Cisco E メール セキュリティ ソリューション 11.1 ラボ v1.3

最終更新日:2018 年 7 月 24 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®

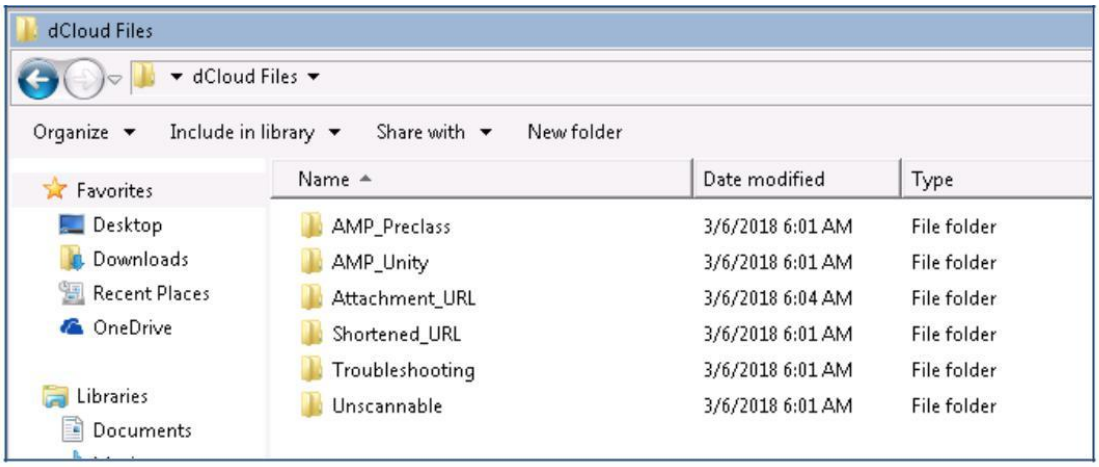
このソリューションについて

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。

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。



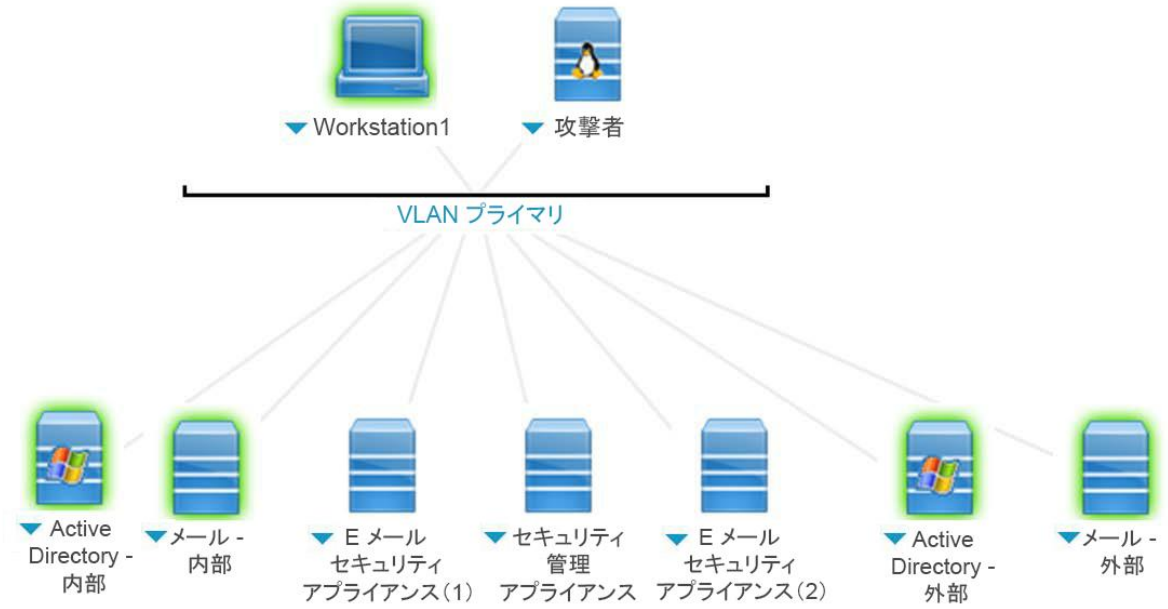
注：一部のシナリオでは、特定の補助ファイルを実行する際に注意を促すセキュリティ警告が表示される場合がありますが、これらは完全に安全です。

「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。

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 クレデンシャルは、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するか、それらを必要とするシナリオ内の手順を調べることで確認できます。

図 1. dCloud のトポロジ



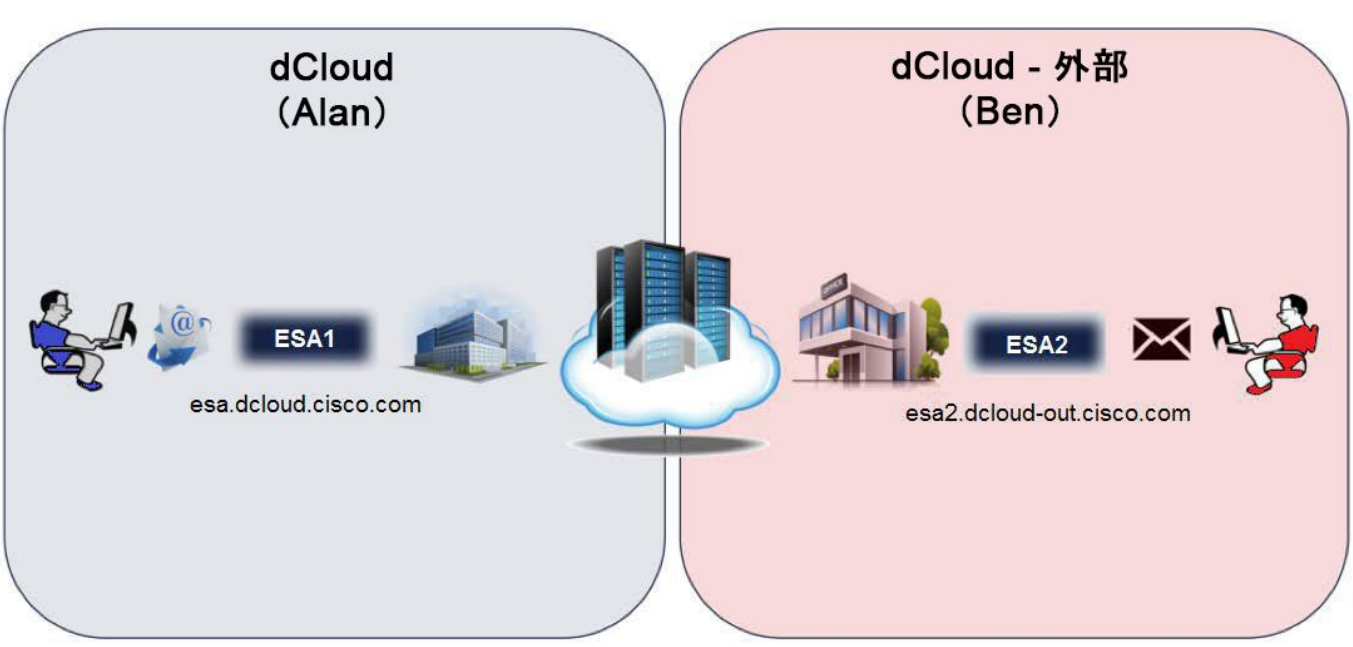
論理トポロジ

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。

「Ben」は、インターネット上のいずれかの場所にいる社外ユーザで、自分の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。偶然にも Cisco E メール セキュリティ ソリューションを採用して、自身の電子メール ドメインから送信されるメールをスプーフィングから効果的に保護しています。

Alan Alpha - alan@dcloud.cisco.com　　Ben Bravo - ben@dcloud-out.cisco.com



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。

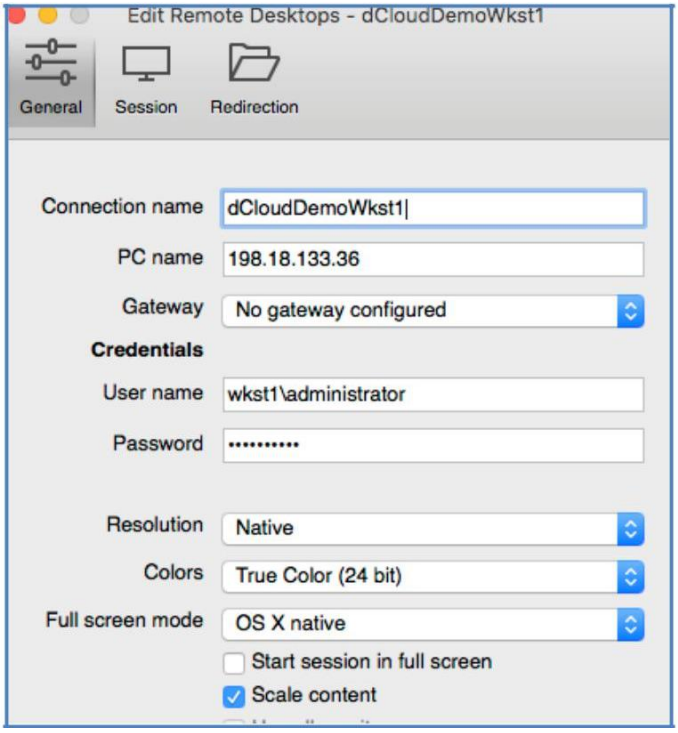
次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. 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。

2. 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、この方法では、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 社では、Cisco E メール セキュリティの AsyncOS を 1 年以上使用した結果、スパムと悪意のある脅威を含むメールの量がきわめて減少しました。シスコは、オペレーティング システムの新しいバージョンであるバージョン 11.1 をすべてのお客様に一般提供することを発表しました。新しいバージョンでは、現在のソリューションで提供しているスキャン エンジンの性能をさらに向上させ、一般的な使用例に対応する業界トップクラスの機能を追加しています。こうした機能には、さまざまな側面を可視化できる Advanced Malware Protection for Unity の統合、URL 短縮サービスにより変更された URL のスキャンのサポート、ドキュメント内の URL のスキャンなどが含まれるほか、ファイルを分析する AMP エンジンでは多くの点が改善されています。

Voyage Corp 社はメールのセキュリティ体制を良好に保っていましたが、メッセージング プラットフォームをアップグレードして、追加された新しいセキュリティ機能を活用することを決定しました。現在と将来のために最善のセキュリティを確保することにしたのです。

その後、Voyage Corp 社は戦略上の主要なビジネス パートナーと 18 ヵ月間にわたって協議を続け、最終的に、スプーフィングからの防御対策を強化するために、SPF、DKIM、DMARC といったその他の技術も導入することにしました。

セキュリティ ソリューション

Voyage Corp 社は、メール インフラストラクチャの安全性を高める主な技術として Cisco E メール セキュリティ ソリューションに投資を続けます。AsyncOS をバージョン 11.1 にアップグレードした後に展開される次の機能が安全性を強化します。

- URL フィルタリングの強化：短縮 URL と内部の添付ファイル
- ファイル スキャン不能な動作のモニタリング
- AMP レピュテーションの強化：補助ファイルの種類の追加
- AMP 事前分類機能の強化
- ESA と AMP for Endpoint クラウド コンソールの統合

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 社における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:　疑わしい 短縮 URL からの保護

ユースケース

社内の複数のユーザにメールを介して送信されるハイパーリンクの数は着実に増加しています。Cisco E メール セキュリティは、ユーザ承認制御を適用したり、エンドユーザのワークステーションを侵害しかねないマルウェアの活動をホストする Web サイトにユーザがリダイレクトされないように URL をスキャンする時間を与えたりすることで、こうした URL を管理し実績を上げています。

最近、生産サービス部門のユーザが短縮 URL が含まれた電子メールを受信しました。その URL をクリックすると、最初に要求したサイトとは別のサイトにリダイレクトされ、そのユーザのマシンにマルウェアがダウンロードされました。しかし、疑わしいそのマシンには AMP for Endpoints クライアントがインストールされていたため、被害を受けずに済みました。

このように複数の層で防御していても、InfoSec 部門は、同様の問題が再度発生しないように、Cisco E メール セキュリティの管理者に必要な制御機能を直ちに実装するように指示しました。

セキュリティ制御

AsyncOS バージョン 11.1 を使用する Cisco E メール セキュリティ ソリューションには、HTTP 要求の送信先を特定するために、最大 10 レベルの短縮 URL を照会するオプションが含まれています。

目的

このシナリオでは、マルウェアのホスティング サイトを参照する短縮 URL に URL フィルタリングを設定する方法について説明します。

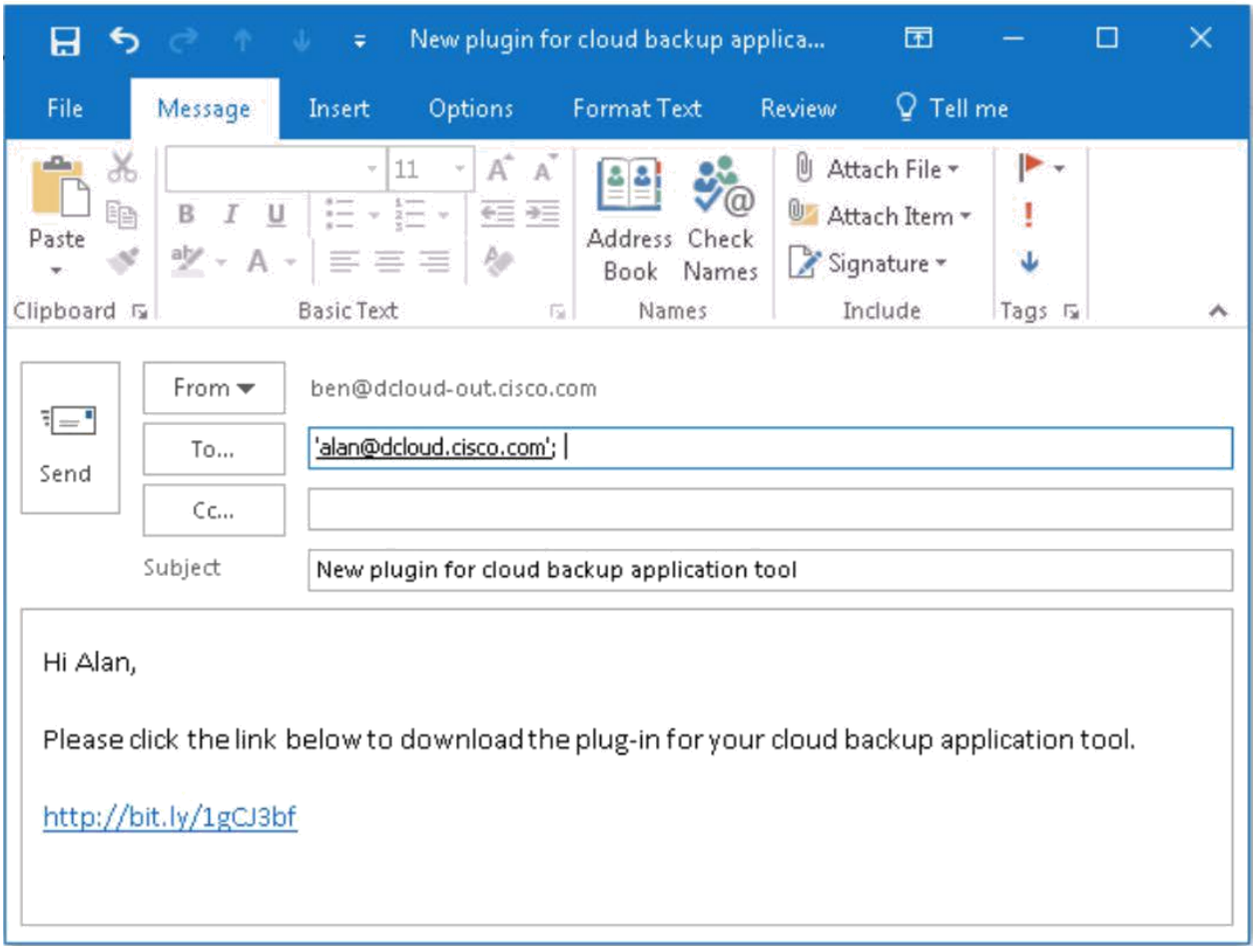
手順

短縮 URL を含むメールを送信する（推定所要時間：5 分）

このシナリオでは、社外ユーザの Ben から社内ユーザの Alan に短縮 URL を含むメールを送信します。短縮 URL のフィルタリング ポリシーの有無によって最終的な結果がどう変わるかを確認します。

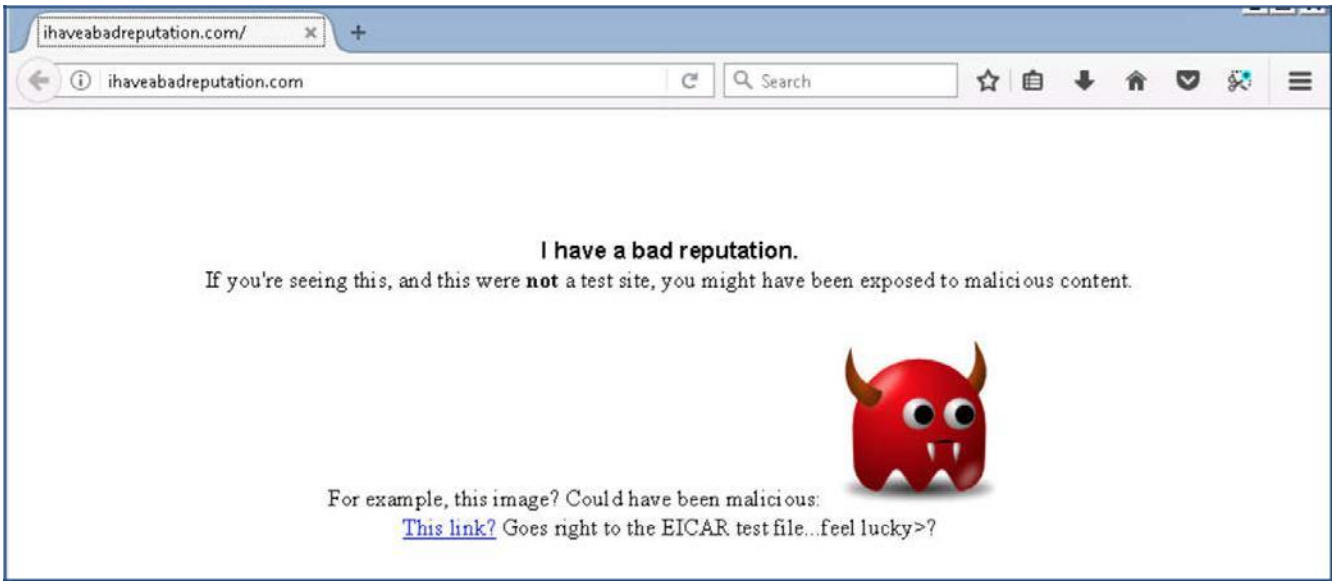
1. ワークステーション 1（以降、ワークステーションと呼ぶ）のタスク バーから Microsoft Outlook を起動し、次のパラメータでメールを準備します。

送信者：	ben@dcloud-out.cisco.com
受信者：	alan@dcloud.cisco.com
件名：	クラウド バックアップ アプリケーション ツールの新しいプラグイン
本文：	こんにちは、Alan 以下のリンクをクリックして、最新のクラウド バックアップ アプリケーション ツールのプラグインをダウンロードしてください。（Please click the link below to download the latest plug-in for your cloud backup application tool.） http://bit.ly/1qCJ3bf



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。
5. 短縮 URL のフィルタリング ポリシーが存在しないため、メールは短縮ハイパーリンクがまったく変更されずに Alan のメールボックスに配信されますが、これは想定内の動作です。メッセージ内の短縮ハイパーリンクを一度クリックします。サイトにアクセス可能な状態でブラウザが起動します。

6. メッセージ内の短縮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。

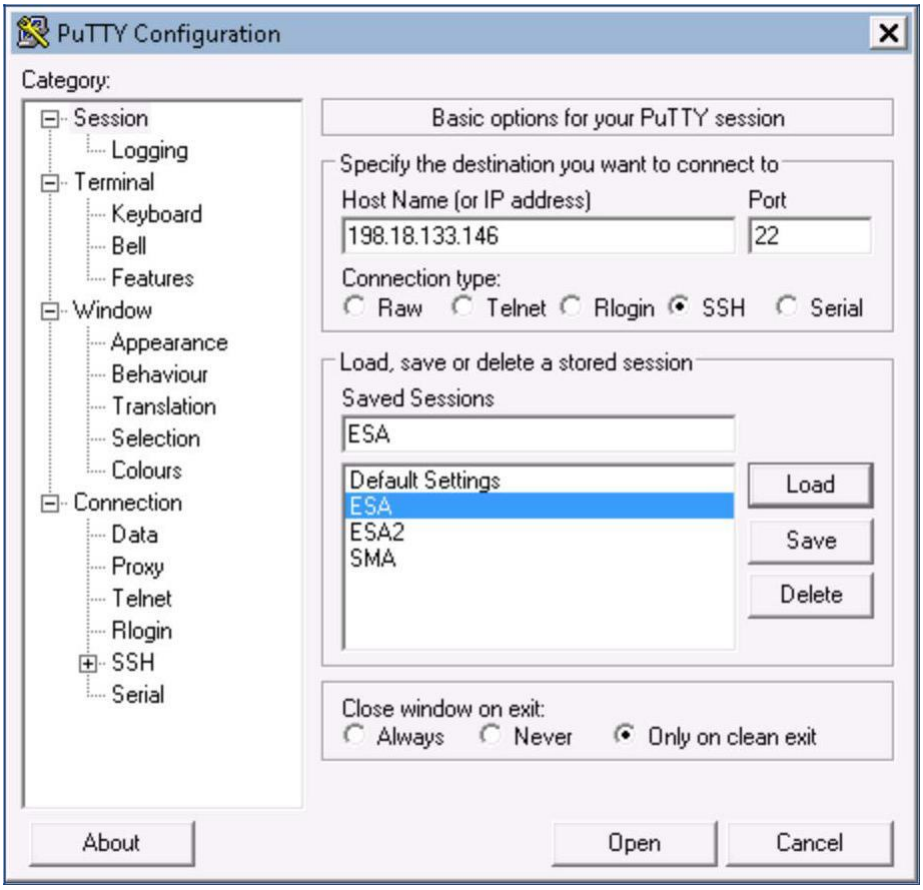


7. 次のタスクでは、エンド ユーザを悪意のあるコンテンツから常に保護できるように、短縮 URL フィルタリング機能を備えた Cisco E メール セキュリティ ソリューションを構成して、必要な制御を実装します。

短縮 URL のフィルタリングを有効にする（推定所要時間：15 分）

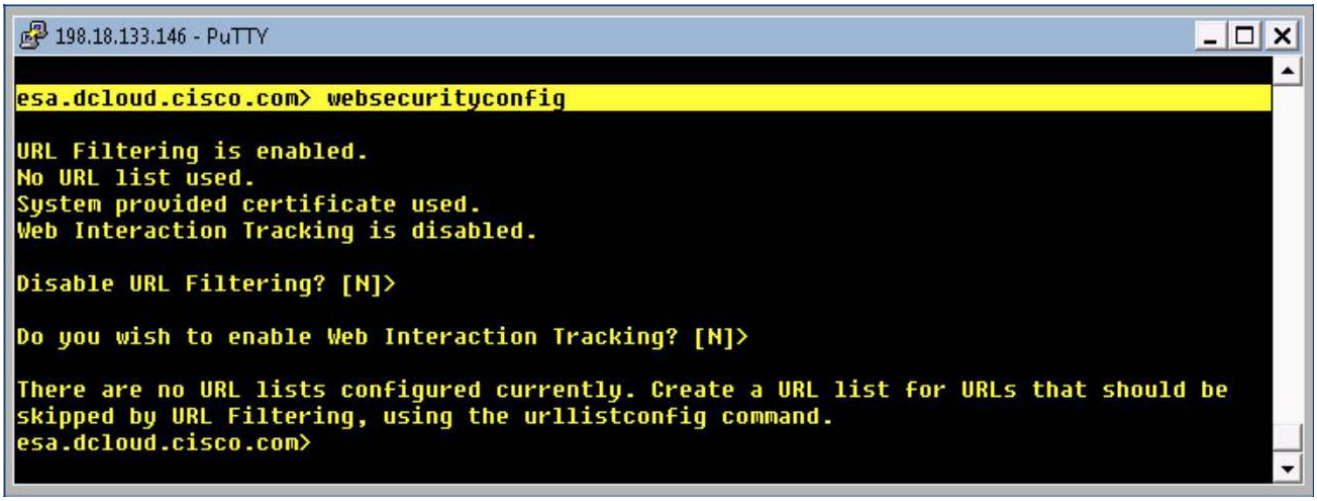
このタスクでは、高度な Web セキュリティ設定の短縮 URL オプションを CLI セッション経由で有効にします。

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、[Saved Sessions] から ESA を選択して、[Open] をクリックします。表示されるセキュリティ警告をすべて認めます。

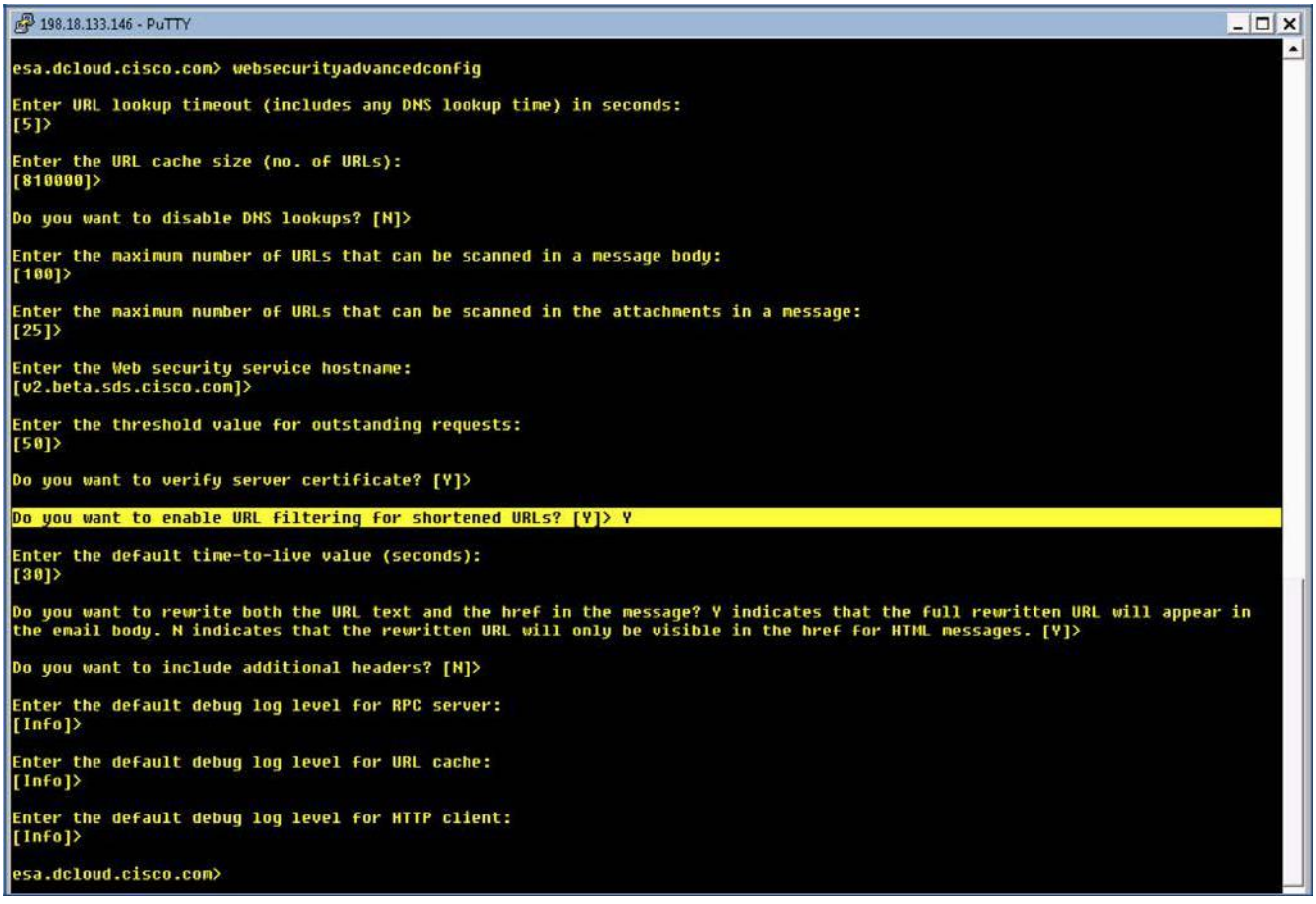


2. 次のクレデンシャルを使用してログインします：**ユーザ名**：admin、**パスワード**：C1sco12345

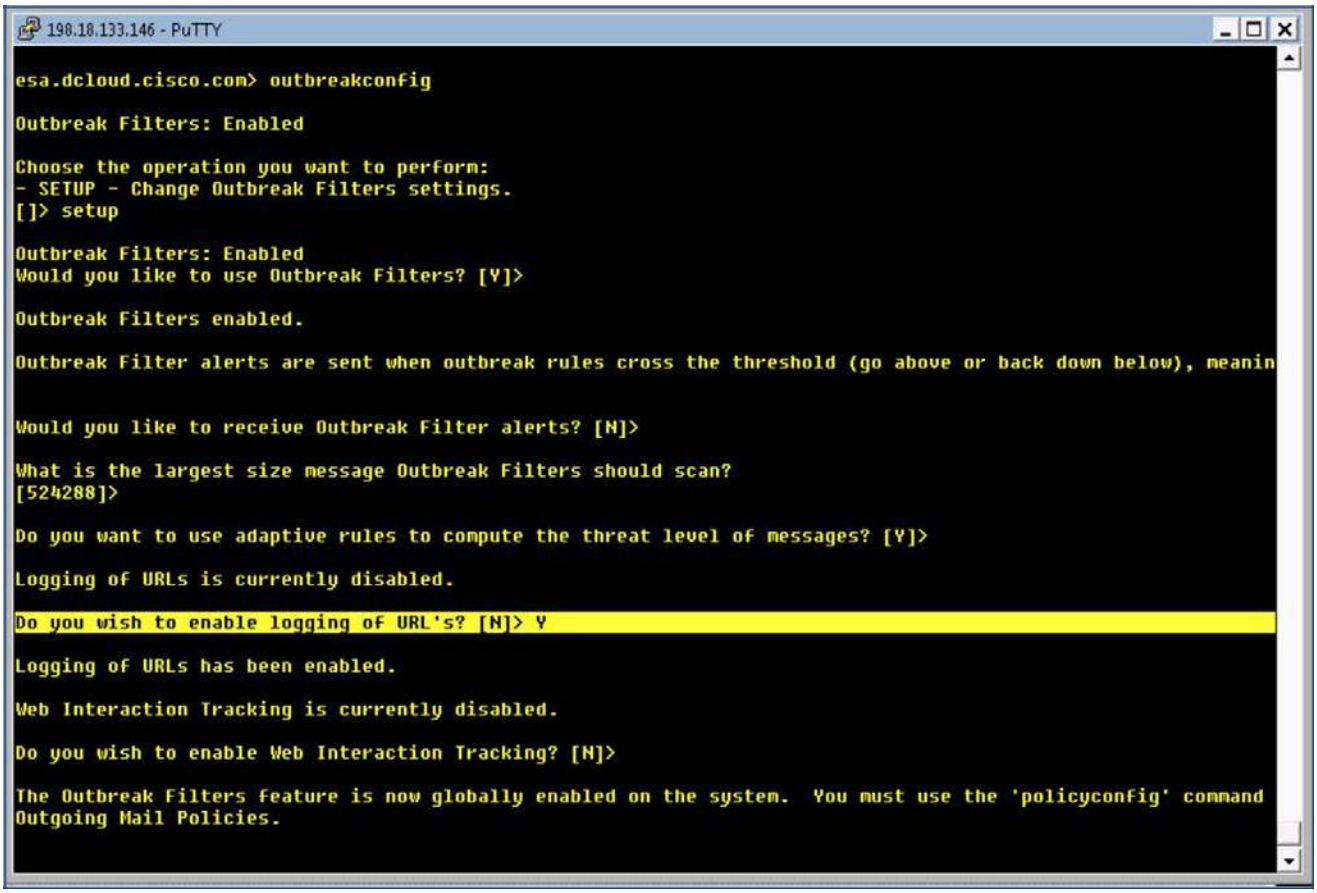
3. ログインしたら、**websecurityconfig** コマンドを入力して Enter キーを押します。URL フィルタリングが **Enabled** の状態であることを確認してください。その状態でない場合は、**Enable URL Filtering?** オプションに対し Y と入力し、URL フィルタリング サービスを有効にします。



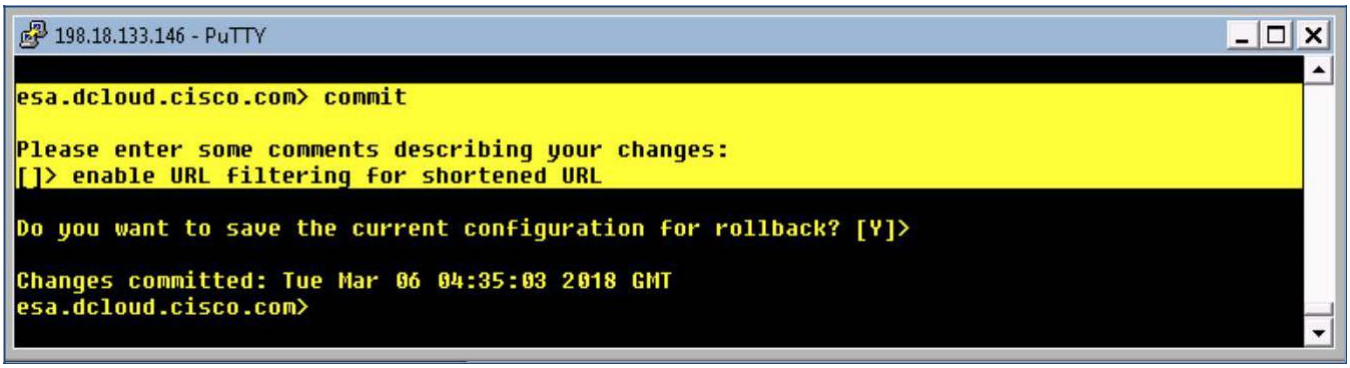
4. 同じ CLI セッション内で **websecurityadvancedconfig** コマンドを入力し、Enter キーを押します。すべてのオプションがデフォルトの設定のままになるように、キーボードの Enter キーを数回押し、**Do you want to enable URL filtering for shortened URLs?** オプションが、Y に設定されていることを確認します。



5. 次に、**outbreakconfig** コマンドを入力して Enter キーを押します。アウトブレイク フィルタが有効になっていることを確認します。その他のオプションはすべてデフォルト値のままで構いません。**Do you wish to enable logging of URLs?** に対しては Y を入力します。この設定により、URL フィルタリング ルールのアクティビティの詳細がメールのログに出力されます。



6. 設定を確認したら、**commit** コマンドを実行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ます。



コンテンツ フィルタを設定する（推定所要時間：10 分）

このタスクでは、短縮ハイパーリンクに書き換えられた疑わしい 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、その特定された 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。

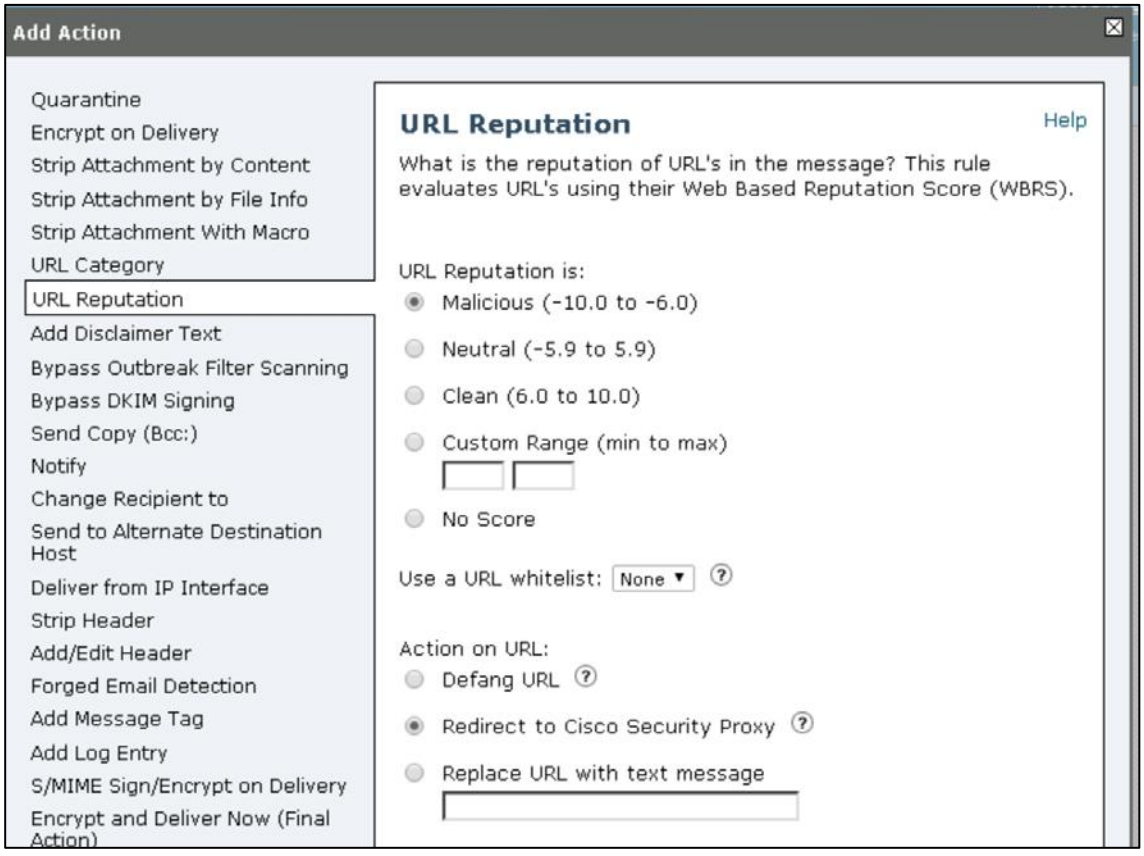
1. ワークステーションから Google Chrome を起動します。ブックマークの ESA をクリックし、[詳細設定（Advanced）]、[esa.dcloud.cisco.com（安全ではない）に進む（Proceed to esa.dcloud.cisco.com (unsafe)）] の順に選択すると、デフォルト ページが自動的にロードされます。これが、Cisco E メール セキュリティの GUI ページになります。次のクレデンシャルでログインします。**ユーザ名**：admin、**パスフレーズ**：C1sco12345。

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。

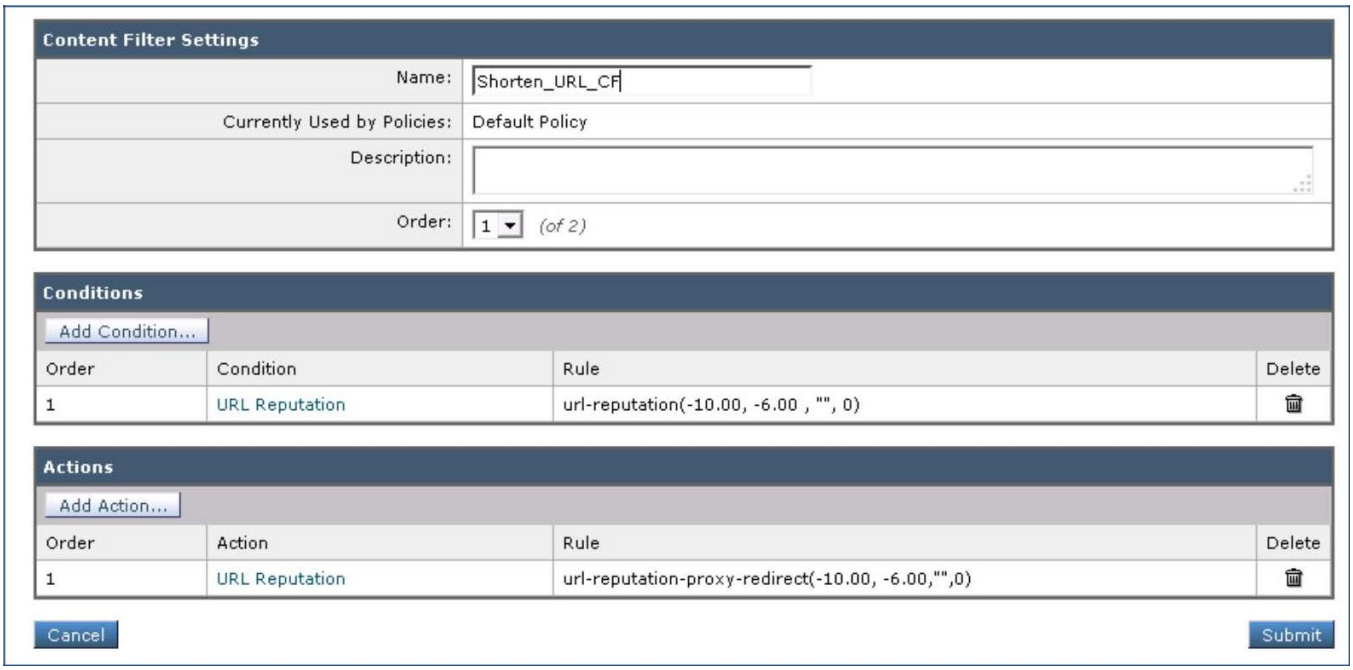
3. ワークステーションから GUI にアクセスし、[メールポリシー（Mail Policy）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動して、[フィルタの追加（Add Filter）] をクリックします。

4. 次の設定で*条件*と*アクション*を設定します。

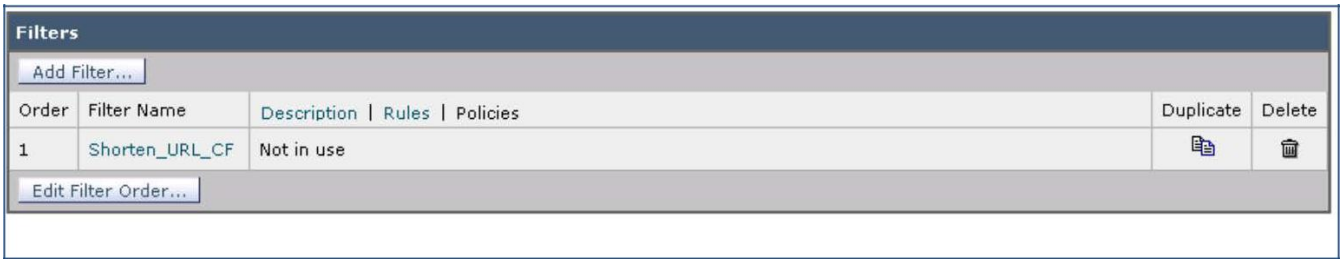
名前：	Shortened_URL_CF
説明：	E メール メッセージに含まれる悪意のあるレピュテーションの URL をリダイレクトします。
アクション 1：	[URLレピュテーション（URL Reputation）] > [Ciscoセキュリティプロキシにリダイレクト（Redirect to Cisco Security Proxy）]



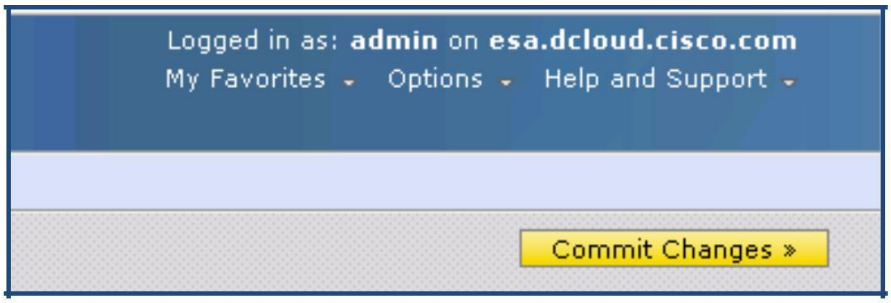
5. [OK] をクリックします。



6. [送信（Submit）] をクリックしてアクションを適用します。



7. 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。

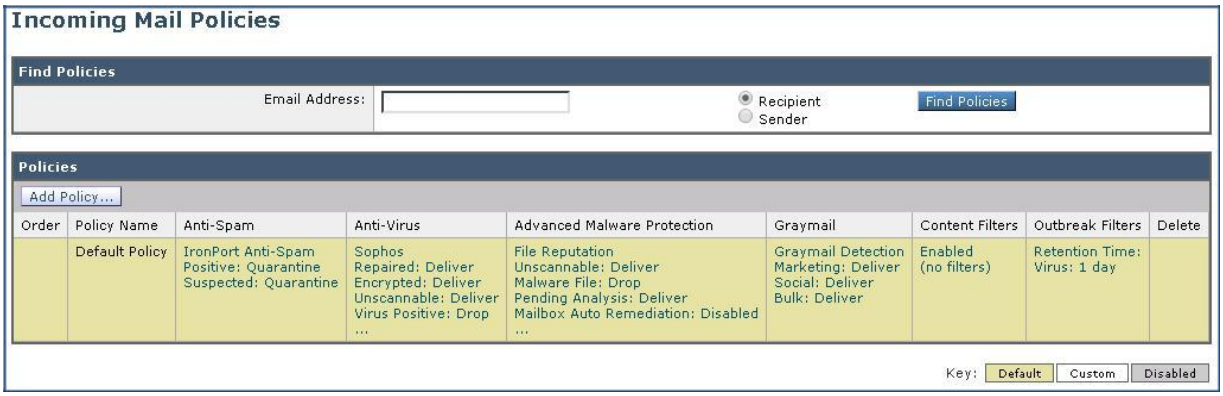


注:コンテンツ フィルタの動作とその柔軟性の詳細については、「Content Filters」を参照してください。

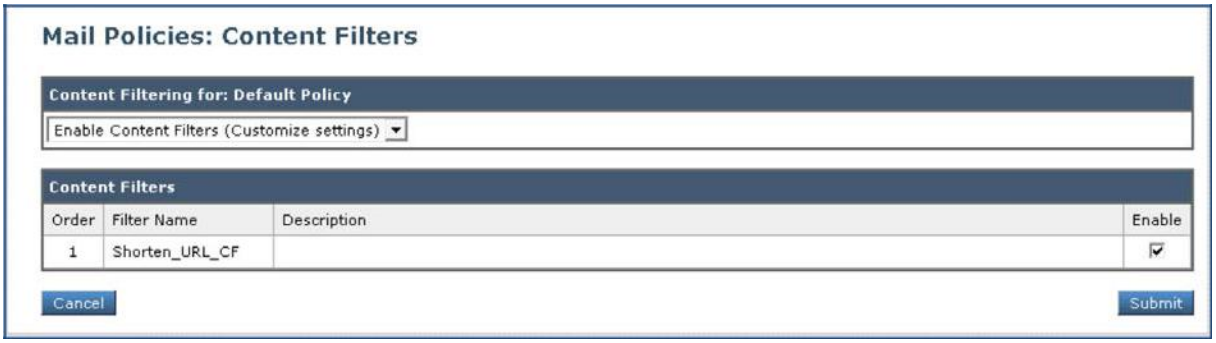
受信メール ポリシーを編集する（推定所要時間：3 分）

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。

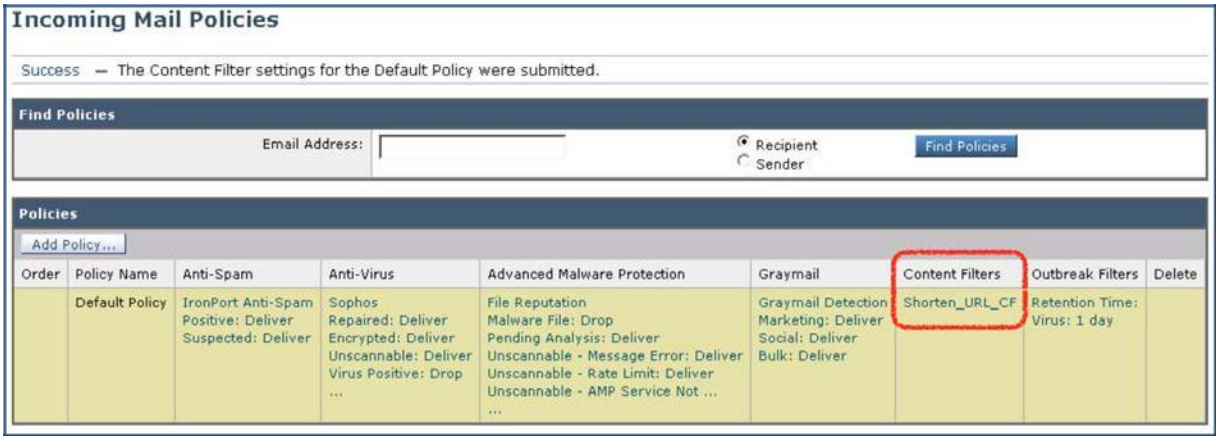
1. ワークステーションから ESA の GUI にアクセスし、[メール ポリシー（Mail Policy）] > [受信メール ポリシー（Incoming Mail Policies）] に移動して、[デフォルト ポリシー（Default Policy）] の [コンテンツ フィルタ（Content Filters）] ボックス内をクリックします。



