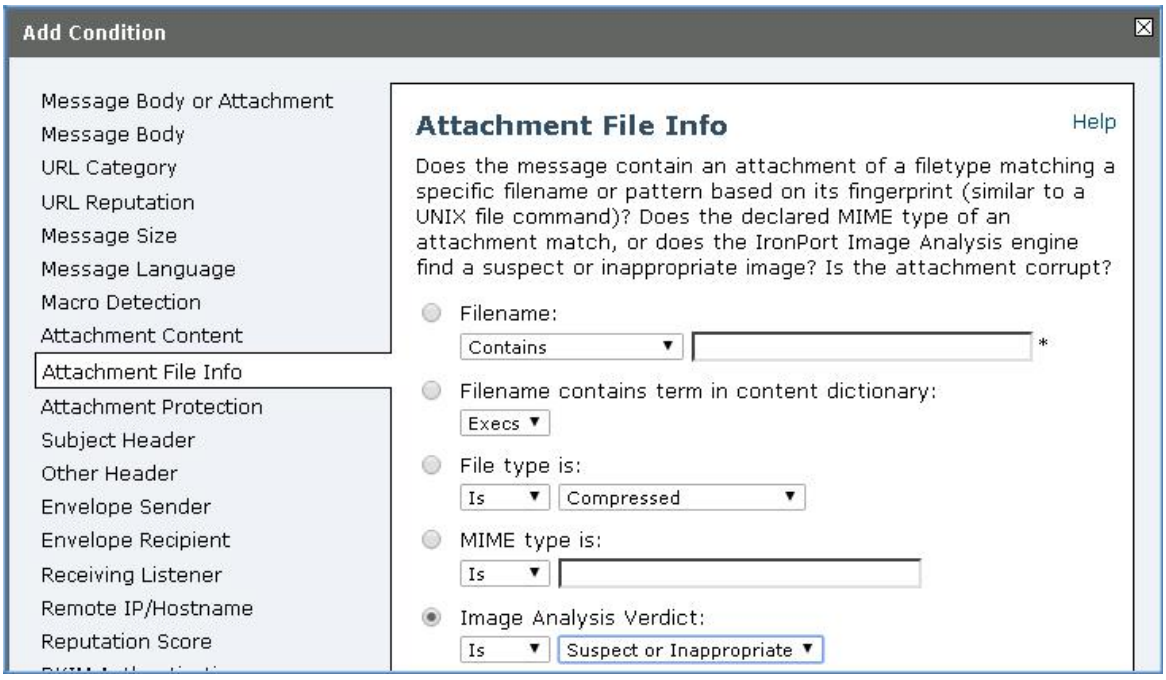


3. 同意すると、この機能をコンテンツ フィルタまたはメッセージ フィルタとともに使用できるようになったことを通知する確認メッセージが表示されます。

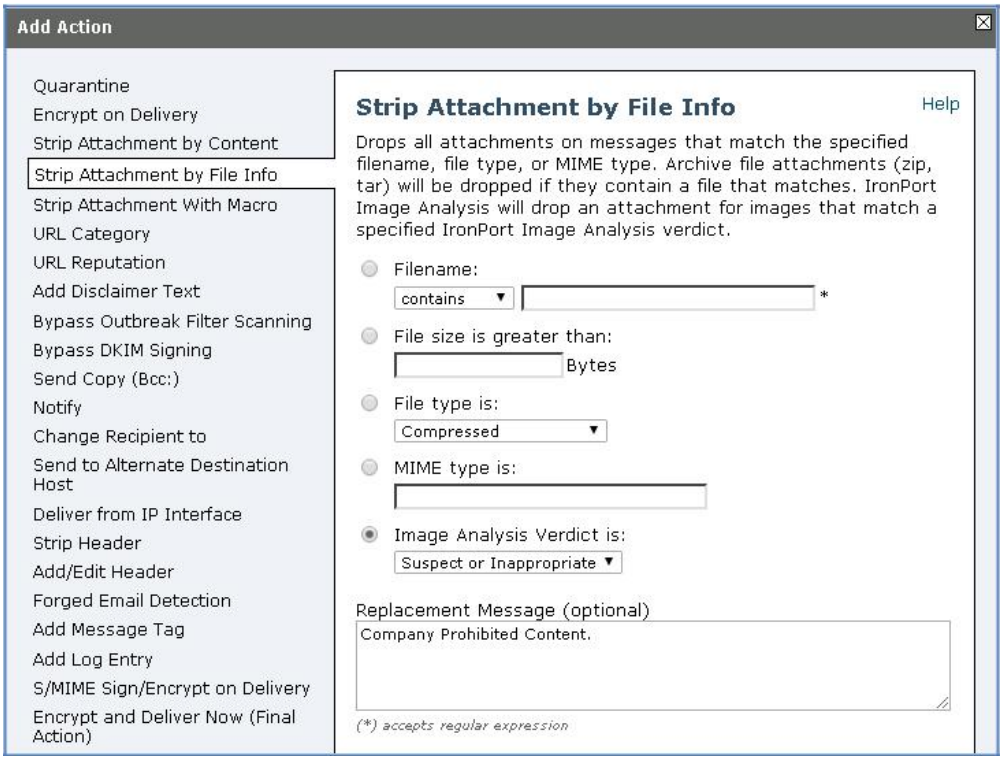
タスク:コンテンツ フィルタを設定する(推定所要時間:3 分)

このタスクでは、電子メール メッセージに含まれる不適切なコンテンツを識別し、添付ファイルを削除するアクションを適用してから、このアクションが実行された理由を受信者に通知する新しいコンテンツ フィルタを作成します。

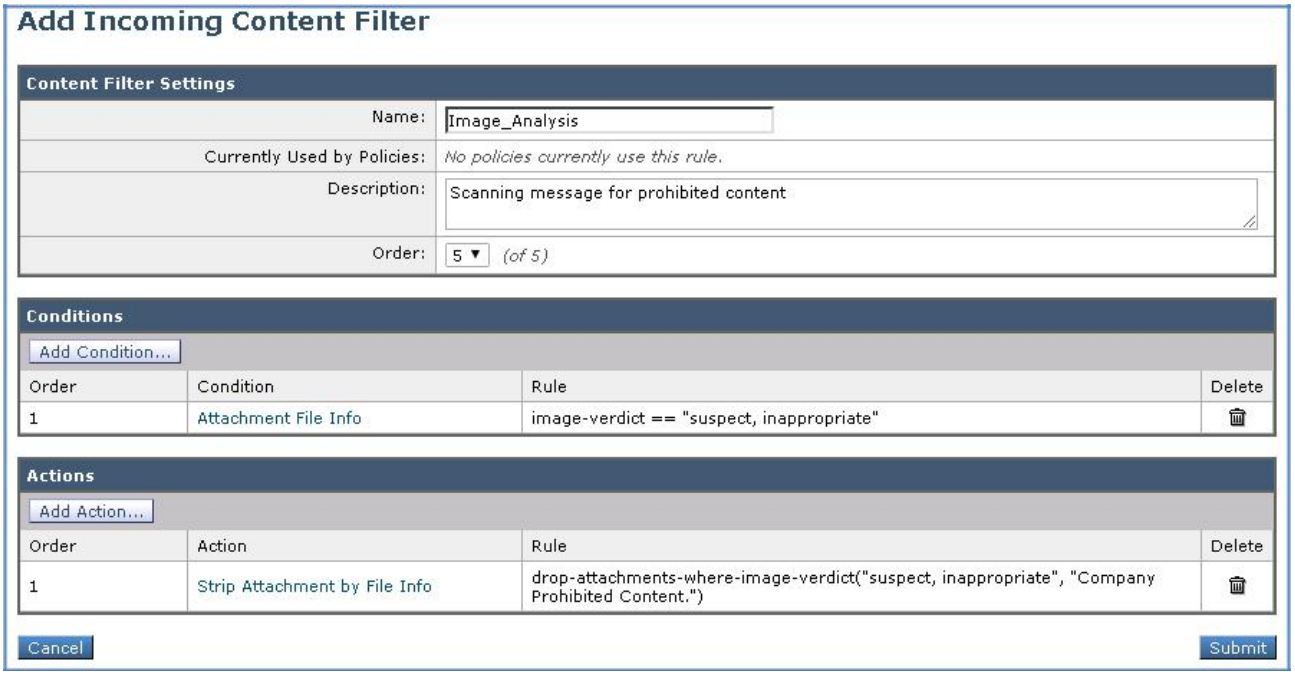
1. ワークステーションから GUI にアクセスし、[メール ポリシー(Mail Policy)] > [受信コンテンツ フィルタ(Incoming Content Filters)] に移動して、[フィルタの追加(Add Filter)] をクリックします。
2. 次の設定で条件とアクションを設定します。
   - [名前(Name)]:Image_Analysis
   - [説明(Description)]:禁止されたコンテンツを含むメッセージがないかスキャンします
   - [条件(Condition)]:[添付ファイル情報(Attachment File Info)] > [画像分析の判定(Image Analysis Verdict)]:Is(が)、Suspect or Inappropriate(不審または不適切)
   - [アクション(Actions)]:[ファイル情報による添付ファイルの削除(Strip Attachment by File Info)] > [画像分析の判定が(Image Analysis Verdict is)]:Suspect or Inappropriate(不審または不適切)
   - [置換メッセージ(任意)(Replacement Message (optional))]:Company prohibited content.(会社で禁止されているコンテンツです。)