2. 前の手順で作成した「Shortened_URL_CF」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。



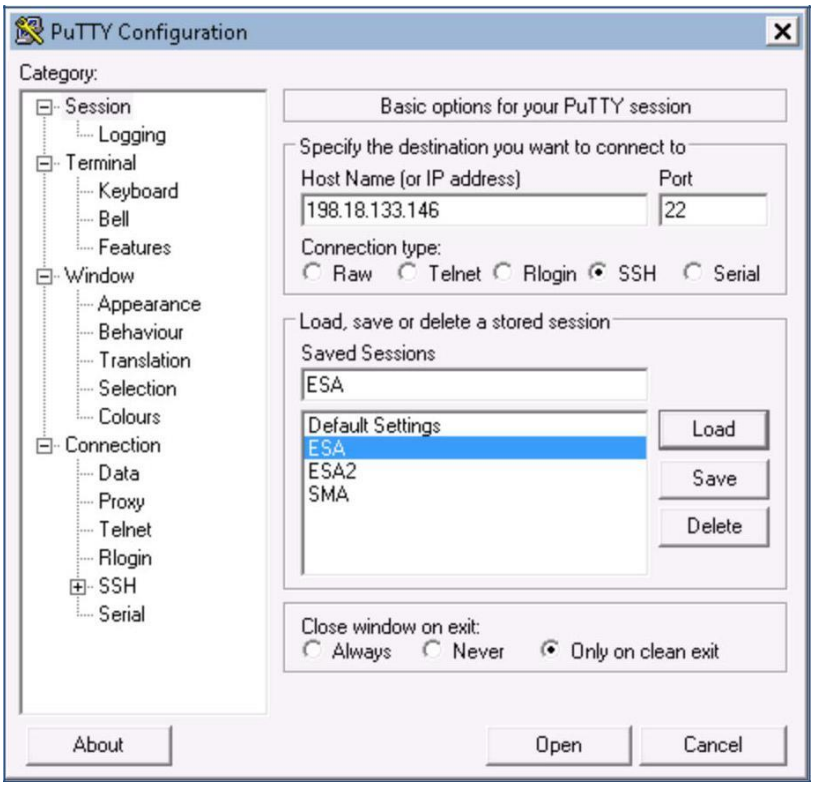
4. 完了したら画面の右上にある [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

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。

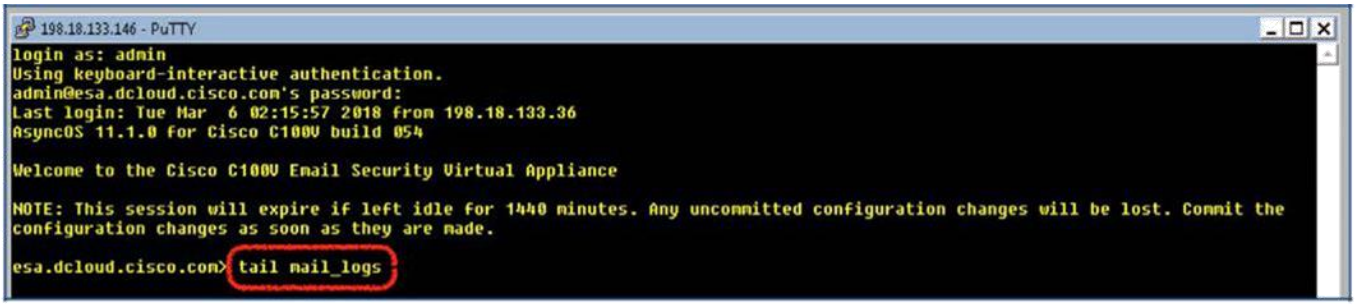
URL フィルタリングをテストする（推定所要時間：15 分）

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 Ben 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。

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、[Saved Sessions] から ESA を選択して、[Open] をクリックします。表示されるセキュリティ警告をすべて認めます。



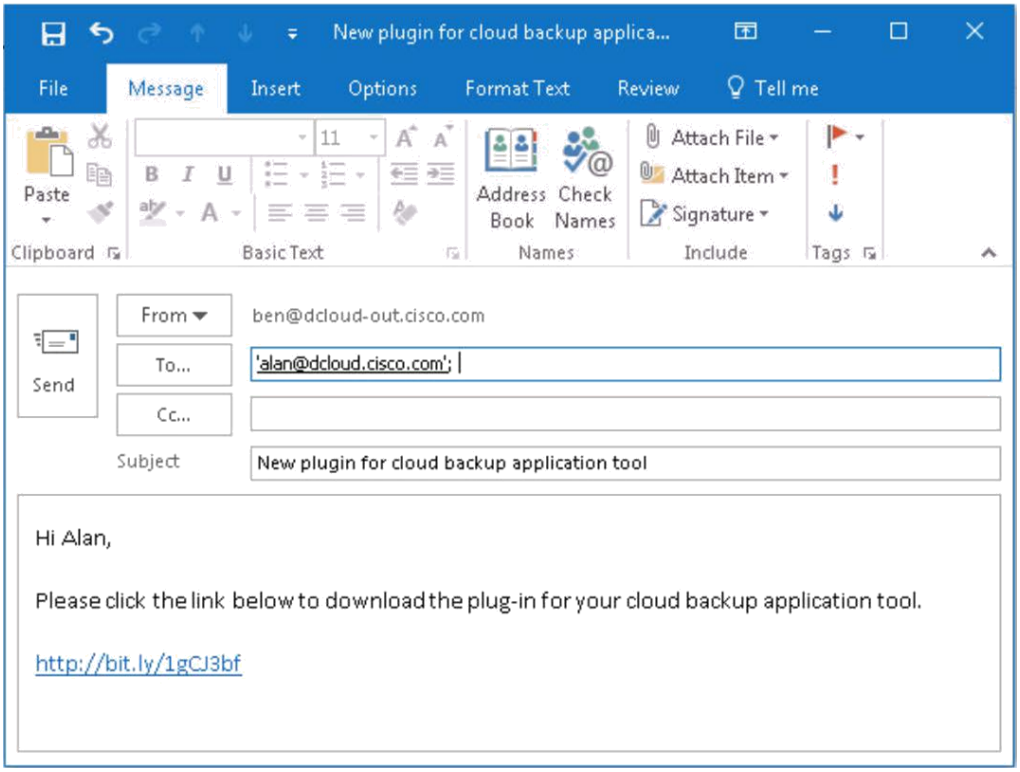
2. 前述のクレデンシャルを使用してログインします。ログインしたら、**tail mail_logs** コマンドを入力して Enter キーを押します。これをバックグラウンドで実行したまま、次の手順に進みます。



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。

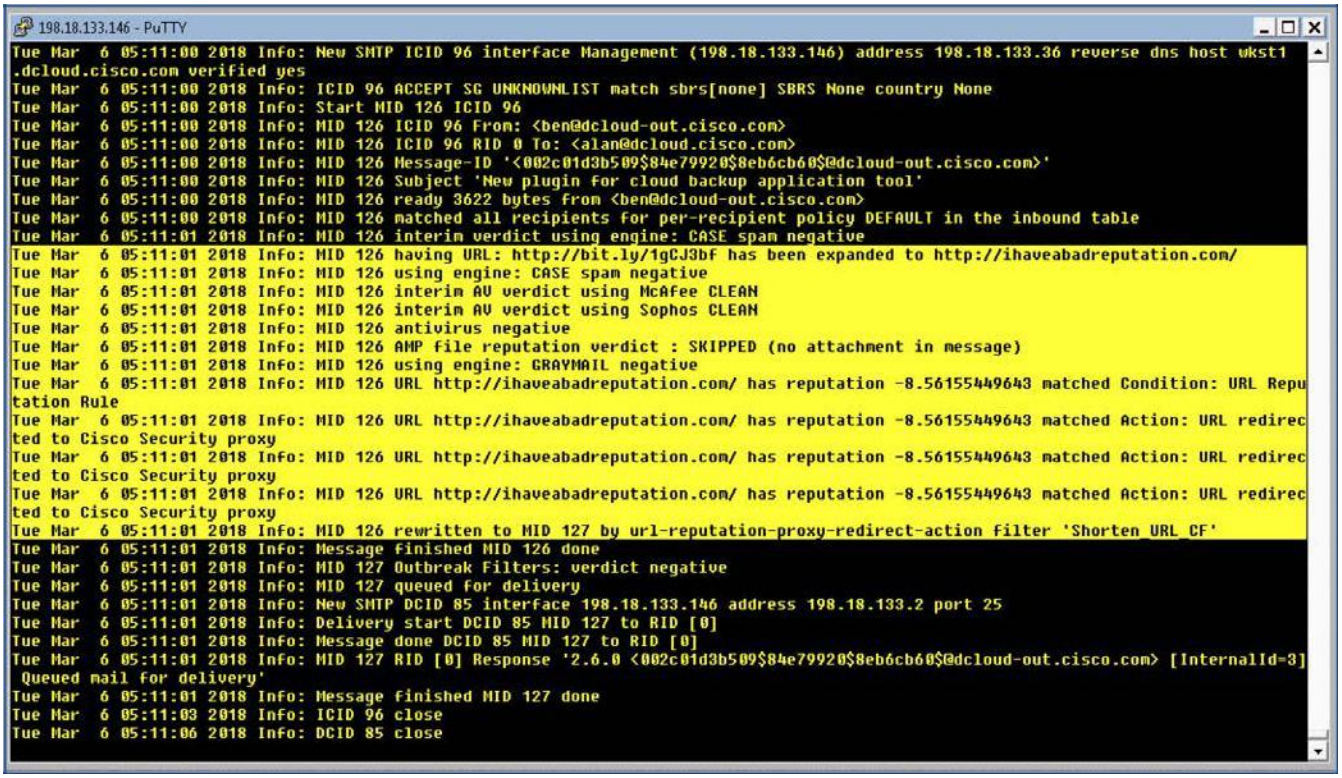
3. ワークステーションから Microsoft Outlook を起動し、Ben の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。

送信者:	ben@dcloud-out.cisco.com
受信者:	alan@dcloud.cisco.com
件名:	クラウド バックアップ アプリケーション ツールの新しいプラグイン
本文:	こんにちは、Alan 以下のリンクをクリックして、最新のクラウド バックアップ アプリケーション ツールのプラグインをダウンロードしてください。(Please click the link below to download the latest plug-in for your cloud backup application tool.) http://bit.ly/1gCJ3bf

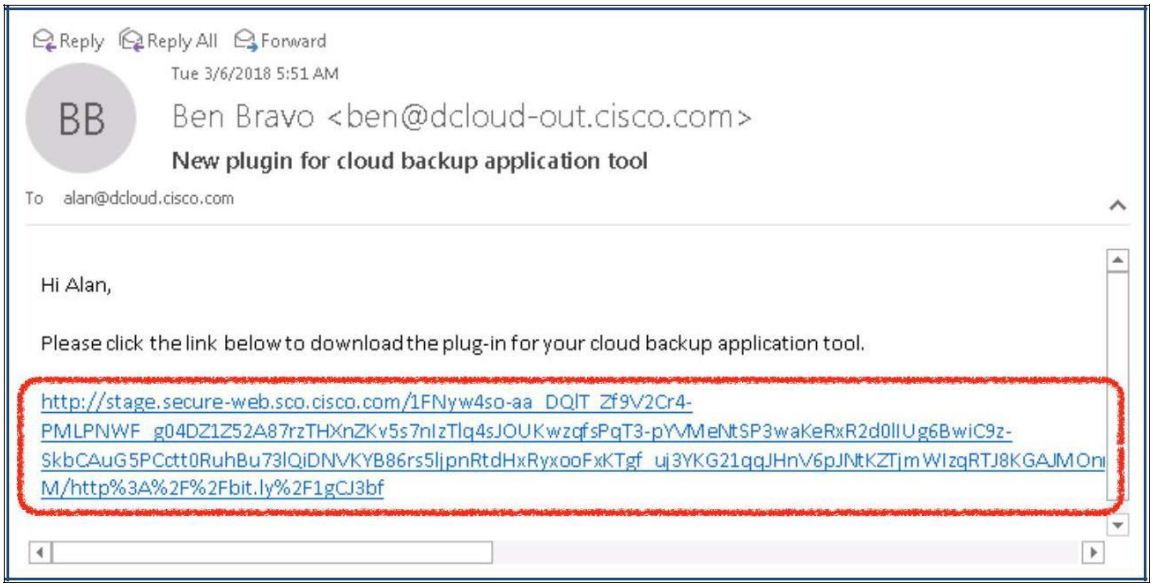


4. メールを送信します。[すべてのフォルダを送受信(Send/Receive Folder)] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

5. ESA の CLI セッションに戻り、Shortened_URL_CF ルールによってメッセージがどのように処理されたかを確認します。短縮ハイパーリンクに書き換えられた元の URL（http://ihaveabadreputation.com）が明らかになり、Cisco セキュリティ プロキシにリダイレクトされています。プロキシでは、メッセージ内の URL が危険である可能性があるかどうかが Web レピュテーションに基づいて判定されます。

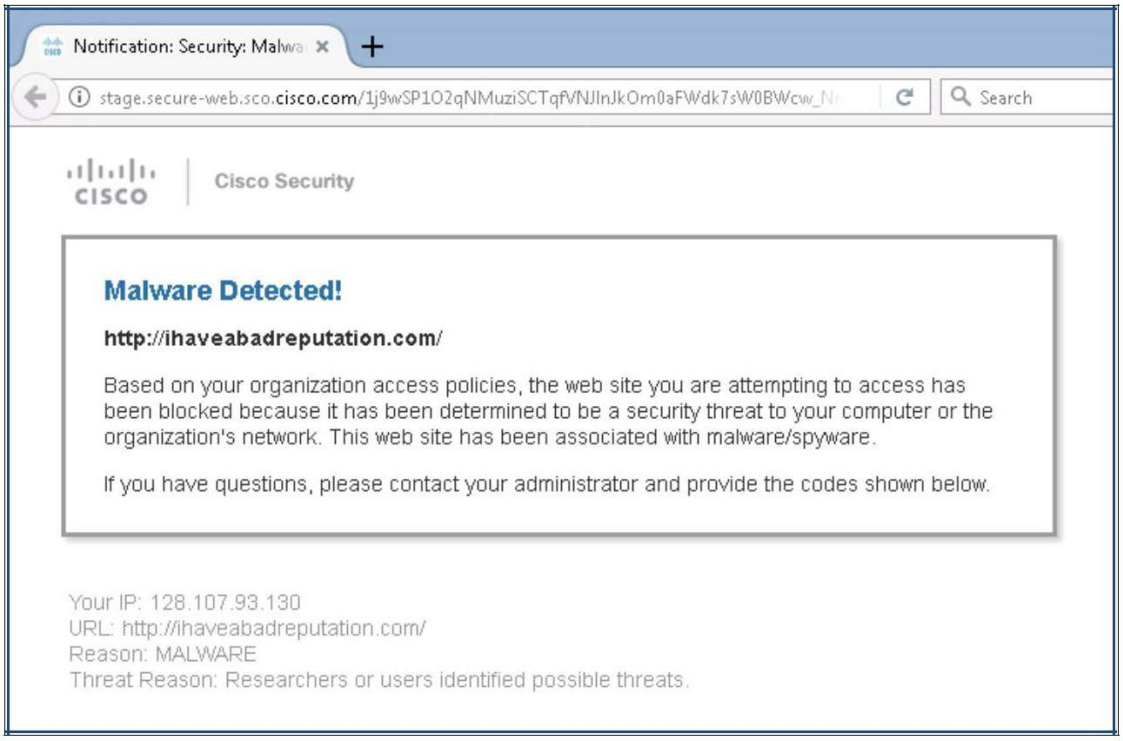


6. Alan の受信トレイに戻り、この時点で URL がどのように変更されているかを確認します。ハイパーリンクは、Cisco セキュリティ プロキシへのリダイレクトが含まれているため、はるかに長くなっています。



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。

7. Cisco セキュリティ プロキシにリダイレクトされる 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。



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 2:　添付ファイル内の疑わしい URL からの保護

ユースケース

ビジネス パートナー間の主要な通信手段としてメールの利用が増え、州規模の環境対策の一部としてもドキュメントの不要な印刷を減らすために、メール メッセージによる契約が交わされるようになりました。こうしたドキュメントには、ビジネス上の契約条件へのリンクが含まれることが多く、そのリンク先のほとんどが、さまざまな地理的位置にある外部の Web サーバでホストされています。

最近、ある法務担当者が、そのようなサイトへのリンクを含む Portable Document Format（PDF）が添付されたメールを受信しました。ハイパーリンクの 1 つをクリックすると、悪意のあるペイロードを含むスクリプトをダウンロードするサイトにリダイレクトされ、その担当者の Web ブラウザが感染するようになっていました。

セキュリティ制御

AsyncOS バージョン 11.1 を使用する Cisco E メール セキュリティ ソリューションには、ドキュメント内の URL をスキャンし、それらをシスコの Web プロキシによりリダイレクトして悪意のある添付内容を確認できるオプションが追加されています。

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、企業のポリシーにより禁止されている Web サイト、または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、メールの添付ファイルに含まれる悪意のある URL から保護します。

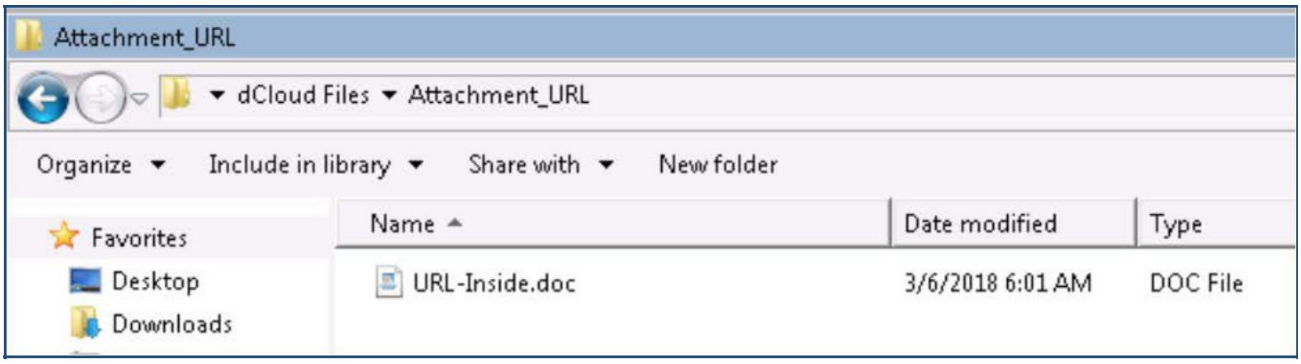
手順

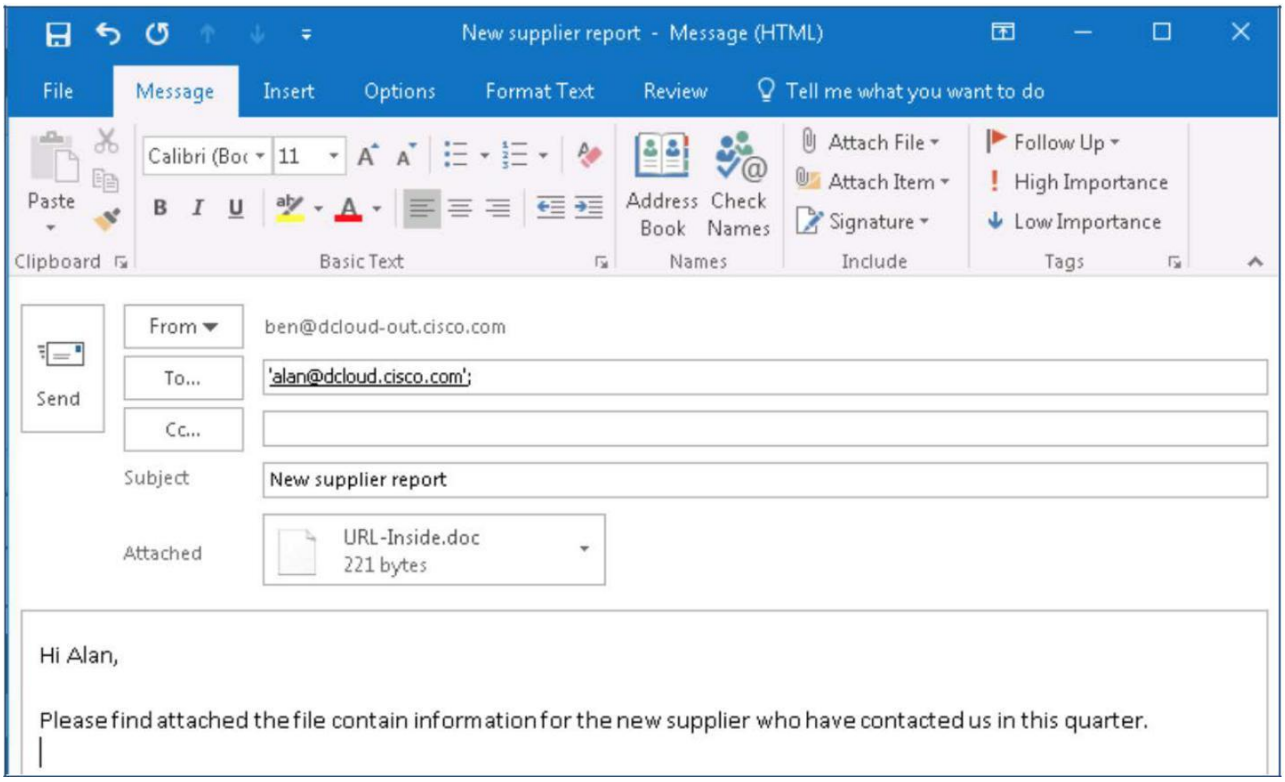
メッセージ内の URL にアクセスする（推定所要時間：5 分）

最初のタスクでは、メールの添付ファイルに含まれる疑わしい URL を通知するメカニズムが導入されていない状況で、そうしたファイル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。

1. ワークステーションから Microsoft Outlook を起動し、Ben 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。

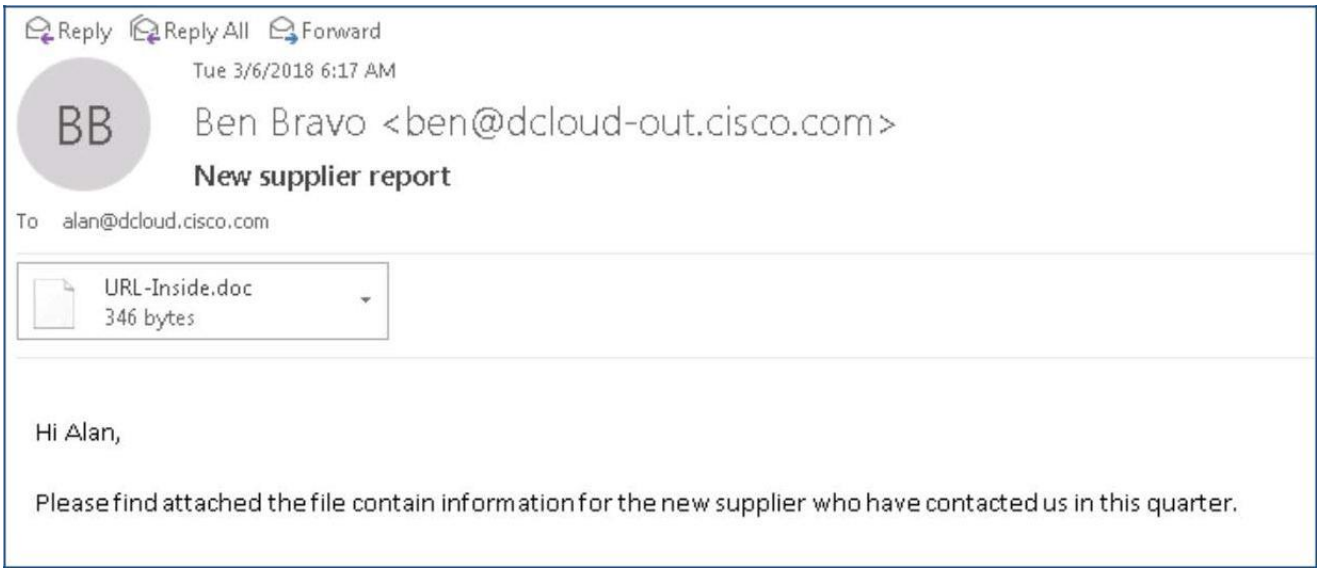
送信者：	ben@dcloud-out.cisco.com
受信者：	alan@dcloud.cisco.com
件名：	新しいサプライヤのレポート
本文：	こんにちは、Alan この四半期に連絡を受けた新しいサプライヤの情報が含まれるファイルを添付しましたので確認してください。（Please find attached the file contain information for the new suppliers who have contacted us in this quarter.）
添付ファイル：	デスクトップ上の **Attachment_URL** サブフォルダにある **URL-Inside.doc**





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. 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。



添付ファイルの URL フィルタリングの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 Alan 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 Word 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。

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。

次のタスクでは、添付ファイルの URL フィルタリング機能を備えた Cisco E メール セキュリティ ソリューションを設定して、内部ユーザが許可されていない Web サイトにアクセスすることを防ぐために必要な制御を実装します。

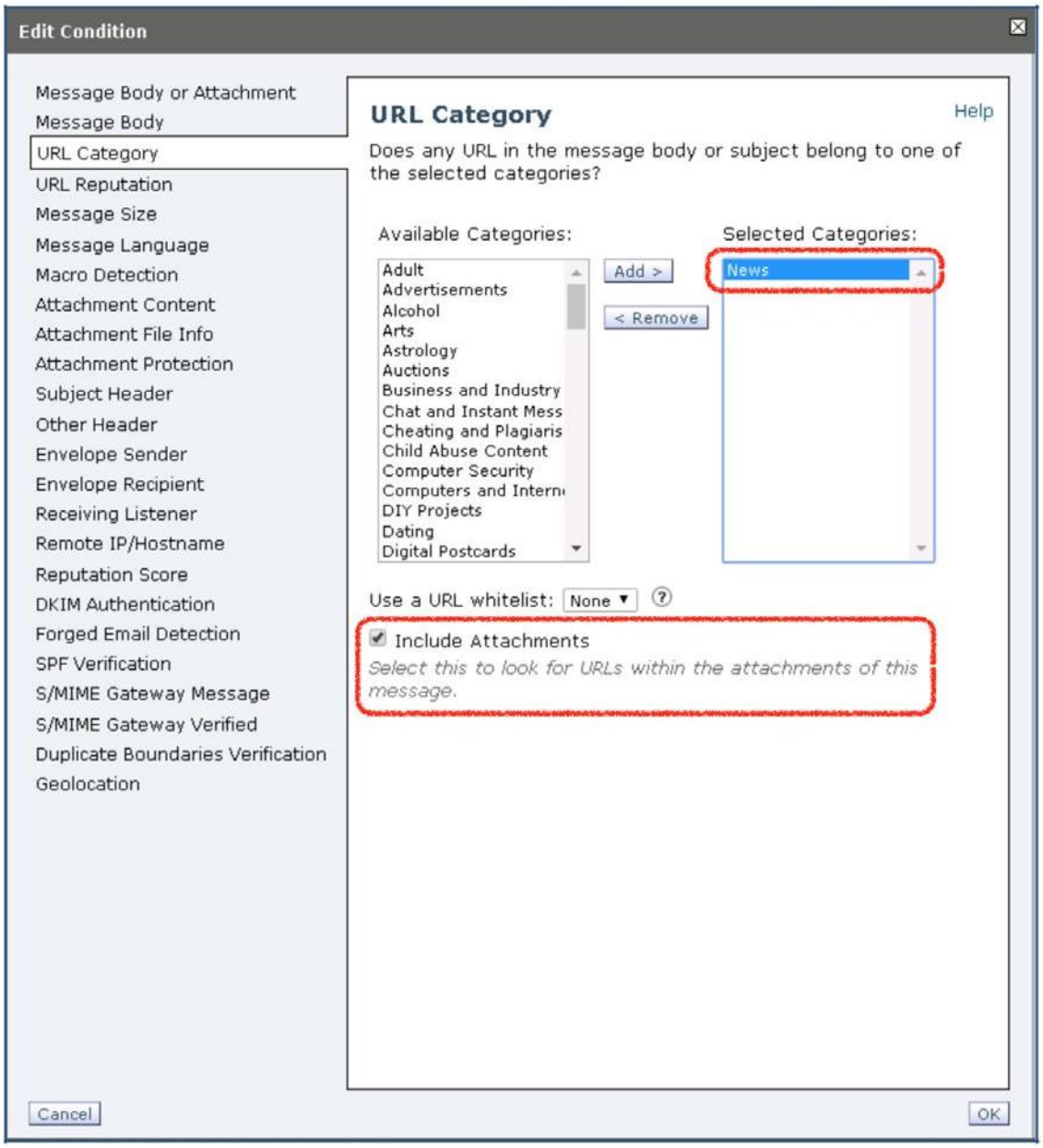
コンテンツ フィルタを設定する（推定所要時間：10 分）

コンテンツ フィルタは、ウイルス対策スキャン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。

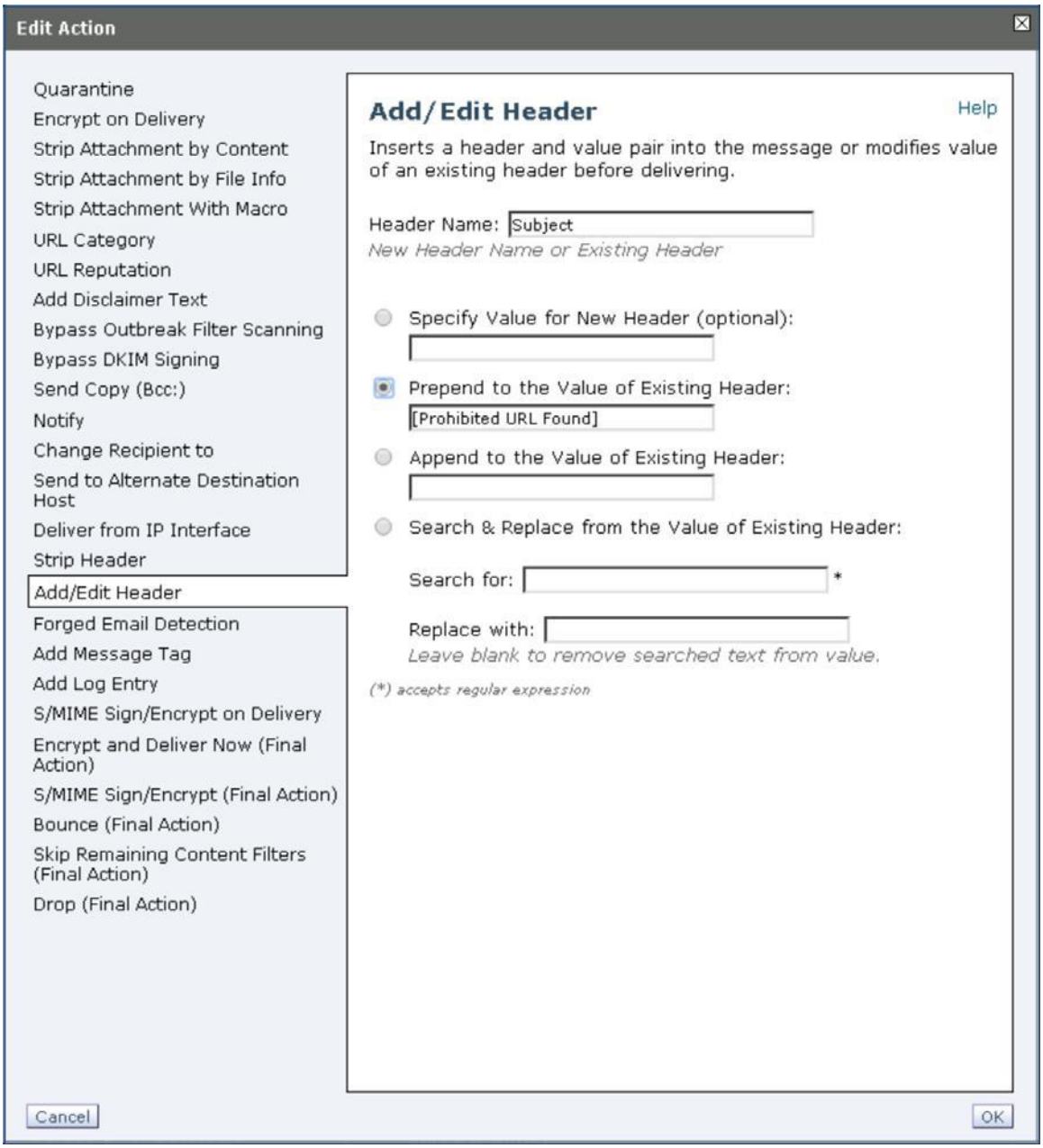
このタスクでは、メール添付のファイル内の悪意のある、または望ましくない可能性のある URL を特定し、そのメッセージに対して適切なアクションを取るコンテンツ フィルタを新規作成します。

1. ワークステーションから ESA の 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：	Attachment_URL_CF
説明：	添付ファイル内に禁止されている URL がある場合、ヘッダー前に付加します。
条件 1：	[URLカテゴリ（URL Category）] > [選択済みカテゴリ（Selected Categories）] > [ニュース（News）]	選択 > [添付ファイルを含める（Include Attachments）]
アクション 1：	[ヘッダーの追加と編集（Add/Edit Header）] > [ヘッダー名（Header Name）]：Subject > [既存ヘッダーの値の前に付加（Prepend to the Value of Existing Header）]：[Prohibited URL Found]（禁止されている URL が検出されました）

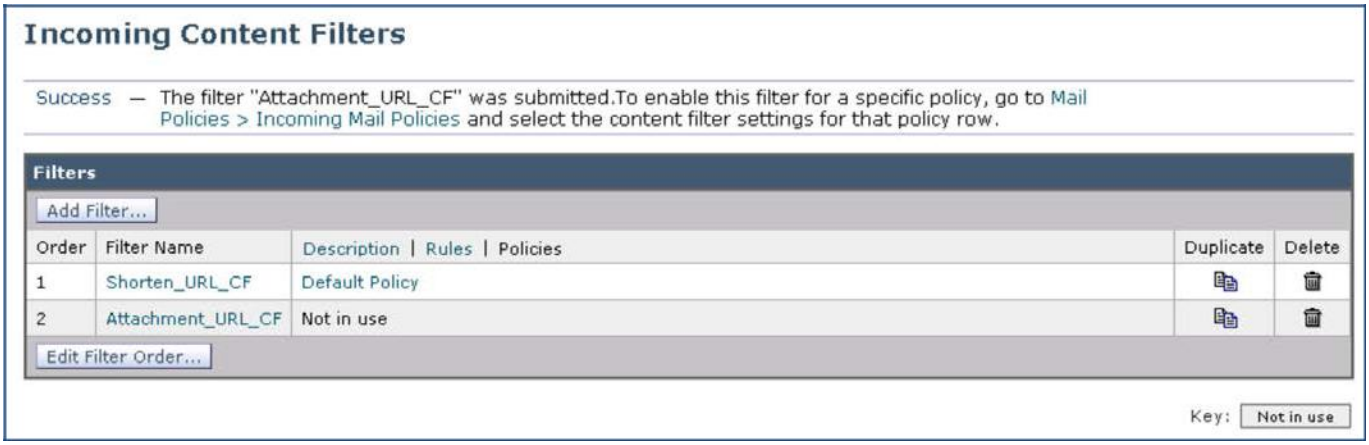


2. [OK] をクリックします。



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。

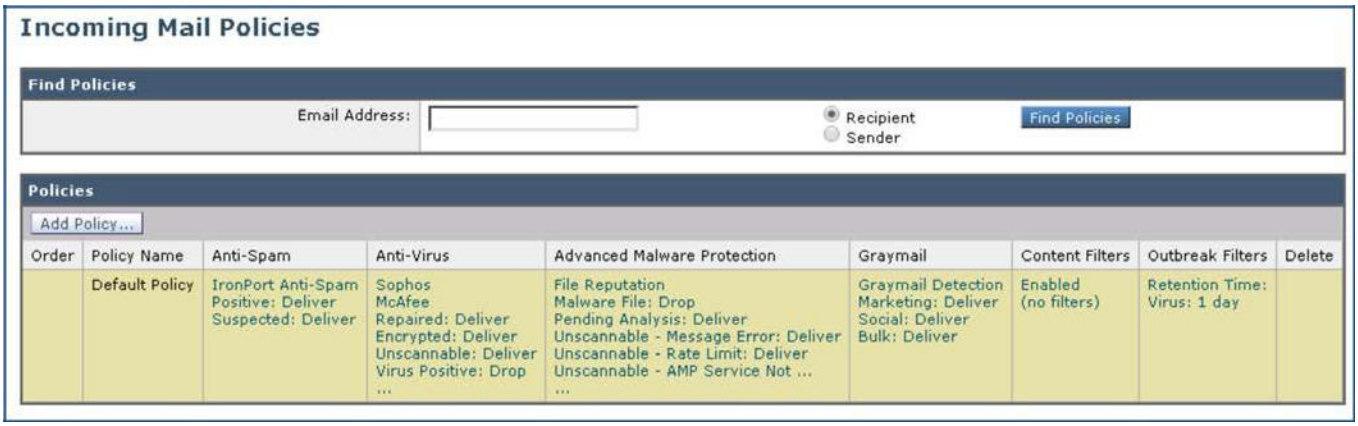


5. 完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

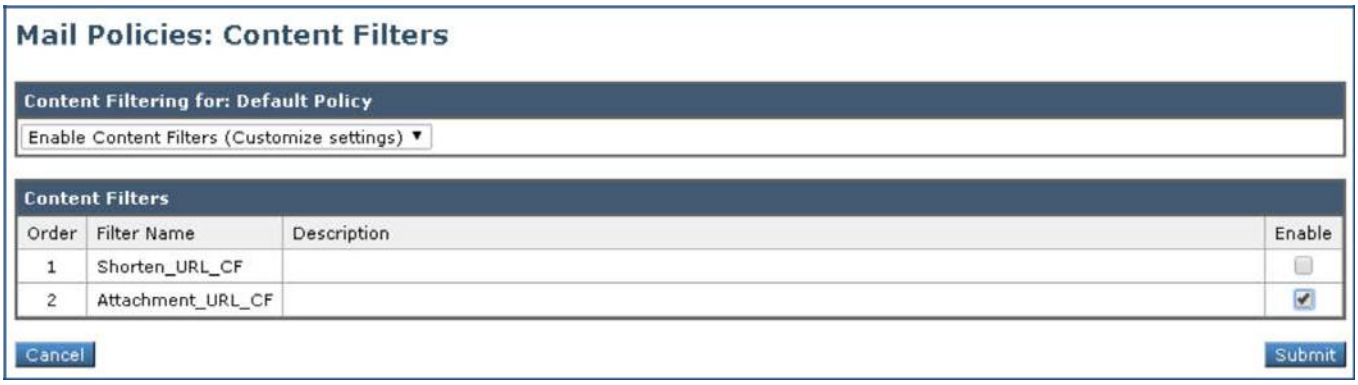
受信メール ポリシーを編集する（推定所要時間：3 分）

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。

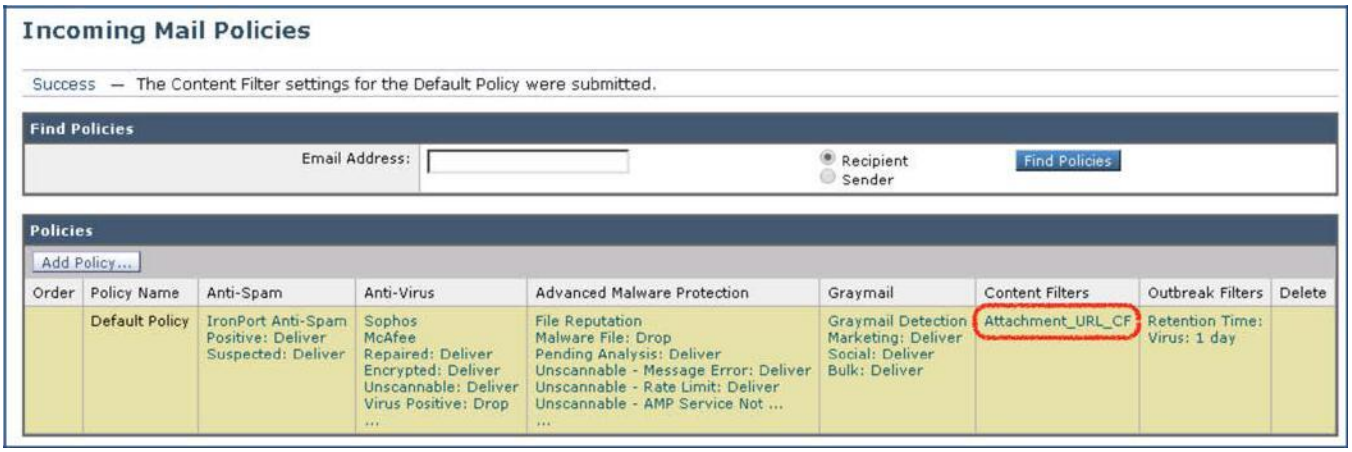
1. ワークステーションから ESA の GUI にアクセスし、[メールポリシー（Mail Policy）] > [受信メールポリシー（Incoming Mail Policies）] に移動して、[デフォルトポリシー（Default Policy）] の [コンテンツフィルタ（Content Filters）] ボックス内をクリックします。



2. 前の手順で作成した「Attachment_URL_CF」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。

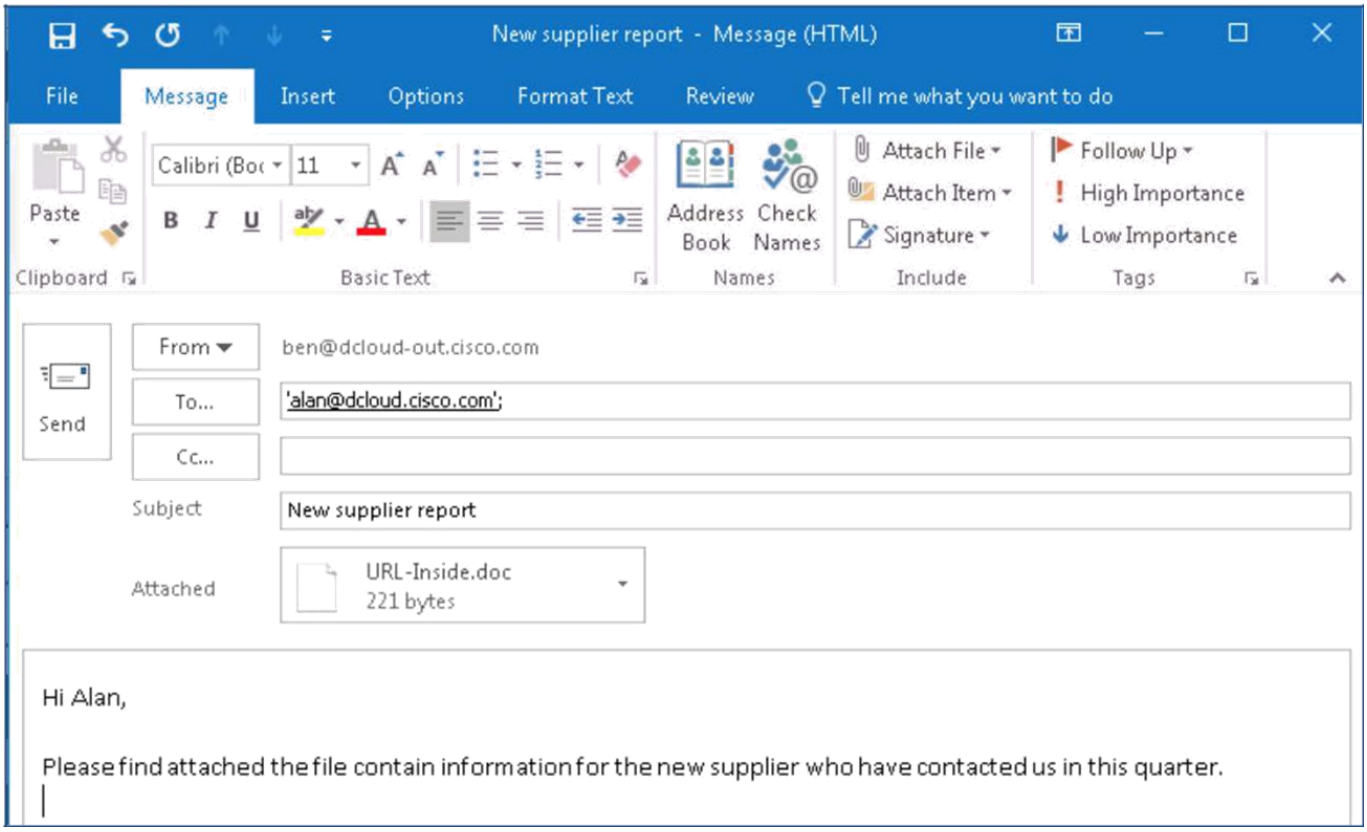
添付ファイルの URL フィルタリングをテストする（推定所要時間：3 分）

前提条件となる構成が完了していれば、メッセージの添付ファイルに危険である可能性のある URL を含むメールを社外ユーザの Ben から Alan に送信することによって、添付ファイルの URL フィルタリング機能をテストできます。