3. [OK] をクリックします。
4. [アクションを追加(Add Action)] をクリックします。



5. [OK] をクリックします。

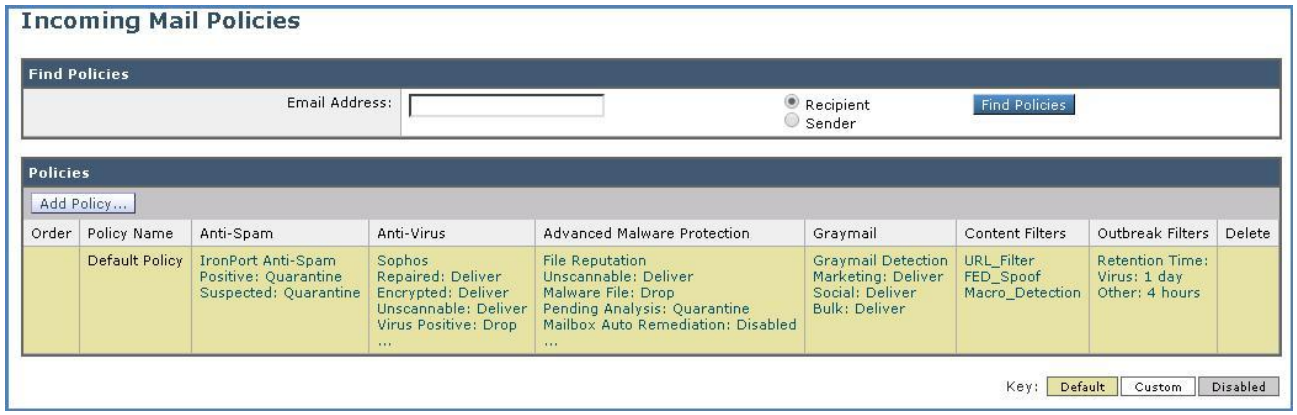


6. [送信（Submit）] をクリックしてアクションを適用し、変更内容を確定します。

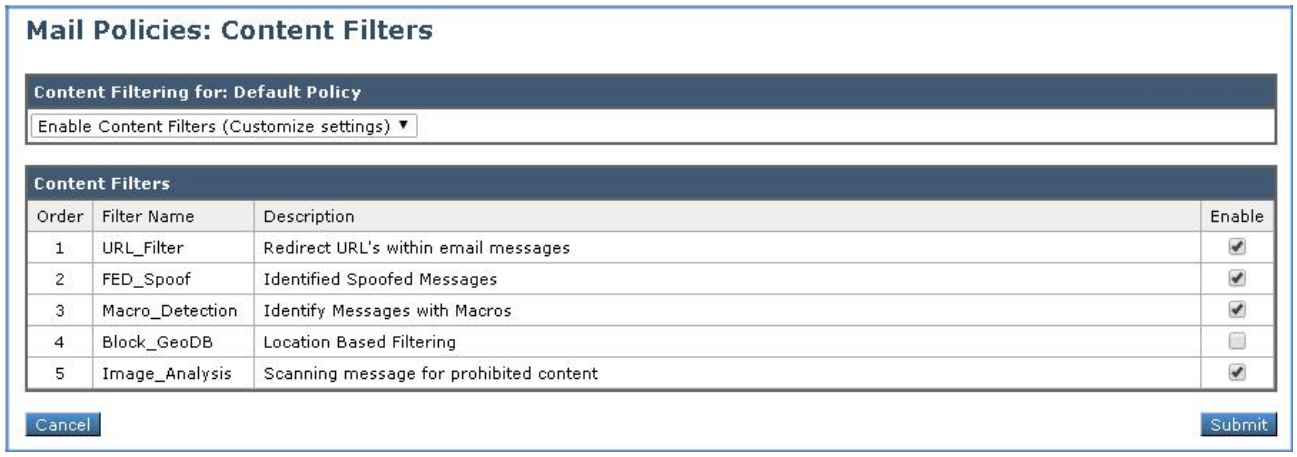
タスク:受信メール ポリシーを編集する(推定所要時間:1 分)

必要なコンテンツ フィルタが用意されている場合、最後のタスクは、前の手順で指定した条件を実装して必要なアクションを実行する受信メール ポリシーを作成することです。

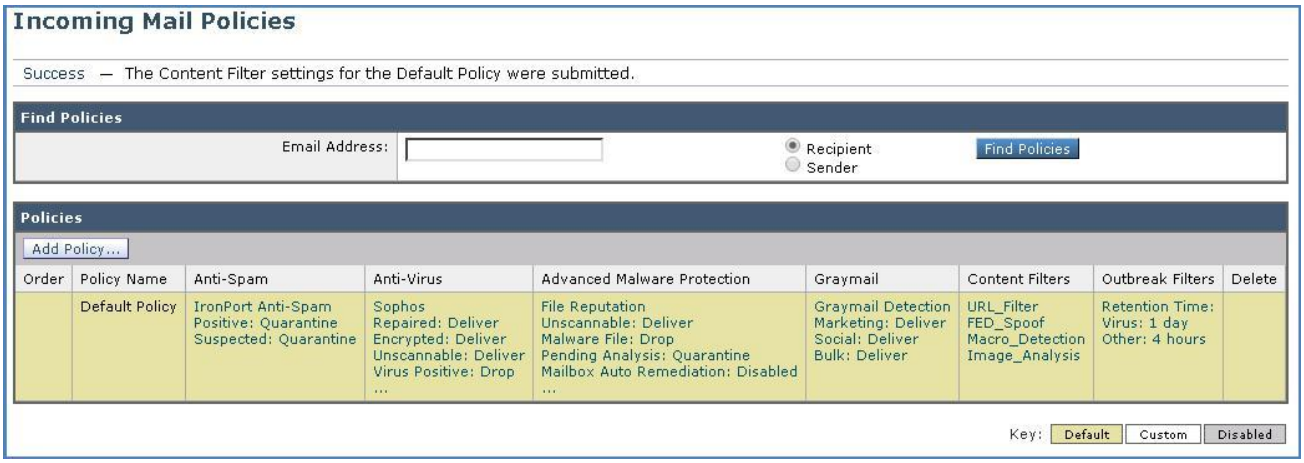
1. ワークステーションから GUI にアクセスし、[メール ポリシー(Mail Policy)] > [受信メール ポリシー(Incoming Mail Policies)] に移動して、[デフォルト ポリシー(Default Policy)] の [コンテンツ フィルタ(Content Filters)] ボックス内をクリックします。