メッセージを準備する前に、CLI を使用して ESA への接続を開始し、メール ログを表示します（ログの確認には「tail」コマンドを使います）。メッセージが一連のメール メッセージングの設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。

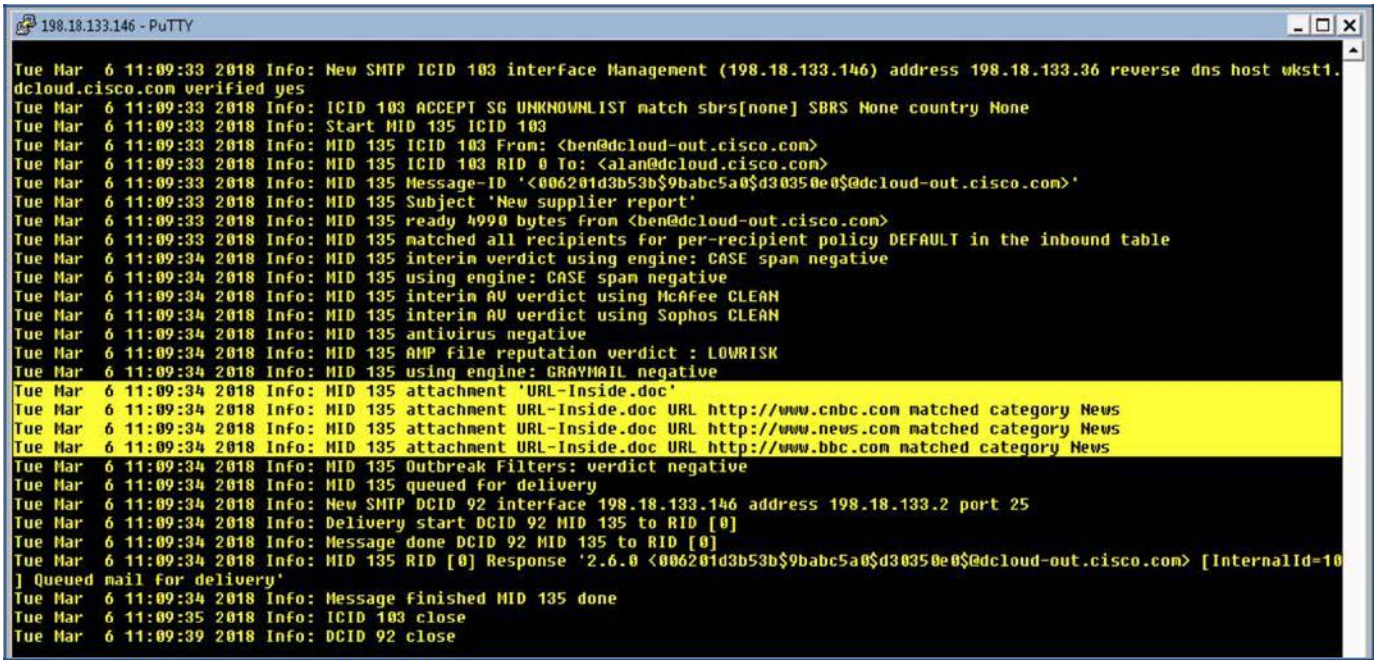
1. ワークステーションから Microsoft Outlook を起動し、Ben の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。

送信者：	ben@dcloud-out.cisco.com
受信者：	alan@dcloud.cisco.com
件名：	新しいサプライヤのレポート
本文：	こんにちは、Alan この四半期に連絡を受けた新しいサプライヤの情報が含まれるファイルを添付しましたので確認してください。（Please find attached the file contain information for the new suppliers who have contacted us in this quarter.）
添付ファイル：	デスクトップ上の **Attachment_URL** サブフォルダにある **URL-Inside.doc**

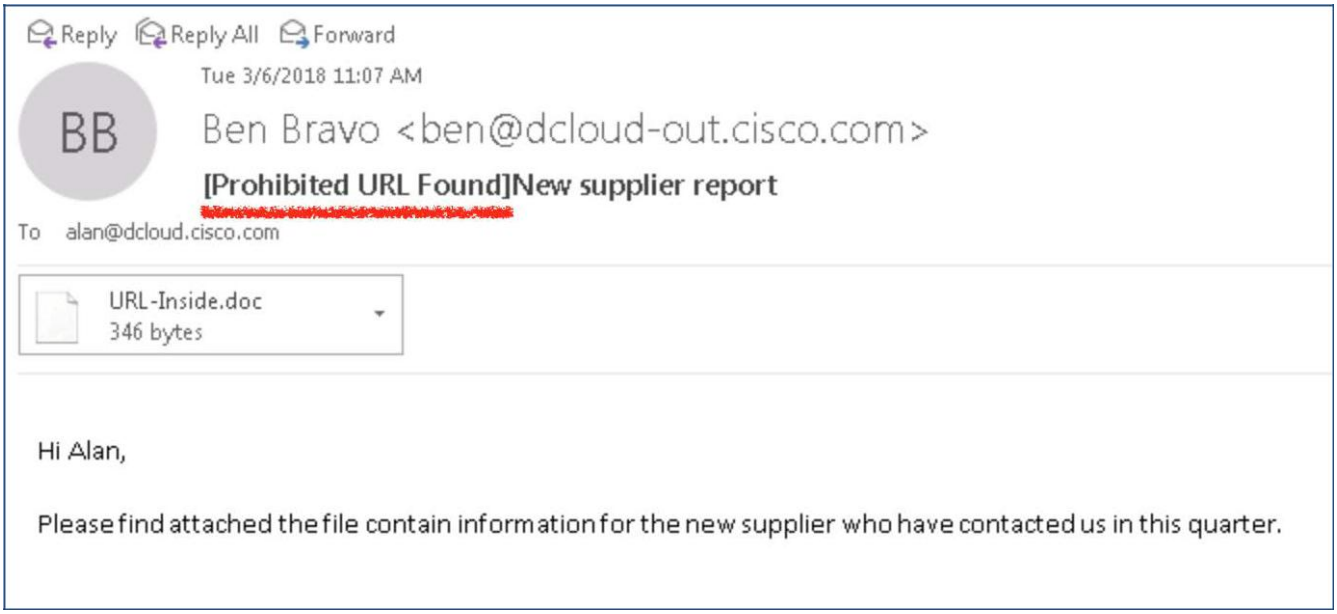


2. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

3. ESA の CLI に戻り、Attachment_URL_CF コンテンツ フィルタ ルールがメールの添付ファイルをどのように処理したかを確認します。このルールは、コンテンツ フィルタの条件で選択した Web のカテゴリに基づいて、元の件名ヘッダーの前に [Prohibited URL Found] を追加します。



4. Alan の受信トレイに戻り、件名がどのように変更されたかを確認します。件名の前に [Prohibited URL Found] というテキストが追加され、メッセージの受信者が、添付されたドキュメント内で何かが禁止されたことにすぐに気が付くようになっています。



シナリオ 3:　スキャン不能のメッセージをインテリジェントに処理する

ユースケース

IT 部門は、所定のさまざまなシステムで記録されない潜在的な問題を直ちに特定するために、すべてのログを定期的にレビューしています。ある若手のメール管理者がメールに関するすべてのログのレビューを任され、Microsoft Exchange で構築したオンプレミスのメッセージング サーバから Cisco E メール セキュリティ ソリューションまでのログに目を通しています。

ある定期的なレビュー中に、この管理者はこれまでに見たことのない「MID 274 は RFC 違反のため「スキャン不能」のマークが付けられました（MID 274 was marked Unscannable due to RFC violation）」というメッセージの行があることに気が付きます。初めて記録されたメッセージであったため、経験のあるメール管理者に相談したところ、そのベテランの管理者は、このメッセージは Cisco E メール セキュリティのスキャン エンジンの検査をすり抜け、内部システムを侵害した可能性があるとすぐに懸念を示しました。

未解決の問題を議論する社内のチーム会議の後、Cisco AsyncOS v11.1 で「スキャン不能」の機能を有効にすることが決定されました。

セキュリティ制御

不正な形式のヘッダーを持つメール、または複数に分かれたメッセージと宣言しているもののその一部や区切り文字が不足しているメールは、メール メッセージの Request for Comments（RFC）に違反していると見なされます。

Cisco E メール セキュリティでは、「スキャン不能」の条件によってメール メッセージを特定し、管理者が指定したアクションを実行するという予防措置を講じることができます。

目的

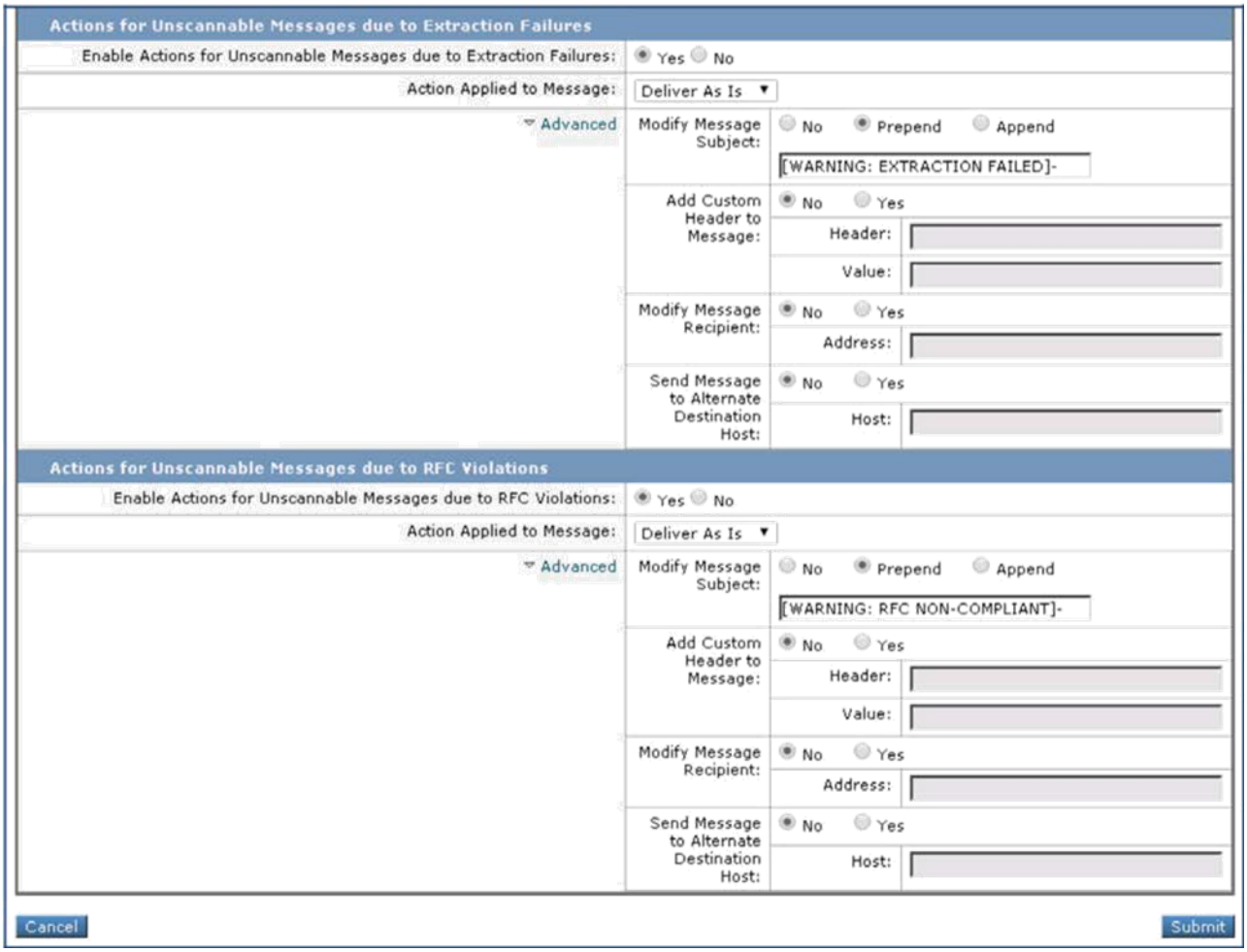
このシナリオでは Cisco E メール セキュリティの基本のオペレーティング システムに、RFC 違反のメール メッセージをインテリジェントに検出する機能を直接組み込む方法を示します。

スキャンの動作を構成する（推定所要時間：1 分）

このタスクでは、[スキャンの動作（Scan Behaviour）] グローバル設定での展開失敗と RFC 違反の条件に基づいて追加の「スキャン不能」の設定が有効になります。

1. ワークステーションから ESA の GUI にアクセスして [セキュリティサービス（Security Services）] に移動し、[スキャンの動作（Scan Behavior）] をクリックします。[グローバル設定の編集（Edit Global Setting）] をクリックし、次の設定を使用して、展開失敗と RFC 違反が原因でスキャンできないメッセージに対する *アクション* を構成します。

名前:	展開失敗によりスキャン不能なメッセージに対するアクション
アクション 1:	[はい(Yes)] > [送信(Deliver As Is)]
[詳細設定(Advanced)]をクリック:	件名の前にメッセージを追加 > [WARNING: UNSCANNABLE EXTRACTION FAILED](警告:展開できないためスキャン不能)
名前:	RFC 違反によりスキャン不能なメッセージに対するアクション
アクション 1:	[はい(Yes)] > [送信(Deliver As Is)]
[詳細設定(Advanced)]をクリック:	件名の前にメッセージを追加 > [WARNING: UNSCANNABLE RFC NON-COMPLIANT](警告:RFC に準拠していないためスキャン不能)



2. [送信(Submit)] をクリックします。
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。

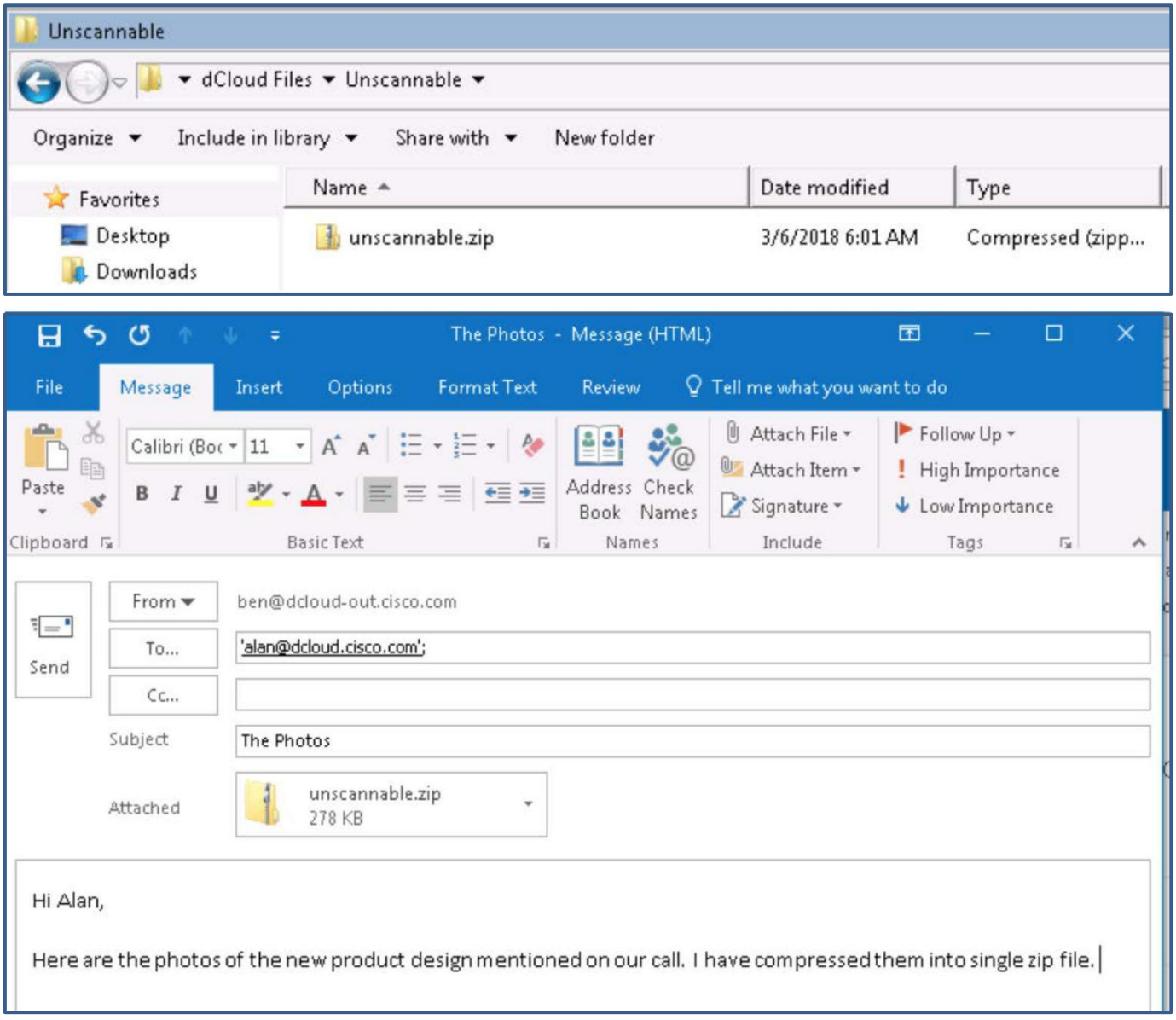
スキャン不能なメッセージの検出をテストする（推定所要時間：5 分）

Cisco E メール セキュリティが、スキャンできないファイル、または不正な形式メッセージをどのように処理するのかをデモンストレーションするには、Ben 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。

1. メッセージを準備する前に、CLI を使用して ESA への接続を開始し、メール ログを表示します（ログの確認には「tail」コマンドを使います）。メッセージが一連の設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。

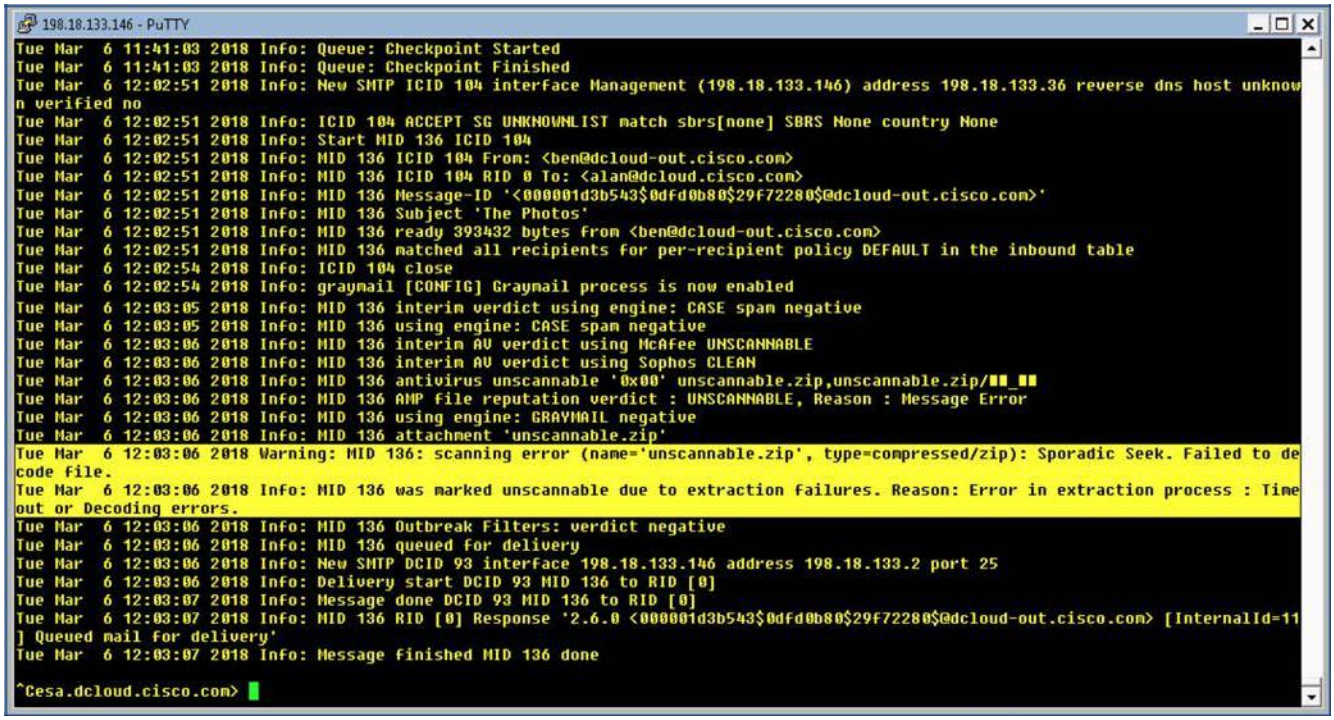
2. デスクトップから Outlook を起動し、Ben のメールボックスから、次のパラメータを使用してメールを作成します。

送信者：	ben@dcloud-out.cisco.com
受信者：	alan@dcloud.cisco.com
件名：	写真
本文：	電話で話した新しい製品に関するデザインの写真です。1 つの zip ファイルにまとめて圧縮しています。
添付：	デスクトップ上の Unscannable サブフォルダにある unscannable.zip。

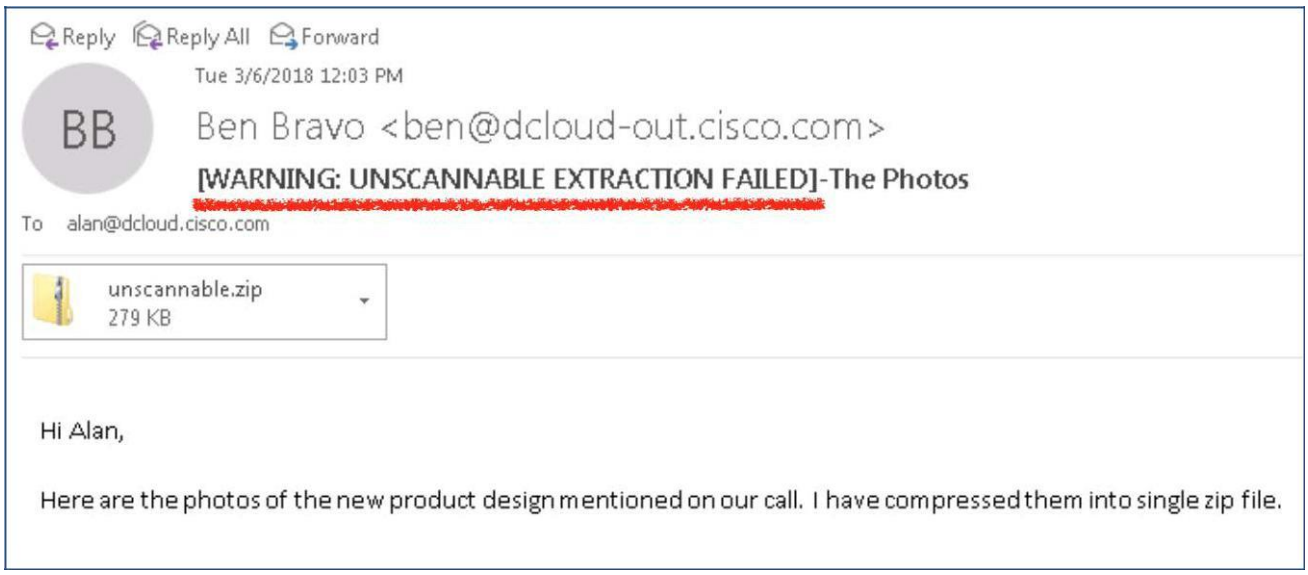


3. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

4. 開いたままにしておいた CLI シェルに移動し、ファイルがスキャンできない旨のログ メッセージを探します。添付ファイルが展開の失敗によりスキャン不能としてマークされたこととその理由をメール ログの詳細で確認してください。



5. 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 Alan のメール ボックスに表示されます。以前に [スキャンの動作（Scan Behavior）] で設定したテキストが件名のヘッダーに追加されていることを確認できます。



シナリオ 4:　事前分類の強化によって AMP クラウドのインテリジェンスを活用する

ユースケース

会社の予測どおりメールの量が大幅に増加し、結果的にメールを介して社内に流入するファイルの数も増加しました。Voyage Corp 社は、複数のスキャン エンジンに多額の投資を行いましたが、その後特定のファイルが、分析を行う Cisco ThreatGrid（TG）に送信されないことが分かりました。

この問題を調査したところ、アップロードの制限に達したことにより、その制限を超えたファイルが分析されなかったことが判明しました。シスコ アカウント チームは選択肢として追加のサンプル パックの購入を提示しましたが、これには、営業部門の資金提供が必要なうえ承認に数週間かかります。

メール管理者は、改善された Cisco AsyncOS v11.1 の事前分類エンジンを活用するという暫定的な解決策を提案しました。これにより、エンド ユーザを侵害しかねない動的コンテンツがファイルに含まれる場合に、送信して分析と早期の判断を行う必要のあるファイルの数を、Cisco E メール セキュリティ ソリューションで大幅に削減できます。

セキュリティ制御

AMP の事前分類機能では、悪意のあるファイル内に存在することが多いメタデータ フィールドのプロパティをチェックします。一般的な例は、ドキュメントに埋め込まれたスクリプトです。悪意のあるドキュメントの大半にスクリプトまたはマクロが含まれていますが、多くのクリーンなドキュメントにはそれらが含まれていません。こうしたヒューリスティックの目的は、悪意の有無を判定するために綿密に調査（例：サンドボックス）すべきファイルを特定することです。

目的

このシナリオでは、AMP 事前分類によって、クラウド インテリジェンスを活用し、受信したメールの添付ファイルに含まれるアクティブ コンテンツや動的コンテンツを判定する方法のほか、サポート対象ファイルを増やすだけでなく TG アナリストが低リスクファイルを分析する時間を削減できる機能を示します。

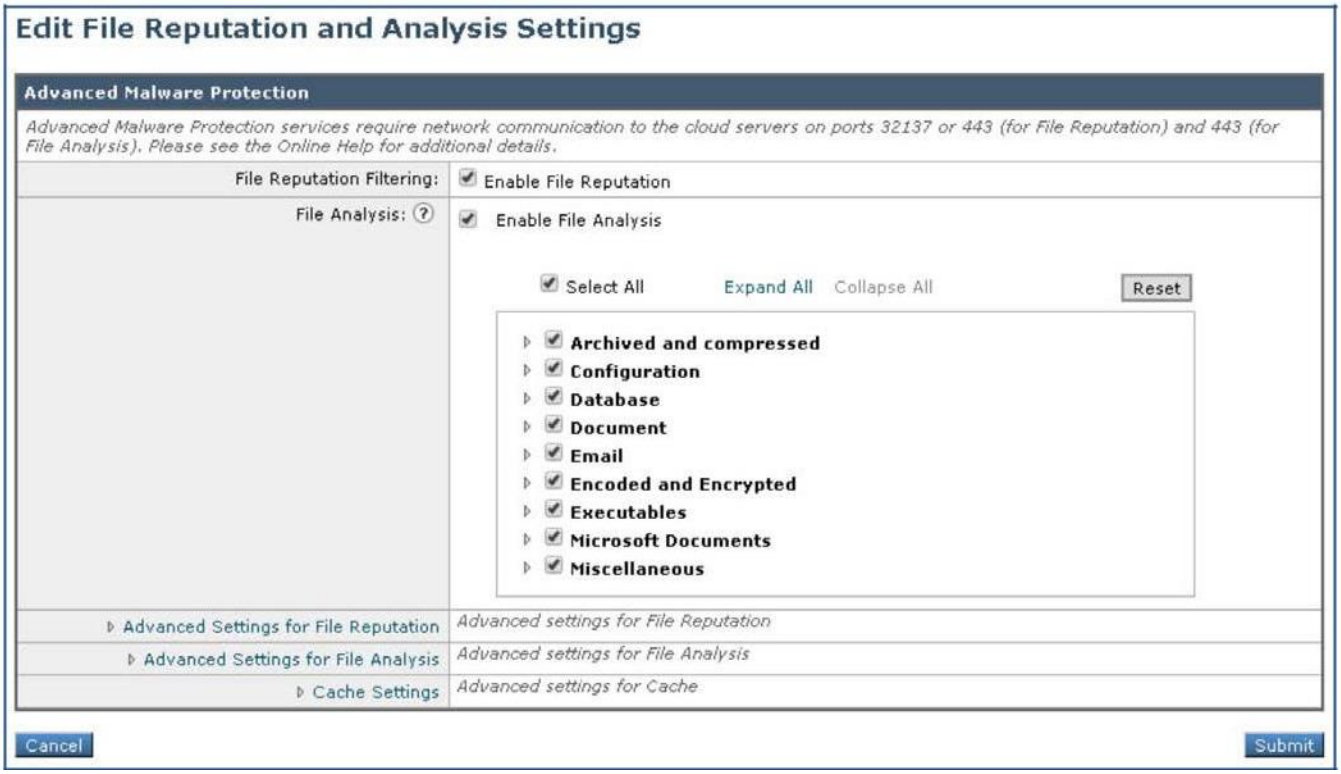
注：高度なマルウェア防御の詳細については、「Advanced Malware Protection」を参照してください。

サポート対象ファイルの種類を選択する（推定所要時間：1 分）

サポート対象ファイルの種類が 380 以上に拡張されたほか、AMP 事前分類の向上によって、メタデータ フィールドにスクリプトやマクロを含む不明なファイルが組み込まれているかどうかを判断したり、パイプラインの次の検査レイヤに安全に渡すことのできる静的コンテンツ ファイルのみをすばやく検出したりすることができます。

1. ワークステーションから ESA の GUI にアクセスして [セキュリティ サービス（Security Services）] に移動し、[ファイルレピュテーションと分析（File Reputation and Analysis）] をクリックします。[グローバル設定の編集（Edit Global Setting）] をクリックし、次の設定を使用して [ファイル分析（File Analysis）] セクション内のサポート対象ファイルの種類を選択します。

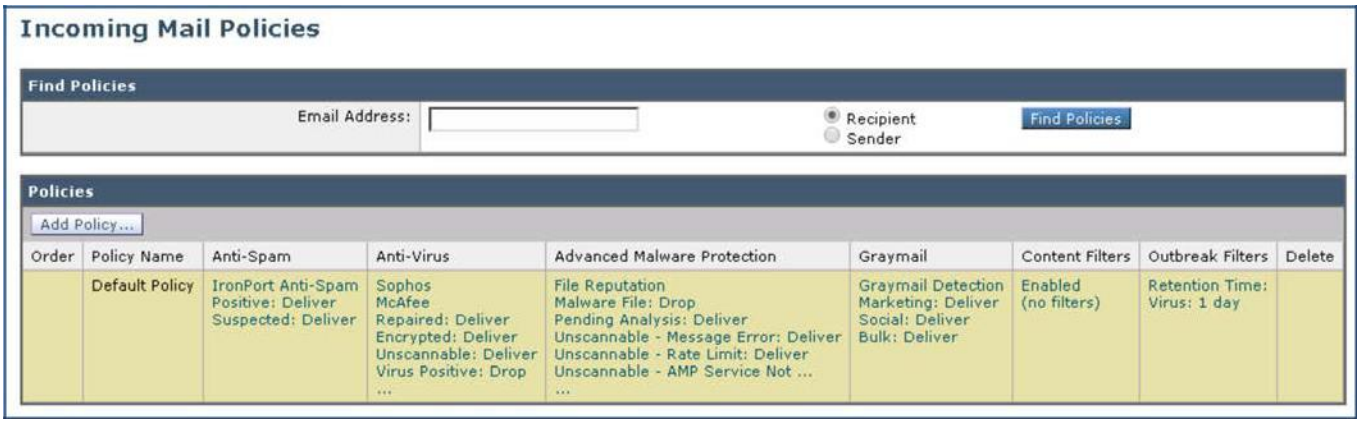
名前:	ファイル分析
アクション 1:	[ファイル解析を有効にする(Enable File Analysis)] を選択します。
アクション 2:	[すべてを選択(Select All)] をクリックします。



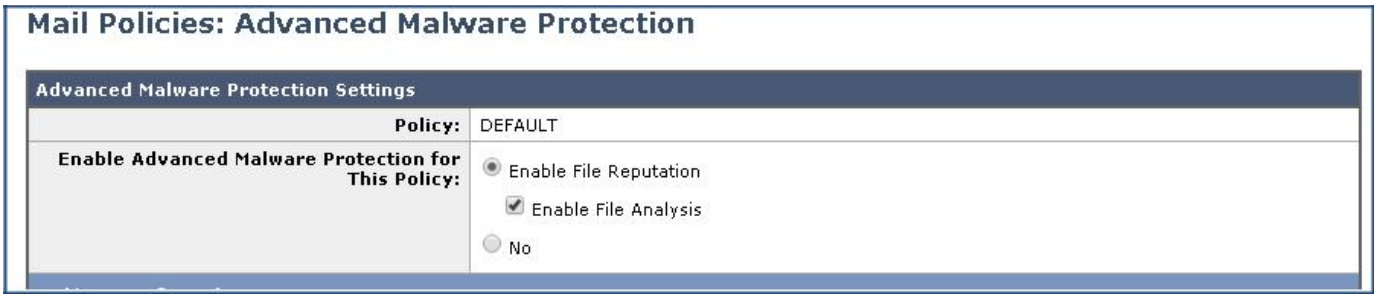
2. [送信(Submit)] をクリックします。
3. 完了したら画面の右上にある [変更内容を確定(Commit Changes)] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

受信メール ポリシーを編集する(推定所要時間:3 分)

1. デフォルト ポリシーを編集し、Cisco AMP クラウドに分析目的で送信したファイルが添付されていたメッセージに適用するアクションを変更します。
2. ワークステーションから ESA の 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 [送信（Deliver As Is）] 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。

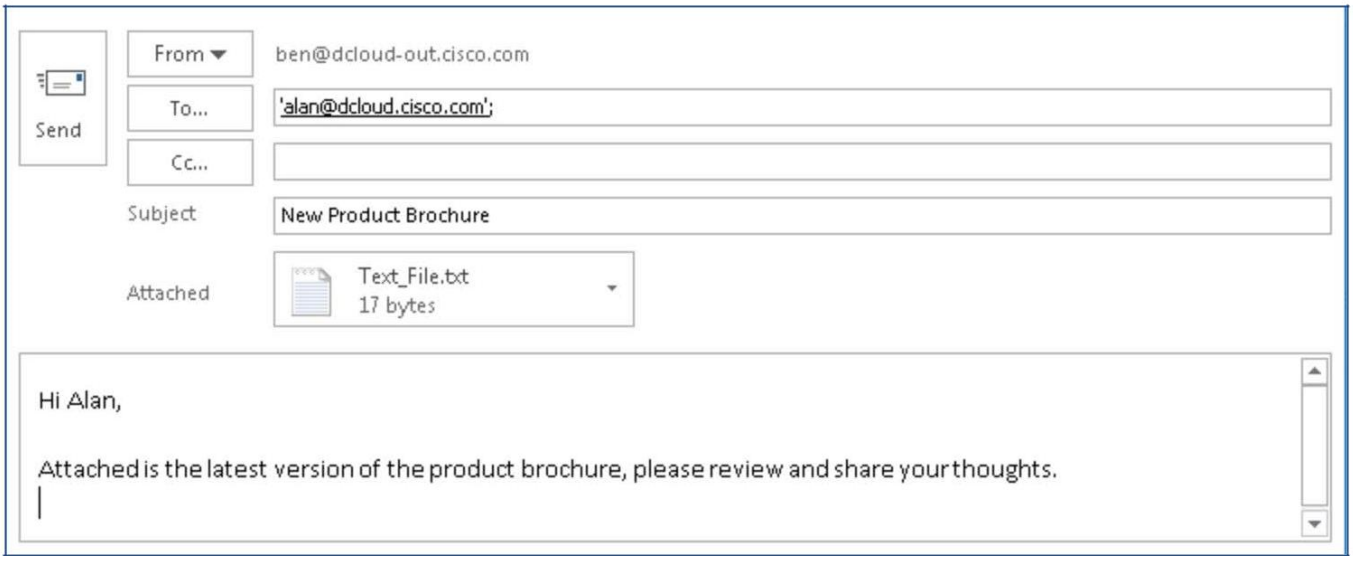
クリーン ファイルが添付されたメッセージを送信する（推定所要時間：3 分）

ここで、テキスト ファイルを添付して Ben から Alan にメッセージを送信します。これだけで、AMP 事前分類が開始され、必要な判定が行われます。

1. メッセージを準備する前に、CLI を使用して ESA への接続を開始し、メール ログを表示します（ログの確認には「tail」コマンドを使います）。メッセージが一連の設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。

2. ワークステーションから Microsoft Outlook を起動し、Ben 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。

送信者:	ben@dcloud-out.cisco.com
受信者:	alan@dcloud.cisco.com
件名:	製品の新しいパンフレット
本文:	こんにちは、Alan 最新バージョンの製品パンフレットを添付しました。確認して、意見を聞かせてください。(Attached is the latest version of the product brochure, please review it and share your thoughts.)
添付:	デスクトップ上の AMP_Preclass > Low Risk サブフォルダにある次の Text_File.txt ファイルを添付します。

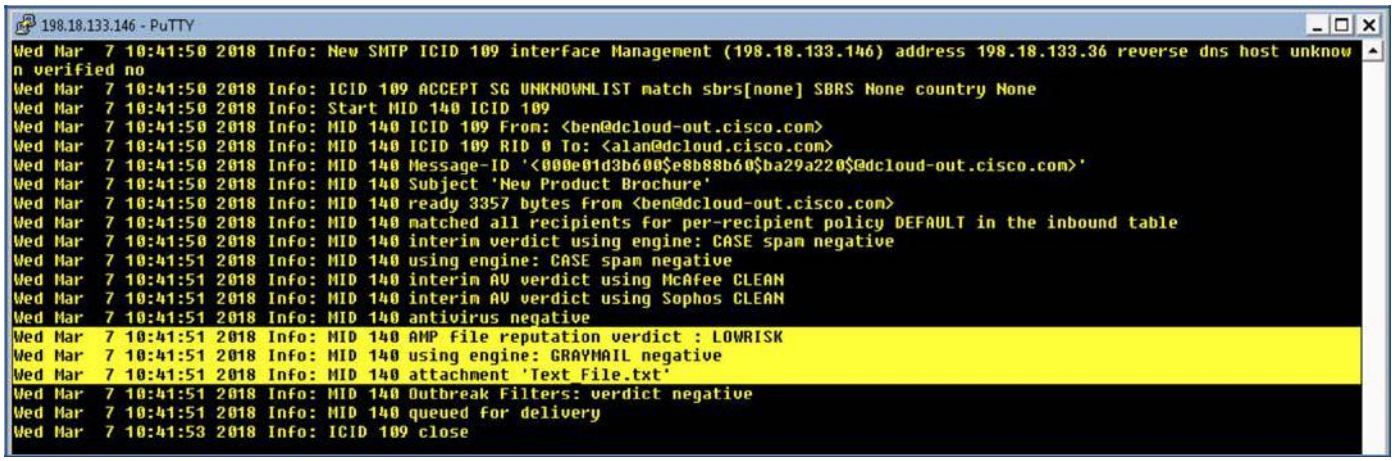


3. メッセージを送信します。[すべてのフォルダを送受信(Send/Receive All Folders)] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

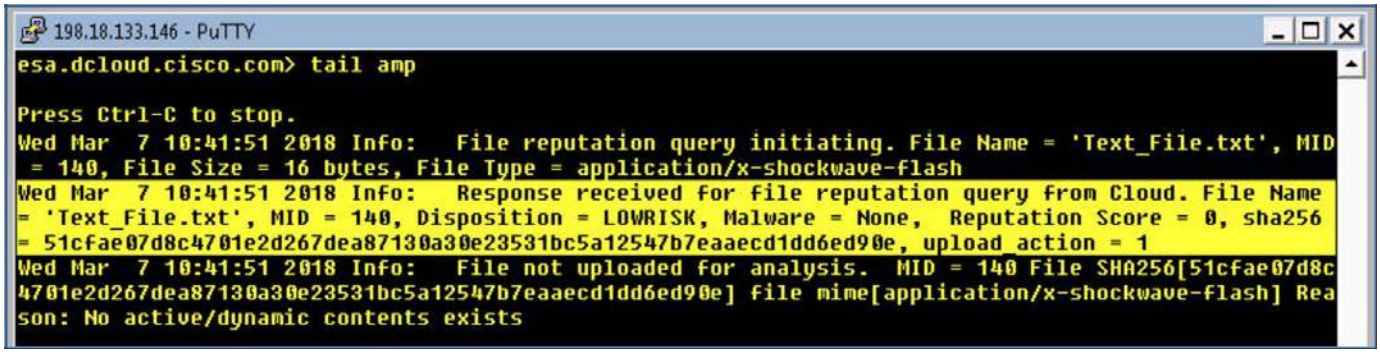
テキスト ファイルに対する AMP のアクションをモニタする(推定所要時間:15 分)

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、強化された AMP の事前分類エンジンによって、プレーン テキスト ファイルがどのように処理されるのかを示します。

1. ESA の 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。
2. 次のログで強調表示されている行とその前の行によってファイル レピュテーションの判定が LOWRISK(低リスク)であることが分かります。したがって、このファイルは分析目的で送信されることはなく、同じ受信メール ポリシーの残りの検査レイヤーに直ちに転送されます。



3. 同じ CLI セッションで **tail amp** コマンドを入力し Enter キーを押します。AMP のログは、AMP クラウドからクエリが返ったことと、アクティブ コンテンツまたは動的コンテンツが存在しないと判定されたためファイルが分析用にアップロードされないことを明らかに示しています。

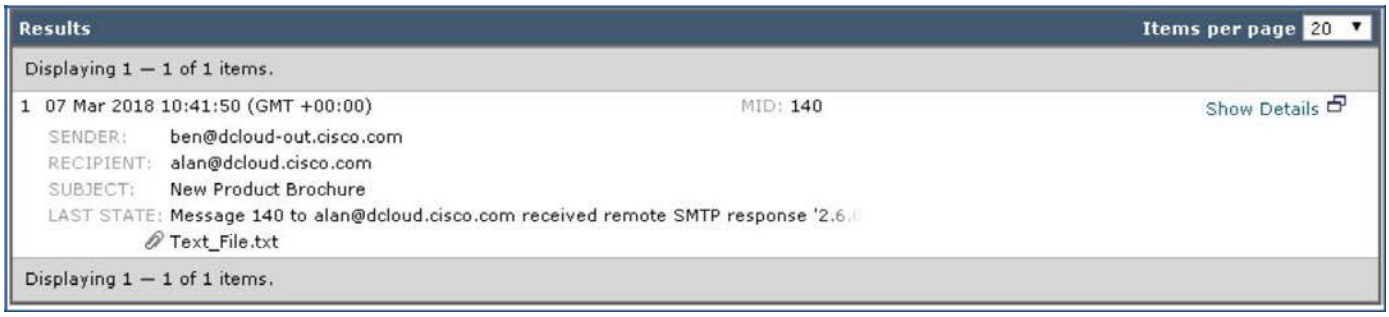


4. Alan の受信トレイに移動し、[すべてのフォルダを送受信（Send/Receive All Folders）] をクリック、または **F9** キーを 2 ～ 3 回押して、メール クライアントを同期させます。

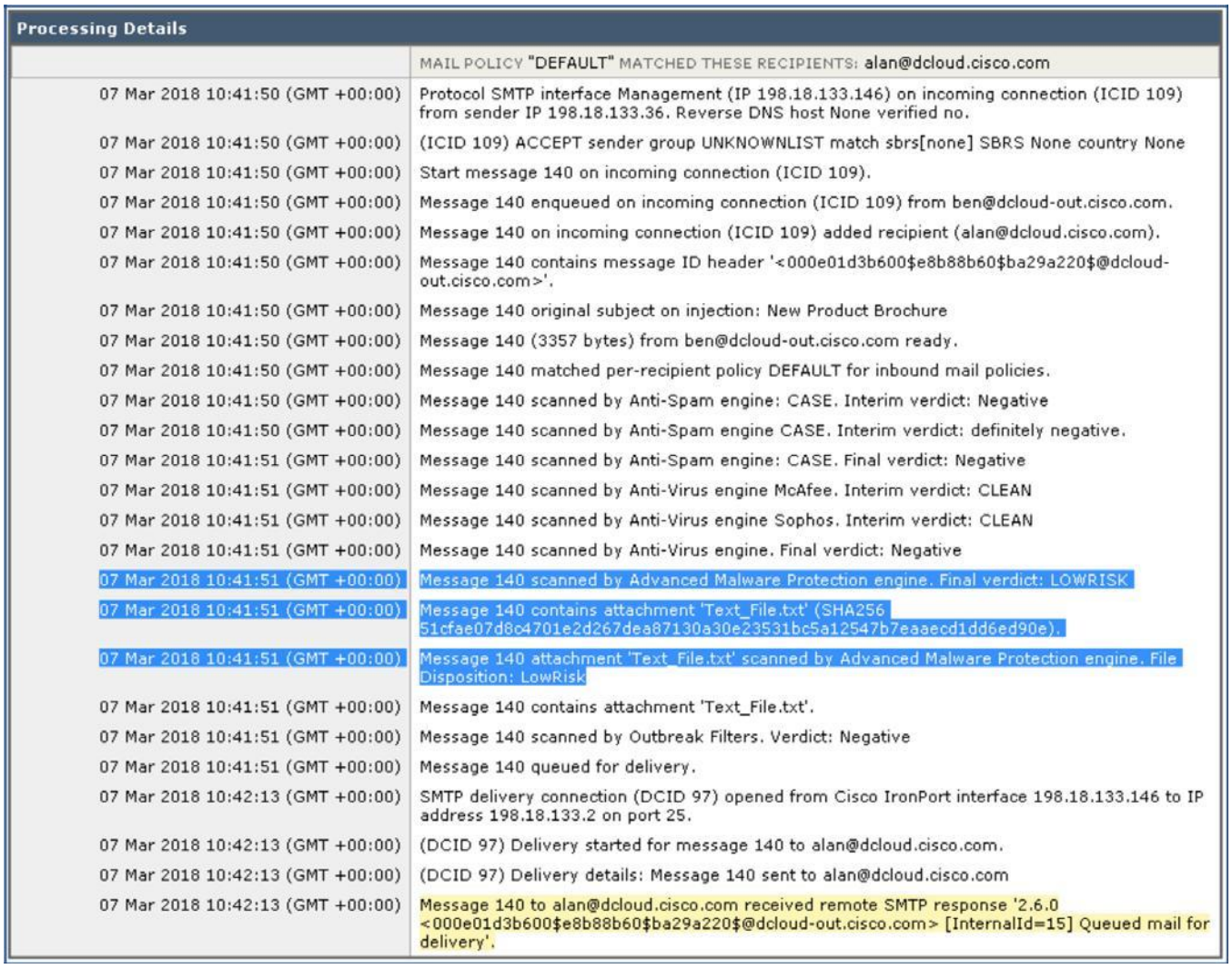
5. 判定結果が LOWRISK（低リスク）に設定されているため、Text_File.txt が添付されたメールは Alan のメール ボックスに配信されますが、想定内の動作です。添付ファイルを開いて、テキスト ファイルのコンテンツを表示します。コンテンツが正常に表示され、電子メールのメッセージも変更されることはありません。

6. ESA の GUI セッションで [モニタ（Monitor）] > [高度なマルウェア防御（Advanced Malware Protection）] レポートに移動すると、AMP が処理したファイルの概要に判定結果 [LowRisk] のインシデントが記録されています。

7. 判定結果 [LowRisk] 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。



8. [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。



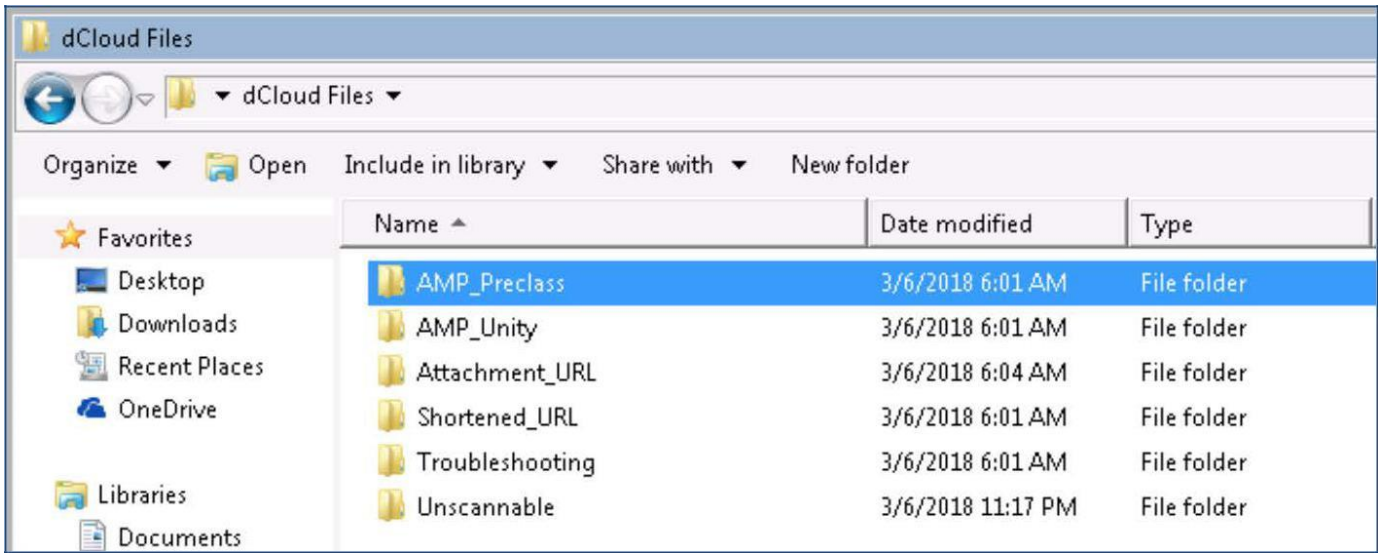
Processing Details

	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: alan@dcloud.cisco.com
07 Mar 2018 10:41:50 (GMT +00:00)	Protocol SMTP interface Management (IP 198.18.133.146) on incoming connection (ICID 109) from sender IP 198.18.133.36. Reverse DNS host None verified no.
07 Mar 2018 10:41:50 (GMT +00:00)	(ICID 109) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS None country None
07 Mar 2018 10:41:50 (GMT +00:00)	Start message 140 on incoming connection (ICID 109).
07 Mar 2018 10:41:50 (GMT +00:00)	Message 140 enqueued on incoming connection (ICID 109) from ben@dcloud-out.cisco.com.
07 Mar 2018 10:41:50 (GMT +00:00)	Message 140 on incoming connection (ICID 109) added recipient (alan@dcloud.cisco.com).
07 Mar 2018 10:41:50 (GMT +00:00)	Message 140 contains message ID header '<000e01d3b600$e8b88b60$ba29a220$@dcloud-out.cisco.com>'.
07 Mar 2018 10:41:50 (GMT +00:00)	Message 140 original subject on injection: New Product Brochure
07 Mar 2018 10:41:50 (GMT +00:00)	Message 140 (3357 bytes) from ben@dcloud-out.cisco.com ready.
07 Mar 2018 10:41:50 (GMT +00:00)	Message 140 matched per-recipient policy DEFAULT for inbound mail policies.
07 Mar 2018 10:41:50 (GMT +00:00)	Message 140 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
07 Mar 2018 10:41:50 (GMT +00:00)	Message 140 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 scanned by Anti-Spam engine: CASE. Final verdict: Negative
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 scanned by Anti-Virus engine McAfee. Interim verdict: CLEAN
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 scanned by Anti-Virus engine. Final verdict: Negative
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 scanned by Advanced Malware Protection engine. Final verdict: LOWRISK
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 contains attachment 'Text_File.txt' (SHA256 51cfae07d8c4701e2d267dea87130a30e23531bc5a12547b7eaaecd1dd6ed90e).
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 attachment 'Text_File.txt' scanned by Advanced Malware Protection engine. File Disposition: LowRisk
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 contains attachment 'Text_File.txt'.
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 scanned by Outbreak Filters. Verdict: Negative
07 Mar 2018 10:41:51 (GMT +00:00)	Message 140 queued for delivery.
07 Mar 2018 10:42:13 (GMT +00:00)	SMTP delivery connection (DCID 97) opened from Cisco IronPort interface 198.18.133.146 to IP address 198.18.133.2 on port 25.
07 Mar 2018 10:42:13 (GMT +00:00)	(DCID 97) Delivery started for message 140 to alan@dcloud.cisco.com.
07 Mar 2018 10:42:13 (GMT +00:00)	(DCID 97) Delivery details: Message 140 sent to alan@dcloud.cisco.com
07 Mar 2018 10:42:13 (GMT +00:00)	Message 140 to alan@dcloud.cisco.com received remote SMTP response '2.6.0 <000e01d3b600$e8b88b60$ba29a220$@dcloud-out.cisco.com> [InternalId=15] Queued mail for delivery'.