2. 前の手順で作成した「Image_Analysis」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。



3. [送信（Submit）] をクリックしてコンテンツ フィルタを作成し、ポリシーを確認します。



4. 完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

タスク：画像分析をテストする（推定所要時間：5 分）

全体の構成が完了していれば、不適切な画像を電子メールに添付して、社外ユーザの Adam から Alan に送信することで画像分析機能をテストできます。

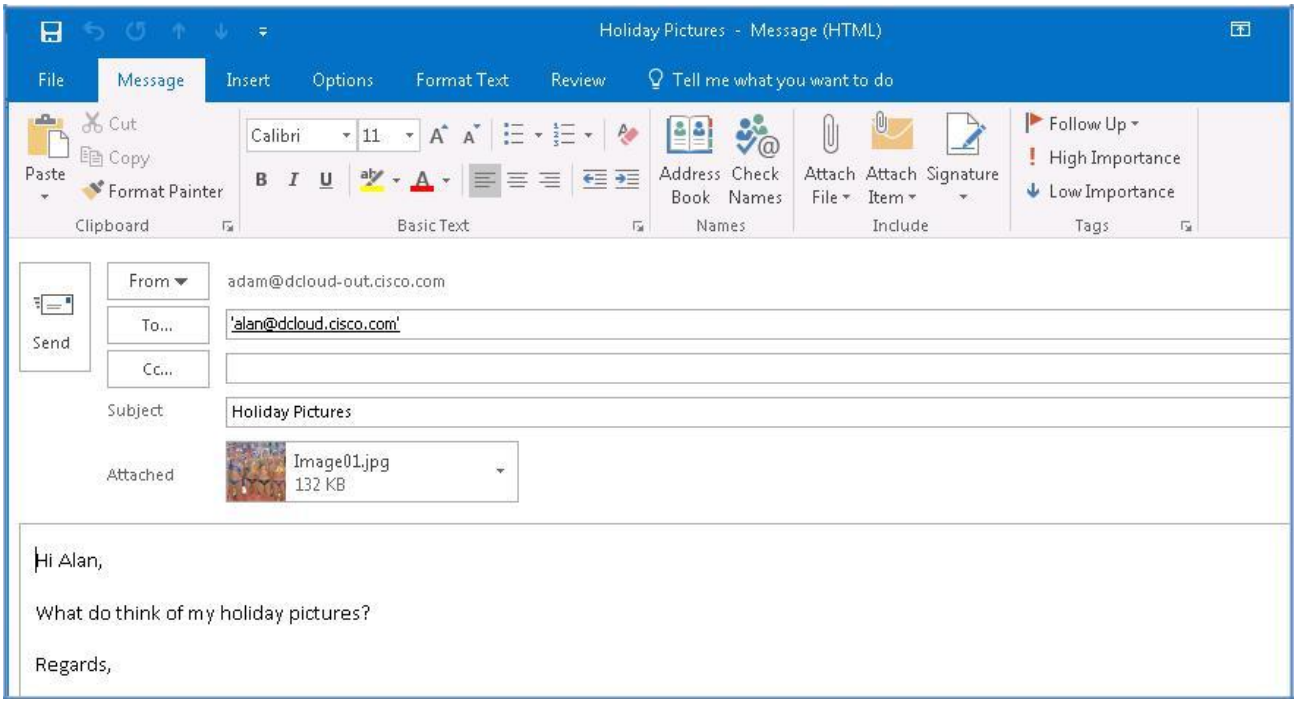
CLI セッションの開始

メッセージを準備する前に、CLI から Cisco E メール セキュリティ ソリューションへの接続を開始します。この目的は、tail コマンドによってメール ログを表示し、パイプラインを流れるように円滑にメッセージが処理され、アクションが適用されることを確認するためです（これを開始するには前のシナリオと同じ手順を繰り返します）。