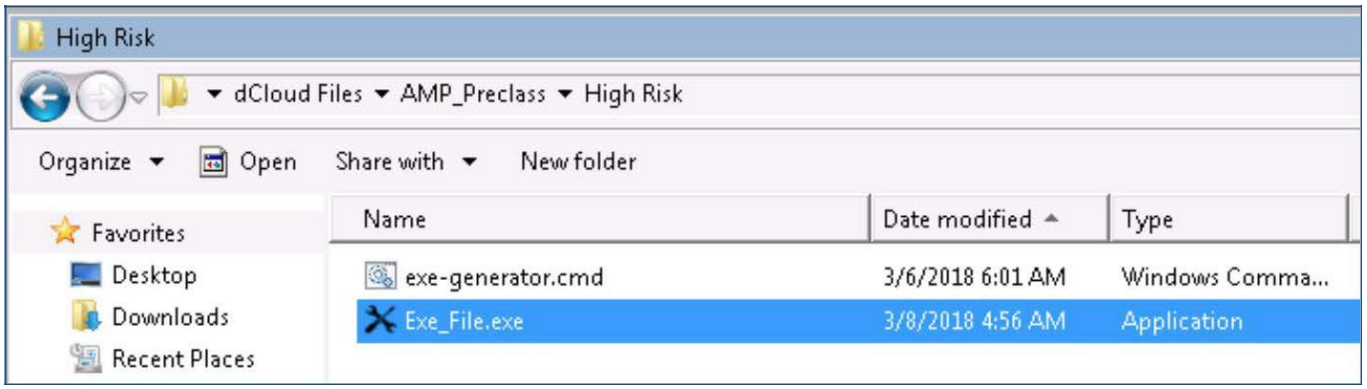
実行ファイルを作成する（推定所要時間：1 分）

AMP クラウドから得られるさまざまな判断をトリガーする実行ファイルが生成されます。

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き、フォルダの中にある「AMP_Preclass」というサブフォルダを開きます。



2. 「High Risk」というサブフォルダを開き **exe-generator.cmd** をダブルクリックし、表示された [実行（Run）] ボタンを確認してクリックします。正常に実行されると、Exe_File.exe という 2 つ目のファイルが生成されます。

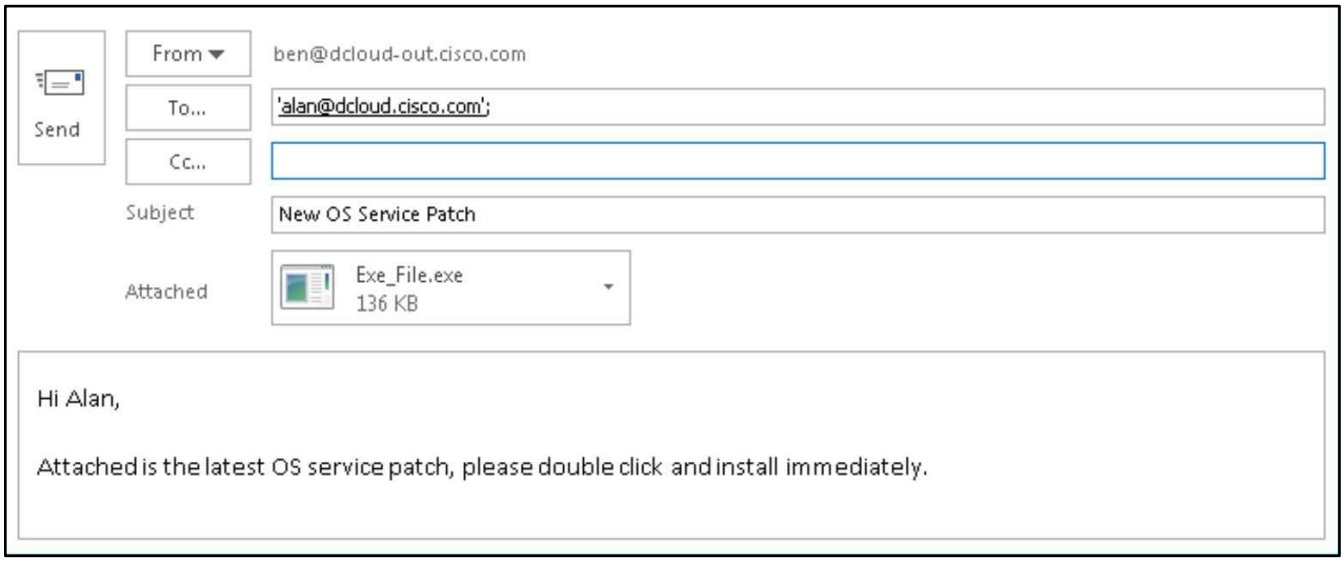


実行ファイルを含むメッセージを送信する（推定所要時間：3 分）

ここで、実行ファイルを添付して Ben から Alan にメッセージを送信します。これだけで、AMP 事前分類が開始され、必要な処理が行われます。

1. メッセージを準備する前に、CLI を使用して ESA への接続を開始し、メール ログを表示します（ログの確認には「tail」コマンドを使います）。メッセージが一連の設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。
2. ワークステーションから Microsoft Outlook を起動し、Ben 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。

送信者：	ben@dcloud-out.cisco.com
受信者：	alan@dcloud.cisco.com
件名：	OS の新しいサービス パッチ
本文：	こんにちは、Alan OS の最新のサービス パッチを添付します。ダブルクリックしてすぐにインストールしてください。（Attached is the latest OS service patch, please double click and install immediately.）
添付：	デスクトップ上の AMP_Preclass > High Risk サブフォルダにある Exe_File.exe。

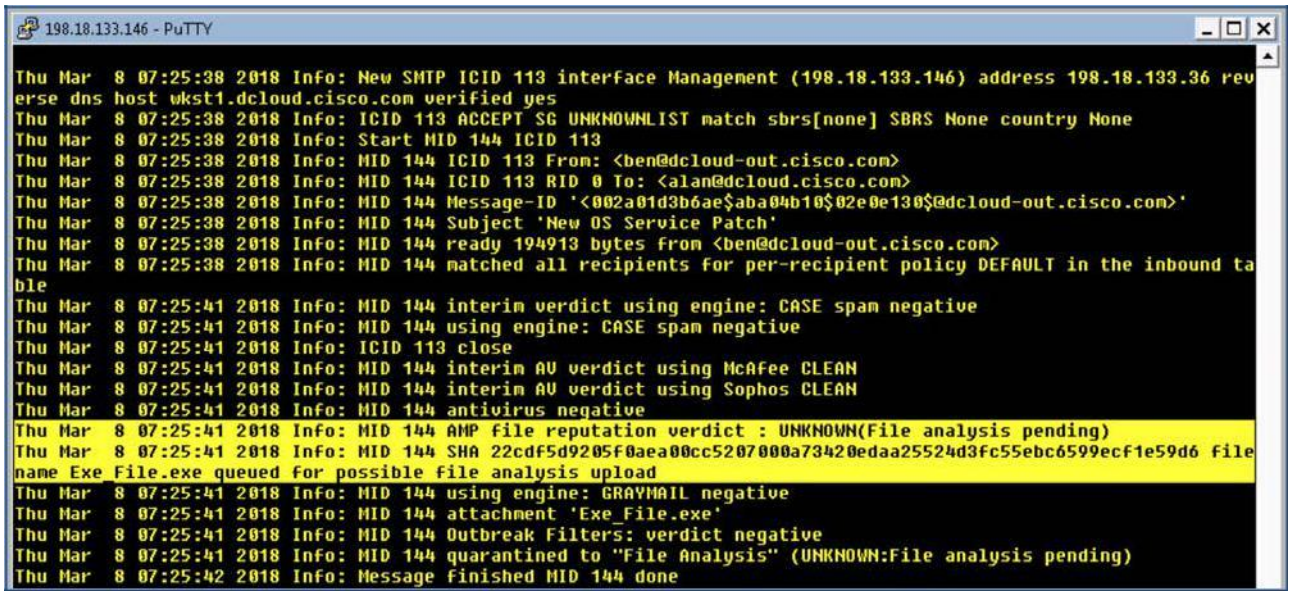


3. メッセージを送信します。Microsoft Outlook によって、安全ではないファイルに関する警告が表示されるので、[はい（Yes）] をクリックしてこの警告を無視します。[すべてのフォルダを送受信（Send/Receive All Folders）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

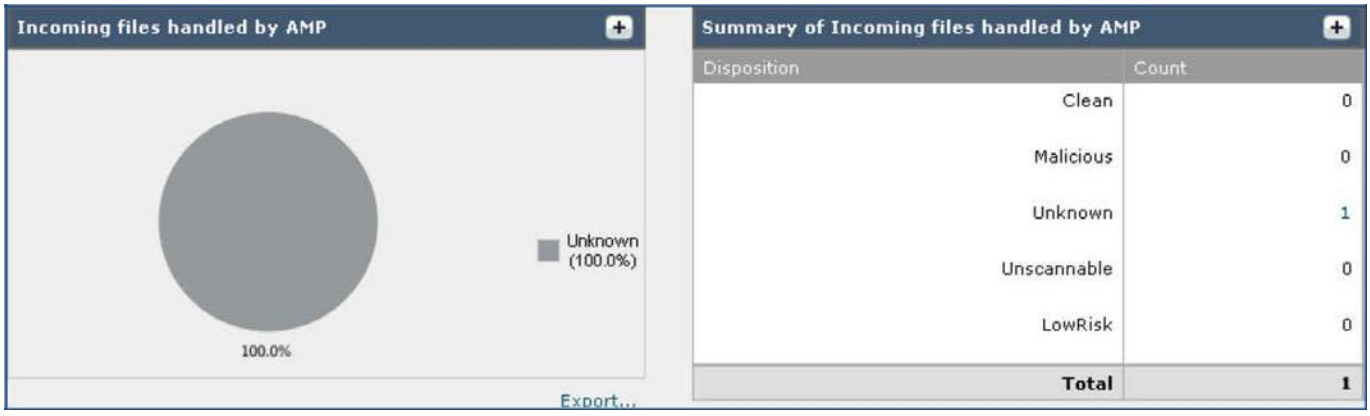
疑わしいファイルに対する AMP のアクションをモニタする（推定所要時間：5 分）

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、強化された AMP の事前分類エンジンによって、疑わしいファイルがどのように処理されるのかを示します。

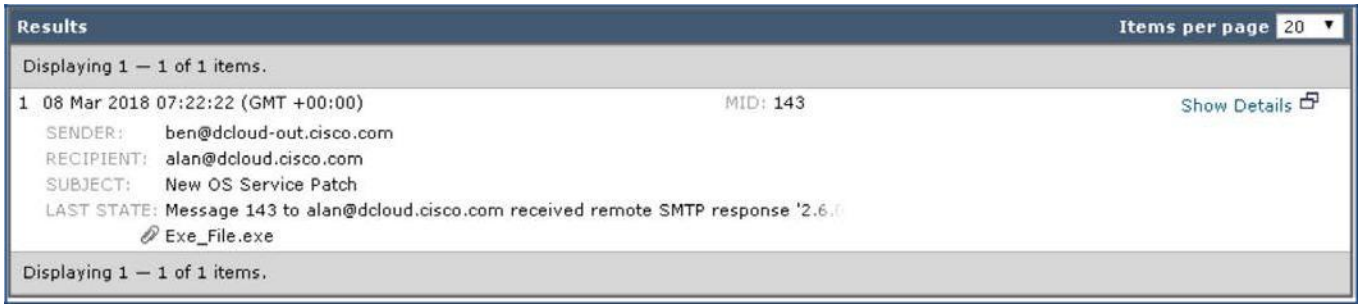
1. ESA の CLI セッションに移動し、ログがスクロールするまで待ちます。新しいアクティビティによって画面の表示が更新されるまでにしばらく時間がかかる場合があります。
2. 次のログの強調表示された行およびそれ以前の行は、ファイル レピュテーションの判定を示しています。判定が UNKNOWN（未知）であるため、ファイルは綿密な分析のために送信されます。またこのとき、SHA256 が割り当てられていることにも注意してください。



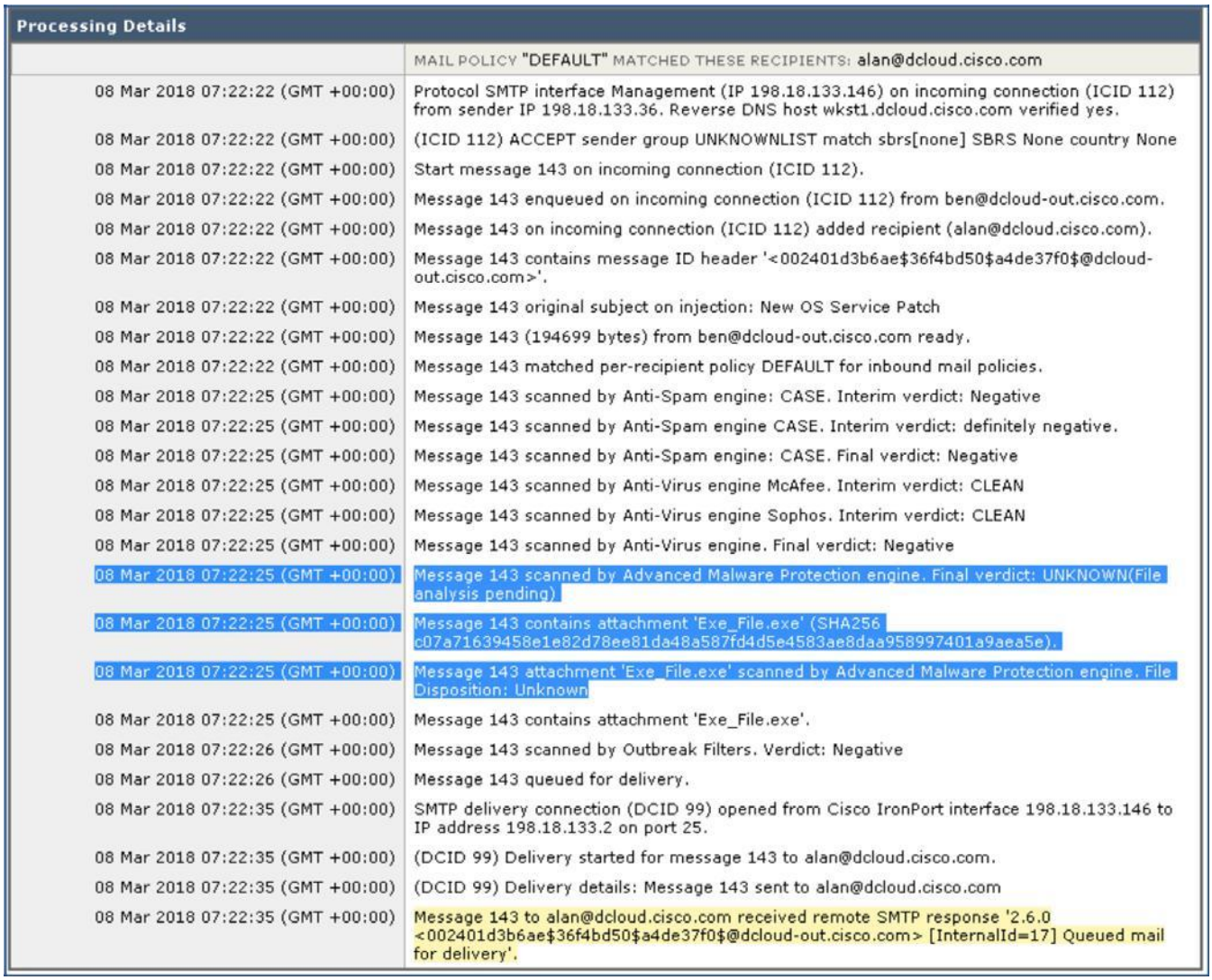
3. ワークステーションの GUI セッションで [モニタ（Monitor）] > [高度なマルウェア防御（Advanced Malware Protection）] レポートに移動すると、AMP が処理したファイルの概要に判定結果 [未知（Unknown）] のインシデントが記録されています。



4. 判定結果 [未知（Unknown）] 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。



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。



シナリオ 5:　ESA の AMP コンソールへの統合

ユースケース

Voyage Corp 社は、実稼働環境にシスコ次世代ファイアウォール（NGFW）、Cisco AMP for Endpoints、Cisco E メール セキュリティなどの幅広いシスコ製品を所有しています。チーフ テクニカル セキュリティ アーキテクトは、悪意のあるアクティビティがネットワークで発生した場合、その阻止にどれほど時間がかかるかを引用しながら、サポート チームがセキュリティ侵害を未然に防ぐ対応で日々直面する課題を強調しました。それぞれの対応の遅れによって、実稼働環境の主要なシステムがある日動作しなくなる可能性が露呈しています。

こうしたプロセスを可能な限り簡素化し、修復時間を短縮しようと全社的なプロジェクト チームが編成されました。このプロジェクトの会議中に、メール アーキテクトが、AMP Unity の機能の使用を提案します。これにより、ホワイトリストと既知の悪意のあるファイルのブラックリストを作成して中央に配置し、修復時間を効果的に短縮できます。

セキュリティ制御

Cisco E メール セキュリティ ソリューションの AMP Unity の機能では、バージョン 11.1 から利用可能になったファイル トラジェクトリに関する情報を共有できます。これにより、AMP クライアントが行った判定を一元的に上書きすることができます。これは特に既知の不正なファイルが組織に侵入後、ネットワークの一部または複数のワークステーションに移動した可能性のある場合に役立ちます。そのファイルを一元的に可視化し、同じ場所からアクションを起こすことで、悪意のあるファイルが及ぼす影響を最小限に抑えられるほか、そうしたアクションについて管理者とオペレーターが統一された情報源を持つことができます。

目的

このシナリオでは、Cisco E メール セキュリティと AMP クラウド ポータルの両方の構成について順を追って説明し、組織に入ってきた既知のクリーン ファイルと不正なファイルを使用してカスタム ホワイトリストとブラックリストを設定します。

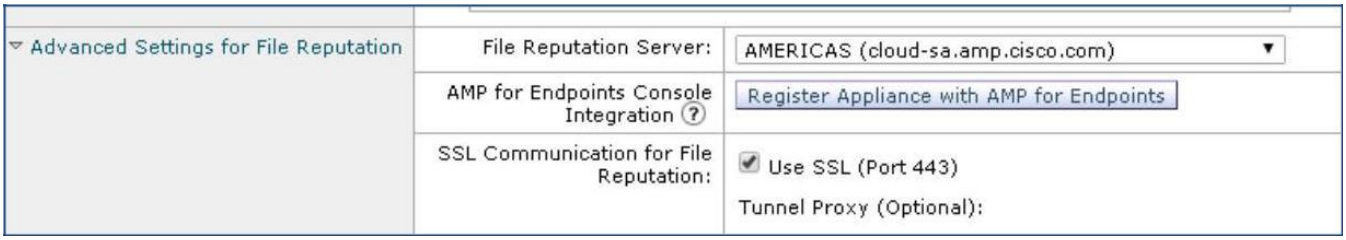
ESA と AMP の統合の詳細については、「Integrating the Appliance with AMP for Endpoints Console」を参照してください。

手順

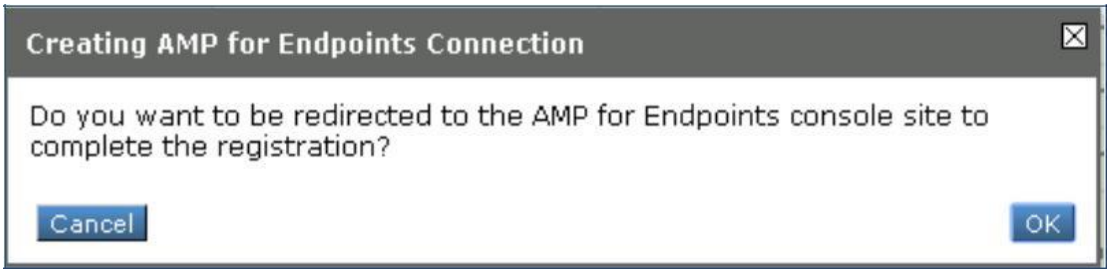
AMP for Endpoints コンソールに登録する（推定所要時間：10 分）

統合を完了するには、Cisco E メール セキュリティを AMP for Endpoints コンソールに登録する必要があります。この統合により、Cisco E メール セキュリティで同じ AMP for Endpoints アカウント内の他の AMP コンポーネントからカスタム ホワイトリストとブラックリストの SHA を受信したり、同様にそうしたコンポーネントに SHA を送信したりすることができます。

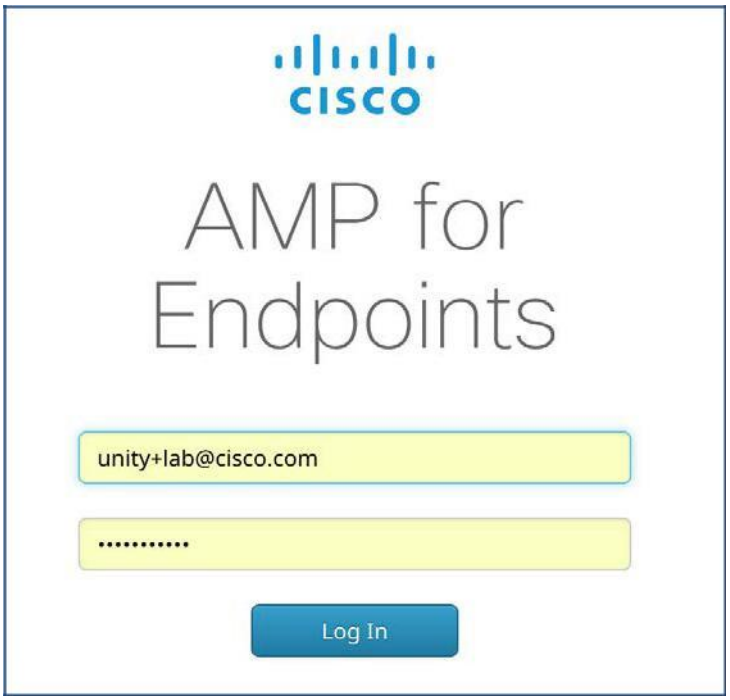
1. ワークステーションから GUI にアクセスして、[セキュリティサービス（Security Services）] > [ファイルレピュテーションと分析（File Reputation and Analysis）] に移動し、[グローバル設定の編集（Edit Global Setting）] をクリックします。[ファイルレピュテーションの詳細設定パネル（Advanced Settings panel for File Reputation）] の [アプライアンスをAMP for Endpointsに登録する（Register Appliance with AMP for Endpoints）] ボタンをクリックします。



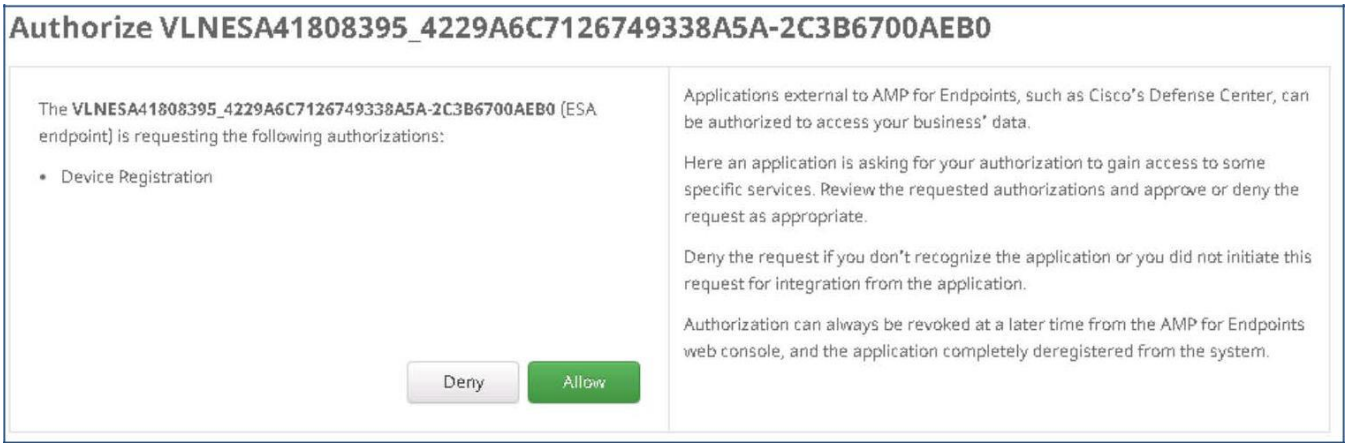
2. ポップアップ ボックスが表示されます。[OK] をクリックします。



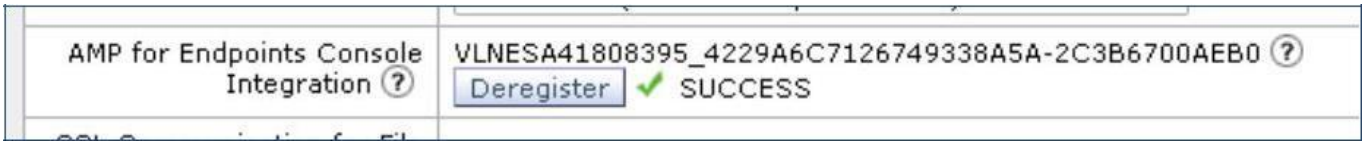
3. AMP for Endpoints コンソールのログイン ページが表示されます。次のクレデンシャルを使用してコンソールにログインします。**ユーザ名**:unity+lab+session_number@cisco.com、(**例**:unity+lab+18@cisco.com)、**パスワード**:C1sco12345!



4. 認証に成功したら、AMP for Endpoints の認証ページにある緑色の [許可（Allow）] ボタンをクリックしてアプライアンスを登録します。



5. これで登録が完了し、AMP for Endpoints コンソールから UI がリダイレクトされ Cisco E メール セキュリティ アプライアンスの [ファイル レピュテーションと分析（File Reputation and Analysis）] に戻ります。これは、登録プロセス全体が正常終了したことを示します。



6. [送信（Submit）] をクリックします。変更内容の確定は必要ありません。

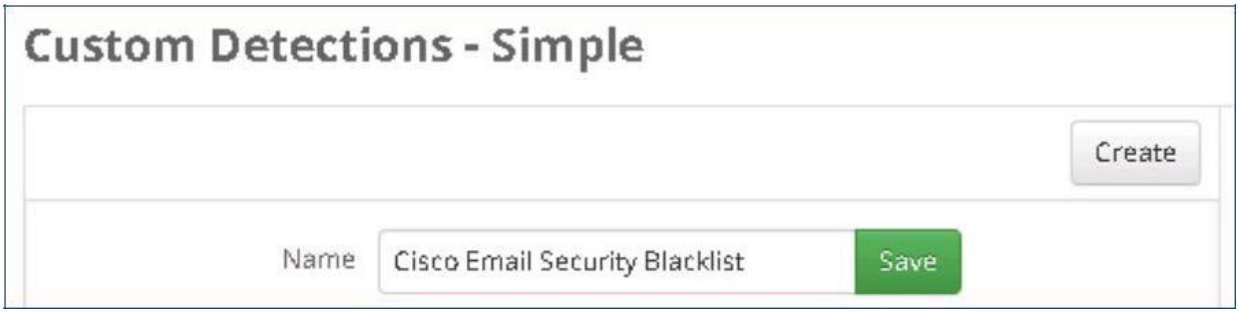
7. ブックマーク [AMPコンソール（AMP Console）] をクリックして AMP for Endpoints コンソール https://auth.amp.cisco.com にアクセスします。

8. [アカウント（Account）] > [アプリケーション（Applications）] に移動してアプライアンスが適切に登録されているかどうかを確認します。AMP for Endpoints コンソール ページの [アプリケーション（Applications）] セクションにアプライアンス名が表示されます。

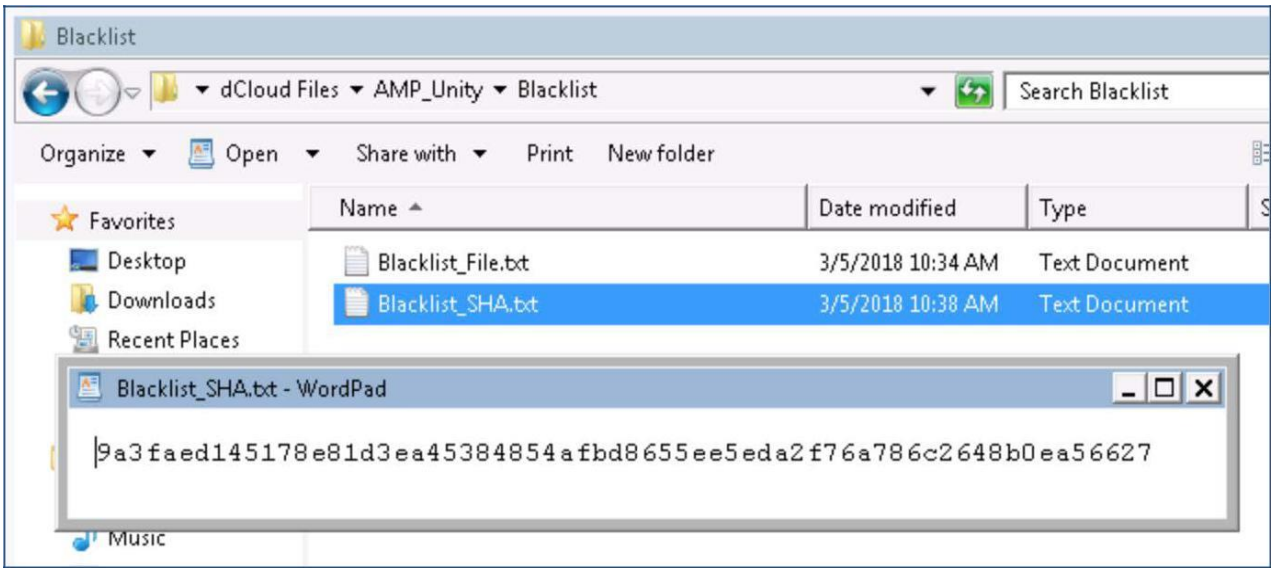
シンプル カスタム検出リストを作成する（推定所要時間：5 分）

シンプル カスタム検出リストはブラックリストに似ており、これにより、検出し検疫する必要のある対象を指定します。シンプル カスタム検出リスト内のエントリは、以降のファイルを検疫するだけでなく、レトロスペクティブ機能により、サービスがすでに確認した、組織内のエンドポイントにあるファイルのインスタンスも検疫します。

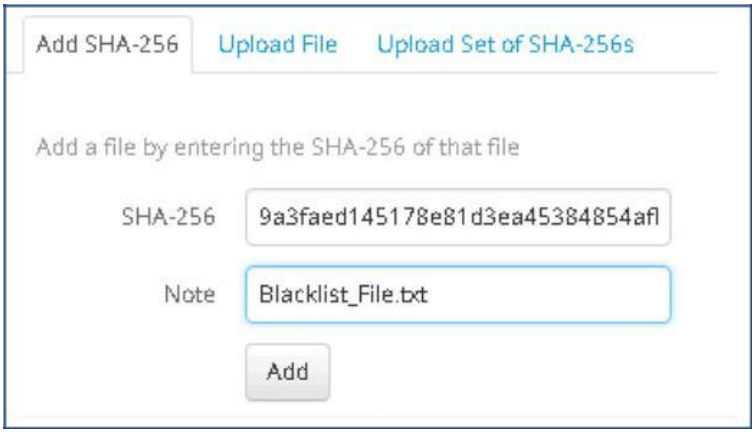
1. 引き続き AMP for Endpoints コンソールを使用します。[（Outbreak Control）] > [シンプル（Simple）] に移動します。[作成（Create）] をクリックして新しいシンプル カスタム検出を作成します。[名前（Name）] に「Cisco Eメールセキュリティのブラックリスト」と入力して [保存（Save）] をクリックします。



2. ワークステーションのデスクトップで、dCloud Files > AMP_Unity > Blacklist サブフォルダ内の Blacklist_SHA.txt ファイルをダブルクリックし、文字列全体（9a3faed145178e81d3ea45384854afbd8655ee5eda2f76a786c2648b0ea56627）をコピーします。



3. AMP for Endpoints コンソールに戻り、[編集（Edit）] をクリックして、[SHA-265] の空白のボックスに、コピーした文字列を追加します。[Note（メモ）] に「Blacklist_File.txt」と入力し [追加（Add）] をクリックします。

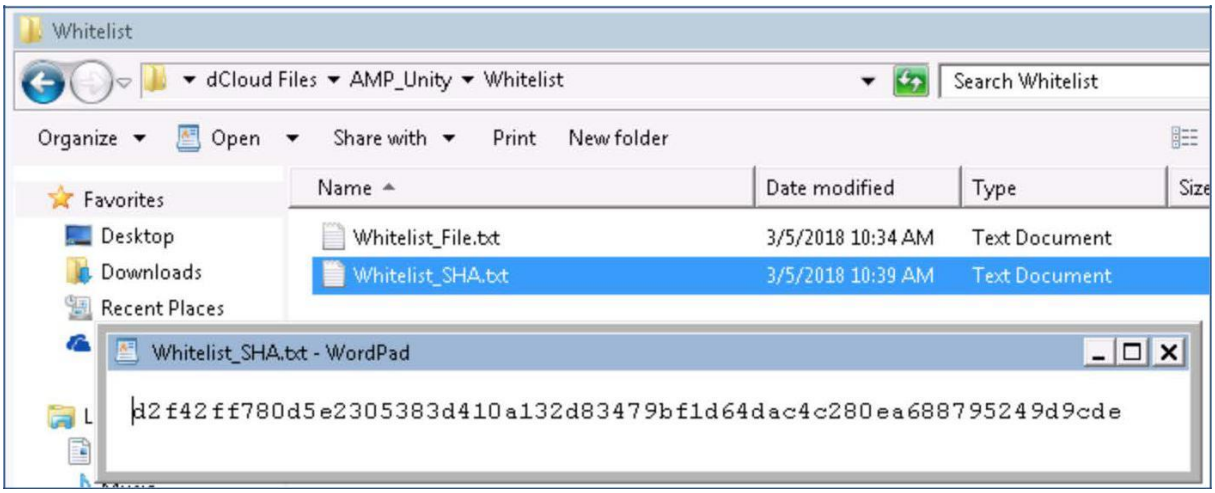


アプリケーション ホワイトリストを作成する（推定所要時間：5 分）

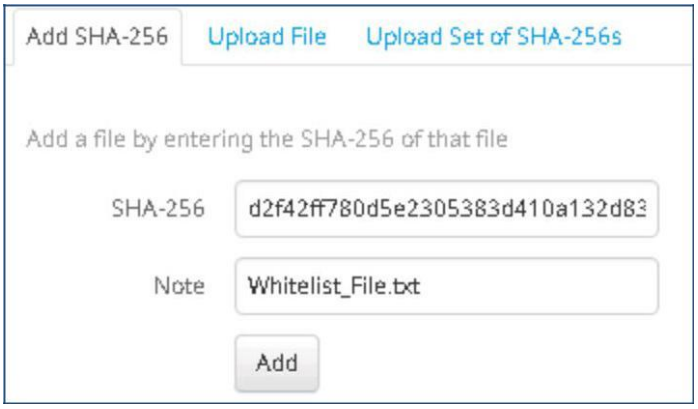
アプリケーション ホワイトリストにより、不正と見なすべきではないファイルを指定できます。こうしたファイルの例として、会社全体で使用する汎用エンジンまたは標準イメージによって検出され、安全に使用できると考えられるカスタム アプリケーションが挙げられます。

1. アプリケーション ホワイトリストを作成するには、[アウトブレイクコントロール（Outbreak Control）] > [ホワイトリスト（Whitelisting）] に移動します。[作成（Create）] をクリックして新しいホワイトリストを作成します。[名前（Name）] に「Cisco Eメールセキュリティのホワイトリスト」と入力して [保存（Save）] をクリックします。

2. ワークステーションのデスクトップで、AMP_Unity > Whitelist サブフォルダ内の Whitelist_SHA.txt ファイルをダブルクリックして、文字列全体（d2f42ff780d5e2305383d410a132d83479bf1d64dac4c280ea688795249d9cde）をコピーします。



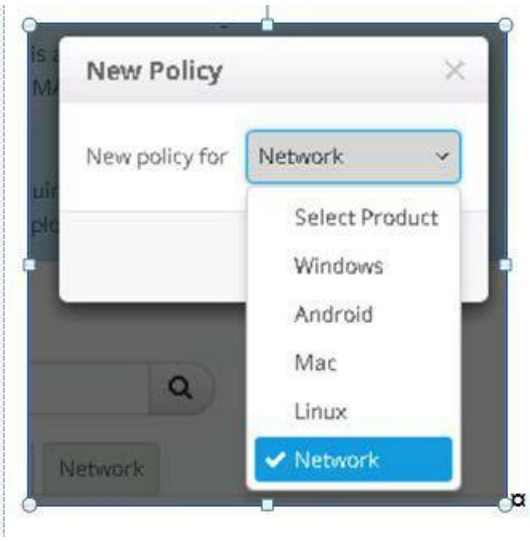
3. AMP for Endpoints コンソールに戻り、[編集（Edit）] をクリックして、[SHA-265] の空白のボックスに、コピーした文字列を追加します。[Note（メモ）] に「Whitelist_File.txt」と入力し [追加（Add）] をクリックします。



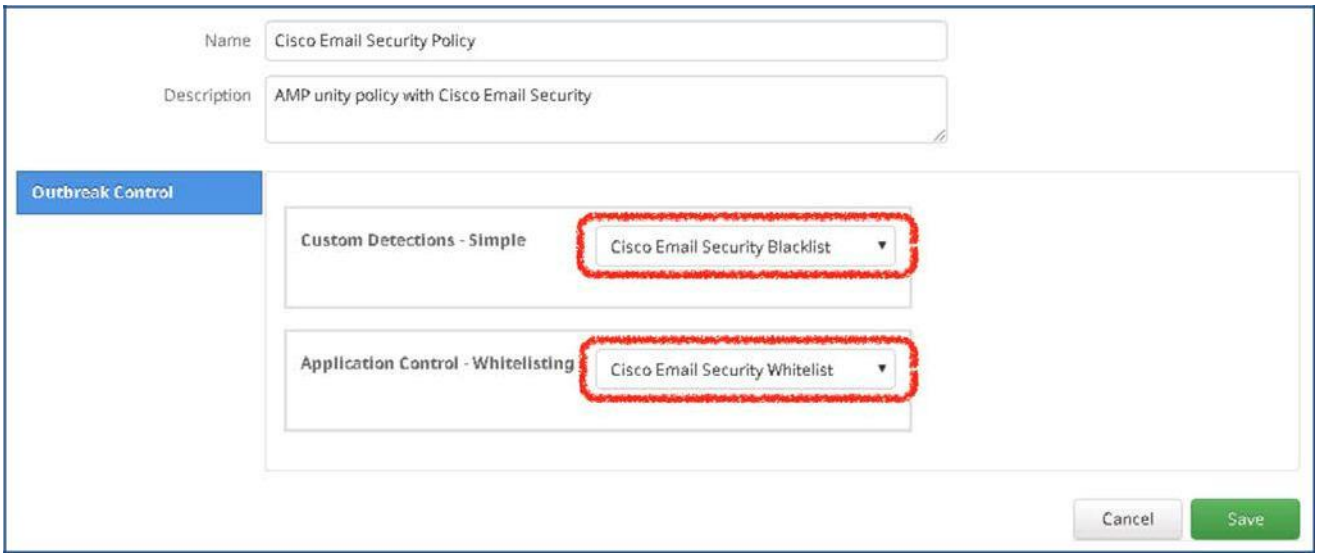
カスタム ポリシーを作成する（推定所要時間：3 分）

カスタム シンプル リストとホワイトリストは、AMP for Endpoints コンソールに登録したアプライアンスの動作に影響を与えるポリシーのその他の設定と組み合わせることができます。

1. カスタム ポリシーを作成するには、[管理（Management）] > [ポリシー（Policies）] に移動します。次に [+ 新しいポリシー（+ New Policy）] をクリックして、ドロップダウンリストの [ネットワーク（Network）] を選択します。[新しいポリシー（New Policy）] をクリックします。



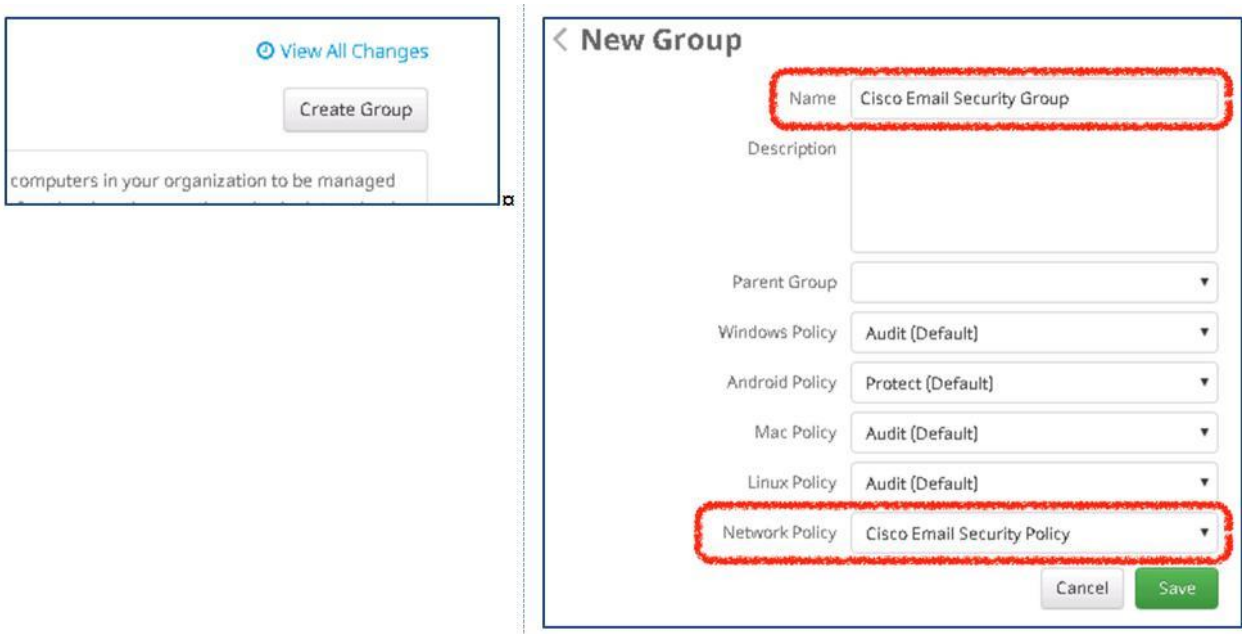
2. [名前（Name）] に「Cisco Eメールセキュリティポリシー」と入力して、前のタスクで作成したシンプル カスタム検出リストとアプリケーション ホワイトリストをドロップダウンリストから選択します。[保存（Save）] をクリックします。



カスタム グループを作成する（推定所要時間：7 分）

カスタム グループは、特に登録済みのアプライアンスにカスタム ポリシーを適用するために必要です。

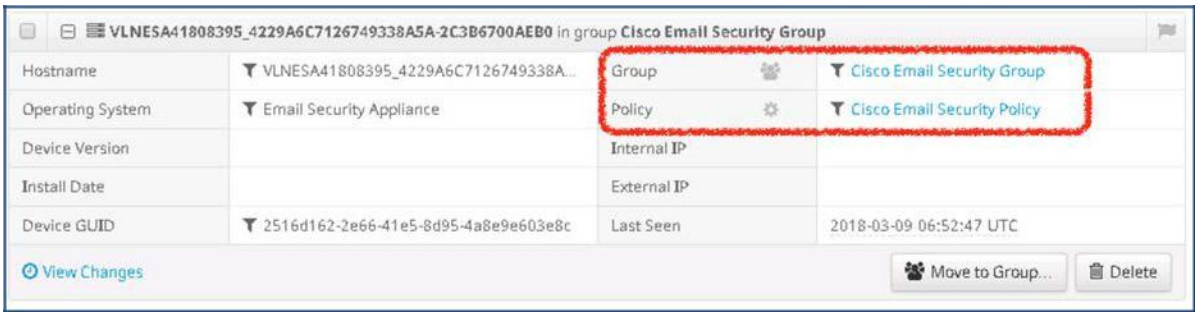
1. カスタム グループを作成するには、[管理（Management）] > [グループ（Groups）] に移動します。次に、[グループの作成（Create Group）] をクリックして、[名前（Name）] に「Cisco Eメールセキュリティグループ」と入力します。[ネットワークポリシー（Network Policy）] で、ドロップダウンリストから前のタスクで作成したカスタム ポリシーを選択します。[保存（Save）] をクリックします。



2. 次に、登録済みのアプライアンスをデフォルトのグループからこのカスタム グループに移動します。[管理（Management）] > [コンピュータ（Computers）] に移動します。[+] アイコンをクリックしてアプライアンスの詳細を展開し、[Move to Group（グループに移動）] をクリックします。

3. [既存のグループ（Existing Group）] ドロップダウンリストからカスタム グループを選択して [移動（Move）] をクリックします。

4. [+] アイコンをクリックしてもう一度アプライアンスの詳細を展開し、移動を確認します。これで、アプライアンスが、「Cisco E メール セキュリティ ポリシー」によって管理される「Cisco E メール セキュリティ グループ」に追加されました。

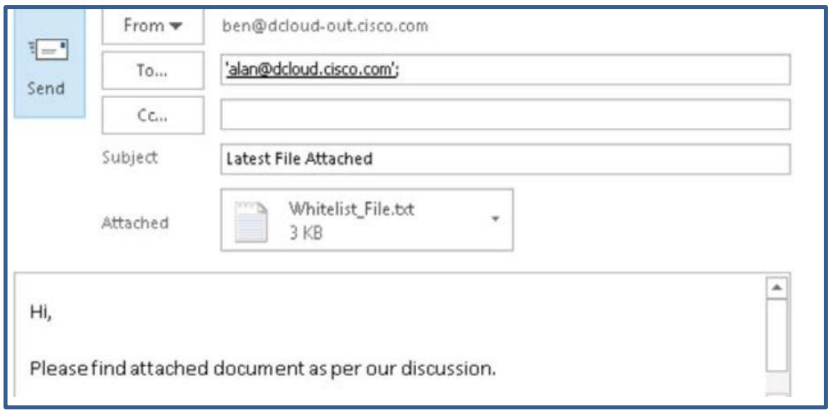


AMP Unity（ホワイトリスト）をテストする（推定所要時間：15 分）

構成をすべて完了したら、AMP for Endpoints コンソールでブラックリストとホワイトリストにそれぞれ登録されている添付ファイルを含むメールを社外ユーザの Ben から Alan に送信することで AMP Unity の機能をテストできます。

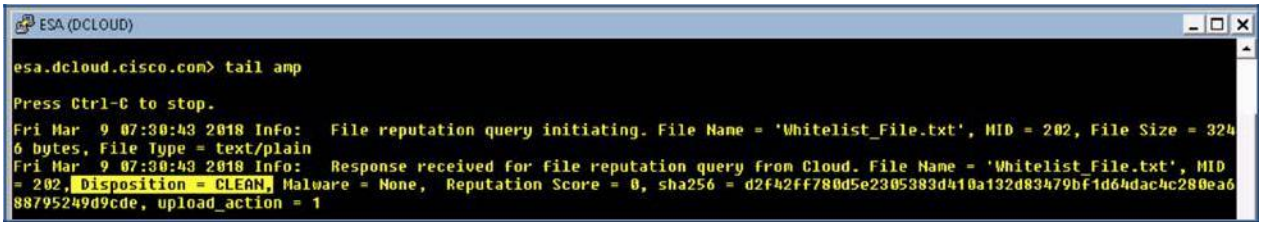
1. メッセージを準備する前に、CLI を使用して ESA への接続を開始し、メール ログを表示します（ログの確認には「tail」コマンドを使います）。メッセージが一連の設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。
2. ワークステーションから Microsoft Outlook を起動し、Ben の受信トレイから、次のパラメータを使用して新しいメッセージを準備します。

送信者：	ben@dcloud-out.cisco.com
受信者：	alan@dcloud.cisco.com
件名：	最新ファイルを添付しています
本文：	お世話になっております。 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：	デスクトップ上の AMP_Unity > Whitelist サブフォルダにある Whitelist_File.txt。

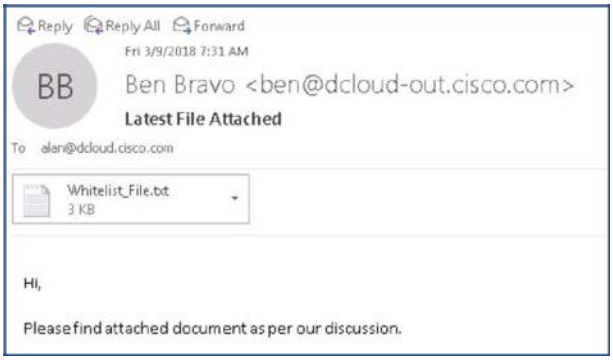


3. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

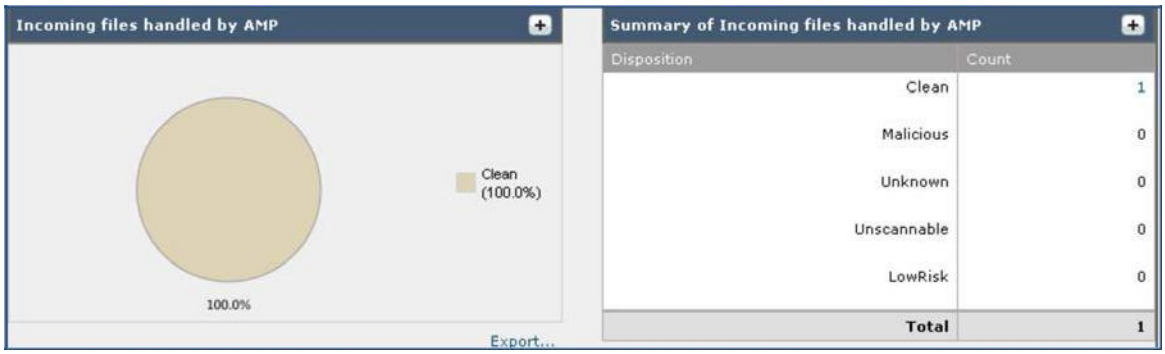
4. ESA の CLI セッションに切り替えて、**tail amp** を入力し Enter キーを押します。AMP ログは、AMP クラウドからクエリが返ったことと、このファイルが即座に「CLEAN」と判定されたことを明らかに示しています。



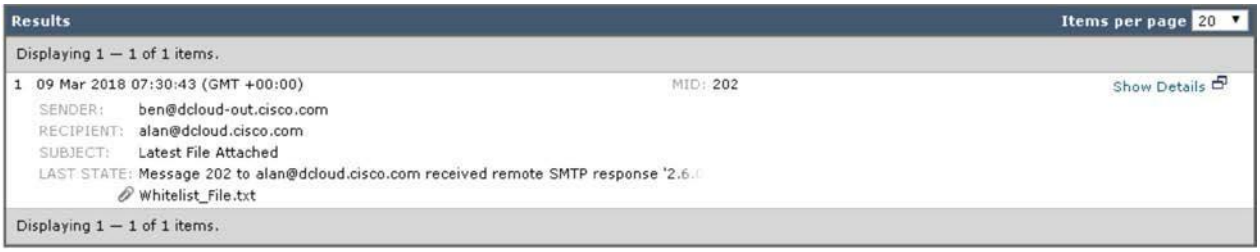
5. メッセージが Alan のメールボックスに正常に届いていることを確認します。添付ファイルの Whitelist_File.txt はすでに AMP コンソールのホワイトリストに登録されているため、これは想定内の動作です。添付ファイルを開いて、テキスト ファイルのコンテンツを表示します。コンテンツが正常に表示され、電子メールのメッセージも変更されることはありません。



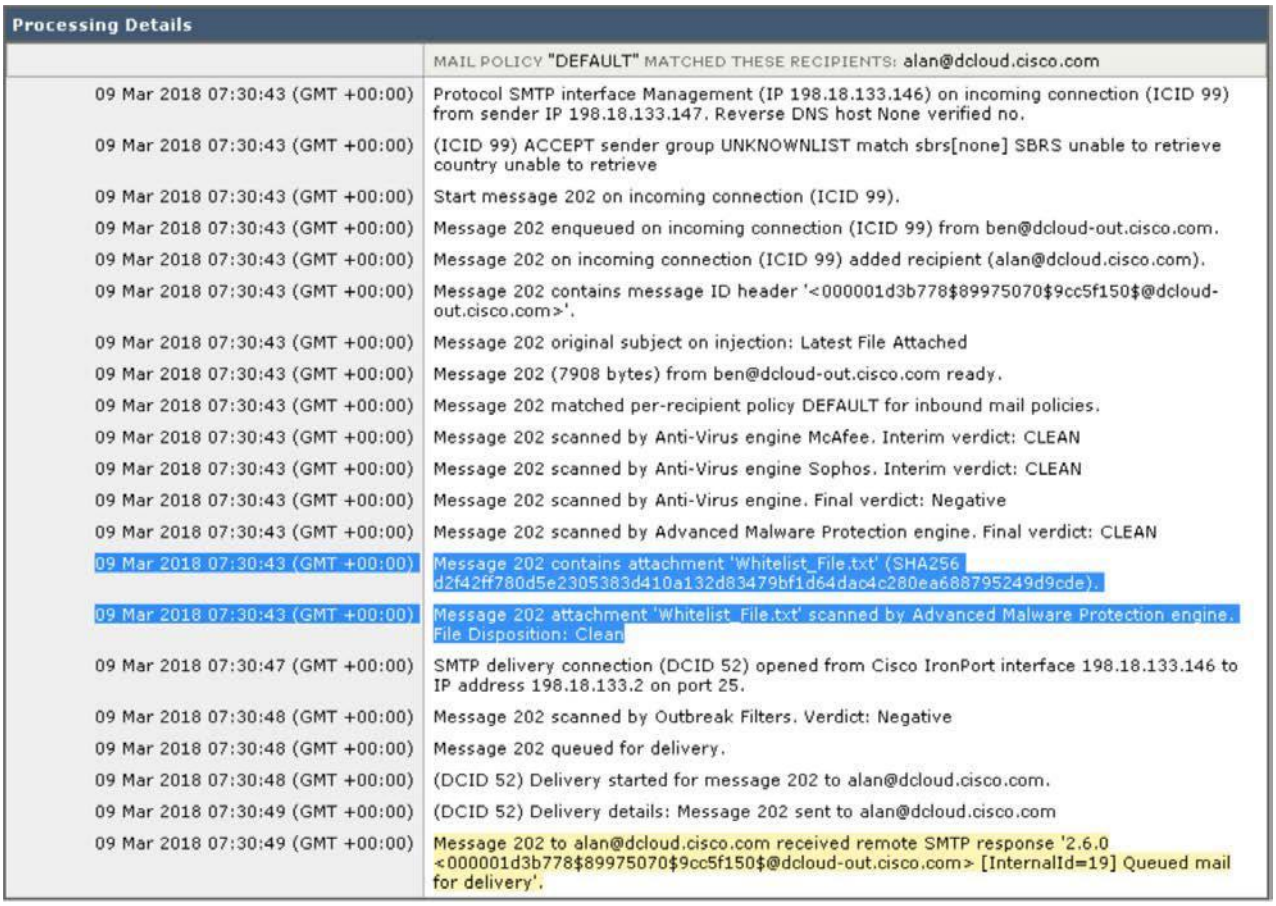
6. ESA の GUI セッションで [モニタ（Monitor）] > [高度なマルウェア防御（Advanced Malware Protection）] レポートに移動すると、AMP が処理したファイルの概要に判定結果 [クリーン（Clean）] のインシデントが記録されています。



7. 判定結果 [クリーン（Clean）] 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。



8. [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。



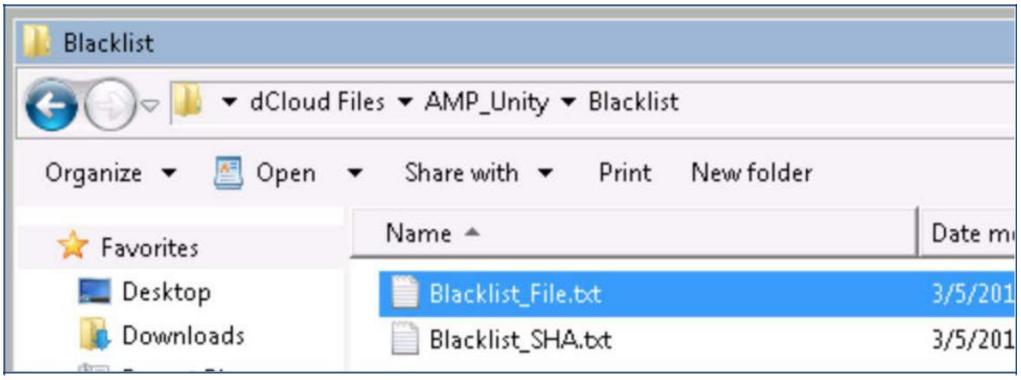
Processing Details

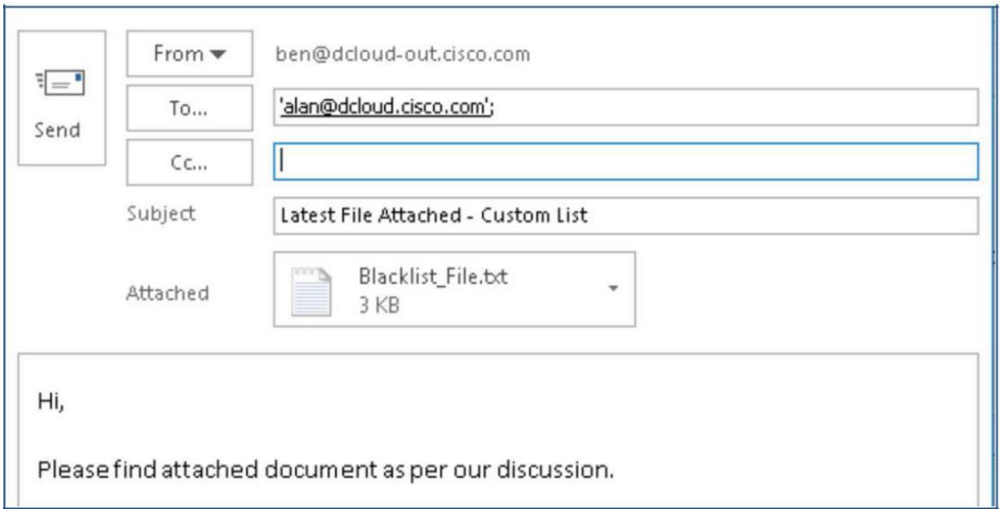
	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: alan@dcloud.cisco.com
09 Mar 2018 07:30:43 (GMT +00:00)	Protocol SMTP interface Management (IP 198.18.133.146) on incoming connection (ICID 99) from sender IP 198.18.133.147. Reverse DNS host None verified no.
09 Mar 2018 07:30:43 (GMT +00:00)	(ICID 99) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS unable to retrieve country unable to retrieve
09 Mar 2018 07:30:43 (GMT +00:00)	Start message 202 on incoming connection (ICID 99).
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 enqueued on incoming connection (ICID 99) from ben@dcloud-out.cisco.com.
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 on incoming connection (ICID 99) added recipient (alan@dcloud.cisco.com).
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 contains message ID header '<000001d3b778$89975070$9cc5f150$@dcloud-out.cisco.com>'.
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 original subject on injection: Latest File Attached
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 (7908 bytes) from ben@dcloud-out.cisco.com ready.
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 matched per-recipient policy DEFAULT for inbound mail policies.
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 scanned by Anti-Virus engine McAfee. Interim verdict: CLEAN
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 scanned by Anti-Virus engine. Final verdict: Negative
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 scanned by Advanced Malware Protection engine. Final verdict: CLEAN
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 contains attachment 'Whitelist_File.txt' (SHA256 d2f42ff780d5e2305383d410a132d83479bf1d64dac4c280ea688795249d9cde).
09 Mar 2018 07:30:43 (GMT +00:00)	Message 202 attachment 'Whitelist_File.txt' scanned by Advanced Malware Protection engine. File Disposition: Clean
09 Mar 2018 07:30:47 (GMT +00:00)	SMTP delivery connection (DCID 52) opened from Cisco IronPort interface 198.18.133.146 to IP address 198.18.133.2 on port 25.
09 Mar 2018 07:30:48 (GMT +00:00)	Message 202 scanned by Outbreak Filters. Verdict: Negative
09 Mar 2018 07:30:48 (GMT +00:00)	Message 202 queued for delivery.
09 Mar 2018 07:30:48 (GMT +00:00)	(DCID 52) Delivery started for message 202 to alan@dcloud.cisco.com.
09 Mar 2018 07:30:49 (GMT +00:00)	(DCID 52) Delivery details: Message 202 sent to alan@dcloud.cisco.com
09 Mar 2018 07:30:49 (GMT +00:00)	Message 202 to alan@dcloud.cisco.com received remote SMTP response '2.6.0 <000001d3b778$89975070$9cc5f150$@dcloud-out.cisco.com> [InternalId=19] Queued mail for delivery'.

AMP Unity（カスタム検出リスト）をテストする（推定所要時間：20 分）

1. メッセージを準備する前に、CLI を使用して ESA への接続を開始し、メール ログを表示します（ログの確認には「tail」コマンドを使います）。メッセージが一連の設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。
2. ワークステーションから Microsoft Outlook を起動し、Ben 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。

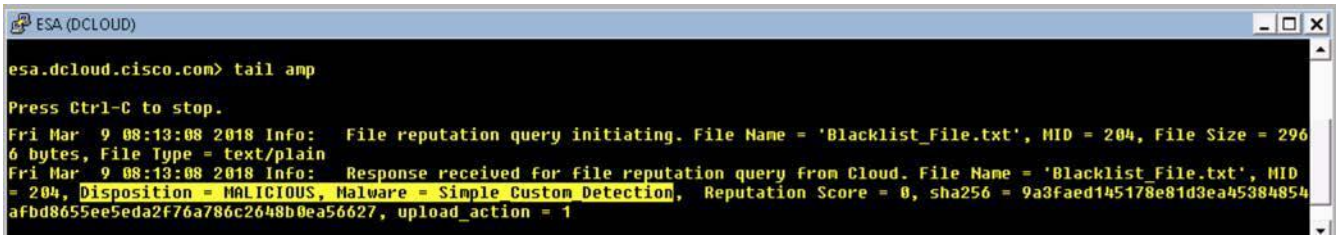
送信者：	ben@dcloud-out.cisco.com
受信者：	alan@dcloud.cisco.com
件名：	最新ファイルを添付しています – カスタム リスト
本文：	お世話になっております。 前回の会議に沿って、ドキュメントを送信します。ご査収ください。（Please find attached document as per our discussion.）
添付ファイル：	デスクトップ上の AMP_Unity > Blacklist サブフォルダにある Blacklist_File.txt。



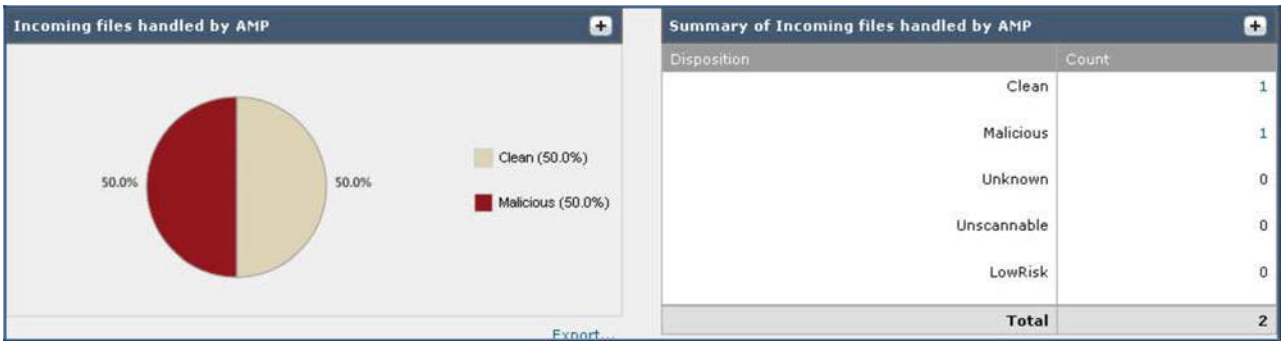


3. メールを送信します。[すべてのフォルダを送受信（Send/Receive Folder）] をクリック、または **F9** キーを押して、同期プロセスを手動実行します。

4. ESA の CLI セッションに切り替えて、**tail amp** を入力し Enter キーを押します。AMP ログは、AMP クラウドからクエリが返ったことと、このファイルがシンプル カスタム検出によって即座に「MALICIOUS」と判定されたことを明らかに示しています。



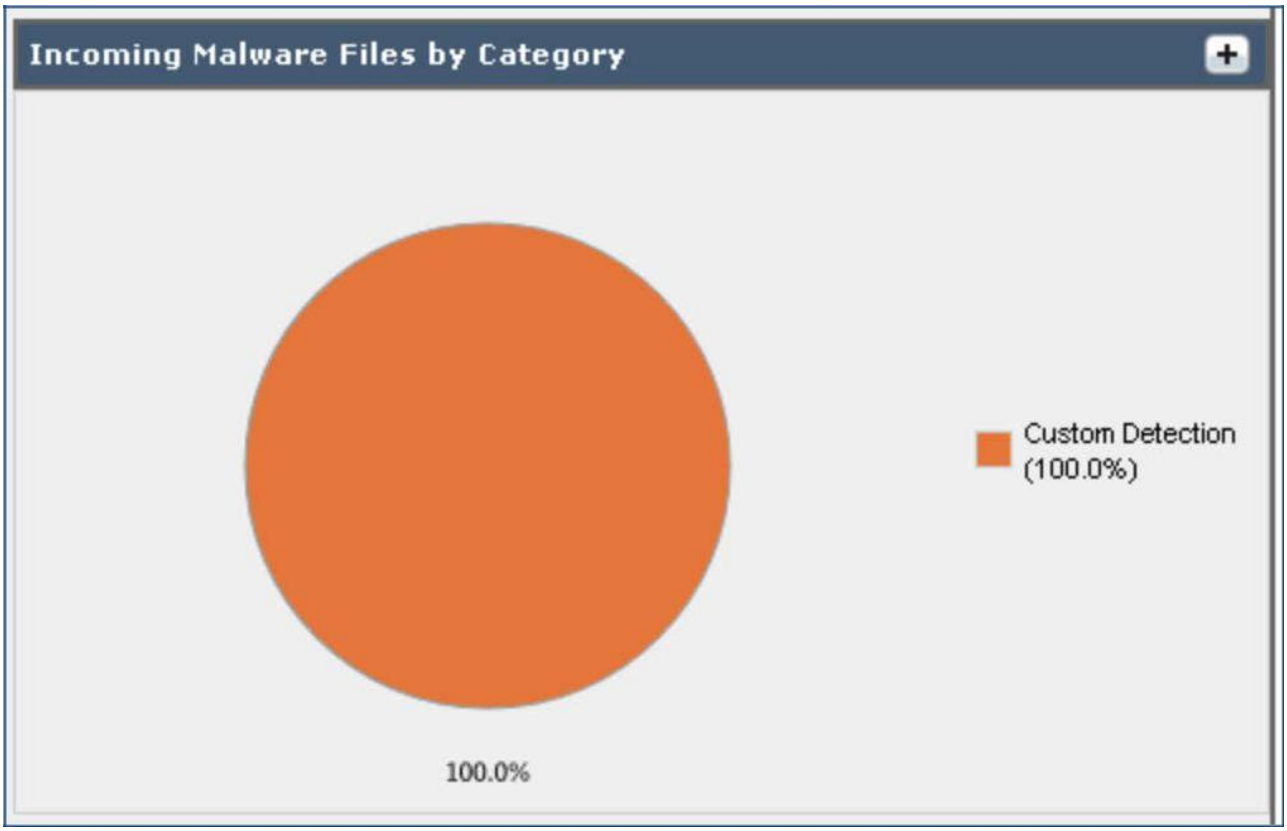
5. ESA の GUI セッションで [モニタ（Monitor）] > [高度なマルウェア防御（Advanced Malware Protection）] レポートに移動すると、AMP が処理したファイルの概要に判定結果 [悪意のあるファイル（Malicious）] のインシデントが記録されています。



6. 判定結果 [悪意のあるファイル（Malicious）] 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。

7. [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。最後のイベントでメッセージが AMP によってドロップされていることを確認してください。

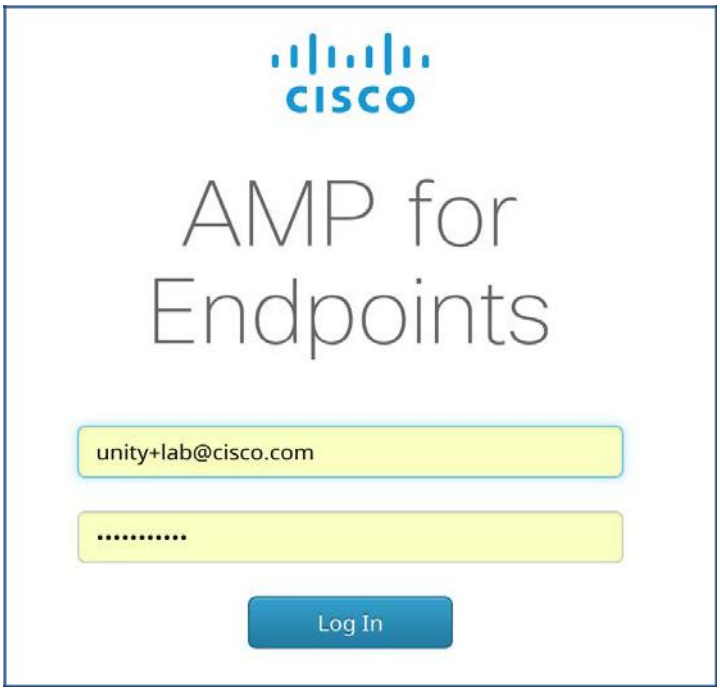
8. [モニタ（Monitor）] > [高度なマルウェア防御（Advanced Malware Protection）] に戻り、新しいセクション [カテゴリ別の受信したマルウェア（Incoming Malware Files by Category）] までスクロールし、AMP for Endpoints コンソールから受信した、[カスタム検出（Custom Detection）] と表示されているブラックリスト ファイルの SHA の割合を表示します。



9. ブラックリスト ファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] セクション内で [シンプルカスタム検出（Simple Custom Detection）] として表示されます。最初の列にある SHA256 の文字列をクリックします。

10. [AMPファイル分析（AMP file analysis）] レポート ページで、レポートの [詳細の表示（More Details）] セクションまでスクロールすると、AMP for Endpoints コンソールにブラックリスト ファイル SHA のファイル トラジェクトリの詳細を表示できます。

11. AMP for Endpoints コンソールのログイン ページが表示されます。次のクレデンシャルを使用してコンソールにログインします。
ユーザ名:unity+lab+session_number@cisco.com、(**例**:unity+lab+18@cisco.com)、**パスワード**:C1sco12345!



12. このファイルのファイル トラジェクトリの詳細が表示されます。ファイル トラジェクトリは、各ファイルの最初の観察時点から最後の観察時点までのライフ サイクルのほか、そのファイルがあったネットワーク上のコンピュータをすべて示します。[トラジェクトリ(Trajectory)] セクションまでスクロール ダウンし、[観察結果(Observed)] アイコンをクリックして詳細を確認します。

シナリオ 6:　DomainKeys Identified Mail（DKIM）を有効にする

ユースケース

Jacob は Voyage Corp 社の最高情報セキュリティ責任者（CISO）です。Jacob の部門は、通信インフラストラクチャに対し徹底したセキュリティ評価を実施しました。特に懸念となった点は、3 ヵ月にわたり発生している特定の従業員を標的としたフィッシング攻撃の数でした。エンドユーザの認識が高まりトレーニングの数も増えたおかげで、従業員がスプーフィング メッセージを見分ける能力が向上しましたが、セキュリティをさらに強化することが決定されました。このために同社は、Sender Policy Framework（SPF）、Domain Keys Identified Mail（DKIM）、Domain-based Message Authentication, Reporting & Conformance（DMARC）といった技術を別途展開します。

SPF はとりわけ簡単に導入できる技術ですが、メッセージング チームは、自社ドメインにとっての正当なメール ソースすべてを十分に認識できていないメッセージング インフラストラクチャが広範囲にわたるのではないかと懸念を抱いていました。

メッセージング インフラストラクチャは Voyage Corp 社に代わって送信を行う複数のサードパーティ関連会社によって運用され、メッセージには通常、ニュースレターや特別なプロモーションのほか、暗号化することもある機密メールも含まれています。こうした幅広い利用と途絶えることのないメール運用を考慮して、外部にまったく依存しない DKIM の導入が決定されました。パスに基づく技術である SPF とは異なり、DKIM ではメッセージに署名を行うことで信頼性を保証しています。

セキュリティ制御

簡単に言うと、DKIM では、メッセージの送信者を認証する暗号化のスタンプが使用されます。DKIM を使用すると、メール メッセージのメッセージ ヘッダーに、パブリック キーと秘密キーの形式を取る電子署名が挿入されます。

こうしたペアの公開キーは、公にアクセス可能な DNS のテキスト レコード内で公開されています。Cisco E メール セキュリティはメールから送信元ドメインを抽出し、DNS のテキスト レコードから公開キーを取得して、メッセージの内容に対して署名を検証することでメッセージを認証します。Cisco E メール セキュリティでは、その結果に基づいて、ドロップ、検疫、管理者に通知するといったアクションを起こすことができます。

目的

このシナリオでは、DKIM の署名によって暗号化ハッシュをメール全体に追加することで、メール内容（本分とヘッダーの両方）のスプーフィングからどのように保護されるのかを示します。社外に送信するメールが DKIM 検証を通過した場合、メールの受信者は、メールが移動中に不正な目的で変更されていないことを確信できます。

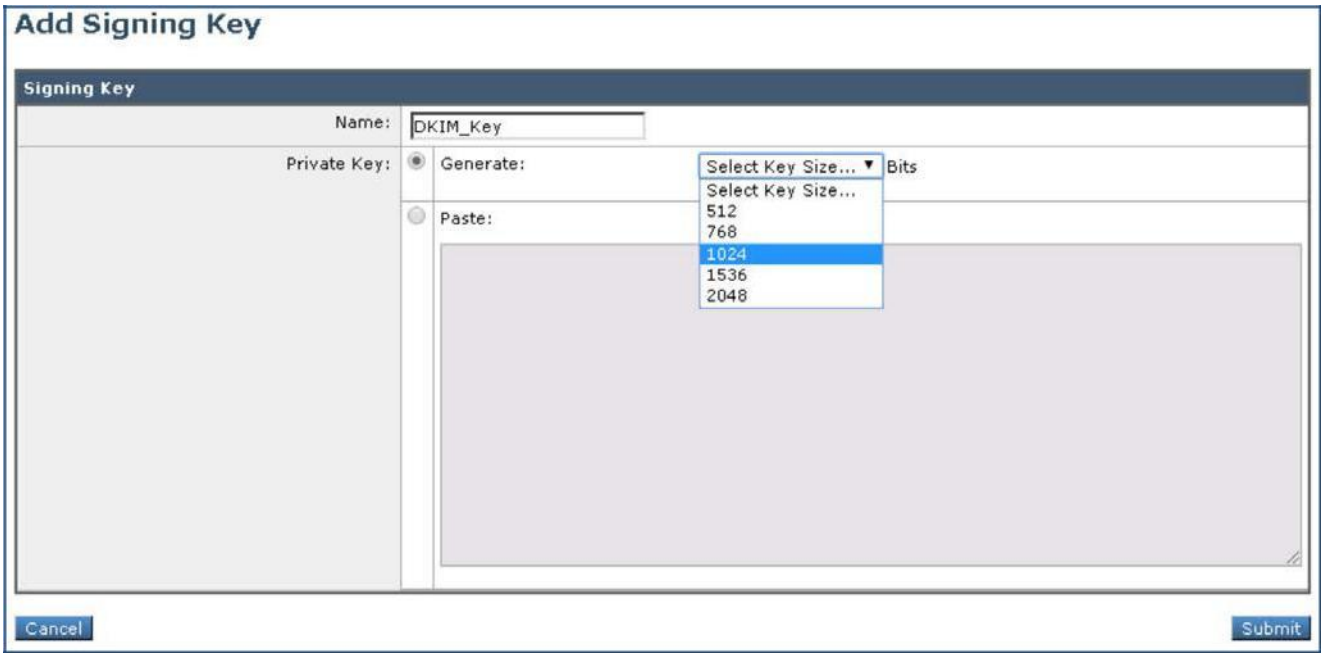
注：DKIM の詳細については、「Email Authentication」を参照してください。

DKIM のキー ペアを設定する（送信者）（推定所要時間：3 分）

最初のタスクでは、社外宛の送信メッセージの署名に使用する公開キーと秘密キーのペアを生成します。公開キーは、DNS の TXT レコードで公開されます。また、秘密キーは保存され、送信メッセージに署名する際に Cisco E メール セキュリティで利用可能になります。

1. ワークステーションから、次のクレデンシャルで ESA2 の GUI にアクセスします。**Username**：admin、**パスフレーズ**：C1sco12345

2. [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] に移動し、[キーの追加（Add Key）] をクリックします。[名前（Name）] に DKIM_Key と入力します。[生成（Generate）] を選択して、1024 ビットのキー サイズを選択します。



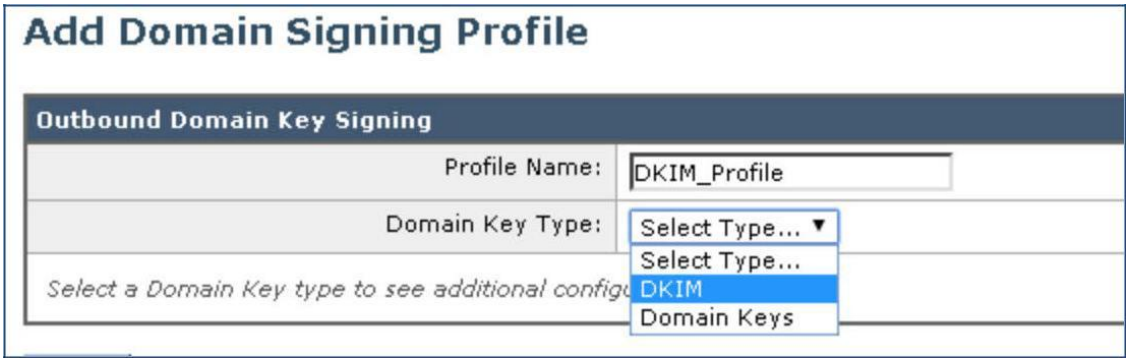
3. [送信（Submit）] をクリックします。

4. 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。

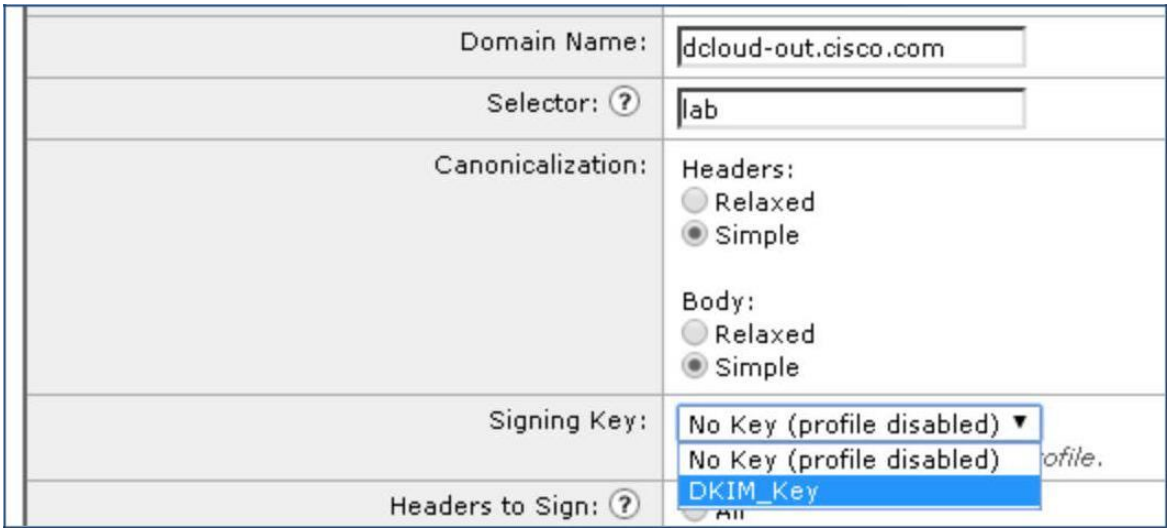
DKIM の署名プロファイルを作成する（送信者）（推定所要時間：7 分）

このタスクでは、メールのどの部分を署名プロセスに含めるかを特定します。メッセージの本文全体、またはメール ヘッダーの特定のフィールドのみを指定できます。前のタスクで作成したキー ペアが、「セレクタ」によって参照されることで DKIM の検証機能がキーを区別できるようになります。プロファイルで定義したドメインに一致するすべての送信メッセージが署名され、DKIM の署名が挿入されます。

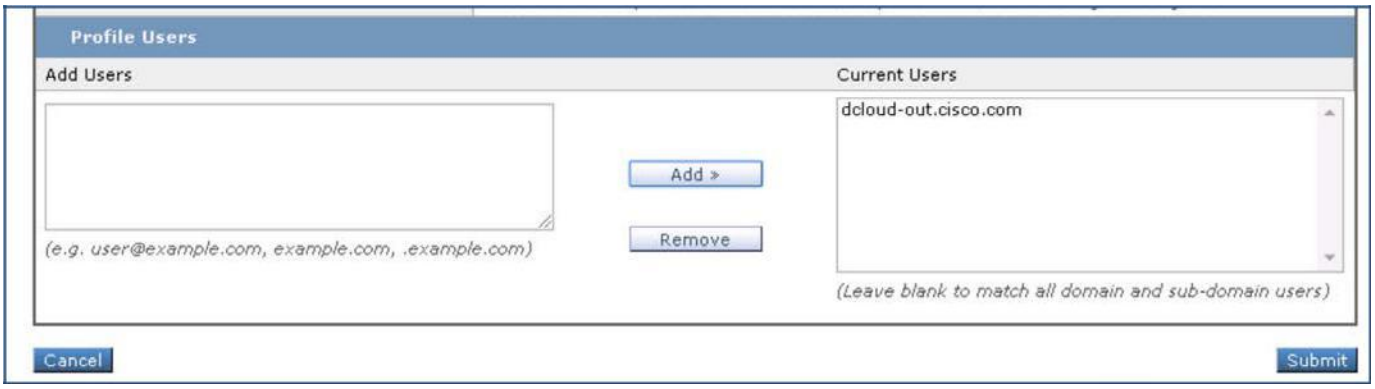
1. 前のタスクの GUI を引き続き使用します。ドメイン プロファイルを作成し、キーをドメイン プロファイルに関連付けます。[メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] に移動し、[プロファイルの追加（Add Profile）] をクリックします。このプロファイルの名前を「DKIM_Profile」と入力し、[ドメインキータイプ（Domain Key Type）] から [DKIM] を選択します。新しいオプションがページに表示されます。



2. [ドメイン名（Domain Name）] に「*dcloud out.cisco.com*」と入力し、[セレクタ（Selector）] に「lab」と入力します。ヘッダーと本文の両方の正規化オプションを [シンプル（Simple）] のままにし、ドロップダウンリストからカスタムの署名キー「DKIM_Key」を選択します。



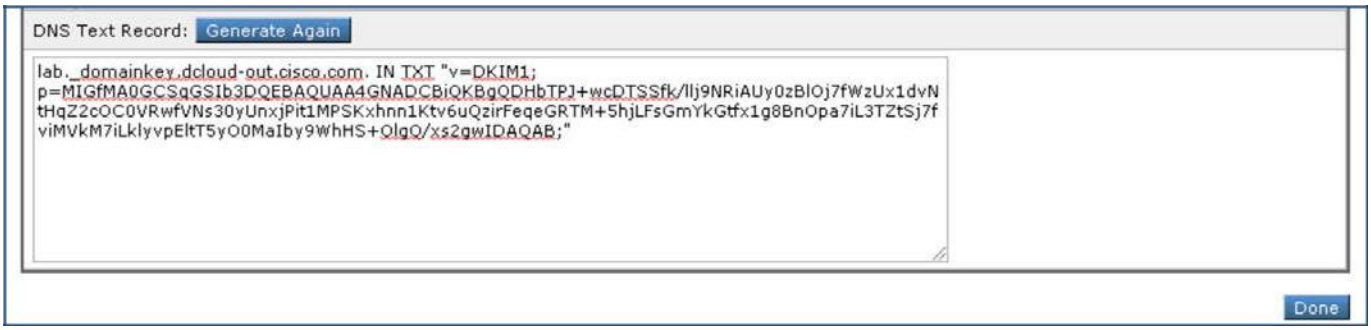
3. その他のオプションはデフォルトの設定のままにします。[ユーザの追加（Add Users）] ボックスに「*dcloud out.cisco.com*」と入力し、[追加（Add）] をクリックして、このドメインをこのプロファイルに追加します。



4. [送信（Submit）] を選択し、[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。

5. 新しい署名プロファイルの [DNSテキストレコード（DNS Text Record）] 列で [生成（Generate）] のリンクをクリックし、DNS のテキストレコードを表示します。

6. DNS のテキスト レコードをコピーします。次に実行するタスクで、送信元ドメインに属している DNS サーバに新しい TXT レコードを作成するときに、そのコピーを使用する必要があります。



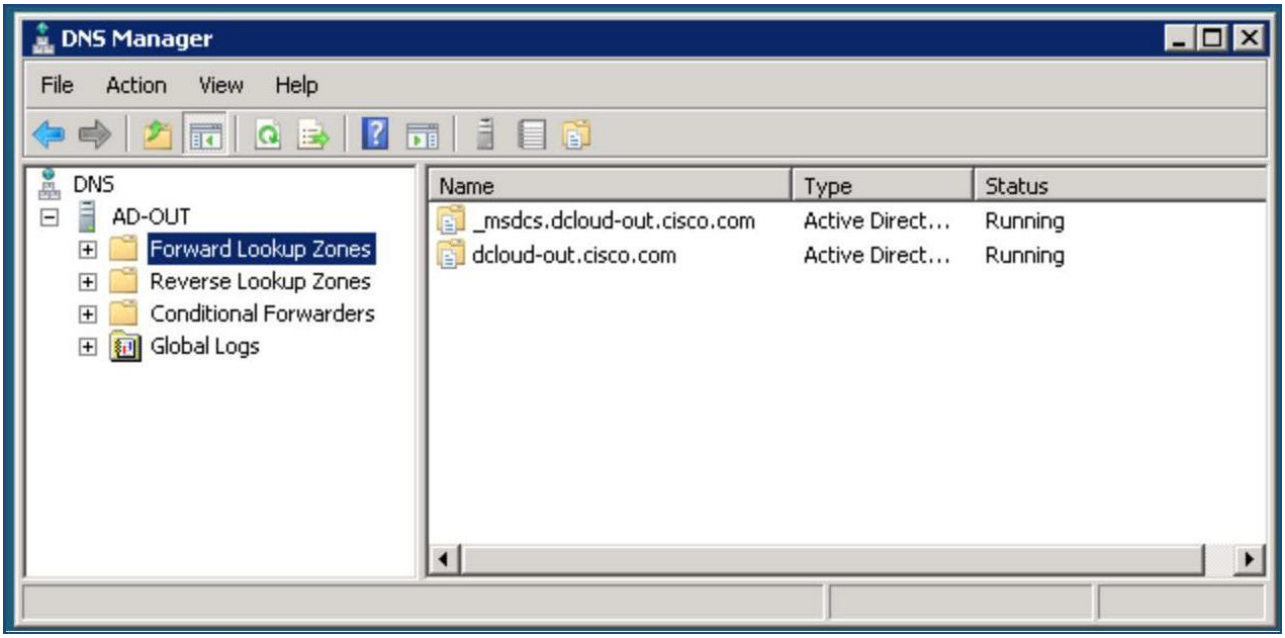
7. レコードをコピーしたら、[完了（Done）] をクリックします。

DKIM レコードを作成する（送信者）（推定所要時間：20 分）

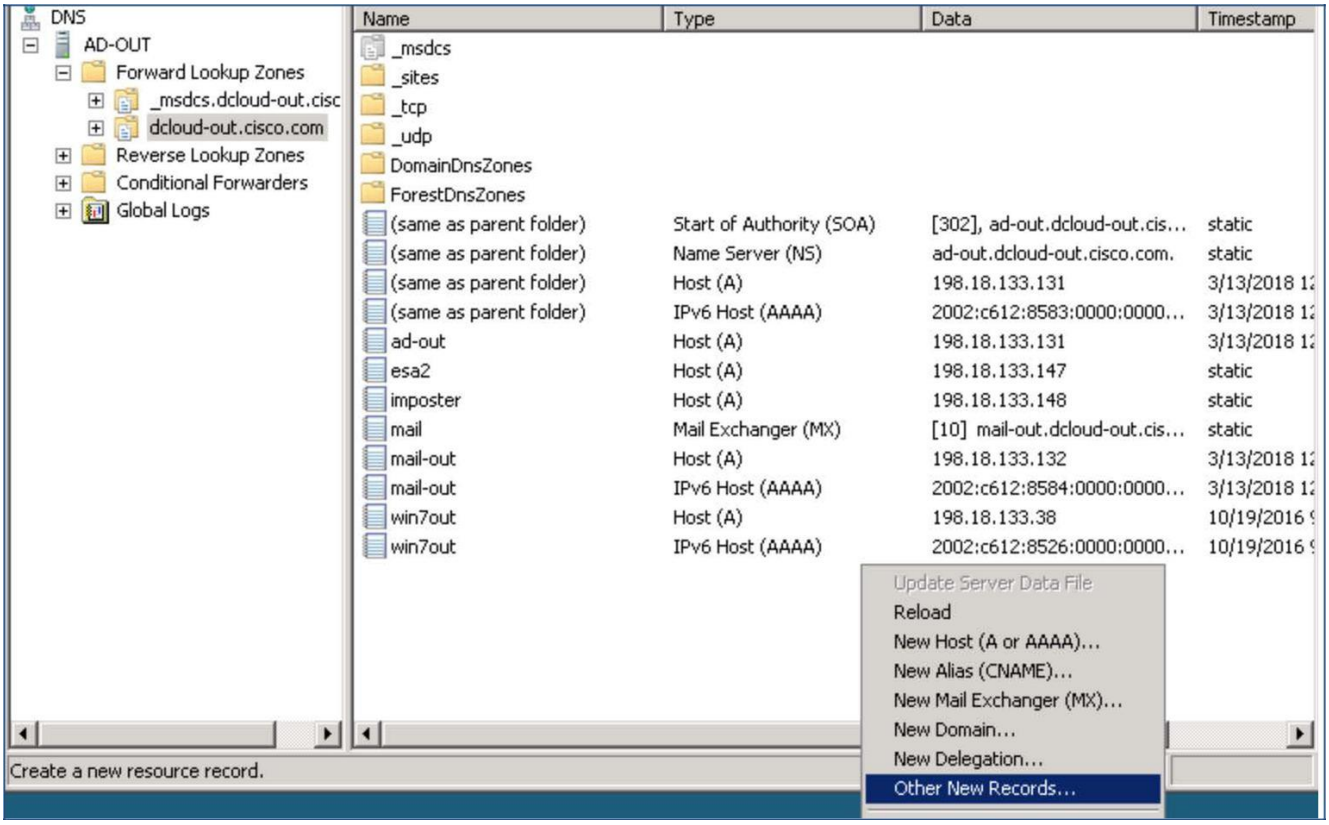
DKIM レコードには、メールの署名に使用する暗号キーの公開部分が含まれています。受信者は、このレコードを使用して送信サーバから受信したメッセージが有効であることを確認します。

1. ワークステーションから、タスクバーにある *RDC* を起動します。[コンピュータ（Computer）] に「*ad-out.dcloud-out.cisco.com*」と入力して [接続（Connect）] をクリックし、DNS サーバにリモートからアクセスします。

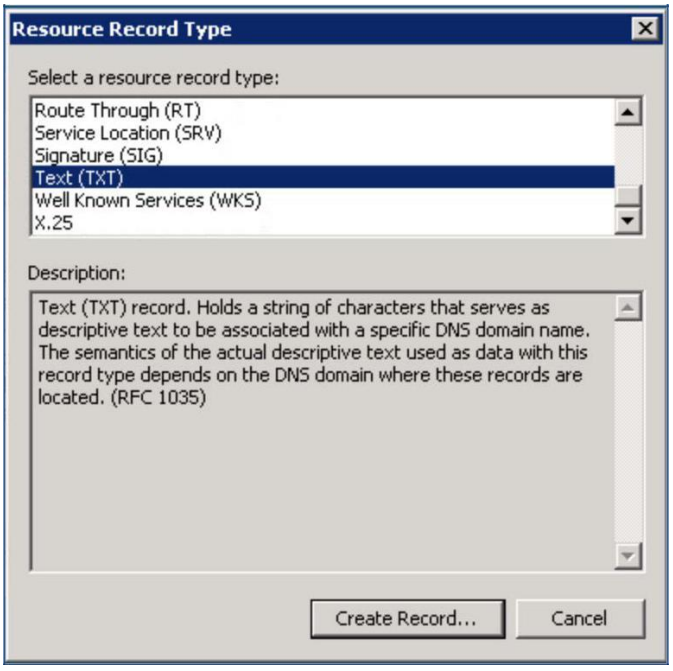
2. 次のクレデンシャルを使用してログインします。表示されるセキュリティ警告をすべて認めます。ログイン後、[DNS] アイコンをクリックして DNS マネージャーのインターフェイスを起動します。**ユーザ名**：DCLOUD-OUT\Administrator、**パスワード**：C1sco12345



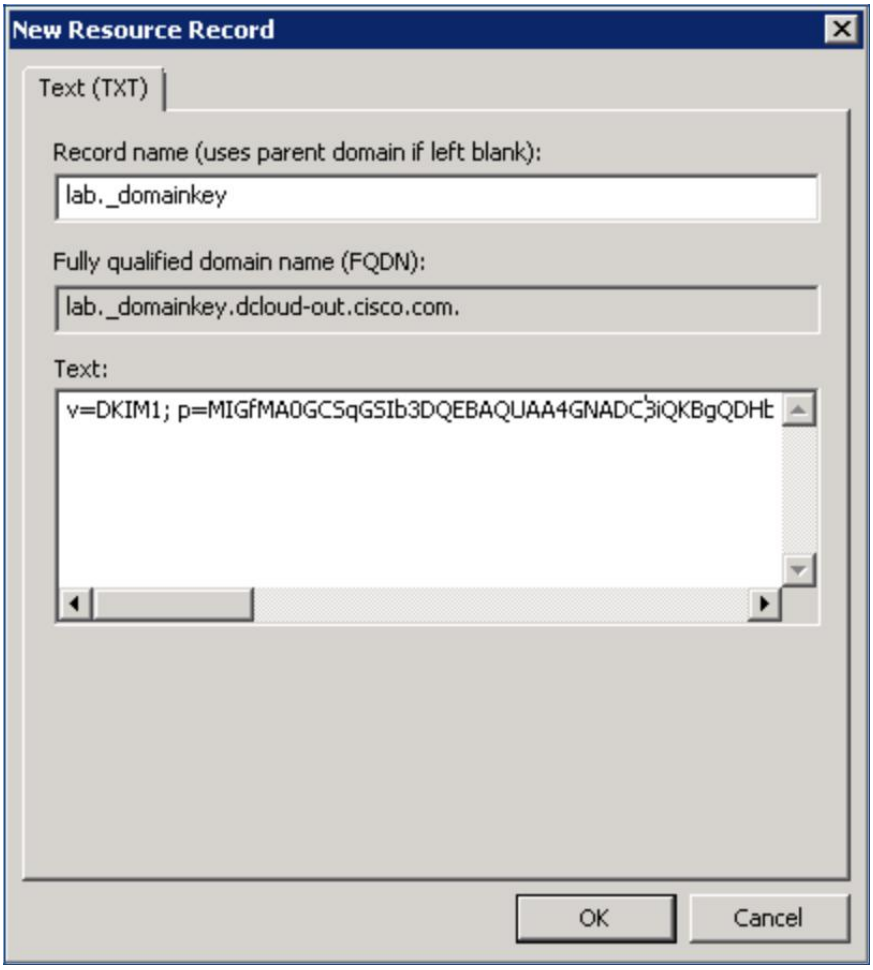
3. [前方参照ゾーン（Forward Lookup Zones）] をダブルクリックし、「dcloud-out.cisco.com」を選択します。右ペインの空白部分を右クリックし、リストから [その他の新しいレコード（Other New Records）] を選択します。



4. ドロップダウンリストを最後までスクロールして [テキスト（TXT）（Text (TXT)）] を選択し、[レコードの作成…（Create Record …）] をクリックします。

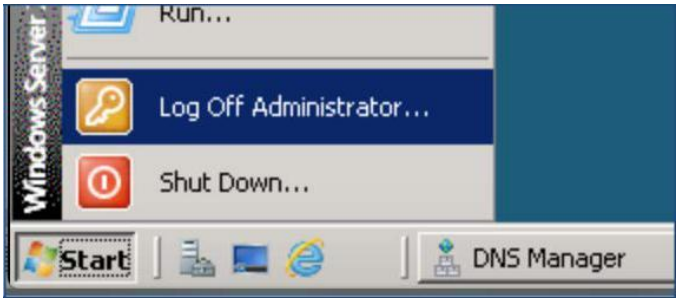


5. [レコード名（Record Name）] に「*lab._domainkey*」と入力して、ESA2 からコピーした「*v=DKIM1; p=MIGf … AQAB;*」の文字列を [テキスト（Text）] ボックスにペーストします。[OK] をクリックします。

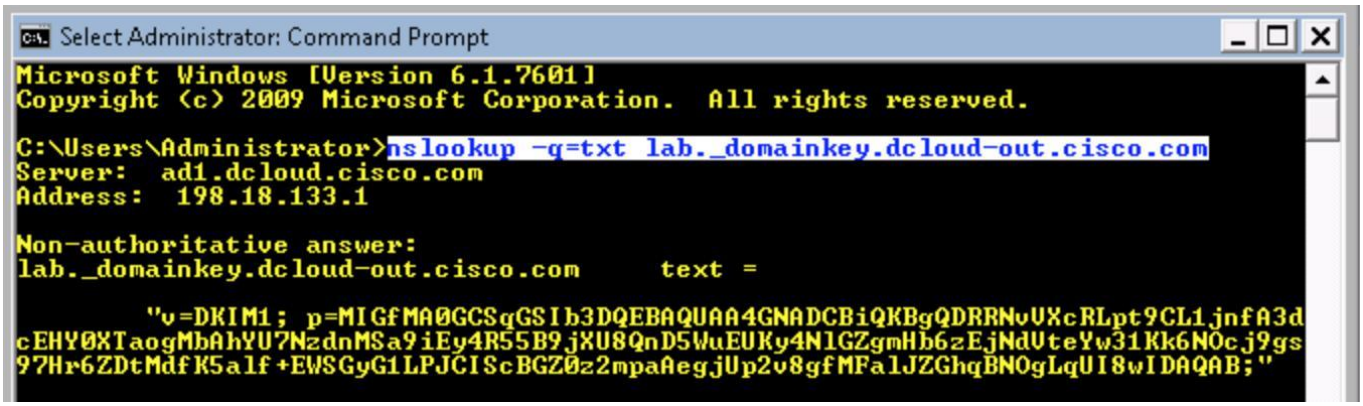


6. [完了（Done）] をクリックします。

7. 完了したら、[スタート（Start）] メニューから [Administratorのログオフ（Log Off Administrator）] をクリックしてリモート デスクトップ セッションを終了します。

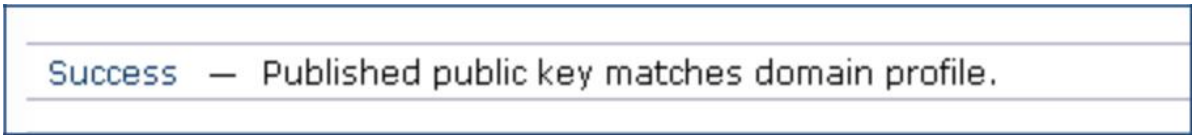


8. ワークステーションのデスクトップで、コマンド プロンプトを起動して、「*nslookup -q=txt lab._domainkey.dcloud-out.cisco.com*」と入力し、DKIM レコードを確認します。



9. ESA2 の GUI に戻ります。新しい署名プロファイルの [テストプロファイル（Test Profile）] 列で、[テスト（Test）] をクリックして DKIM レコードが適切に作成されていることを確認します。

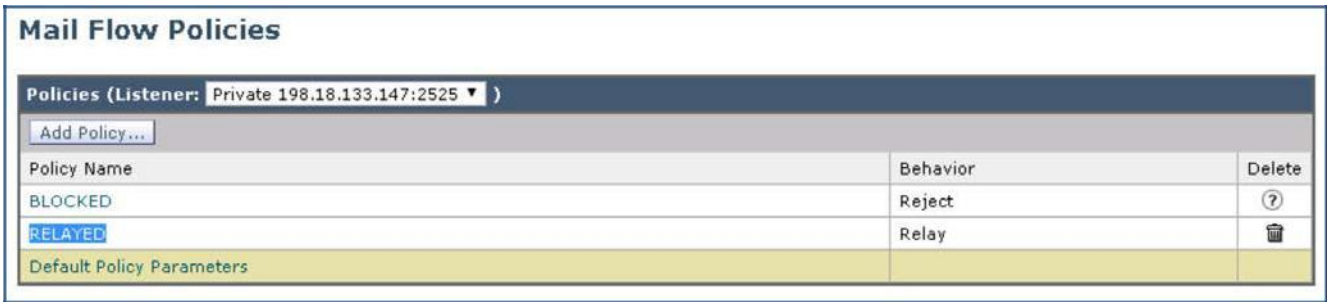
10. [成功-公開した公開キーはドメインプロファイルと一致しています（Success − Published public key matches domain profile）] というテキスト メッセージがプロファイルの上に表示されます。



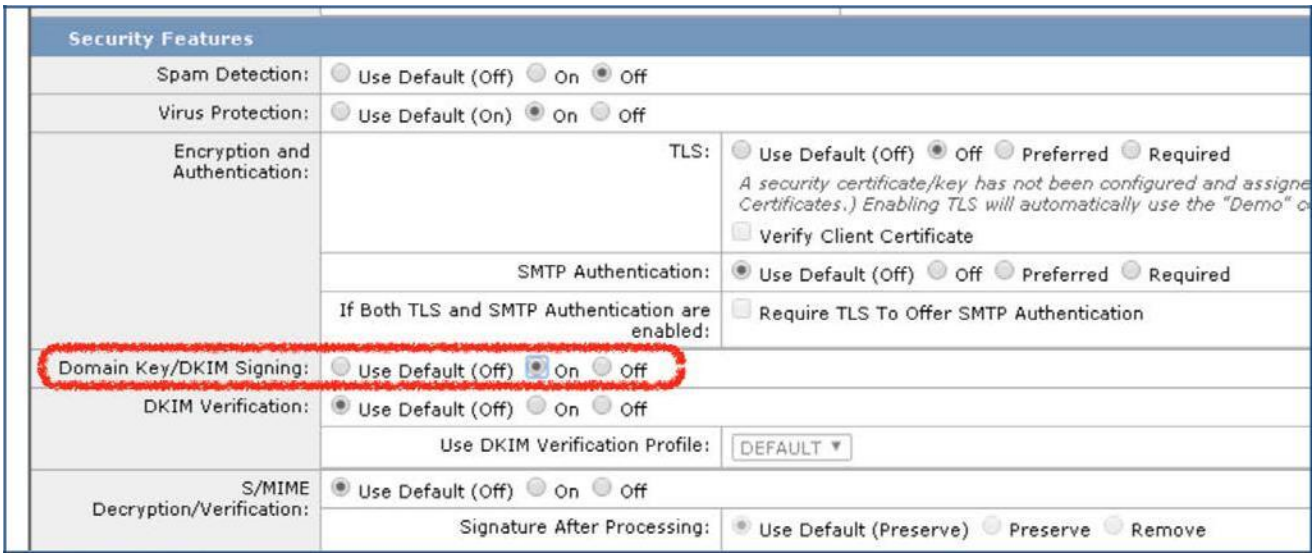
DKIM の署名を有効にする（送信者）（推定所要時間：1 分）

この時点で、送信者は、社外への送信メール フロー ポリシーについて DKIM の署名をいつでも有効にできるようになっています。この機能により、DKIM の秘密キーを使用してメールに署名し、受信者に送信することができます。

1. ESA2 の GUI にログインします。[メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] に移動し、リスナー「Private 198.18.133.147:2525」を選択します。メール フロー ポリシー名 [リレー（RELAYED）] をクリックします。



2. [セキュリティ機能（Security Features）] セクションが表示されるまでページを下にスクロールします。[On] を選択して、[DomainKeys/DKIM署名（DomainKeys/DKIM Signing）] を有効にします。

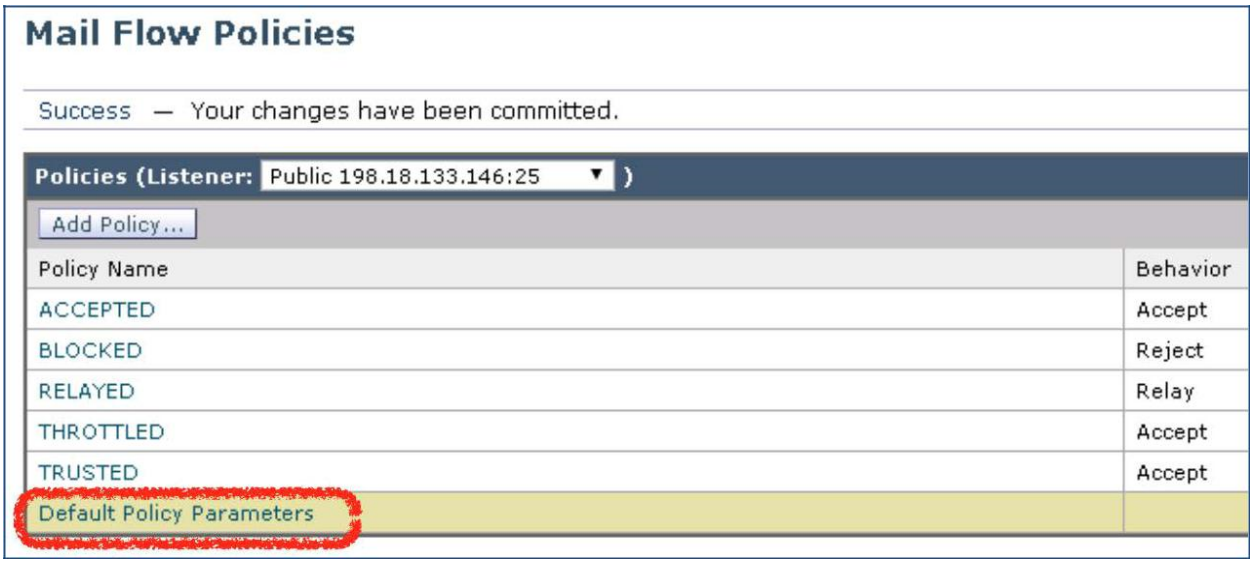


3. このページの一番下にある [送信（Submit）] を選択し、[変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

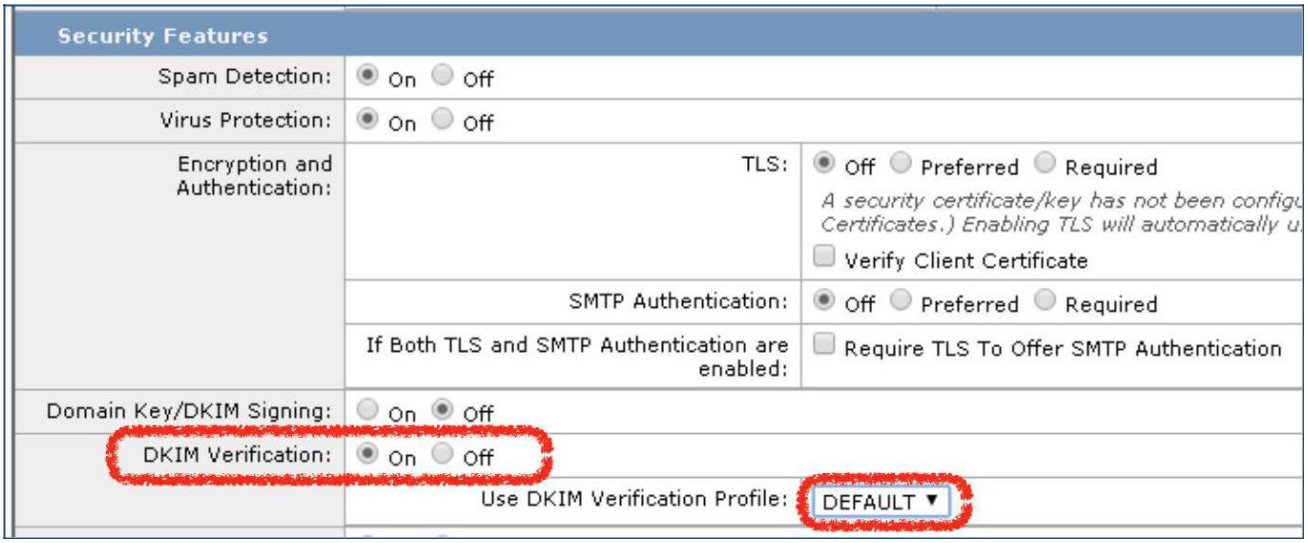
DKIM 検証を有効化する（受信者）（推定所要時間：1 分）

これで、DKIM による署名が機能するようになったので、今度は DKIM 検証を有効にします。Cisco E メール セキュリティ ソリューションではメッセージの受信時に、署名にあるドメインの DNS レコードから公開キーを取得し、そのキーによりメッセージの DKIM の署名をテストして、メッセージの有効性を判定します。DKIM の署名が検証テストを通過すると、メッセージは通常の配信プロセスで次のステップに進みます。こうした機能により、送信者が詐称されたメッセージが分かるだけでなく、署名から受信者への配信までの間にメッセージが変更されていないことも確認できます。

1. ワークステーションで ESA の GUI にアクセスします。[メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] に移動し、リスナー「Public 198.18.133.146:25」を選択します。メール フロー ポリシー名 [デフォルトポリシーパラメータ（Default Policy Parameters）] をクリックします。



2. [セキュリティ機能（Security Features）] セクションが表示されるまでページを下にスクロールします。[On] を選択して、[DKIM検証（DKIM Verification）] を有効にします。事前定義された DKIM 検証プロファイル（デフォルト）が、すでに Cisco E メール セキュリティで利用可能になっていることを確認してください。



3. このページの一番下にある [送信（Submit）] を選択し、[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。

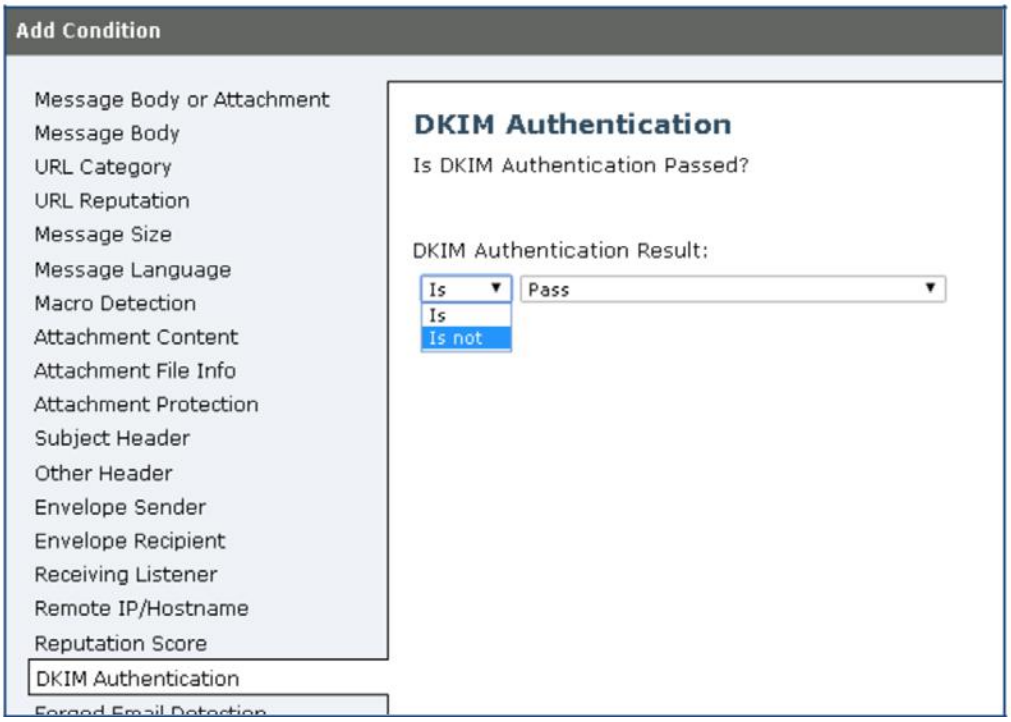
コンテンツ フィルタを設定する（受信者）（推定所要時間：8 分）

このタスクでは、受信側メール サーバでの DKIM 署名のテスト結果に基づいてアクションを適用する新しいコンテンツ フィルタを作成します。たとえば、DKIM の検証プロセス中に署名が一致しないことが確認されると、DKIM の署名付きメッセージがドロップまたは検疫されることがあります。

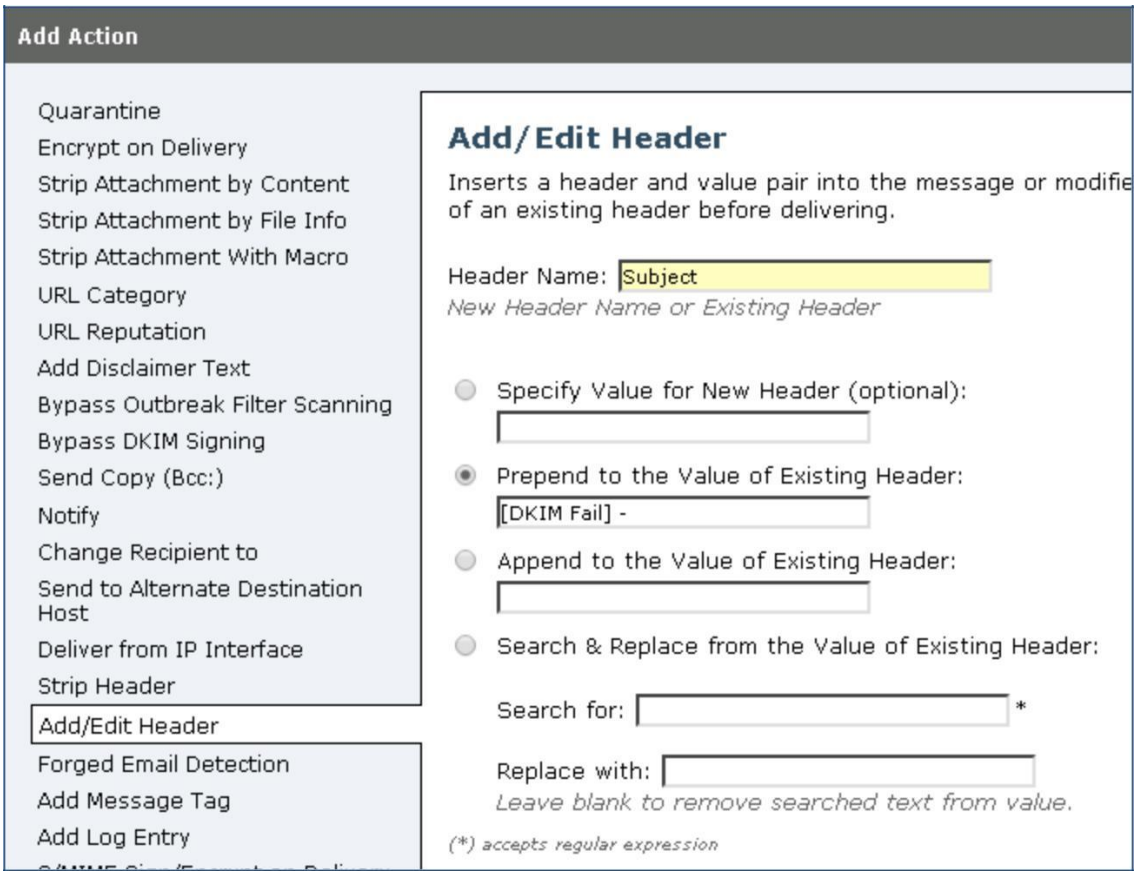
1. 前のタスクの GUI を引き続き使用し、[メールポリシー（Mail Policy）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動して、[フィルタの追加（Add Filter）] をクリックします。

2. 次の設定で*条件*と*アクション*を設定します。

名前:	DKIM_Verification
説明:	特定の送信者に対する DKIM 検証（オプション）
条件:	[DKIM認証（DKIM authentication）] > [が次の判定ではない（Is not）] > [通過（Pass）]
アクション 1:	[ヘッダーの追加と編集（Add/Edit Header）] > [ヘッダー名（Header Name）]：Subject > [既存ヘッダーの値の前に付加（Prepend to the Value of Existing Header）]：[DKIM FAIL]（DKIM 失敗）



3. [OK] をクリックします。



4. [OK] をクリックします。

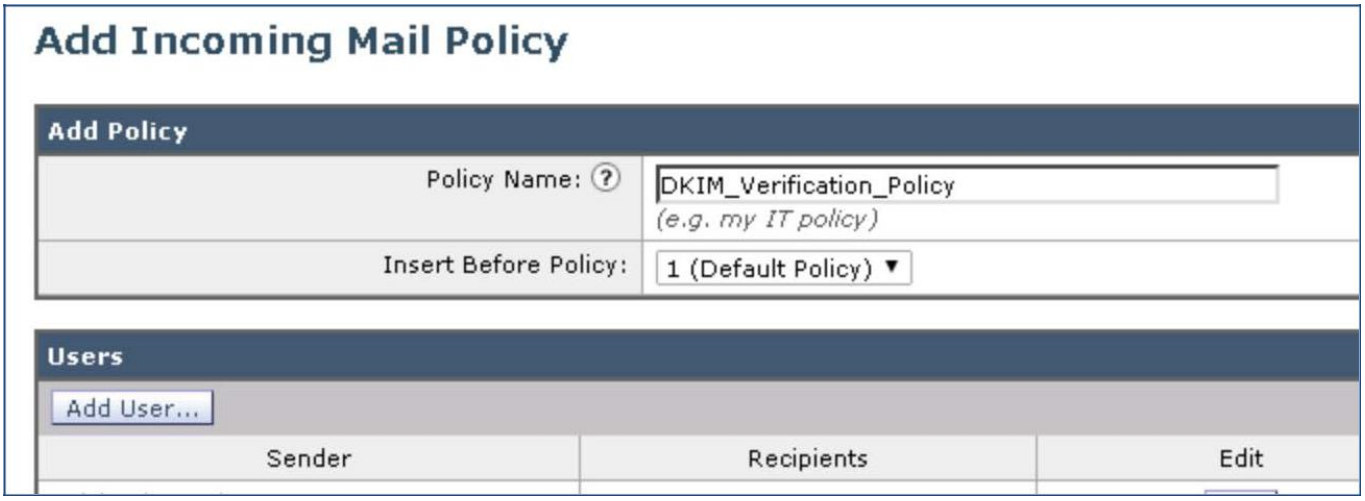
5. [送信（Submit）] をクリックしてコンテンツ フィルタを作成します。完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

受信メール ポリシーを編集する（受信者）（推定所要時間：15 分）

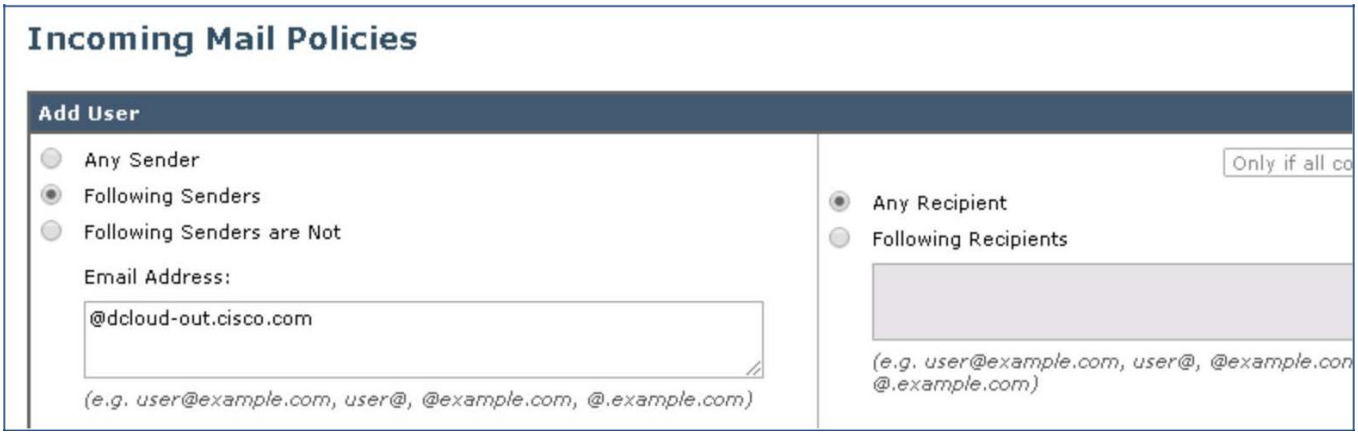
最後のタスクはデフォルトの受信メール ポリシーを変更して、コンテンツ フィルタを有効にすることです。

1. [メールポリシー（Mail Policy）] >[受信コンテンツフィルタ（Incoming Content Filters）] に移動し、[ポリシーの追加...（Add Policy...）] をクリックして新しいポリシーを作成します。

2. ポリシー名を「DKIM_Verification_Policy」とし、[ユーザの追加（Add Users）] をクリックします。

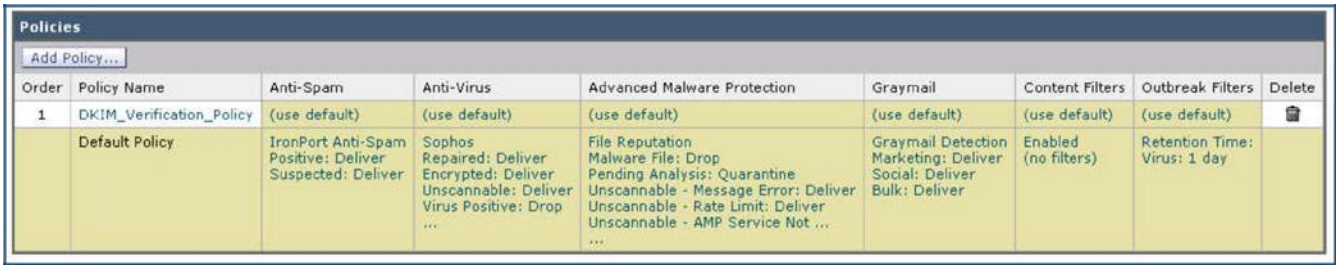


3. ボックスの左側で、[次の送信者（Following Senders）] を選択して、[メールアドレス：（Email Address:）] ボックスに「@dcloud-out.cisco.com」を追加します。

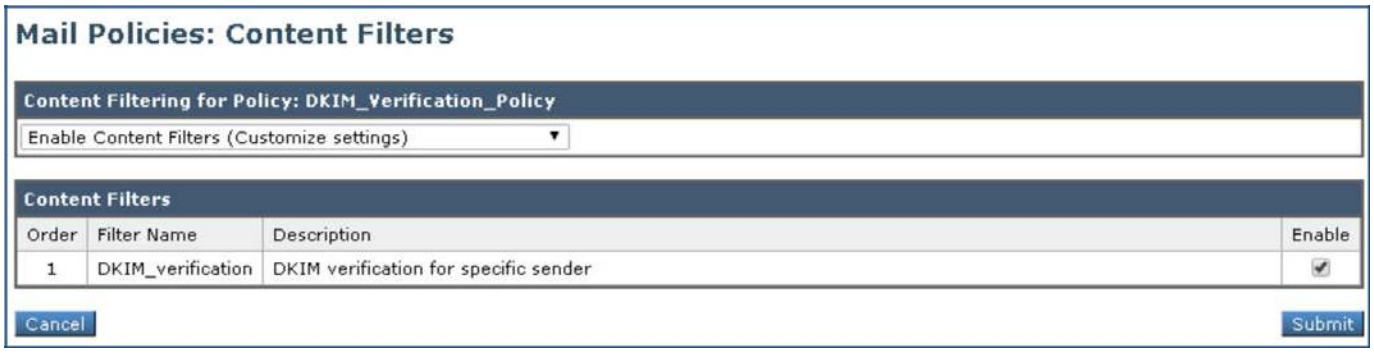


4. [OK] をクリックし、[送信（Submit）] を選択します。

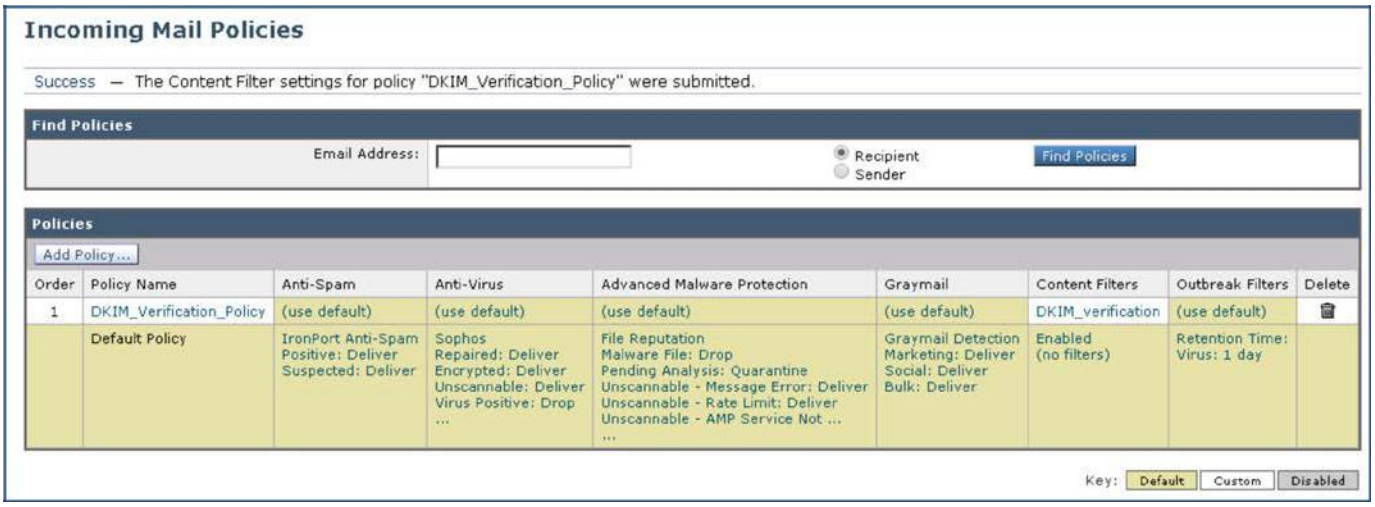
5. 新しいポリシー「DKIM_Verification_Policy」の [コンテンツフィルタ（Content Filters）] ボックス内をクリックします。



6. [コンテンツフィルタを有効にする（カスタマイズ設定）] を選択します。前のタスクで作成した「DKIM_Verification」コンテンツ フィルタにチェックマークを付けて有効にします。



7. [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。

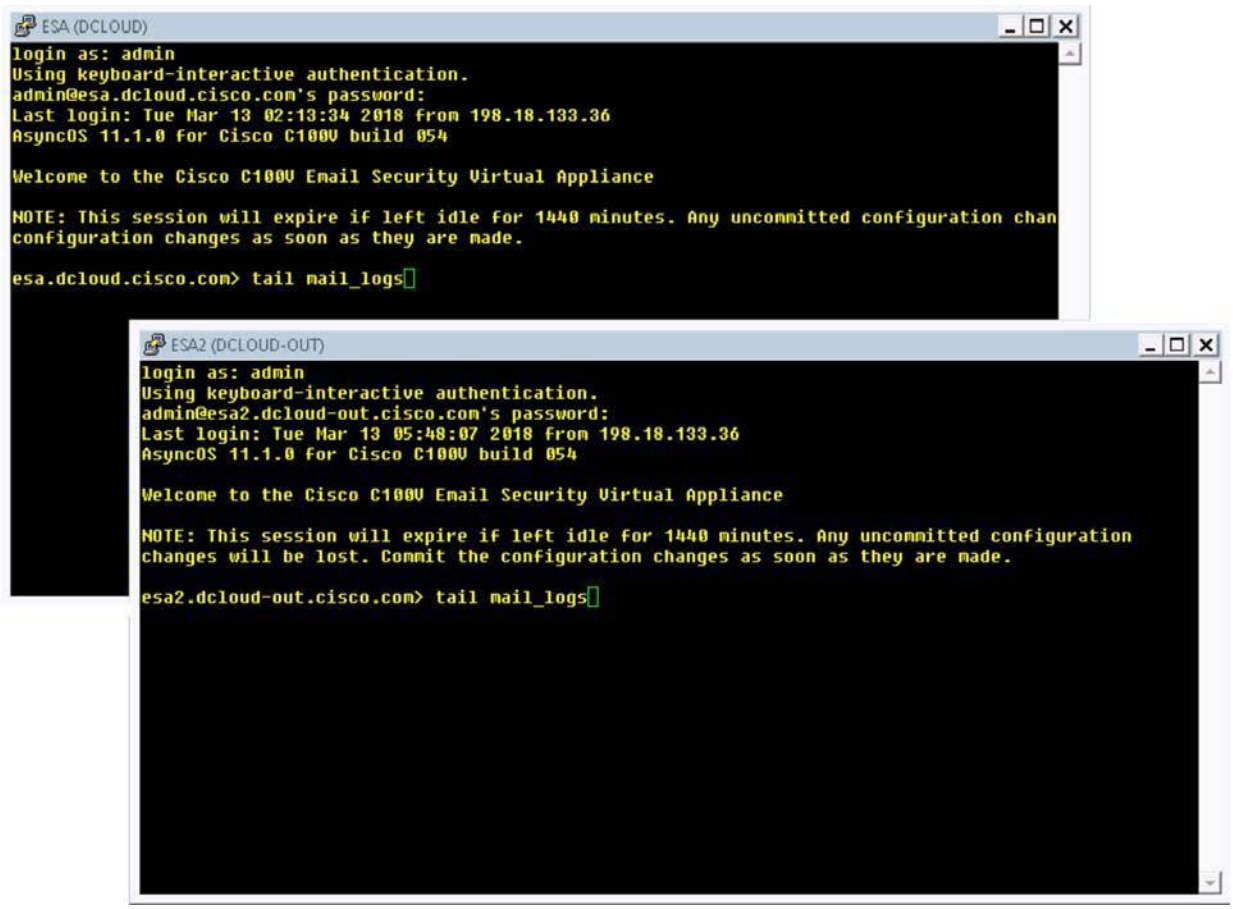


8. 完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

DKIM（送信者と受信者）をテストする（推定所要時間：10 分）

構成をすべて完了したら、@dcloud-out.cisco.com で終わるメールアドレスを使用して社外ユーザから Alan にメールを送信することで、DKIM 署名と DKIM 検証の両方の機能をテストできます。

1. メッセージを準備する前に、CLI を使用して ESA と ESA2 の両方への接続を開始し、メール ログを表示します（ログの確認には「tail」コマンドを使います）。メッセージが一連の設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。



2. ワークステーションから Microsoft Outlook を起動し、Ben 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。

送信者:	ben@dcloud-out.cisco.com
受信者:	alan@dcloud.cisco.com
件名:	DKIM のテスト
本文:	こんにちは、Alan これは、DKIM をテストするためのメール送信です。

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。

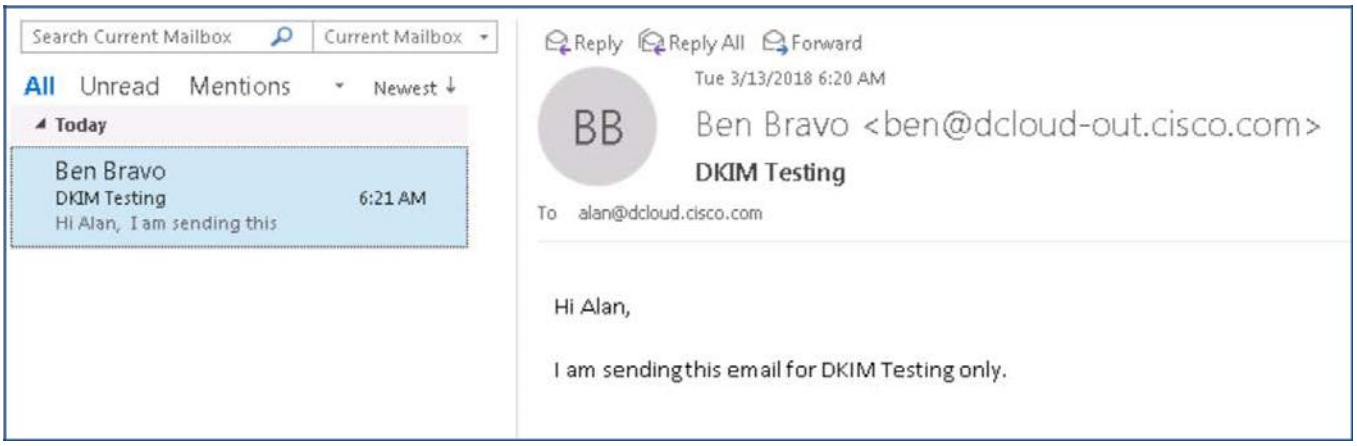
4. ESA2 の CLI に切り替えます。DKIM プロファイルによって、どのようにメール ドメインに一致する送信者が確認され、宛先ホストへの配信の開始前にメッセージが署名されるのかに注目します。

```
Tue Mar 13 06:20:26 2018 Info: New SMTP ICID 134 interface Management (198.18.133.147) address 198.18.133.36 reverse dns
host wkst1.dcloud.cisco.com verified yes
Tue Mar 13 06:20:26 2018 Info: ICID 134 RELAY SG RELAYLIST match 198.18.133.0/24 SBRS not enabled country not enabled
Tue Mar 13 06:20:26 2018 Info: Start MID 170 ICID 134
Tue Mar 13 06:20:26 2018 Info: MID 170 ICID 134 From: <ben@dcloud-out.cisco.com>
Tue Mar 13 06:20:26 2018 Info: MID 170 ICID 134 RID 0 To: <alan@dcloud.cisco.com>
Tue Mar 13 06:20:26 2018 Info: MID 170 Message-ID '<000001d3ba93$60592490$210b6db0$@dcloud-out.cisco.com>'
Tue Mar 13 06:20:26 2018 Info: MID 170 Subject 'DKIM Testing'
Tue Mar 13 06:20:26 2018 Info: MID 170 ready 2825 bytes from <ben@dcloud-out.cisco.com>
Tue Mar 13 06:20:26 2018 Info: MID 170 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Mar 13 06:20:26 2018 Info: MID 170 DomainKeys: cannot sign - no profile matches ben@dcloud-out.cisco.com
Tue Mar 13 06:20:26 2018 Info: MID 170 DKIM: signing with DKIM_Signing - matches ben@dcloud-out.cisco.com
Tue Mar 13 06:20:26 2018 Info: MID 170 queued for delivery
Tue Mar 13 06:20:26 2018 Info: New SMTP DCID 127 interface 198.18.133.147 address 198.18.133.146 port 25
Tue Mar 13 06:20:26 2018 Info: Delivery start DCID 127 MID 170 to RID [0]
Tue Mar 13 06:20:26 2018 Info: MID 170 DKIM: signed with DKIM_Signing
Tue Mar 13 06:20:26 2018 Info: Message done DCID 127 MID 170 to RID [0]
Tue Mar 13 06:20:26 2018 Info: MID 170 RID [0] Response 'ok:  Message 192 accepted'
Tue Mar 13 06:20:26 2018 Info: Message finished MID 170 done
Tue Mar 13 06:20:28 2018 Info: ICID 134 close
Tue Mar 13 06:20:31 2018 Info: DCID 127 close
```

5. 次に、ESA の CLI を見て、DKIM 検証により「通過（Pass）」と判定されたメッセージが受信されたことを確認してください。

```
Tue Mar 13 06:20:27 2018 Info: New SMTP ICID 123 interface Management (198.18.133.146) address 198.18.133.147 reverse dns host u
nknown verified no
Tue Mar 13 06:20:27 2018 Info: ICID 123 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country None
Tue Mar 13 06:20:27 2018 Info: Start MID 192 ICID 123
Tue Mar 13 06:20:27 2018 Info: MID 192 ICID 123 From: <ben@dcloud-out.cisco.com>
Tue Mar 13 06:20:27 2018 Info: MID 192 ICID 123 RID 0 To: <alan@dcloud.cisco.com>
Tue Mar 13 06:20:27 2018 Info: MID 192 DKIM: pass signature verified (d=dcloud-out.cisco.com s=lab i=@dcloud-out.cisco.com)
Tue Mar 13 06:20:27 2018 Info: MID 192 Message-ID '<000001d3ba93$60592490$210b6db0$@dcloud-out.cisco.com>'
Tue Mar 13 06:20:27 2018 Info: MID 192 Subject 'DKIM Testing'
Tue Mar 13 06:20:27 2018 Info: MID 192 ready 3418 bytes from <ben@dcloud-out.cisco.com>
Tue Mar 13 06:20:27 2018 Info: MID 192 matched all recipients for per-recipient policy DKIM_Verification_Policy in the inbound t
able
Tue Mar 13 06:20:27 2018 Info: MID 192 interim AV verdict using McAfee CLEAN
Tue Mar 13 06:20:27 2018 Info: MID 192 interim AV verdict using Sophos CLEAN
Tue Mar 13 06:20:27 2018 Info: MID 192 antivirus negative
Tue Mar 13 06:20:27 2018 Info: MID 192 AMP file reputation verdict : SKIPPED (no attachment in message)
Tue Mar 13 06:20:27 2018 Info: MID 192 using engine: GRAYMAIL negative
Tue Mar 13 06:20:31 2018 Info: MID 192 Outbreak Filters: verdict negative
Tue Mar 13 06:20:31 2018 Info: MID 192 queued for delivery
Tue Mar 13 06:20:31 2018 Info: New SMTP DCID 49 interface 198.18.133.146 address 198.18.133.2 port 25
Tue Mar 13 06:20:31 2018 Info: Delivery start DCID 49 MID 192 to RID [0]
Tue Mar 13 06:20:32 2018 Info: ICID 123 close
Tue Mar 13 06:20:33 2018 Info: Message done DCID 49 MID 192 to RID [0]
Tue Mar 13 06:20:33 2018 Info: MID 192 RID [0] Response '2.6.0 <000001d3ba93$60592490$210b6db0$@dcloud-out.cisco.com> [Internall
d=1] Queued mail for delivery'
Tue Mar 13 06:20:33 2018 Info: Message finished MID 192 done
Tue Mar 13 06:20:38 2018 Info: DCID 49 close
```

6. ワークステーションに戻り、メッセージをもう一度同期します。これで、Alan のメールボックスにメッセージが表示されますが、件名のヘッダーが変更されていないことを確認します。



シナリオ 7:　Sender Policy Framework（SPF）を有効にする

ユースケース

前のシナリオの結果、Jacob の会社のゲートウェイすべてに DKIM が展開された頃に、メッセージング チームは正当な送信者についてのデータをすべての関係者から首尾よく収集することができました。メール送信が許可されたすべての IP アドレスのリスト化を自社ではなく SPF で行うことで保護機能を拡張できるため、Jacob は DKIM と連携する SPF の導入を進め、スプーフィングからの防御対策を強化することにしました。

セキュリティ制御

Send Policy Framework（SPF）は今でも偽装メールやスプーフィングをブロックする効果的なツールと考えられています。SPF では、受信メール サーバへのメールの配信前に、送信者のメール サーバが検証されます。SPF による確認を有効にした受信側メール ゲートウェイで社外からのメールが受信されると、Cisco E メール セキュリティ ソリューションでは、管理者が、送信者のドメインを DNS に公開された SPF レコードと照合して検証できます。また、送信サーバの IP アドレスが許可リストにあるかどうかを確認でき、一致するアドレスがない場合は検証に失敗します。

目的

このシナリオでは、SPF において、送信メール サーバの IP アドレスを、DNS に公開された、送信者のメール ドメインの SPF レコードと比較することで、エンベロープの送信者アドレスを保護する方法を説明します。メールと送信者を DNS レコードのリストで確認できない場合は、SPF 認証に失敗します。

注: SPF の詳細については「Overview of SPF and SIDF Verification」を参照してください。

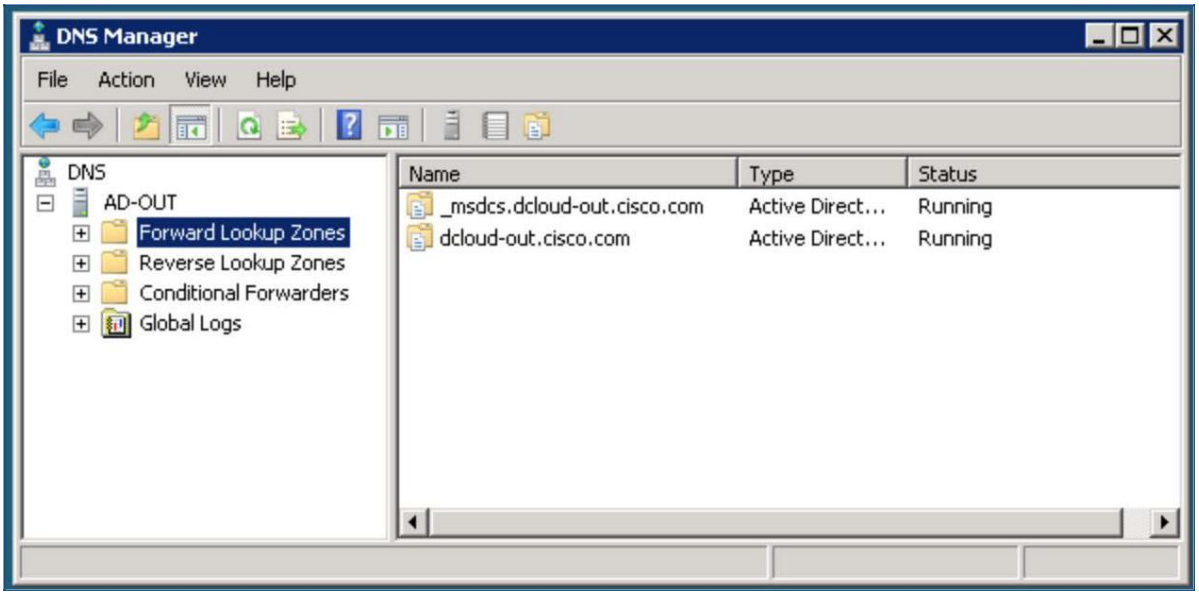
手順

タスク:SPF レコードを作成する（送信者）（推定所要時間:15 分）

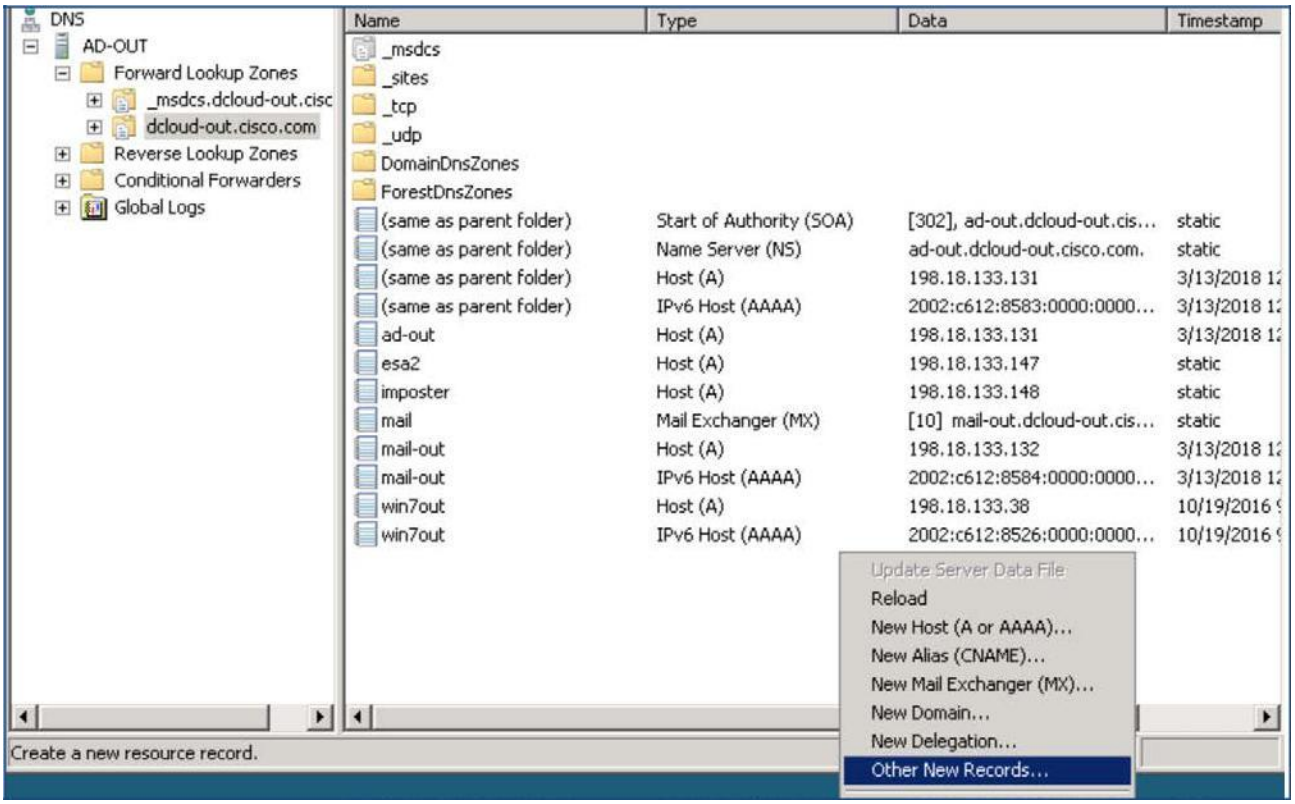
SPF レコードとは、送信元ドメインからのメール送信を許可したサーバの一覧です。SPF レコードの目的は、スパム送信者を検出し、そのような送信者が送信元ドメインの From アドレスを詐称したメッセージを送信できないようにすることです。

1. ワークステーションから、タスクバーにある *RDC* を起動します。[コンピュータ（Computer）] に「*ad-out.dcloud-out.cisco.com*」と入力して [接続（Connect）] をクリックし、DNS サーバにリモートからアクセスします。

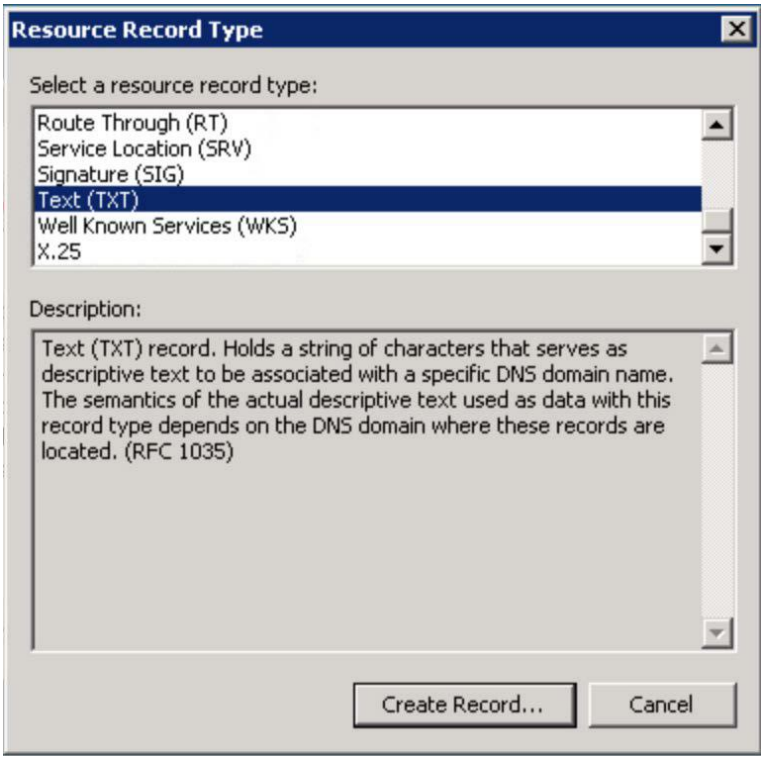
2. 次のクレデンシャルを使用してログインします。表示されるセキュリティ警告をすべて認めます。ログイン後、[DNS] アイコンをクリックして DNS マネージャーのインターフェイスを起動します。**ユーザ名**:DCLOUD-OUT\Administrator、**パスワード**:C1sco12345



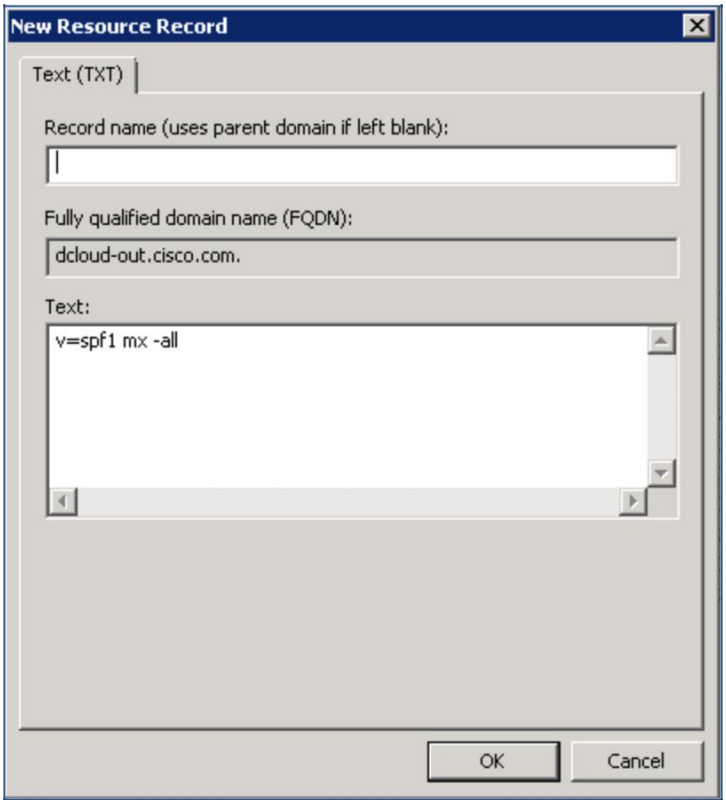
3. [前方参照ゾーン(Forward Lookup Zones)] をダブルクリックし、「dcloud-out.cisco.com」を選択します。右ペインの空白部分を右クリックし、リストから [その他の新しいレコード(Other New Records)] を選択します。



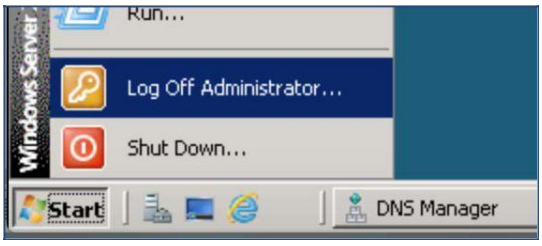
4. ドロップダウンリストを最後までスクロールして [テキスト（TXT）（Text (TXT)）] を選択し、[レコードの作成…（Create Record …）] をクリックします。



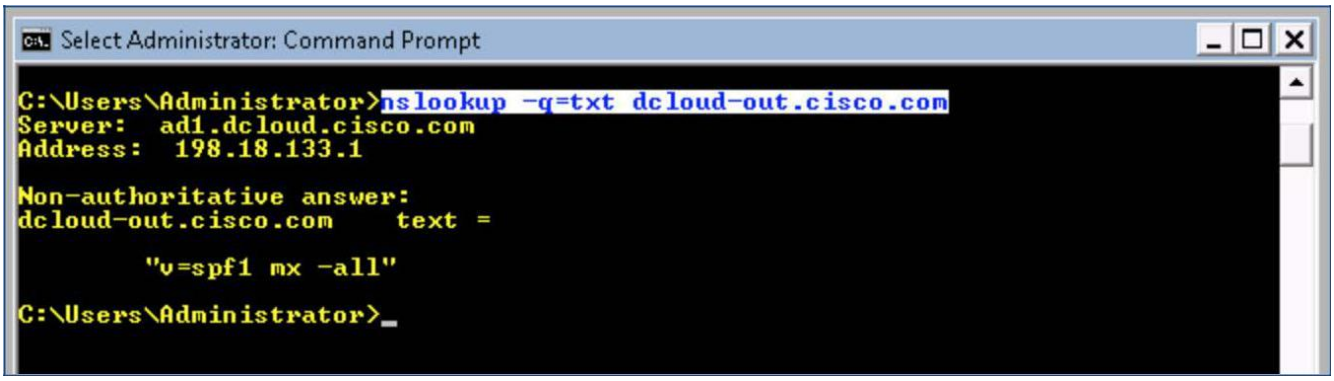
5. [レコード名（Record Name）] は空白のままにし、この文字列「*v=spf1 mx –all*」を [テキスト（Text）] ボックスに入力します。[OK] をクリックします。



6. [完了（Done）] をクリックします。
7. 完了したら、[スタート（Start）] メニューから [Administrator のログオフ（Log Off Administrator）] をクリックしてリモート デスクトップ セッションを終了します。



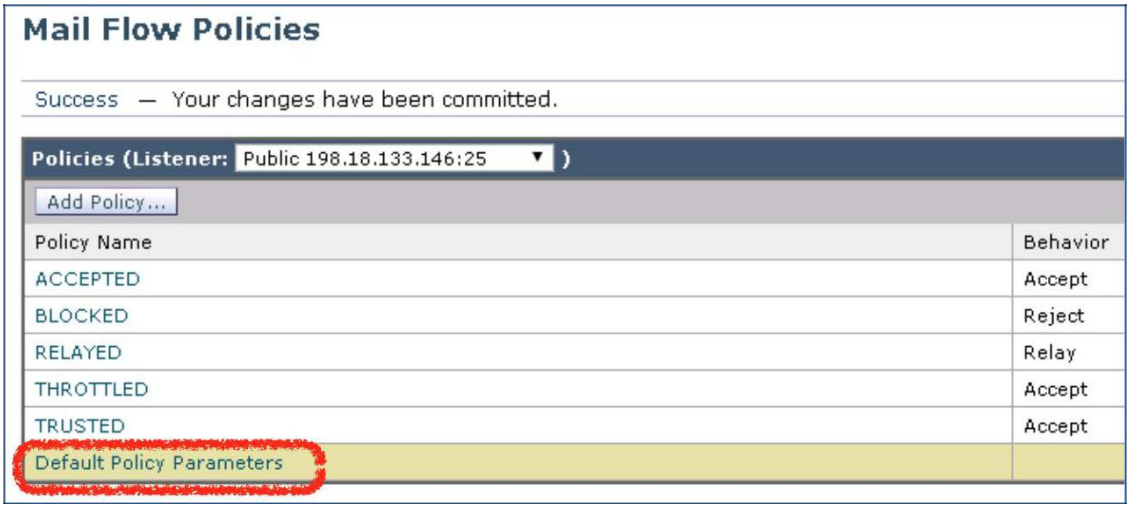
8. ワークステーションのデスクトップで、コマンド プロンプトを起動して、「nslookup –q=txt dcloud-out.cisco.com」と入力し、SPF レコードを確認します。



タスク:SPF 検証を有効にする(受信者)(推定所要時間:1 分)

SPF 検証を有効にすると、受信側の Cisco E メール セキュリティ ソリューションで、公開 DNS 内の送信元 IP アドレスを評価し、送信者からのメール送信が許可されていることを確認できます。SPF では、HELO アイデンティティ(送信メール サーバ)と MAIL FROM アイデンティティ(メッセージの送信元を示すメールアドレス)が確認されます。

1. ワークステーションで ESA の GUI にアクセスします。[メール ポリシー(Mail Policies)] > [メール フロー ポリシー(Mail Flow Policies)] に移動し、リスナー「Public 198.18.133.146:25」を選択します。メール フロー ポリシー名 [デフォルト ポリシー パラメータ(Default Policy Parameters)] をクリックします。



2. [セキュリティ機能(Security Features)] セクションが表示されるまでページを下にスクロールします。[On] を選択して、[SPF/SIDF 検証(SPF/SIDF Verification)] を有効にします。[Resent-Sender: または Resent-From: が使用されていた場合 PRA 検証をダウングレードする:(Choose Downgrade PRA verification result if Resent-Sender: or Resent-From: where used:)] で [はい(Yes)] を選択し、[HELO テスト(HELO Test)] で [On] を選択します。

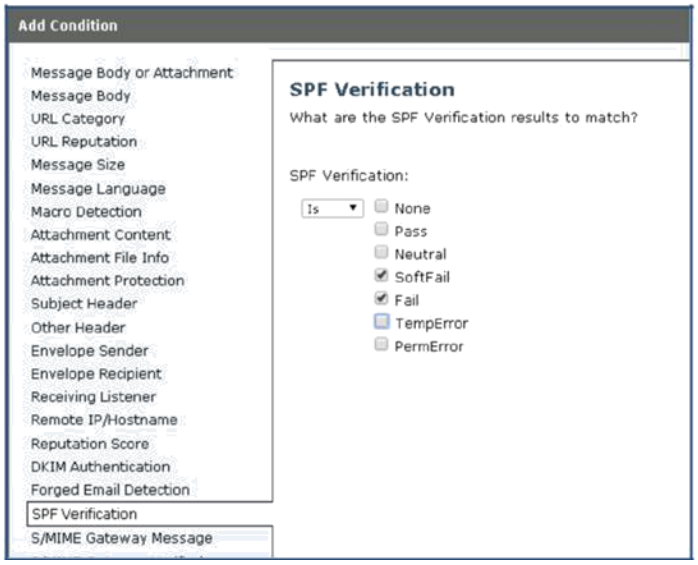
3. [送信(Submit)] を選択し、画面の右上にある [変更内容を確定(Commit Changes)] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

タスク:コンテンツ フィルタを設定する(受信者)(推定所要時間:5 分)

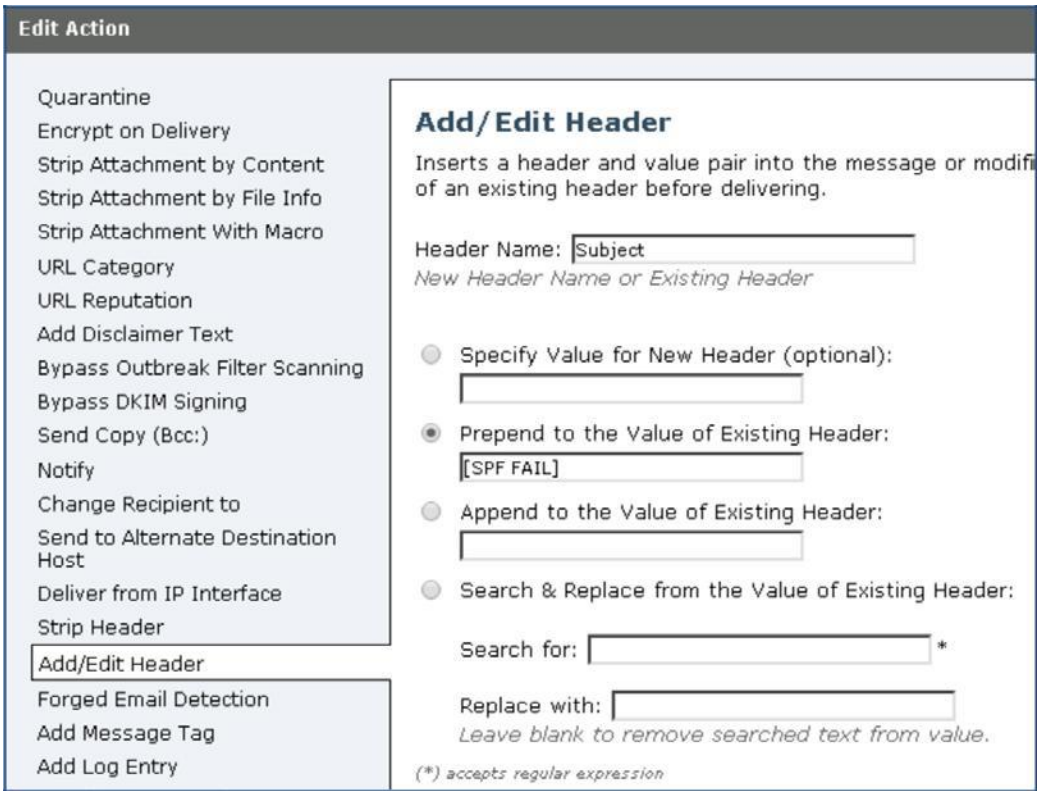
このタスクでは、受信側メール サーバでの SPF 検証のテスト結果に基づいてアクションを適用する新しいコンテンツ フィルタを作成します。たとえば、メッセージが未知の IP アドレスから配信された場合、送信者によっては不正なメッセージの可能性があると考えられます。

1. 前のタスクの GUI を引き続き使用し、[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。

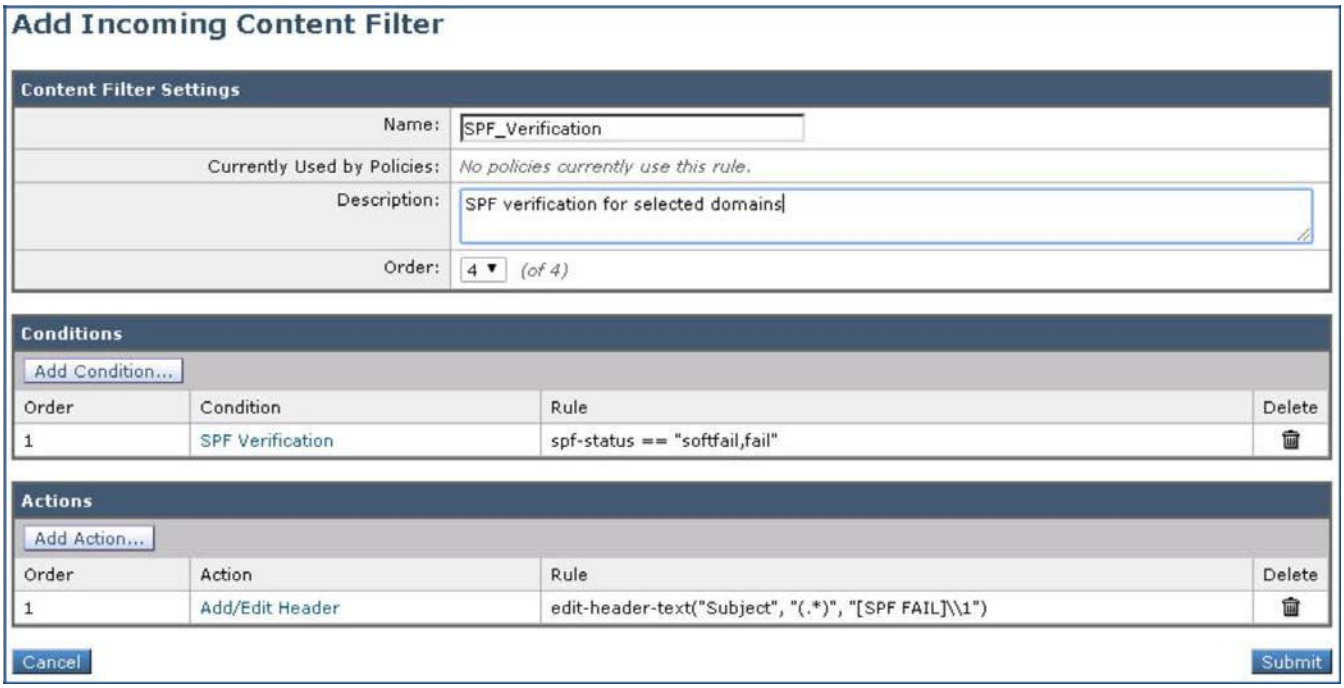
名前:	SPF_Verification
説明:	選択したドメインの SPF 検証
条件:	[SPF 検証(SPF Verification)] > [の結果(Is)] > [SoftFail]、[Fail]
アクション 1:	[ヘッダーの追加と編集(Add/Edit Header)] > [ヘッダー名(Header Name)]:Subject > [既存ヘッダーの値の前に付加(Prepend to the Value of Existing Header)]:[SPF FAIL](SPF 失敗)



2. [OK] をクリックします。



3. [OK] をクリックします。

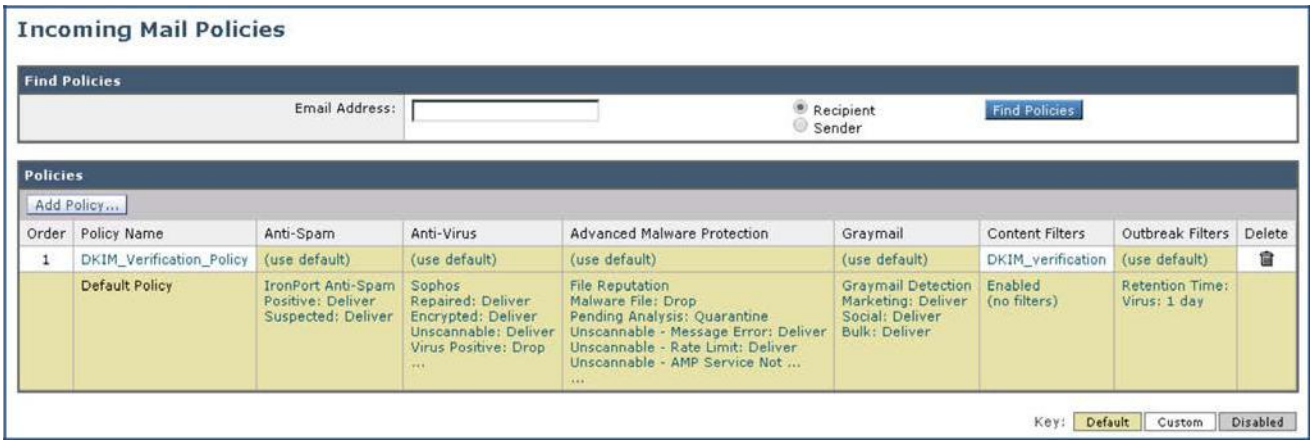


4. [送信（Submit）] をクリックしてコンテンツ フィルタを作成します。完了したら [変更内容を確定（Commit Changes）] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

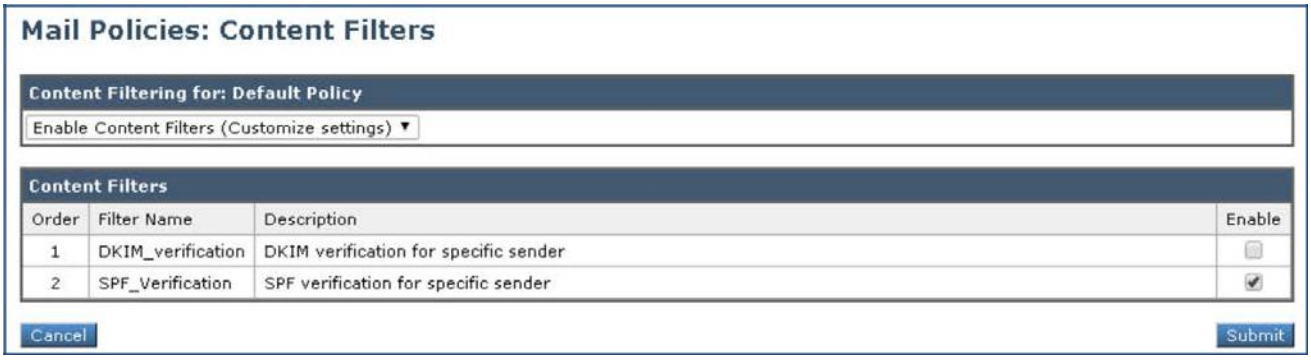
タスク：受信メール ポリシーを編集する（受信者）（推定所要時間：3 分）

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。

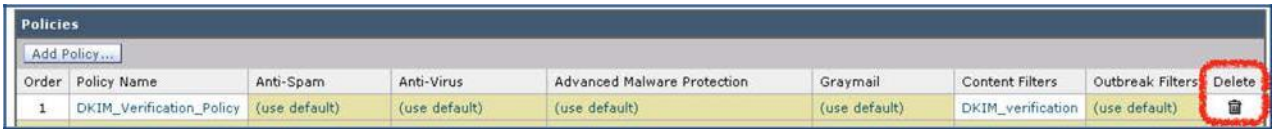
1. ワークステーションから ESA の GUI にアクセスし、[メール ポリシー（Mail Policy）] > [受信メール ポリシー（Incoming Mail Policies）] に移動して、[デフォルト ポリシー（Default Policy）] の [コンテンツ フィルタ（Content Filters）] ボックス内をクリックします。



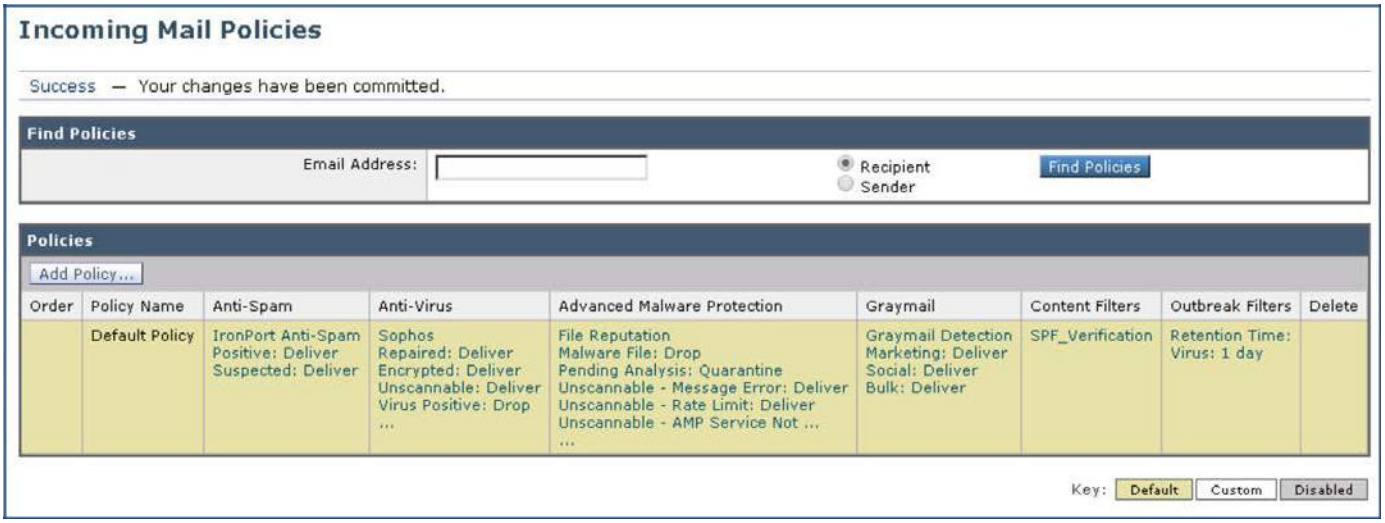
2. 前のタスクで作成した「SPF_Verification」コンテンツ フィルタにチェックマークを付けて有効にします。



3. ラボのテストが目的の場合、[削除（Delete）] アイコンをクリックして [受信メールポリシー（Incoming Mail Policies）] セクションの「DKIM_Verification_Policy」を、削除してください。



4. [送信（Submit）] をクリックします。[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：SPF 検証をテストする（推定所要時間：5 分）

構成をすべて完了したら、dcloud-out.cisco.com で終わるメールアドレスを使用して社外ユーザから Alan にメールを送信することで、SPF 検証の機能をテストできます。

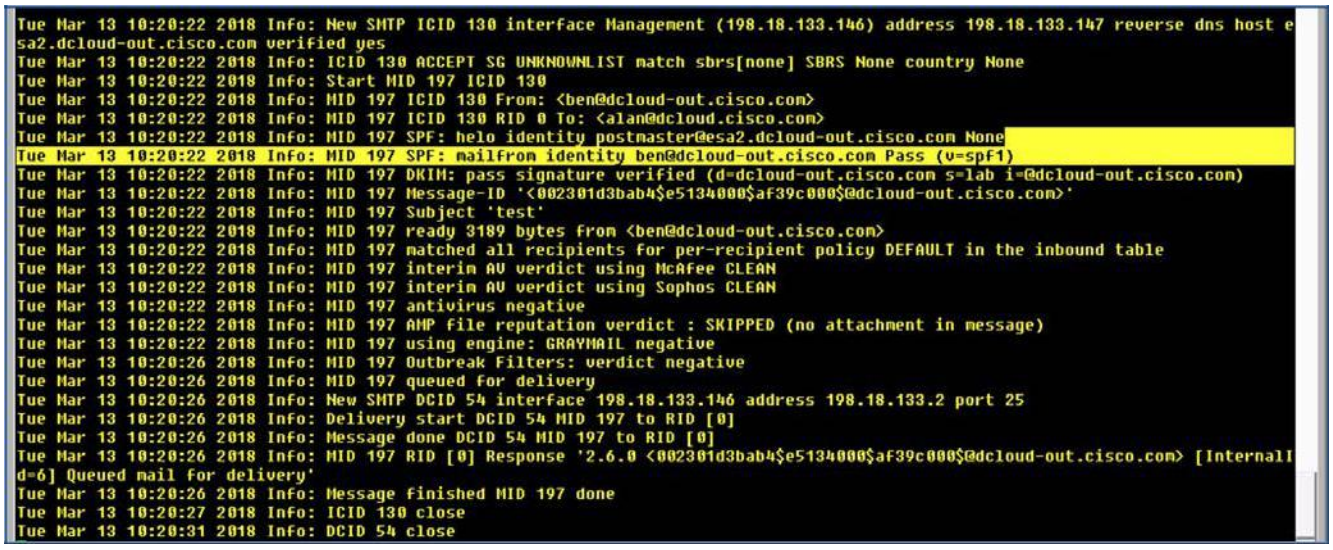
メッセージを準備する前に、CLI を使用して ESA への接続を開始し、メール ログを表示します（ログの確認には「tail」コマンドを使います）。メッセージが一連の設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。

1. ワークステーションから Microsoft Outlook を起動し、Ben 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。

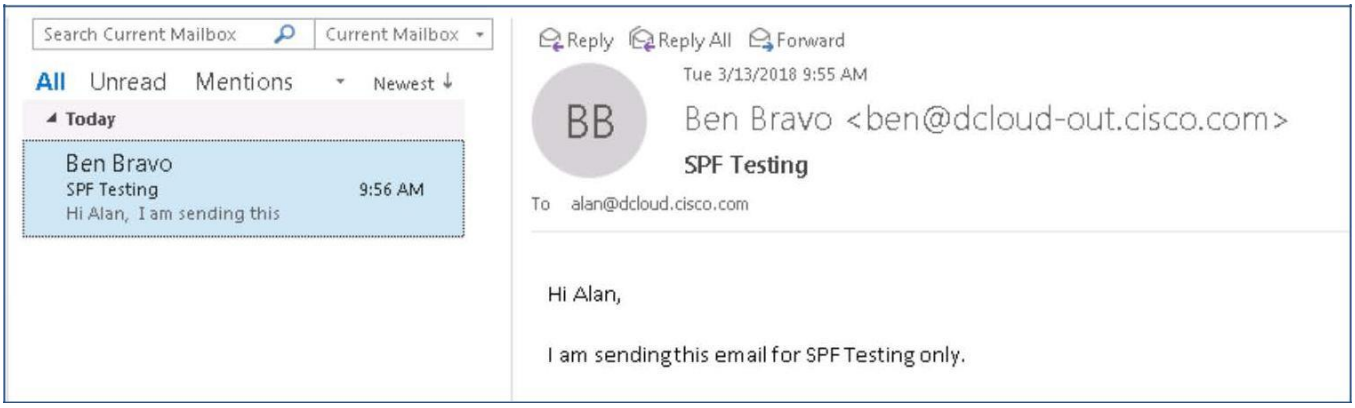
送信者：	ben@dcloud-out.cisco.com
受信者：	alan@dcloud.cisco.com
件名：	SPF のテスト
本文：	こんにちは、Alan これは、SPF をテストするためのメール送信です。

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. ESA の CLI に切り替えます。SPF の機能によって、Mail From アドレスが公開 DNS の SPF レコードと一致していることが明らかになっています。SPF の最終的な判定は「Pass（通過）」です。



4. ワークステーションに戻り、メッセージをもう一度同期します。これで、Alan のメールボックスにメッセージが表示されますが、件名のヘッダーが改ざんされていないことを確認します。



シナリオ 8: Domain-based Message Authentication, Reporting and Conformance（DMARC）の有効化

ユースケース

フィッシング詐欺対策における防御戦略の最後のステップとして、Jacob は DMARC の段階的な展開を計画しています。
DMARC では、最終受信者に表示される From: ヘッダーの情報を使用し SPF または DKIM によって認証した情報（送信元ドメインの情報や署名）を組み合わせて、SPF または DKIM の識別子と From: ヘッダーの識別子が一致しているかどうかを確認します。これにより、Jacob は、会社のドメインから送信したように見せかけ、検証を通過できなかったメッセージをどう処理するかをインターネット上の他のシステムに明示的に指示できます。また、DMARC が備える強力なレポート コンポーネントにより、会社のアイデンティティを悪用する潜在的なフィッシングの試みやキャンペーンを可視化できます。
さらに、専用の分析システムに DMARC のレポートの情報を入力して、自社のブランドの信頼性と不正使用の試みを詳細に把握でき、メール ドメインがどのように利用されるかについて深い洞察を得られます。

セキュリティ制御

Cisco E メール セキュリティ ソリューションにより、管理者は、DMARC を活用して SPF と DKIM を越える機能を得られます。DMARC では、インターネット上でのより安全なメールの通信の実現に送信者と受信者が協力して取り組めます。
DMARC は既存の 2 つのメカニズム、Sender Policy Framework（SPF）と DomainKeys Identified Mail（DKIM）の上に構築します。これにより、ドメインを管理する所有者は、ドメインからメールを送信するときに、採用する仕組み（DKIM、SPF またはその両方）と認証の失敗時に受信者が行うべき対処についてのポリシーを公表できます。

目的

このシナリオでは、DMARC 検証の実装方法と使用方法を示します。DMARC のポリシーでは、メールの SPF または DKIM の整合性チェックが失敗した場合に受信側メール サーバが従うべき処理を指示できます。その後、送信元ドメインでは、社外に送信したメールに対する DMARC 検証の通過または失敗について、レポートを要求できます。

注: DMARC の詳細については「DMARC Verification」を参照してください。

手順

タスク: DMARC レコードを作成する（送信者）（推定所要時間: 15 分）

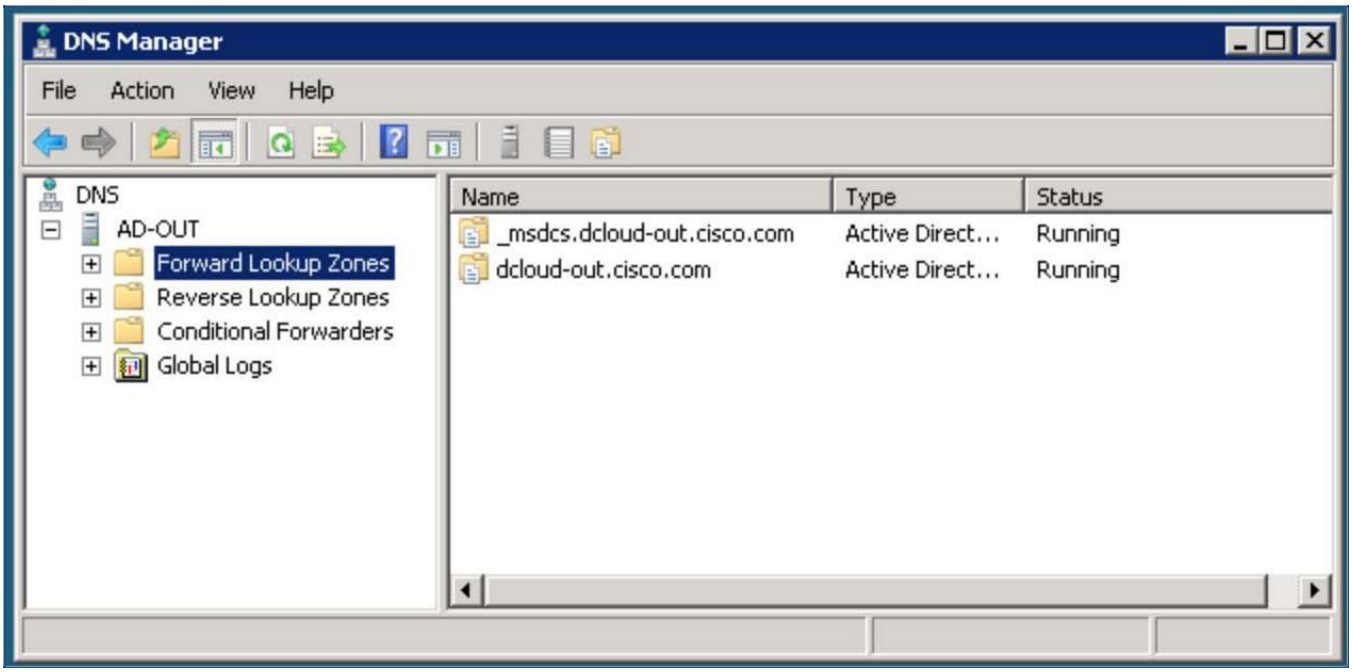
SPF と DKIM のレコードが整うと、管理者は、送信元のメール ドメインにポリシーを追加することで DMARC レコードを設定できます。DMARC ポリシーは、TXT レコードとして公開され、受信したメールが一致しない場合、受信側が何をすべきかを定義します。

1. ワークステーションから、タスクバーにある *RDC* を起動します。[コンピュータ(Computer)] に「*ad-out.dcloud-out.cisco.com*」と入力して [接続(Connect)] をクリックし、DNS サーバにリモートからアクセスします。

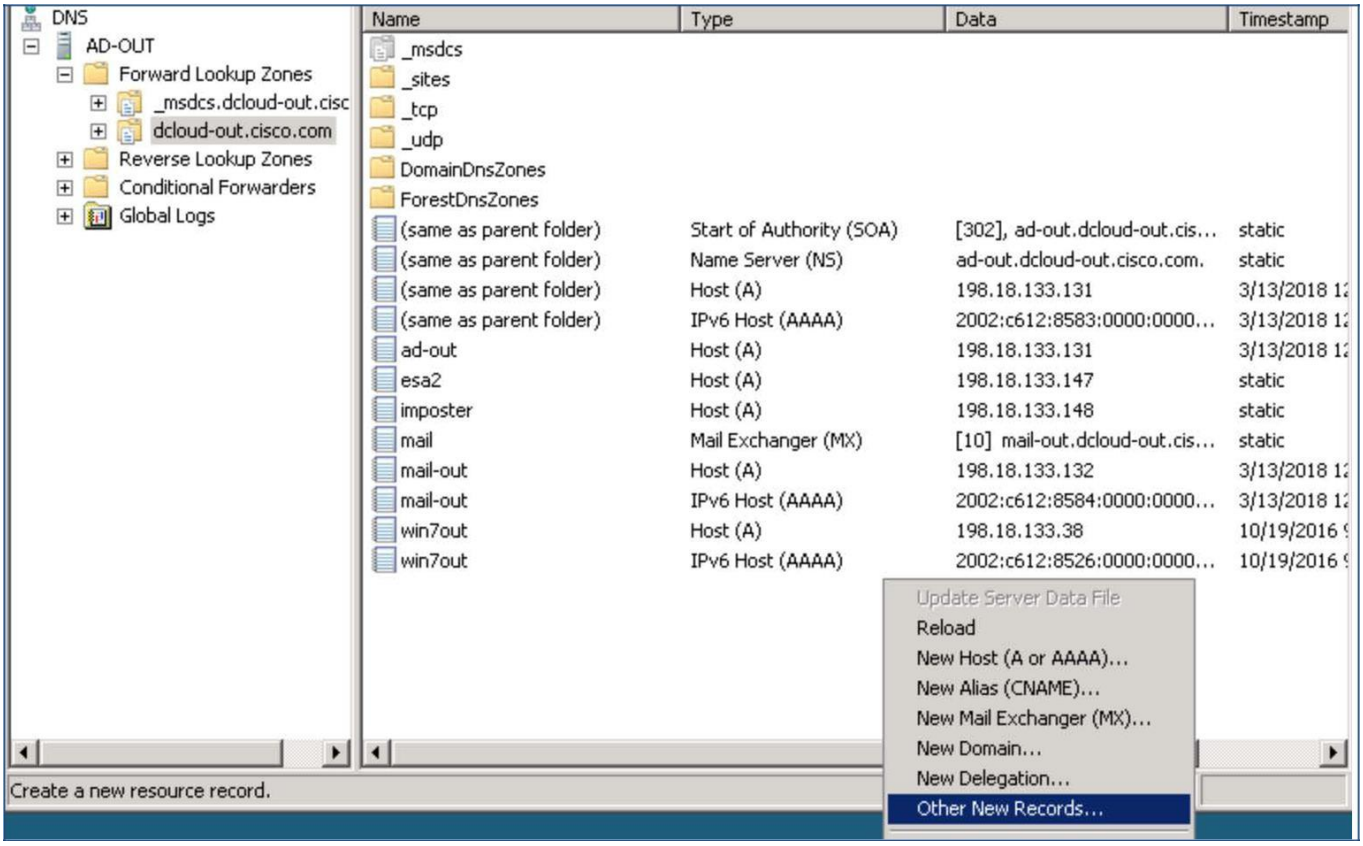
2. 以下のクレデンシャルを使用してログインします。表示されるセキュリティ警告をすべて認めます。ログイン後、[DNS] アイコンをクリックして DNS マネージャーのインターフェイスにアクセスします。

ユーザ名: DCLOUD-OUT\Administrator

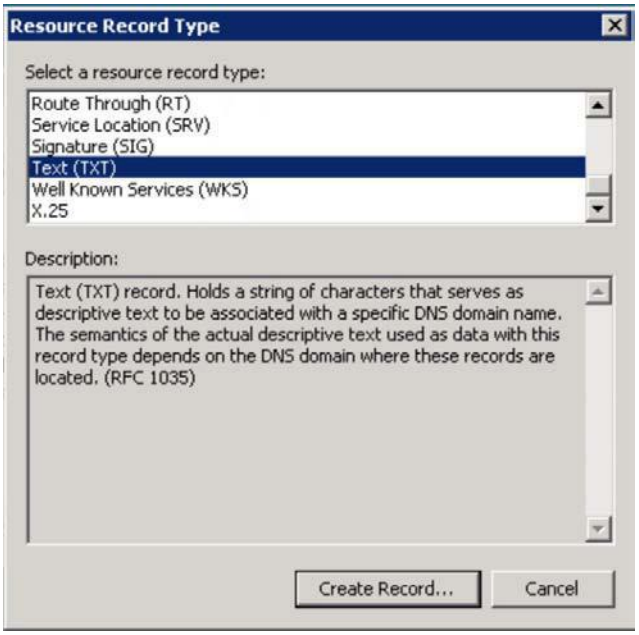
パスワード: C1sco12345



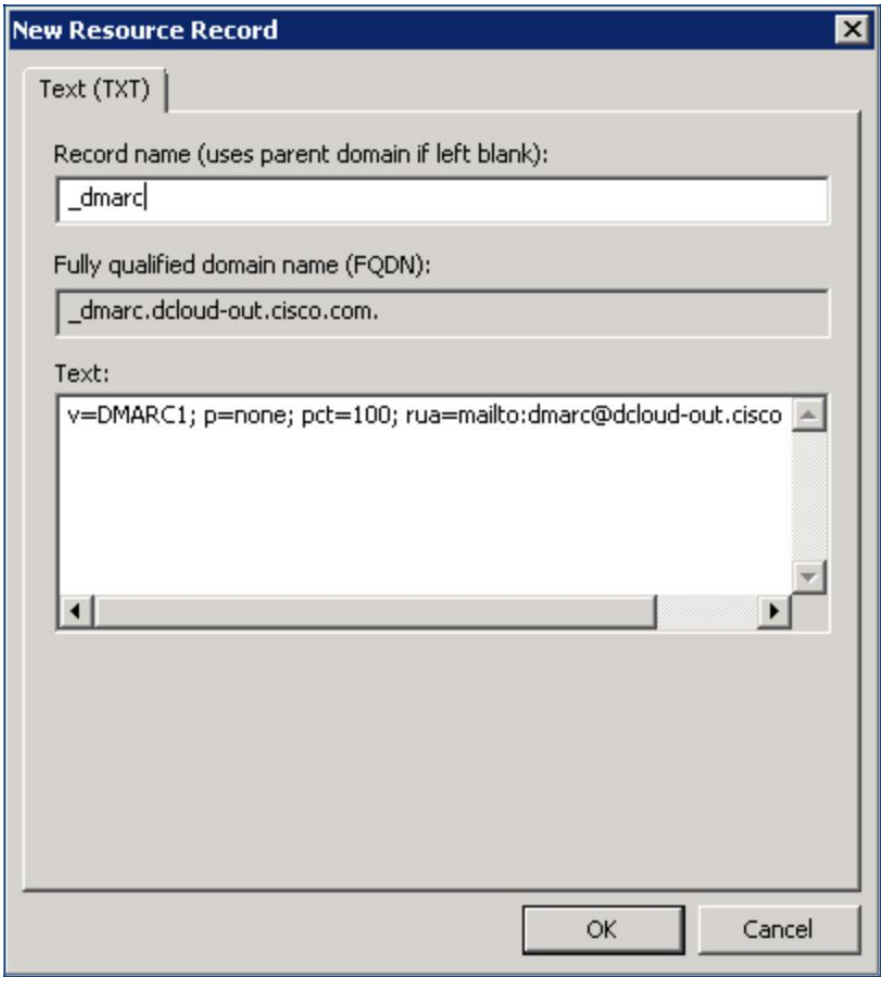
3. [前方参照ゾーン（Forward Lookup Zones）] をダブルクリックし、「dcloud-out.cisco.com」を選択します。右ペインの空白部分を右クリックし、リストから [その他の新しいレコード（Other New Records）] を選択します。



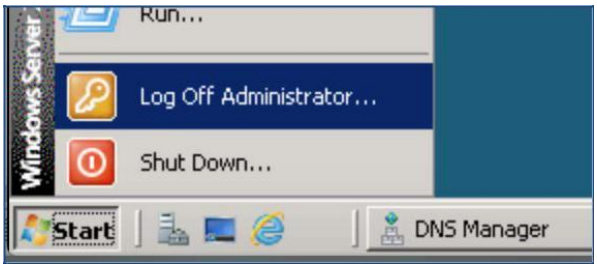
4. ドロップダウンリストを最後までスクロールして [テキスト（TXT）（Text (TXT)）] を選択し、[レコードの作成…（Create Record …）] をクリックします。



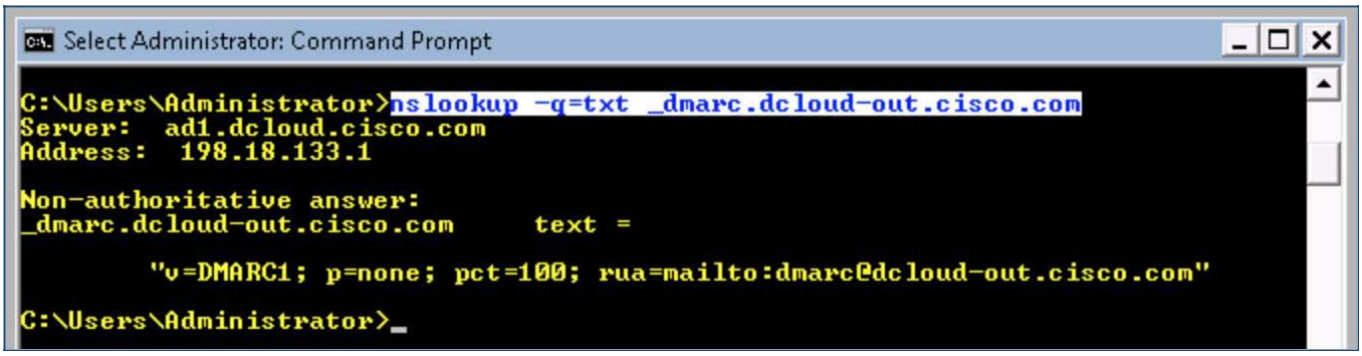
5. [レコード名（Record Name）] に「*_dmarc*」と入力し、「*v=DMARC1; p=none; pct=100; rua=mailto:dmarc@dcloud-out.cisco.com*」の文字列を [テキスト（Text）] にペーストします。[OK] をクリックします。



6. [完了（Done）] をクリックします。
7. 完了したら、[スタート（Start）] メニューから [Administrator のログオフ（Log Off Administrator）] をクリックしてリモート デスクトップ セッションを終了します。



8. ワークステーションのデスクトップで、コマンド プロンプトを起動して、「nslookup -q=txt lab._domainkey.dcloud-out.cisco.com」と入力し、DKIM レコードを確認します。

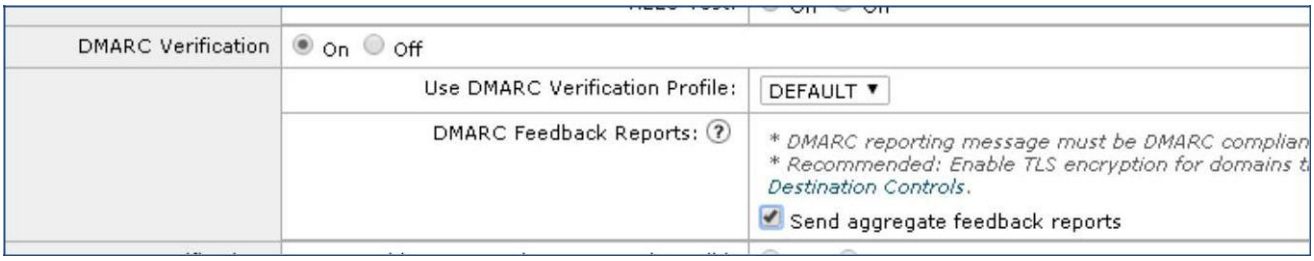


タスク:DMARC 検証を有効にする(受信者)(推定所要時間:1 分)

DMARC 検証を有効にすると、受信側の Cisco E メール セキュリティ ソリューションで、Mail From フィールドに表示されるメールアドレス、または DKIM の署名の d=domain ヘッダーが、From ヘッダーに含まれるアドレスと同一かどうかが検証されます。

1. ワークステーションで ESA の GUI にアクセスします。[メール ポリシー(Mail Policies)] > [メール フロー ポリシー(Mail Flow Policies)] に移動し、リスナー「Public 198.18.133.146:25」を選択します。メール フロー ポリシー名 [デフォルト ポリシー パラメータ(Default Policy Parameters)] をクリックします。

2. [セキュリティ機能(Security Features)] セクションが表示されるまでページを下にスクロールします。[On] を選択して、[DMARC 検証(DMARC Verification)] を有効にします。事前定義された DMARC 検証プロファイル(デフォルト)が、すでに Cisco E メール セキュリティで利用可能になっていることを確認してください。[集約フィード バック レポートの送信(send aggregate feedback reports)] オプションを有効にします。



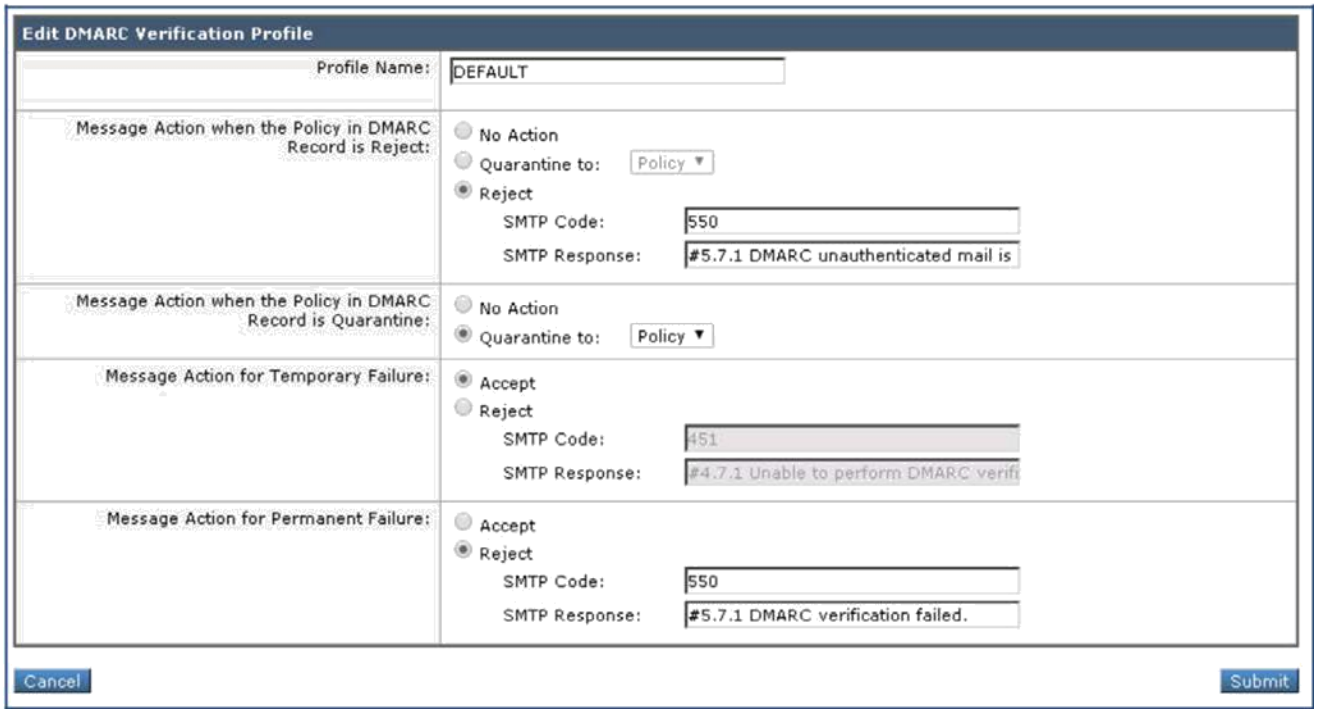
3. [送信(Submit)] をクリックします。[変更内容を確定(Commit Changes)] ボタンをクリックして、変更が適用されていることを確認します。必要に応じて任意のコメントを追加してください。

タスク:DMARC 検証プロファイルの設定(受信者)(推定所要時間:2 分)

このタスクでは、受信側の Cisco E メール セキュリティ ソリューションにおけるデフォルトの DMARC 検証プロファイルを変更します。これにより、DMARC 検証の結果と指定した検証プロファイルを基に、メッセージに許可、検疫、拒否のいずれかの処理が行われます。集約レポートの送信を有効にすると、Cisco E メール セキュリティでは DMARC 検証データが収集され、日次のレポートとしてドメインの所有者に送信されます。

1. 前のタスクの GUI を引き続き使用し、[メールポリシー(Mail Policy)] > [DMARC] に移動して、プロファイル名 [デフォルト(DEFAULT)] をクリックします。次の設定を使用して、DMARC ポリシーの要求に基づくメッセージ アクションを構成します。

DMARC レコードのポリシーが拒否の場合	[拒否(Reject)] を選択します。
DMARC レコードのポリシーが検疫の場合	[検疫(Quarantine)] を選択します。> [ポリシー(Policy)] を選択します。
一時的な失敗の場合	[許可(Accept)] のままにします。
永続的な失敗の場合	[拒否(Reject)] を選択します。



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。

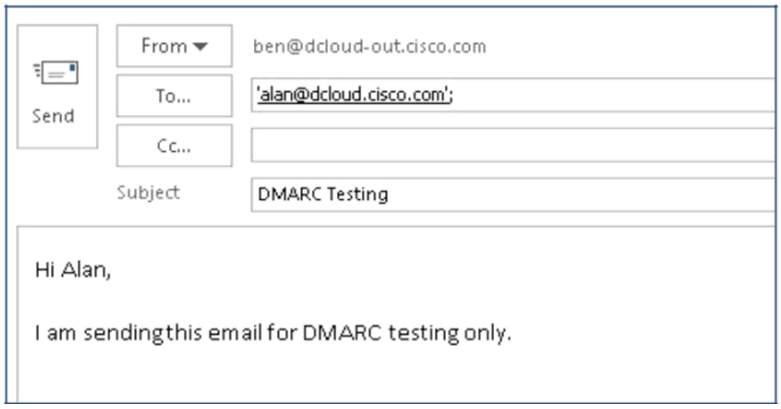
タスク:DMARC をテストする(推定所要時間:10 分)

構成をすべて完了したら、dcloud-out.cisco.com で終わるメールアドレスを使用して社外ユーザから Alan にメールを送信することで、DMARC 検証の機能をテストできます。

メッセージを準備する前に、CLI を使用して ESA への接続を開始し、メール ログを表示します(ログの確認には「tail」コマンドを使います)。メッセージが一連の設定を通過する際に、メッセージが処理され、アクションが適用されることをログで確認します。

1. ワークステーションから Microsoft Outlook を起動し、Ben 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。

送信者:	ben@dcloud-out.cisco.com
受信者:	alan@dcloud.cisco.com
件名:	DMARC のテスト
本文:	こんにちは、Alan これは、DMARC をテストするためのメール送信です。



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. ESA の CLI に切り替えます。DMARC の機能によって SPF と DKIM の両方のレコードが DMARC のポリシーと一致したことが明らかになっていることを確認します。DMARC の最終的な判定は「Pass(通過)」です。

```
Tue Mar 13 11:05:23 2018 Info: New SMTP ICID 131 interface Management (198.18.133.146) address 198.18.133.147 reverse dns host e
sa2.dcloud-out.cisco.com verified yes
Tue Mar 13 11:05:23 2018 Info: ICID 131 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country None
Tue Mar 13 11:05:23 2018 Info: Start MID 198 ICID 131
Tue Mar 13 11:05:23 2018 Info: MID 198 ICID 131 From: <ben@dcloud-out.cisco.com>
Tue Mar 13 11:05:23 2018 Info: MID 198 ICID 131 RID 0 To: <alan@dcloud.cisco.com>
Tue Mar 13 11:05:23 2018 Info: MID 198 SPF: helo identity postmaster@esa2.dcloud-out.cisco.com None
Tue Mar 13 11:05:23 2018 Info: MID 198 SPF: mailfrom identity ben@dcloud-out.cisco.com Pass (v=spf1)
Tue Mar 13 11:05:23 2018 Info: MID 198 DKIM: pass signature verified (d=dcloud-out.cisco.com s=lab i=@dcloud-out.cisco.com)
Tue Mar 13 11:05:23 2018 Info: MID 198 DMARC: Message from domain dcloud-out.cisco.com, DMARC pass (SPF aligned True, DKIM align
ed True)
Tue Mar 13 11:05:23 2018 Info: MID 198 DMARC: Verification passed
Tue Mar 13 11:05:23 2018 Info: MID 198 Message-ID '<002a01d3babb$2f2b64a0$8d822de0$@dcloud-out.cisco.com>'
Tue Mar 13 11:05:23 2018 Info: MID 198 Subject 'DMARC Testing'
Tue Mar 13 11:05:23 2018 Info: MID 198 ready 3600 bytes from <ben@dcloud-out.cisco.com>
Tue Mar 13 11:05:23 2018 Info: MID 198 matched all recipients for per-recipient policy DEFAULT in the inbound table
Tue Mar 13 11:05:23 2018 Info: MID 198 interim AV verdict using McAfee CLEAN
Tue Mar 13 11:05:23 2018 Info: MID 198 interim AV verdict using Sophos CLEAN
Tue Mar 13 11:05:23 2018 Info: MID 198 antivirus negative
Tue Mar 13 11:05:23 2018 Info: MID 198 AMP file reputation verdict : SKIPPED (no attachment in message)
Tue Mar 13 11:05:23 2018 Info: MID 198 using engine: GRAYMAIL negative
Tue Mar 13 11:05:28 2018 Info: ICID 131 close
Tue Mar 13 11:05:28 2018 Info: MID 198 Outbreak Filters: verdict negative
Tue Mar 13 11:05:28 2018 Info: MID 198 queued for delivery
Tue Mar 13 11:05:28 2018 Info: New SMTP DCID 55 interface 198.18.133.146 address 198.18.133.2 port 25
Tue Mar 13 11:05:28 2018 Info: Delivery start DCID 55 MID 198 to RID [0]
Tue Mar 13 11:05:28 2018 Info: Message done DCID 55 MID 198 to RID [0]
Tue Mar 13 11:05:28 2018 Info: MID 198 RID [0] Response '2.6.0 <002a01d3babb$2f2b64a0$8d822de0$@dcloud-out.cisco.com> [InternalI
d=7] Queued mail for delivery'
Tue Mar 13 11:05:28 2018 Info: Message finished MID 198 done
Tue Mar 13 11:05:33 2018 Info: DCID 55 close
```

4. ワークステーションに戻り、メッセージをもう一度同期すると、DMARC のテスト メッセージが Alan のメールボックスに表示されます。

5. ワークステーションから ESA の GUI にアクセスし、[モニタ（Monitor）] > [DMARC検証（DMARC Verification）] に移動して、レポートの内容を確認します。

付録 A　トラブルシューティング

このセクションは、一連のトラブルシューティングのシナリオで構成されています。事前設定済みの Cisco E メール セキュリティ アプライアンスと Microsoft アプリケーション サーバがトポロジに含まれて提示されます。

このセクションの所要時間は 1 時間ほどです。

1. デバイスの次の設定は変更してはなりません。
    - すべてのデバイスのホスト名
    - ユーザ アカウント パスワード
    - LDAP または AD 認証の設定
    - ESA のネットワークとシステムの管理メニュー リスト内にあるすべての機能
    - NTP、ライセンス、構成のバックアップなどを含む、システム レベル ベースの設定
    - IP アドレス、サブネットマスク、ゲートウェイ、ルートなどを含むネットワーク レベル ベースの設定
2. インシデントを解決するために設定されている機能はどれも無効にしないでください。事前に設定されたポリシーの削除ではなく、構成の誤りを解決する必要があります。
3. あるインシデントの解決は、以前のインシデントの解決に左右されることがあります。
4. あなたには、リモート デスクトップ接続、Web UI またはコマンド ライン インターフェイスを使用してすべてのデバイスにアクセスできる完全な管理者権限があります。
5. デバイスの到達可能性や検証の確認が必要な場合、ラボの試験官に依頼できます。

背景

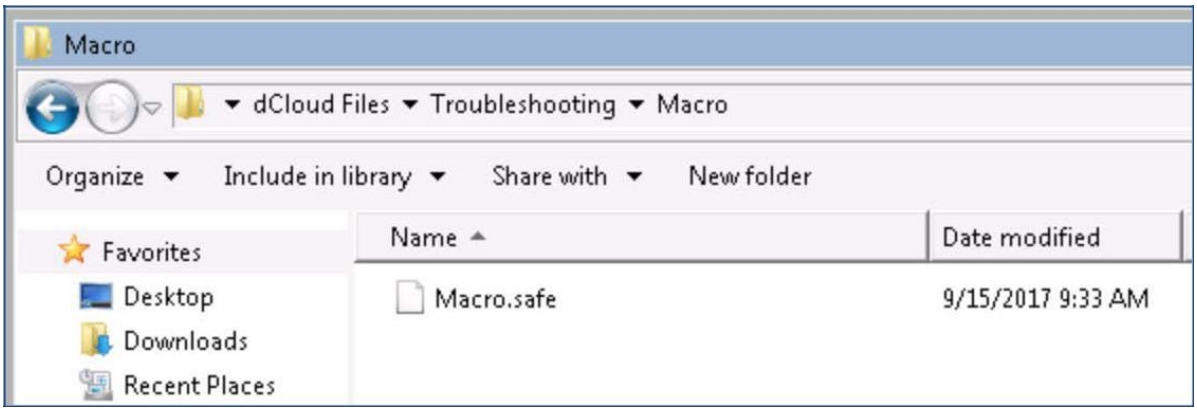
Ben Bravo は、シスコの dCloud-Out 営業部門 のメッセージング セキュリティ管理者です。このセクションでは、あなたは、Ben を支援してすべてのインシデントの根本原因を特定し、適切な解決策を講じる責任を負います。インシデント対応では、トラブルシューティングのガイドラインや詳細な説明書をいつでも参照できます。

インシデント：マクロの検出

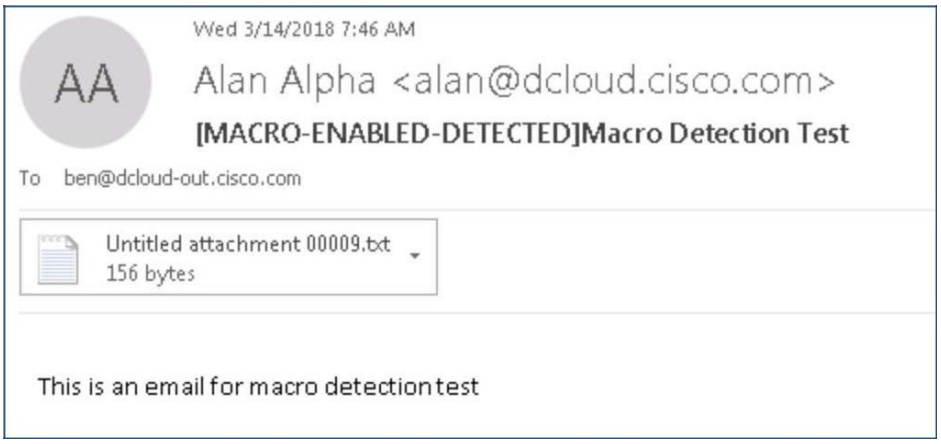
Ben は、ESA2 の dCloud 営業部門から届く、マクロを含む添付ファイルを検疫するために社外からのメールにポリシーを設定しました。しかし、いまだにマクロを含むファイルが添付されたメール メッセージを受信しています。

ヒント：このインシデントは ESA2 上の 1 つの誤りが原因になっています。解決策を講じたら、マクロを含むファイルを添付したメールを Alan から Ben に送信できます。

送信者：	alan@dcloud.cisco.com
受信者：	ben@dcloud-out.cisco.com
件名：	マクロ検出のテスト
本文：	これはマクロ検出のテスト用メールです。
添付ファイル：	デスクトップ上の dCloud Files > Troubleshooting > Macro サブフォルダ内、Macro.safe ファイル



想定される結果: Ben のメールボックスにメッセージが届きます。受信者がすぐに気が付くように件名ヘッダーの先頭に [MACRO-ENABLED-DETECTED]（有効なマクロが検出されました）が追加されています。Ben のメールボックスのメッセージを開き、添付ファイルが削除されていることを確認します。

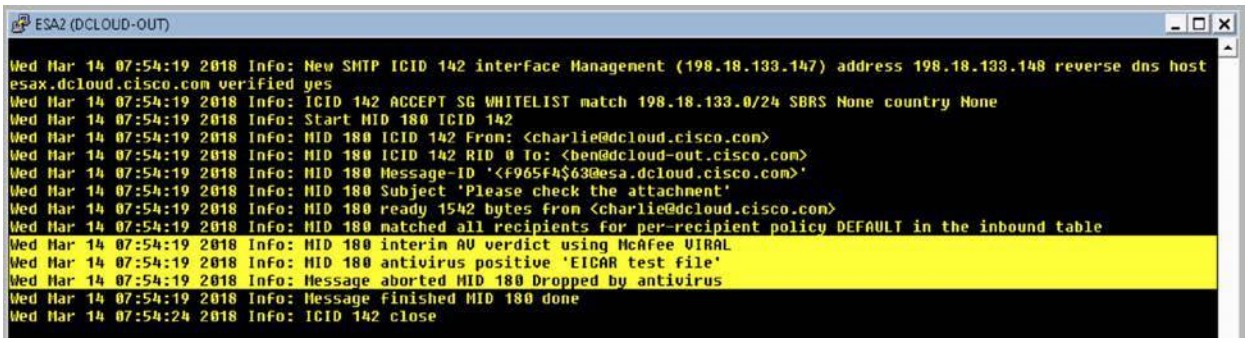


インシデント: ウイルス検出

Ben は、ウイルスに感染したファイルが、外部の送信者 charlie@dcloud.cisco.com からメールボックスに配信されていると、同じ営業部門の従業員から苦情を受けました。インシデントの調査が始まり、Ben が ESA2 を調べたところ該当のメールが Sophos ウイルス対策エンジンによってスキャンされていないことが分かりました。

ヒント: このインシデントは ESA2 上の 1 つの誤りが原因になっています。解決策を講じたら、dCloud Files > Troubleshoot > Virus サブフォルダにある virus-exec.bat をクリックしてください。

想定される結果: ESA2 の CLI セッションがウイルスに感染したファイルが検出されたことを示します。メッセージはその後、Sophos ウイルス対策エンジンによってドロップされます。

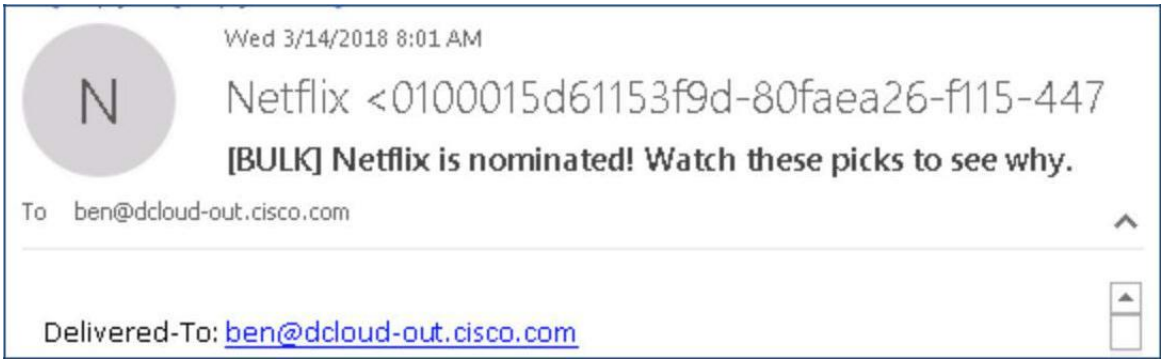


インシデント：グレイメールの検出

マーケティング チームが、Netflix から、新作とリリース予定の映画や特別なイベントに関連する一括メールを受信しました。Ben は、グレイメール検出機能がすべての受信メール ポリシーで有効になっていることを確認しましたが、メール ログによると、グレイメール エンジンは Netflix メールを一括メッセージとして分類していませんでした。

ヒント：このインシデントは ESA2 上の 1 つの誤りが原因になっています。解決策を講じたら、dCloud Files > Troubleshoot > Graymail サブフォルダにある graymail-exec.bat をクリックしてください。

想定される結果：Ben のメールボックスにメッセージが届きます。受信者がすぐに気が付くように件名ヘッダーの先頭に [BULK]（バルク メール）が追加されています。

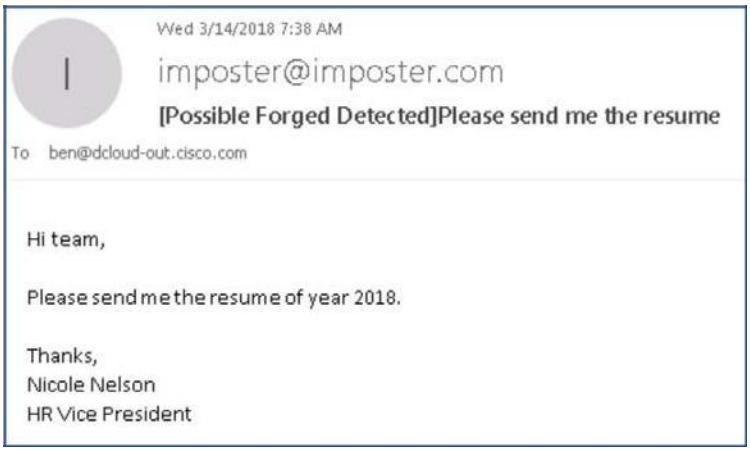


インシデント：偽装メールの検出

Ben は、HR 部門で発生した重大度の高いケースの対応依頼を受けました。ある人事担当者が、HR のバイス プレジント、a Nicole Nelson から送信され、偽装されたと思われるメッセージを受信しました。Ben は、「Forged_Email_CF」コンテンツ フィルタ ルールがデフォルトの受信メール ポリシーで有効になっていることを確認しました。Nicole Nelson は、コンテンツ フィルタ ルールに関連付けられているディクショナリ（Upper_Management）にすでに含まれている名前の 1 つで、です。この偽装メールの From ヘッダーは次のように表示されます。Nlcole N3lson <nick.nelson@dcloud-out.cisco.com>

ヒント：このインシデントは ESA2 上の 1 つの誤りが原因になっています。解決策を講じたら、dCloud Files > Troubleshooting > FED サブフォルダにある fed-exec.bat をクリックしてください。

想定される結果：Ben のメールボックスにメッセージが届きます。メールの受信者がすぐに気が付くように件名ヘッダーの先頭に [Possible Forged Detected]（詐称のおそれがあります）が追加されています。エンベロープの送信者メールアドレスが詐称されていることを示すために、From ヘッダーが、imposter@imposter.com（imposter 偽者）に書き換えられています。



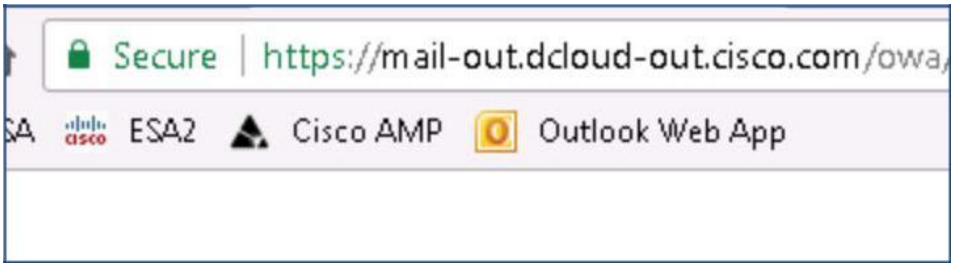
インシデント：複数の受信者宛のメッセージ

Ben は、Joe John から、最高財務責任者（CFO）が主導する変更要求（CR）を受けました。要件は、最近退社した Lucy Lane 宛の社外メールをすべて CFO のメール アカウントにリダイレクトすることです。変更を実施した 1 時間後、Ben は Joe から電話を受けます。メッセージが Joe にもリダイレクトされ、それには他の受信者（Kathy など）も含まれているというのです。Ben は、変更内容を確認し、問題解決に必要な変更を実施できるよう、あなたに緊急の支援を求めています。

ヒント：このインシデントは ESA2 上の 1 つの誤りが原因になっています。Alan の Outlook アカウントから、Lucy および Kathy にメールを送信できます。

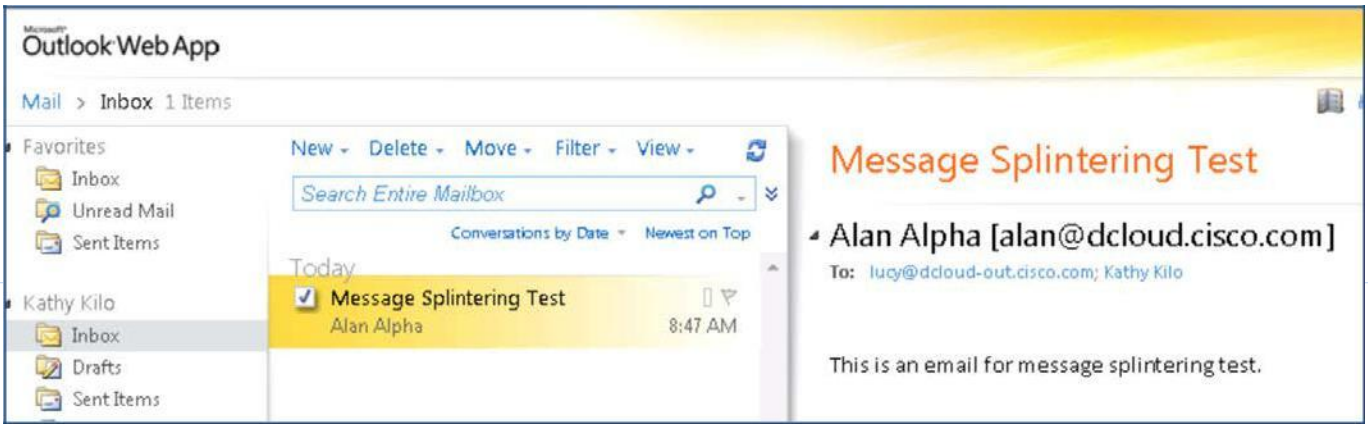
送信者：	alan@dcloud.cisco.com
受信者：	lucy@dcloud-out.cisco.com; kathy@dcloud-out.cisco.com
件名：	複数の受信者宛のメッセージをテストする
本文：	これは複数の宛先に送信されるメッセージのテストです。

想定される結果：メッセージは、Joe と Kathy のメールボックスに届きます。Kathy のメールボックスにアクセスするには、Chrome から Outlook の Web アプリケーションを使用するか、（**https://mail-out.dcloud-out.cisco.com/owa**）ブックマーク Outlook Web App をクリックしてます。



次のクレデンシャルを使用してログインします。**ユーザ名：**kathy@dcloud-out.cisco.com **パスワード：**C1sco12345

問題が解消されていれば、Kathy は Alan からのメッセージを受信できます。

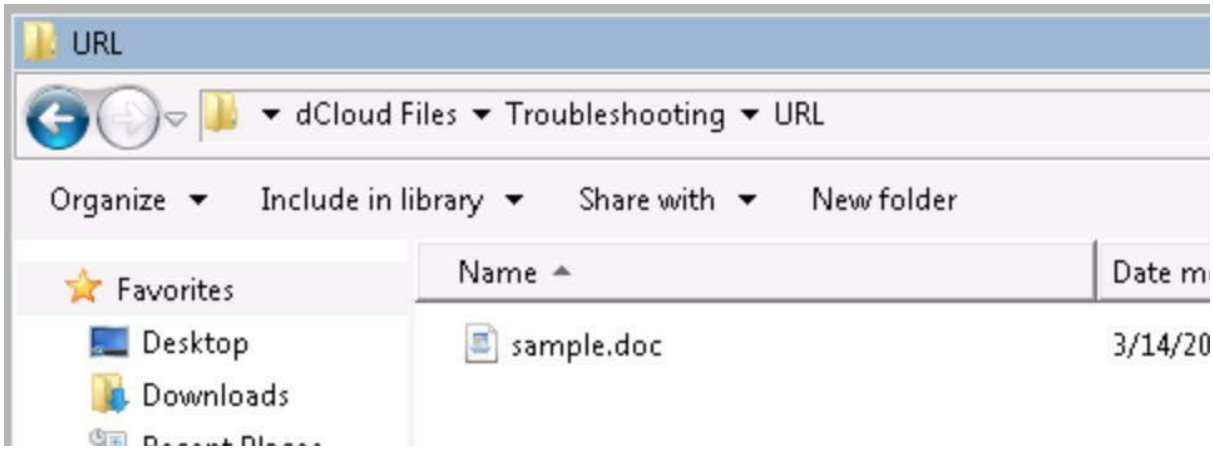


インシデント：URL フィルタリング

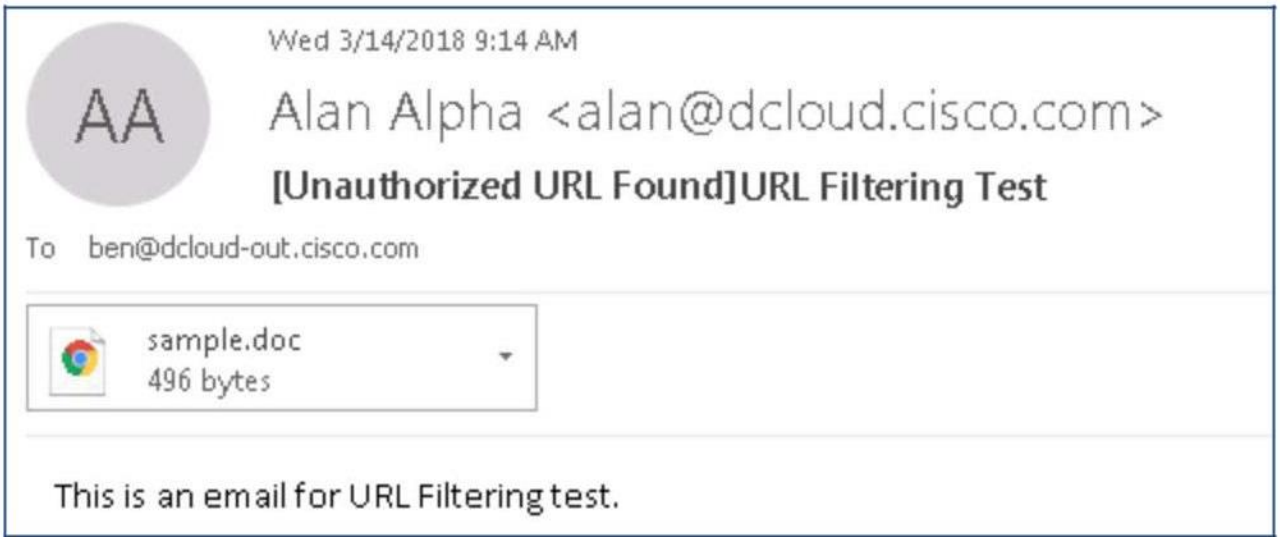
財務管理者が、不正と思われる Web サイト（http://www.casino.com）へのリンクが含まれるメールを社外から受信しました。会社のポリシーでは、これをできるだけ早く報告することが義務付けられています。Ben は、別の変更要求によって最近作成した URL フィルタリング ルールがあると確信していますが、この問題を特定するためにあなたの協力を求めています。

ヒント：このインシデントは ESA2 上の 1 つの誤りが原因になっています。解決策を講じたら、禁止された URL を含むファイルを添付したメールを Alan から Ben に送信できます。

送信者：	alan@dcloud.cisco.com
受信者：	ben@dcloud-out.cisco.com
件名：	URL フィルタリング テスト
本文：	これは URL フィルタリングのテスト用メールです。
添付ファイル：	デスクトップ上の dCloud Files > Troubleshooting > URL サブフォルダ内、sample.doc ファイル



想定される結果：Ben のメールボックスにメッセージが届きます。受信者がすぐに気が付くように件名ヘッダーの先頭に [Unauthorized URL Found]（許可されていない URL が検出されました）が追加されています。



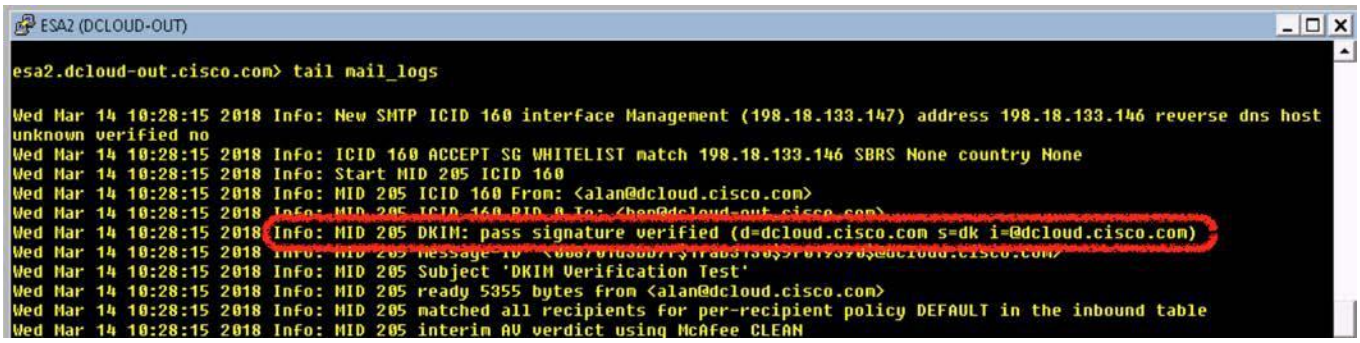
インシデント：DKIM 検証

DCLOUD 営業部門は、ドメイン dcloud.cisco.com に対して DKIM 検証を行い、DKIM 検証を通過できないすべてのメッセージを検疫することを正式に要求しました。Ben は、そのメール フロー ポリシー向けに DKIM 検証を実施し、必要なコンテンツ フィルタを適用することについて、管理部門から承認を得ました。ESA2 では dcloud.cisco.com に関連付けられているすべてのレコードについて DNS クエリを実行できると Ben は確信していますが、社外からメッセージを受信する場合に DKIM 検証が適用されていません。

ヒント：このインシデントは ESA2 上の 1 つの誤りが原因になっています。このトラブルシューティングの後に、Alan の Outlook アカウントから Ben にメッセージを送信することによって問題の解消を確認します。

送信者：	alan@dcloud.cisco.com
受信者：	ben@dcloud-out.cisco.com
件名：	DKIM 検証のテスト
本文：	これは DKIM 検証のテスト用メールです。

想定される結果：DKIM 検証を通過します。Web UI [モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）] または CLI コマンド **tail mail_logs**（Cisco E メール セキュリティ 2）を利用して詳細を表示し、DKIM 検証の成功を確認できます。



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