1. ワークステーションから Microsoft Outlook を起動し、Adam の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。
   - [宛先（To）]：alan@dcloud.cisco.com
   - [件名（Subject）]：旅行先の写真（Holiday Pictures）
   - [本文（Body）]：Hi Alan,（Alan 様）

     旅行先で撮った写真をお送りします（What do you think of my Holiday pictures?）

     Regards,（よろしくお願いします。）
   - [添付ファイル（Attach）]：デスクトップ上の Images サブフォルダにある Image01.jpg。

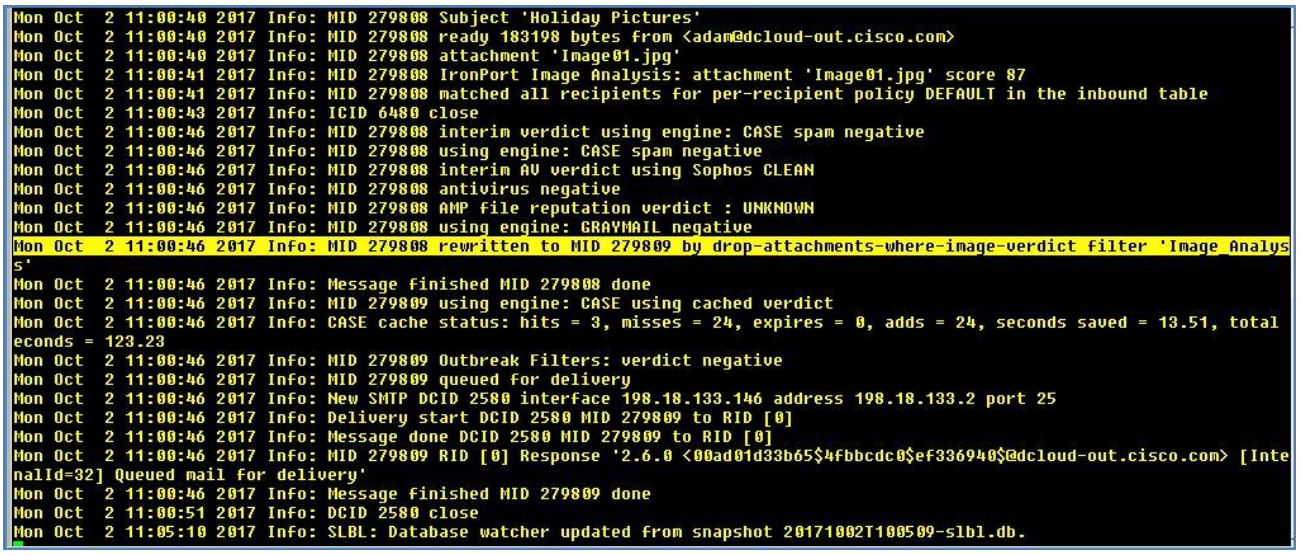


2. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

3. CLI に戻り、コンテンツ フィルタによってメッセージがどのように処理されたのかを確認します。添付ファイルには 87 のスコアが割り当てられました。これは「Inappropriate」（不適切）というカテゴリに該当します。

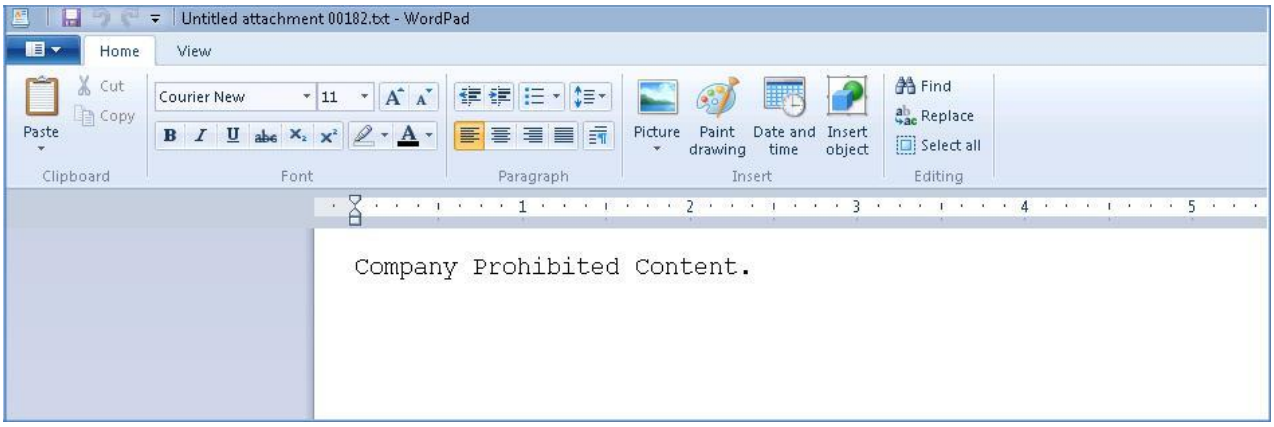
```
Mon Oct  2 11:00:40 2017 Info: MID 279808 ICID 6480 From: <adam@dcloud-out.cisco.com>
Mon Oct  2 11:00:40 2017 Info: MID 279808 ICID 6480 RID 0 To: <alan@dcloud.cisco.com>
Mon Oct  2 11:00:40 2017 Info: MID 279808 Message-ID '<00ad01d33b65$4fbbcdc0$ef336940$@dcloud-out.cisco.com>'
Mon Oct  2 11:00:40 2017 Info: MID 279808 Subject 'Holiday Pictures'
Mon Oct  2 11:00:40 2017 Info: MID 279808 ready 183198 bytes from <adam@dcloud-out.cisco.com>
Mon Oct  2 11:00:40 2017 Info: MID 279808 attachment 'Image01.jpg'
Mon Oct  2 11:00:41 2017 Info: MID 279808 IronPort Image Analysis: attachment 'Image01.jpg' score 87
Mon Oct  2 11:00:41 2017 Info: MID 279808 matched all recipients for per-recipient policy DEFAULT in the inbound table
Mon Oct  2 11:00:43 2017 Info: ICID 6480 close
Mon Oct  2 11:00:46 2017 Info: MID 279808 interim verdict using engine: CASE spam negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 using engine: CASE spam negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 interim AV verdict using Sophos CLEAN
Mon Oct  2 11:00:46 2017 Info: MID 279808 antivirus negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 AMP file reputation verdict : UNKNOWN
Mon Oct  2 11:00:46 2017 Info: MID 279808 using engine: GRAYMAIL negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 rewritten to MID 279809 by drop-attachments-where-image-verdict filter 'Image_Analysi
s'
Mon Oct  2 11:00:46 2017 Info: Message finished MID 279808 done
Mon Oct  2 11:00:46 2017 Info: MID 279809 using engine: CASE using cached verdict
Mon Oct  2 11:00:46 2017 Info: CASE cache status: hits = 3, misses = 24, expires = 0, adds = 24, seconds saved = 13.51, total s
econds = 123.23
Mon Oct  2 11:00:46 2017 Info: MID 279809 Outbreak Filters: verdict negative
Mon Oct  2 11:00:46 2017 Info: MID 279809 queued for delivery
Mon Oct  2 11:00:46 2017 Info: New SMTP DCID 2580 interface 198.18.133.146 address 198.18.133.2 port 25
Mon Oct  2 11:00:46 2017 Info: Delivery start DCID 2580 MID 279809 to RID [0]
Mon Oct  2 11:00:46 2017 Info: Message done DCID 2580 MID 279809 to RID [0]
Mon Oct  2 11:00:46 2017 Info: MID 279809 RID [0] Response '2.6.0 <00ad01d33b65$4fbbcdc0$ef336940$@dcloud-out.cisco.com> [Inter
nalId=32] Queued mail for delivery'
```

4. その後、添付ファイルがメッセージから削除されます。



5. Alan の受信トレイに戻ります。メッセージは配信されていますが、不適切なコンテンツは削除され、置換ファイルが挿入されています。

6. 添付ファイルを開いて、エンドユーザに提示されるメッセージを確認します。



お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp