電子メールのスプーフィングの検出と防止

内容

はじめに

このドキュメントでは、Cisco Secure Emailを使用する際に、電子メールのスプーフィングを検出して防止する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- シスコセキュアEメール

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

このドキュメントについて

このドキュメントは、Cisco Secure Emailを導入しているお客様、シスコチャネルパートナー、およびシスコエンジニアを対象としています。このドキュメントでは、次の内容について説明します。

- 電子メールのスプーフィングとは
- 電子メールスプーフィング対策ワークフロー
- スプーフィング防止ではさらに何ができますか。

電子メールのスプーフィングとは

電子メールのスプーフィングは、メッセージが実際の送信元とは別のユーザまたは場所から発信されたように見える場合の、電子メールヘッダーの偽造です。電子メールのスプーフィングは、フィッシングやスパムキャンペーンで使用されます。これは、正当で信頼できる送信元が電子メールを送信したと考えた場合に、その電子メールを開く可能性が高いためです。スプーフィングの詳細については、「電子メールのスプーフィングとは」および「電子メールのスプーフィングを検出する方法」を参照してください。

電子メールのスプーフィングは次のカテゴリに分類されます。

[Category]	説明	主要なターゲット
直接ドメインスプーフィング	エンベロープの送信元に受信者のドメインと同じようなドメインを偽装します。	従業員
表示名の偽装	Fromヘッダーには、組織の経営幹部名を持つ正当な送信者が表示されます。ビジネスメール侵害(BEC)とも呼ばれます。	従業員
ブランド名の偽装	Fromヘッダーには、既知の組織のブランド名を持つ正当な送信者が表示されます。	お客様/パートナー
フィッシングURLベースの攻撃	被害者から機密データやログイン情報を盗もうとするURLが記載された電子メール。リンクをクリックしてアカウントの詳細を確認するように求める銀行からの偽の電子メールは、フィッシングURLベースの攻撃の一例です。	従業員/パートナー
従兄弟または類似ドメイン攻撃	エンベロープのfromまたはfromヘッダーの値は、実際のアドレスになりすましてSender Policy Framework(SPF)、DomainKeys Identified Mail(DKIM)、およびDomain-based Message Authentication, Reporting and	従業員/パートナー

	Conformance(DMARC)インスペクションをバイパスする類似の送信者アドレスを示します。	
アカウントの乗っ取り/侵害されたアカウント	誰かに属する実際の電子メールアカウントへの不正アクセスを取得し、正当な電子メールアカウントの所有者として他の被害者に電子メールを送信します。	Everyone

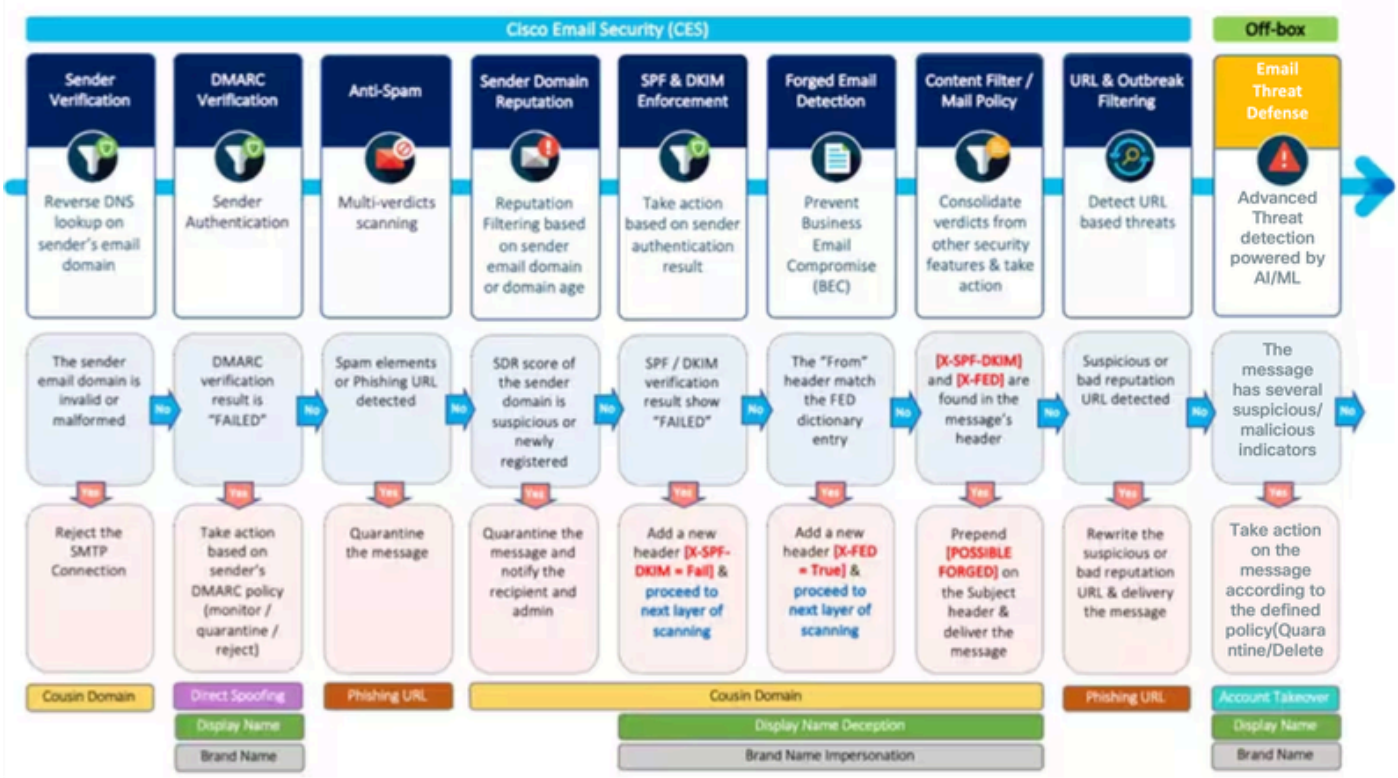
1つ目のカテゴリは、電子メールのインターネットヘッダーの「エンベロープの送信元」の値に含まれる所有者のドメイン名の悪用に関連しています。Cisco Secure Emailでは、送信者のドメインネームサーバ(DNS)検証を使用してこの攻撃を修復し、正当な送信者のみを許可できます。同じ結果は、DMARC、DKIM、およびSPF検証を使用してグローバルに実現できます。

ただし、その他のカテゴリは、送信者の電子メールアドレスのドメイン部分に部分的にしか違反しません。したがって、DNSテキストレコードまたは送信者検証のみを使用する場合は、簡単に阻止できません。理想的には、Cisco Secure Emailのいくつかの機能とCisco Secure Email Threat Defense(ETD)を組み合わせて、このような高度な脅威に対抗するのが最善です。ご存知のとおり、Cisco Secure Emailの管理と機能の設定は組織によって異なり、不適切なアプリケーションによって誤検出が頻繁に発生する可能性があります。したがって、組織のビジネスニーズを理解し、機能を調整することが不可欠です。

電子メールスプーフィング対策ワークフロー

スプーフィング攻撃を監視、警告、および実施するベストプラクティスに対応するセキュリティ機能を図（図1）に示します。各機能の詳細は、このドキュメントに記載されています。ベストプラクティスは、Eメールのスプーフィングを検出するための綿密な防御アプローチです。攻撃者は時間の経過とともに組織に対する方法を変更できるため、管理者は変更を監視し、適切な警告と適用を確認する必要があります。

画像 1.Cisco Secure Emailスプーフィング防御パイプライン

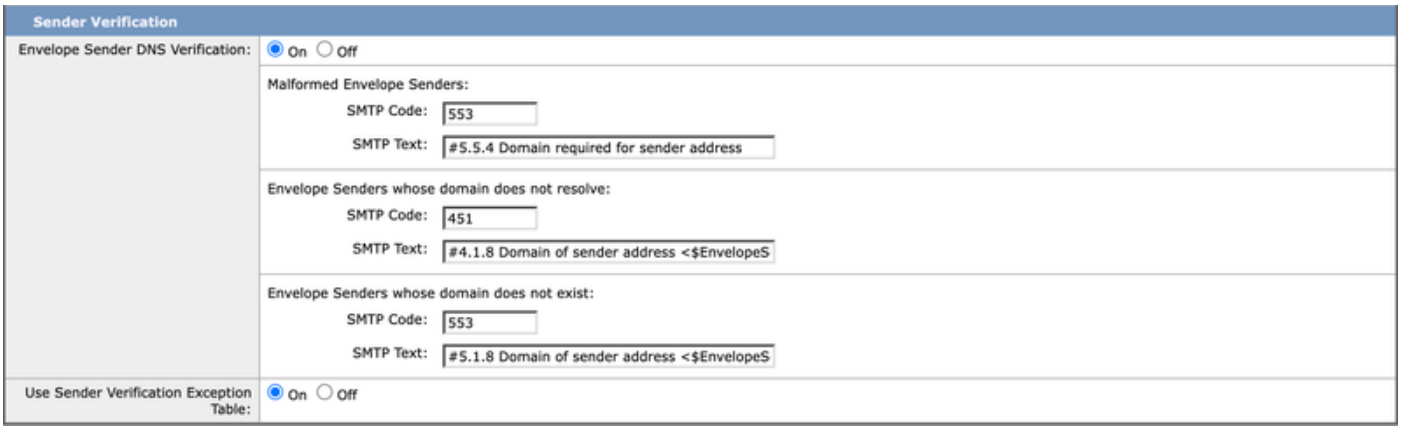


レイヤ1：送信側のドメインの妥当性チェック

送信者検証は、従兄弟ドメインのスプーフィングなど、偽の電子メールドメインから送信された電子メールを防止するより簡単な方法です(たとえば、c1sc0.comはcisco.comの詐欺師です)。Cisco Secure Emailは、送信者の電子メールアドレスのドメインに対してMXレコードクエリを実行し、SMTPカンバセーション中にMXレコードのAレコードルックアップを実行します。DNSクエリからNXDOMAINが返された場合、そのドメインは存在しないものとして扱われます。これは、攻撃者がエンベロープ送信者の情報を偽造し、未確認の送信者からの電子メールが受け入れられ、さらに処理されるようにするための一般的なテクニックです。Cisco Secure Emailでは、送信者のドメインまたはIPアドレスが例外テーブルに事前に追加されていない限り、この機能を使用する検証チェックに失敗したすべての着信メッセージを拒否できます。

ベストプラクティス：エンベロープ送信者フィールドの電子メールドメインが無効な場合にSMTPカンバセーションを拒否するようにCisco Secure Emailを設定します。メールフローポリシー、送信者検証、および例外テーブル（オプション）を設定して、正当な送信者だけを許可します。詳細については、「送信者検証を使用したスプーフィング保護」を参照してください。

画像 2.既定のメールフローポリシーの送信者確認セクション



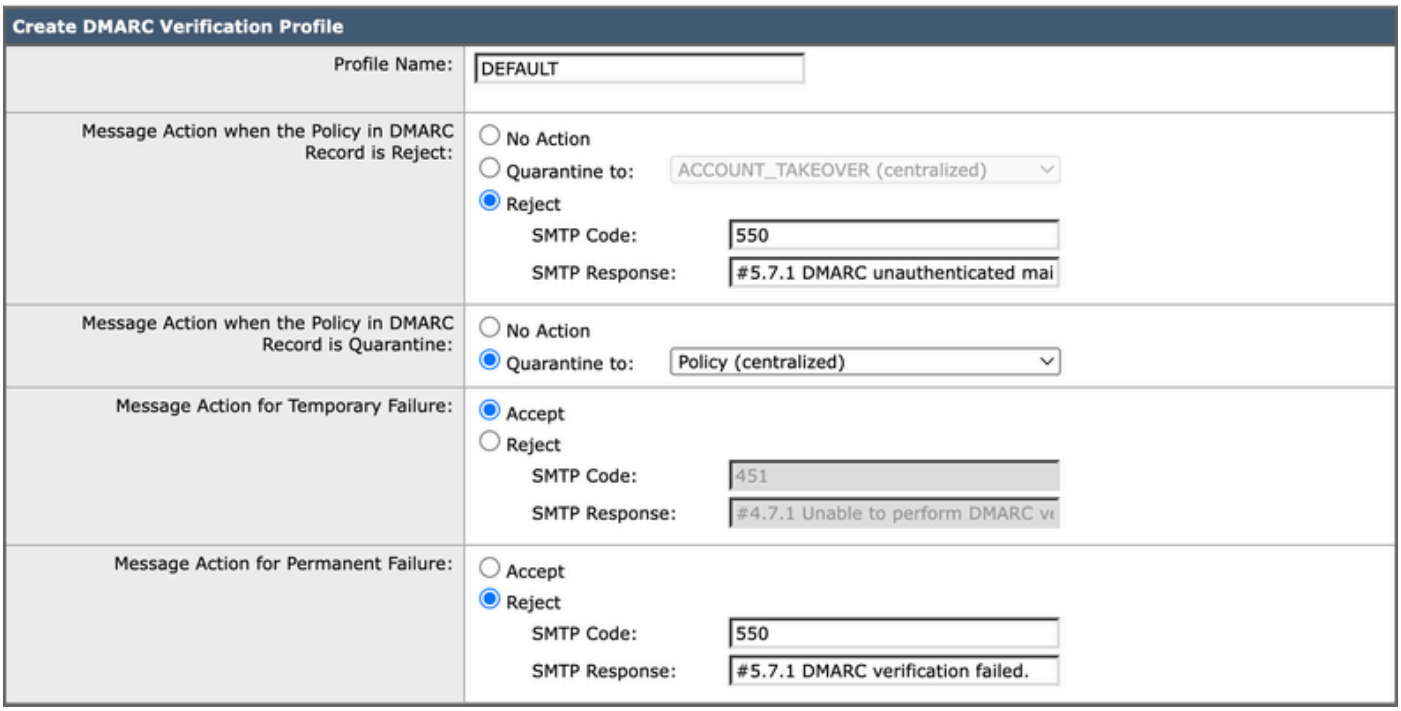
レイヤ2:DMARCを使用したFromヘッダーの確認

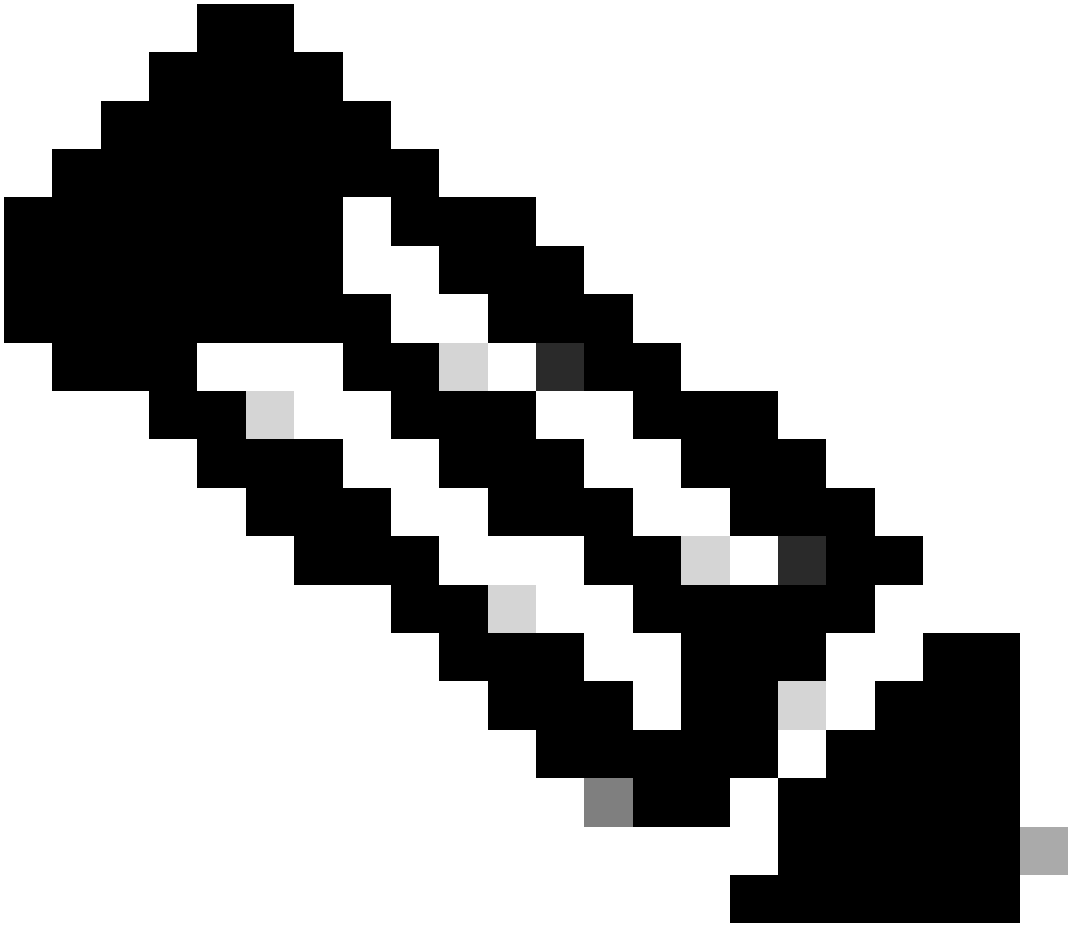
DMARCの検証は、ドメインの直接スプーフィングに対する防御を強化する強力な機能であり、表示名とブランド偽装攻撃も含まれます。DMARCは、SPFまたはDKIM（送信ドメインソースまたはシグニチャ）で認証された情報をFromヘッダーで最終受信者に提示される情報と結び付け、SPFおよびDKIMの識別子がFROMヘッダーの識別子と一致していることを確認します。

DMARCの検証に合格するには、着信Eメールがこれらの認証メカニズムの少なくとも1つに合格する必要があります。さらに、Cisco Secure Emailでは、管理者がDMARC検証プロファイルを定義してドメイン所有者のDMARCポリシーを上書きし、集約(RUA)レポートと障害/法医学的(RUF)レポートをドメイン所有者に送信することもできます。これにより、代わりに認証導入を強化できます。

ベストプラクティス：送信者がアドバイスするDMARCポリシーアクションを使用するデフォルトのDMARCプロファイルを編集します。また、DMARC検証のグローバル設定を編集して、正しいレポートを生成できるようにする必要があります。プロファイルを適切に設定したら、メールフローポリシーのデフォルトポリシーでDMARC検証サービスを有効にする必要があります。

画像 3.DMARC検証プロファイル





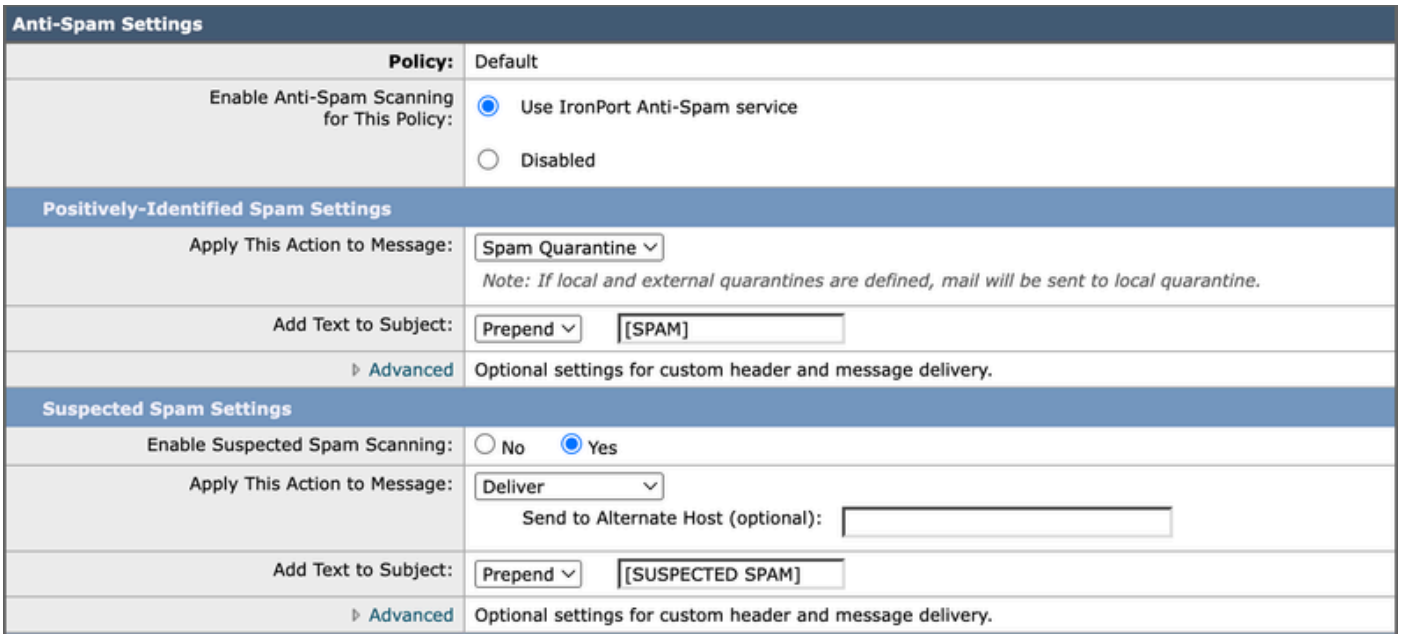
注:DMARCは、Cisco Domain Protectionなどのドメインモニタリングツールとともにドメインのオーナーを送信することによって実装される必要があります。Cisco Secure EmailにDMARCを適切に適用すると、許可されていない送信者やドメインから従業員に送信されるフィッシングメールから保護されます。Cisco Domain Protectionの詳細については、Cisco Secure Email Domain Protection At-A-Glanceを参照してください。

第3層：スパマーによる偽装メールの送信を防止する

スパムキャンペーンのもう1つの一般的な形態は、スプーフィング攻撃です。したがって、スパム/フィッシング要素を含む詐欺的な電子メールを効果的に特定し、確実にブロックするためには、アンチスパム保護を有効にすることが不可欠です。スパム対策は、このドキュメントで詳細に説明されている他のベストプラクティスのアクションと組み合わせることで、正当な電子メールを失うことなく最善の結果を得ることができます。

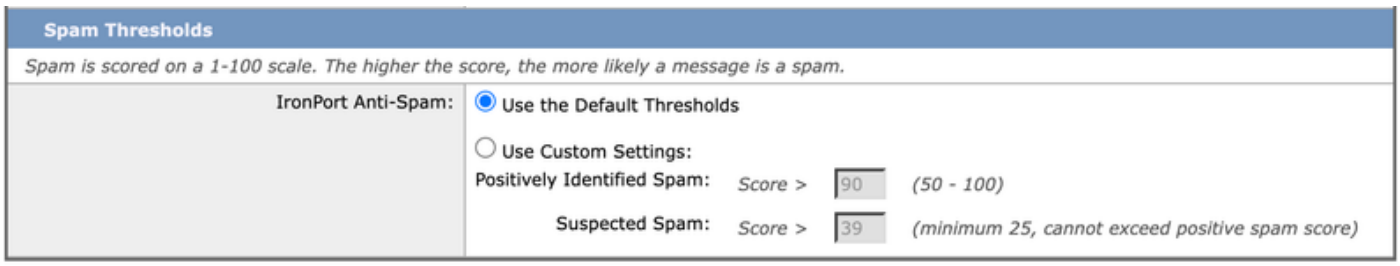
ベストプラクティス：デフォルトのメールポリシーでスパム対策スキャンを有効にし、スパム設定を明確に識別するための隔離アクションを設定します。スパムメッセージの最小スキャンサイズをグローバルで200万以上に増やします。

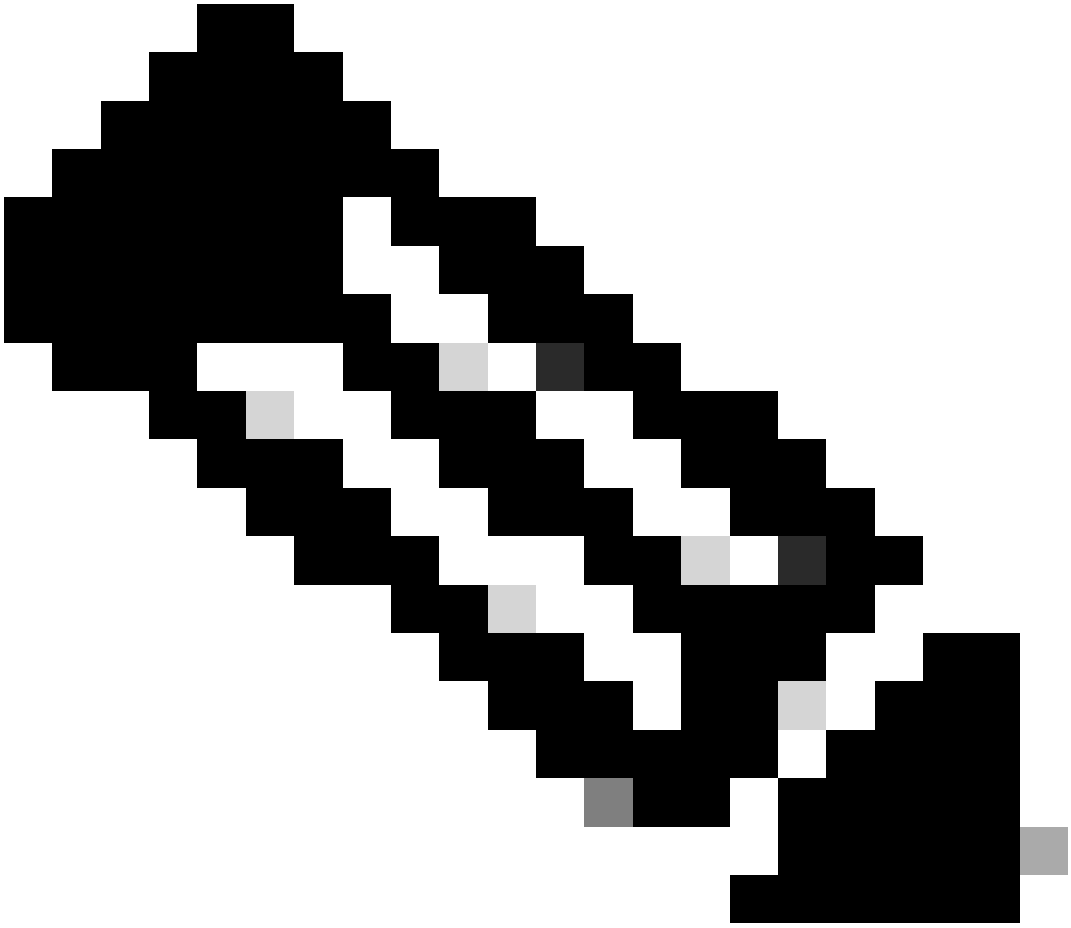
図 4.デフォルトのメールポリシーのスパム対策設定



スパムのしきい値は、スパムの陽性と疑いがあるスパムに対して感度を増減するように調整できます（図5）。ただし、シスコでは、管理者がこの調整を行うことや、シスコが特に指示しない限り、デフォルトのしきい値をベースラインとしてのみ使用することを推奨していません。

図 5.デフォルトのメールポリシーのスパム対策しきい値の設定





注:Cisco Secure Emailには、アドオンのIntelligent Multi-Scan(IMS)エンジンが用意されています。このエンジンは、スパム検出率（最も攻撃性の高い検出率）を高めるために、アンチスパムエンジンとは異なる組み合わせを提供します。

レイヤ4：電子メールドメインによる悪意のある送信者の特定

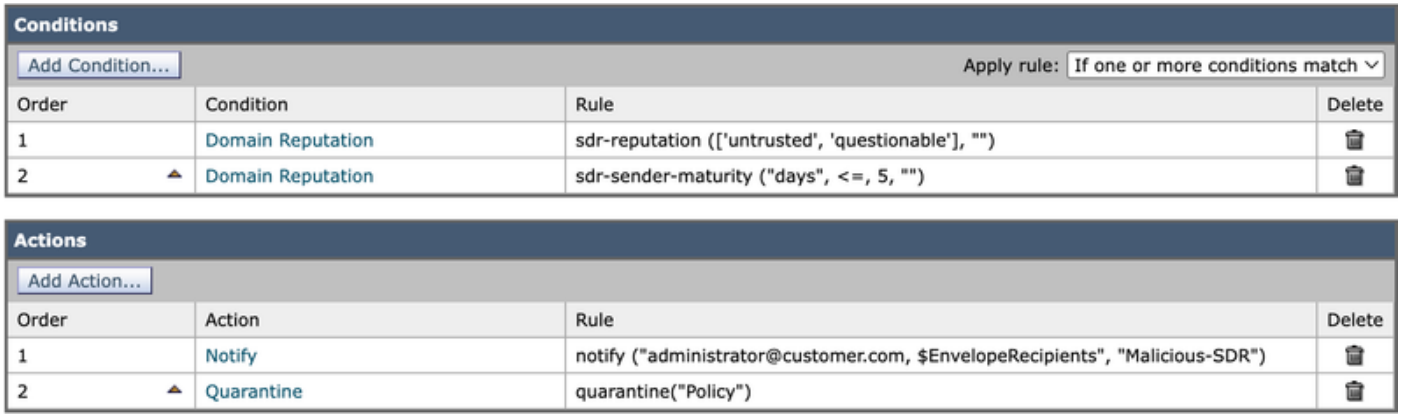
Cisco Talos Sender Domain Reputation(SDR)は、電子メールエンベロープおよびヘッダー内のドメインに基づいて電子メールメッセージのレピュテーション判定を行うクラウドサービスです。ドメインベースのレピュテーション分析では、共有IPアドレス、ホスティング、またはインフラストラクチャプロバイダーのレピュテーションを超えた調査を行うことで、スパム検出率を高めることができます。代わりに、完全修飾ドメイン名(FQDN)に関連する機能と、シンプルメール転送プロトコル(SMTP)メッセージ交換およびメッセージヘッダー内の他の送信者情報に基づいて判定を行います。

送信者の成熟度は、送信者のレピュテーションを確立するために不可欠な機能です。送信者の成熟度は、複数の情報源に基づくスパム分類に対して自動的に生成され、Whoisベースのドメインの有効期間とは異なる場合があります。送信者の成熟度は30日間の制限に設定されており、この

制限を超えると、ドメインは電子メール送信者として成熟したと見なされ、それ以上の詳細は提供されません。

ベストプラクティス：受信コンテンツフィルタを作成して、SDRレピュテーション判定が信頼できない/疑わしい送信ドメインに分類される送信ドメイン、または送信者の成熟度が5日以下である送信ドメインをキャプチャします。推奨処置は、メッセージを隔離し、Eメールセキュリティ管理者と元の受信者に通知することです。SDRの設定方法の詳細については、『Cisco Eメールセキュリティアップデート（バージョン12.0）：送信者ドメインレピュテーション(SDR)』のビデオをご覧ください。

図 6.SDRレピュテーションとドメイン経過時間のコンテンツフィルタと通知および検疫アクション

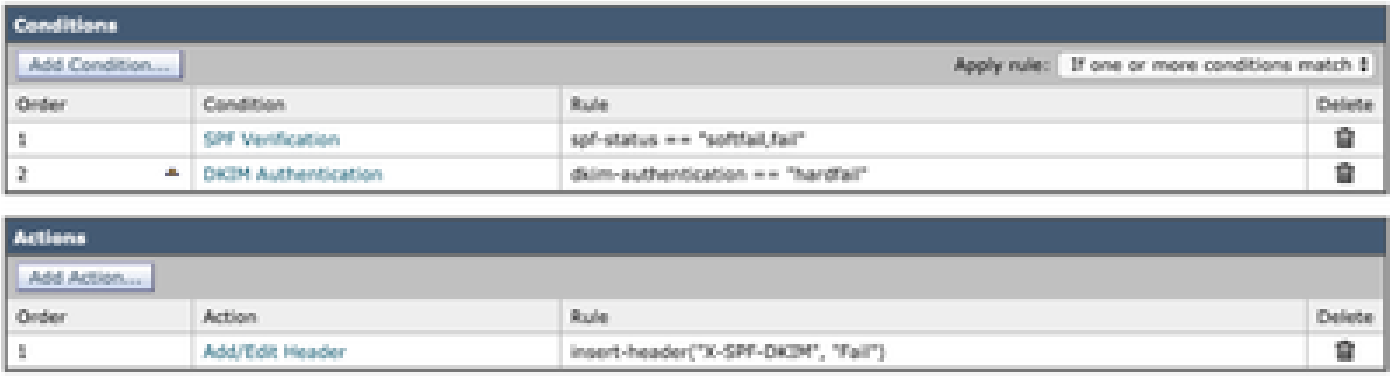


レイヤ5:SPFまたはDKIM検証結果によるFalse Positiveの削減

ほとんどの攻撃タイプに対してスプーフィングEメール検出のマルチレイヤを構築するには、SPFまたはDKIMの検証（両方またはいずれか一方）を実施する必要があります。シスコでは、最終的なアクション（廃棄や検疫など）を実行する代わりに、SPFまたはDKIMの検証に失敗するメッセージに[X-SPF-DKIM]などの新しいヘッダーを追加し、スプーフィング電子メールの捕捉率を向上させるために、その結果をForged Email Detection(FED)機能と連携させることを推奨しています。

ベストプラクティス：以前のインスペクションを通過した各着信メッセージのSPFまたはDKIM検証結果を検査するコンテンツフィルタを作成します。SPFまたはDKIMの検証に失敗し、次のスキャニングレイヤであるForged Email Detection(FED)に配信するメッセージに新しいXヘッダー（X-SPF-DKIM=Failなど）を追加します。

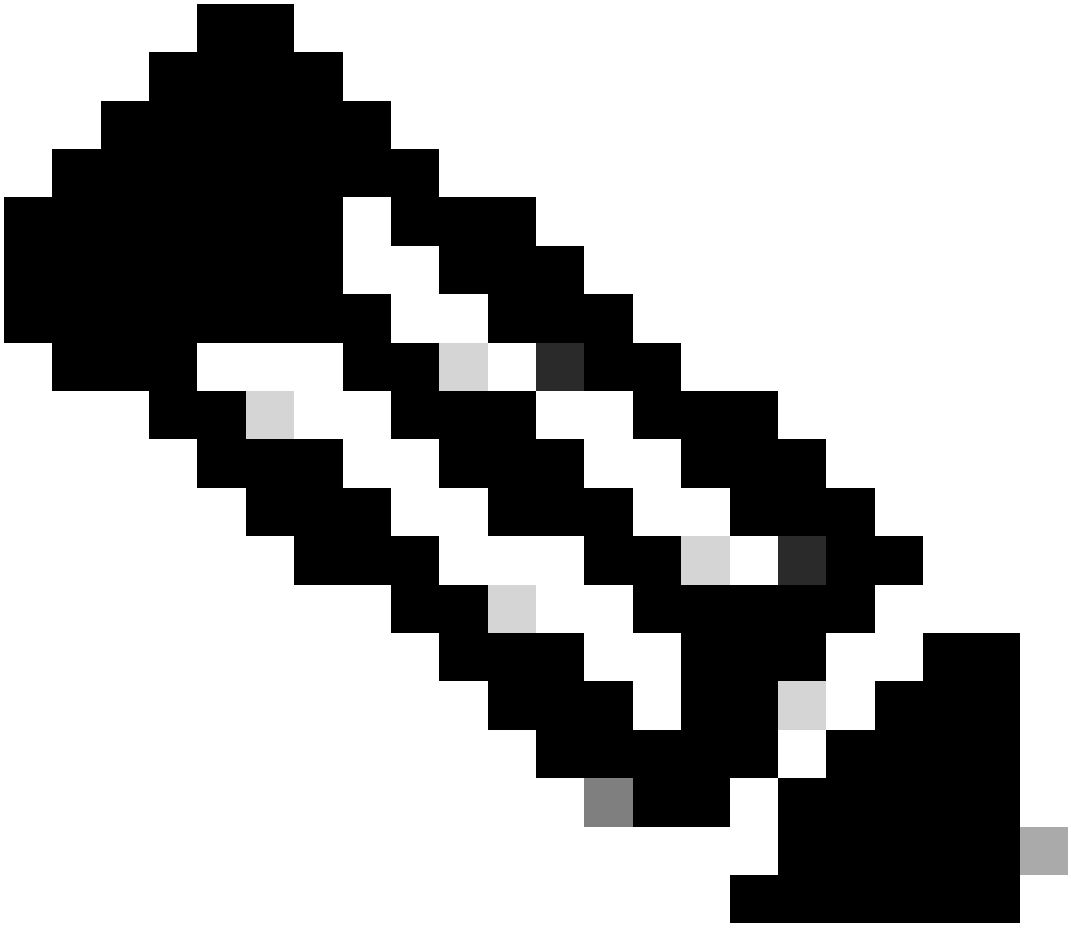
図 7.失敗したSPFまたはDKIMの結果を含むメッセージを検査するコンテンツフィルタ



レイヤ6：偽造された可能性のある送信者名を含むメッセージの検出

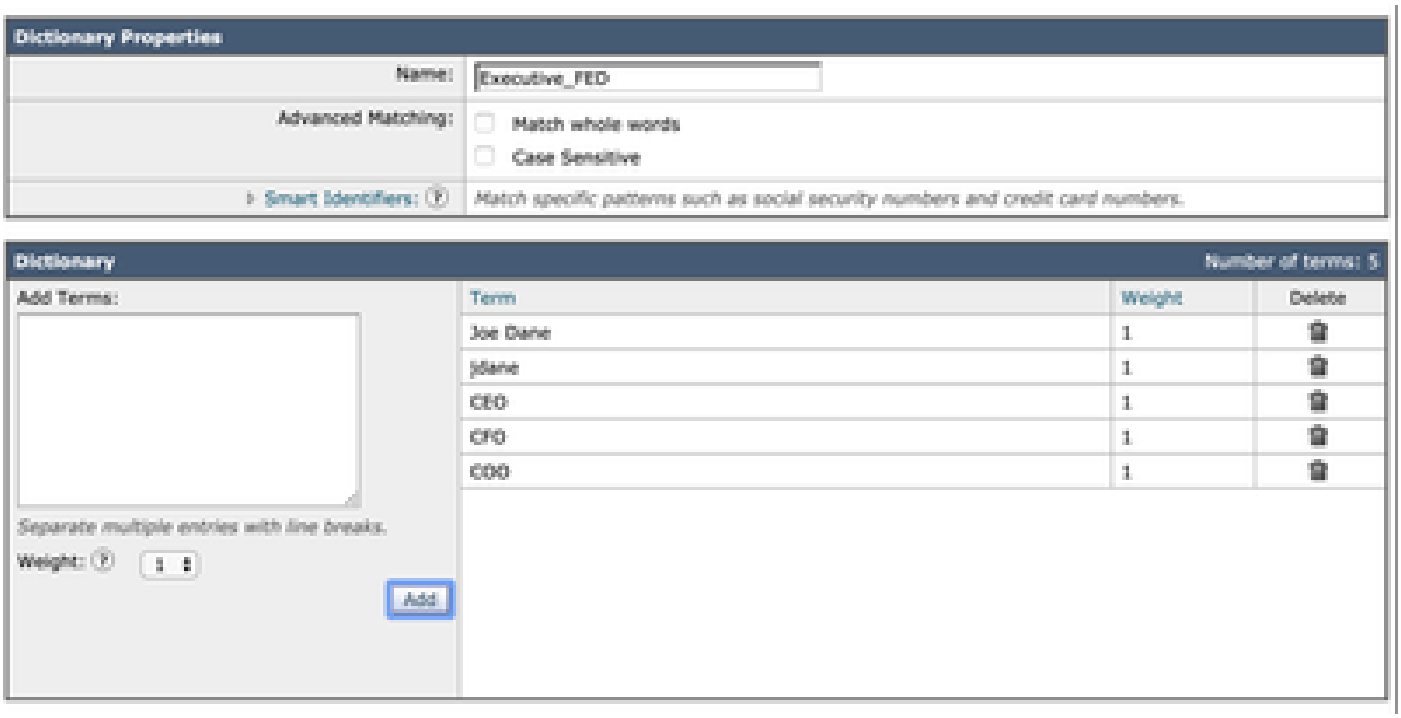
SPF、DKIM、およびDMARCの検証を補完するForged Email Detection(FED)も、電子メールのスプーフィングに対する重要な防衛線です。FEDは、メッセージ本文のFrom値を悪用するスプーフィング攻撃の修復に最適です。組織内の経営幹部の名前を既に知っている場合は、これらの名前のディクショナリを作成し、コンテンツフィルタでFED条件を使用してそのディクショナリを参照できます。さらに、経営幹部名とは別に、DNSTWIST(DNSTWIT)を使用して、類似したドメインスプーフィングと照合することにより、ドメインに基づいていとこまたは類似したドメインのディクショナリを作成できます。

ベストプラクティス：メッセージが偽造されている可能性がある組織内のユーザを特定します。経営幹部を対象としたカスタムディクショナリを作成します。すべての経営幹部の名前に対して、辞書にはユーザ名とすべての可能なユーザ名を用語として含める必要があります（図8）。辞書が完成したら、コンテンツフィルタでForged Email Detection(FED)を使用して、着信メッセージのFrom値をこれらの辞書エントリと照合します。



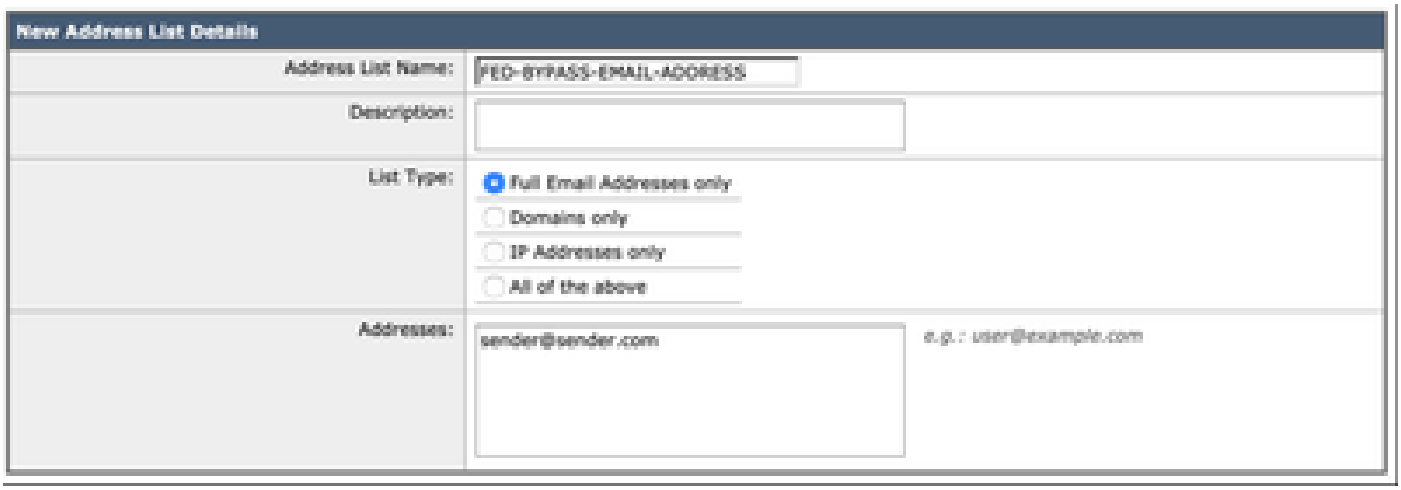
注：ほとんどのドメインは登録された置換ではないため、DNS送信者検証によってそれらのドメインから保護されます。辞書エントリを使用する場合は、登録ドメインだけに注意し、辞書ごとに500 ~ 600エントリを超えないようにしてください。

図 8.偽造電子メール検出のカスタムディレクトリ



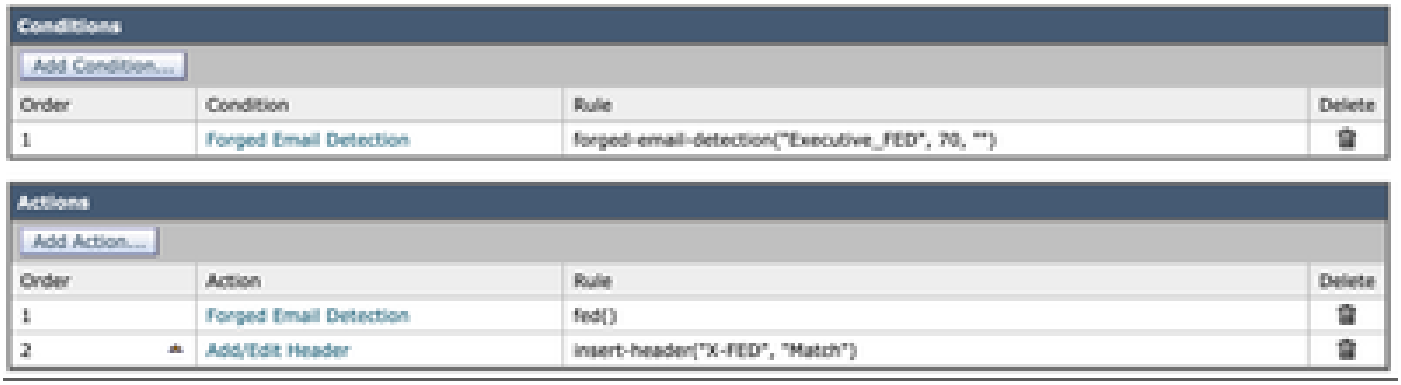
オプションで、エンベロープ送信に電子メールドメインの例外条件を追加して、FEDインスペクションをバイパスできます。または、カスタムアドレスリスト（図9）を作成して、FED検査をバイパスし、Fromheaderに表示される電子メールアドレスのリストを作成することもできます。

図 9.FEDインスペクションをバイパスするためのアドレスリストの作成



Forged Email Detection独自のアクションを適用して、From値を削除し、メッセージの受信トレイで実際のエンベロープ送信者の電子メールアドレスを確認します。次に、最終的なアクションを適用するのではなく、条件に一致するメッセージに新しいXヘッダー（X-FED=Matchなど）を追加し、そのメッセージを次の検査レイヤ（図10）に引き続き配信します。

図 10.FEDの推奨コンテンツフィルタ設定

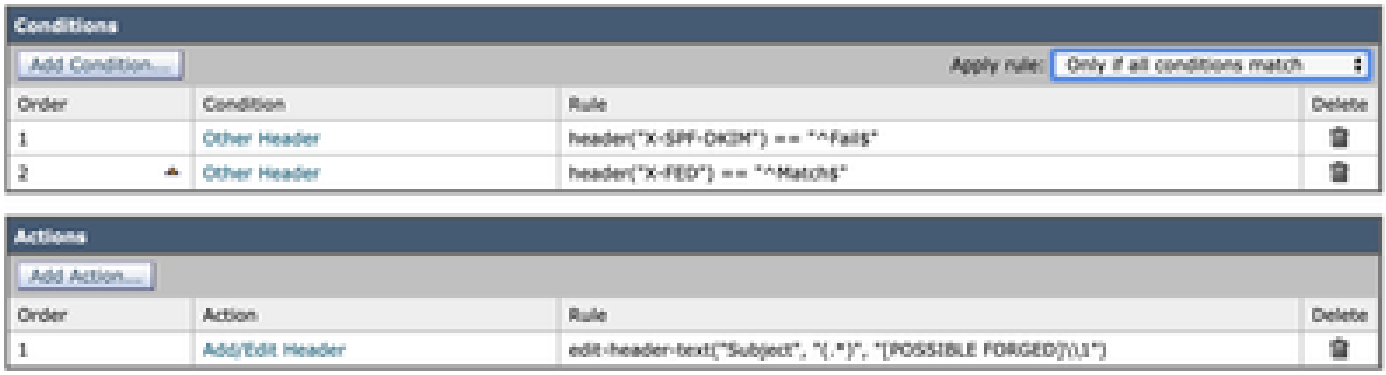


第7層：確実に識別されるスプーフィング電子メール

実際のスプーフィングキャンペーンを特定することは、SPF/DKIM EnforcemenおよびFEによって生成されたXヘッダー情報など、パイプラインのさまざまなセキュリティ機能から他の判定を参照することでより効果的です。たとえば、SPF / DKIM検証結果の失敗(X-SPF-DKIM=Fail)によって新しいXヘッダーと追加されたメッセージ、およびFEDディクショナリエントリに一致するFromヘッダー(X-FED=Match)の両方を識別するコンテンツフィルタを作成できます。

推奨処置は、メッセージを隔離して受信者に通知するか、元のメッセージの配信を続行し、図に示すように受信者に対する警告として[POSSIBLE FORGED]という語を[Subject]行に追加することです（図11）。

図 11.すべてのXヘッダーを1つの（最終）ルールに結合する



第8層：フィッシングURLからの保護

フィッシングリンクに対する保護は、Cisco Secure EmailのURLおよびアウトブレイクフィルタリングに組み込まれています。混合型の脅威は、スプーフィングとフィッシングメッセージを組み合わせて、ターゲットに対してより正当に見えます。アウトブレイクフィルタリングを有効にすることは、このような脅威をリアルタイムで検出、分析、および停止するために不可欠です。URLレピュテーションはアンチスパムエンジン内で評価され、スパム検出の決定の一部として使用できることを知る価値があります。スパム対策エンジンがURLをスパムとして含むメッセージを停止しない場合、セキュリティパイプラインの後半にあるURLおよびアウトブレイクフィルタリングによって評価されます。

推奨事項：悪意のあるレピュテーションスコアを含むURLをブロックし、ニュートラルレピュテーションスコアを含むURLをCisco Security Proxyにリダイレクトするコンテンツフィルタルール

を作成します（図12）。メッセージの変更を有効にして、脅威アウトブレイクフィルタを有効にします。URL書き換えにより、疑わしいURLをCisco Security Proxyで分析できます（図13）。詳細については、「セキュアEメールゲートウェイおよびクラウドゲートウェイのURLフィルタリングの設定」を参照してください。

図 12.URLレピュテーションのコンテンツフィルタ

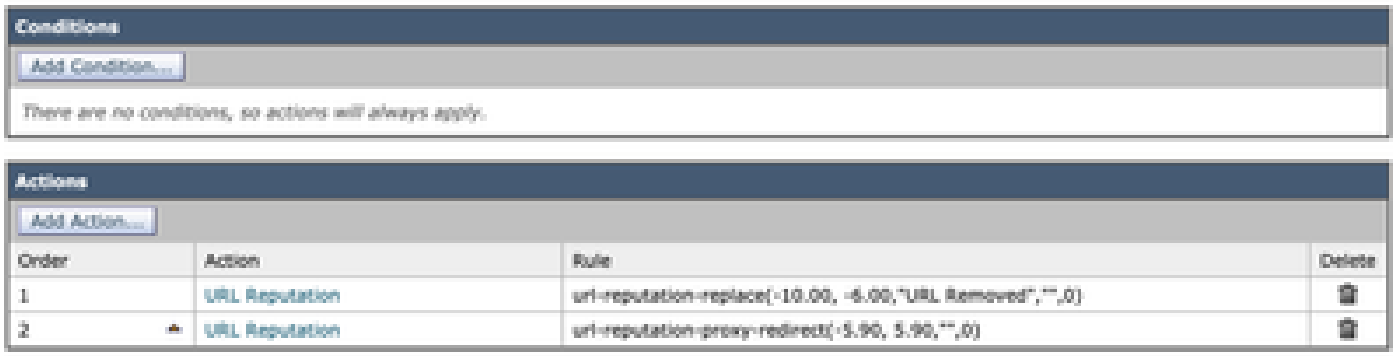
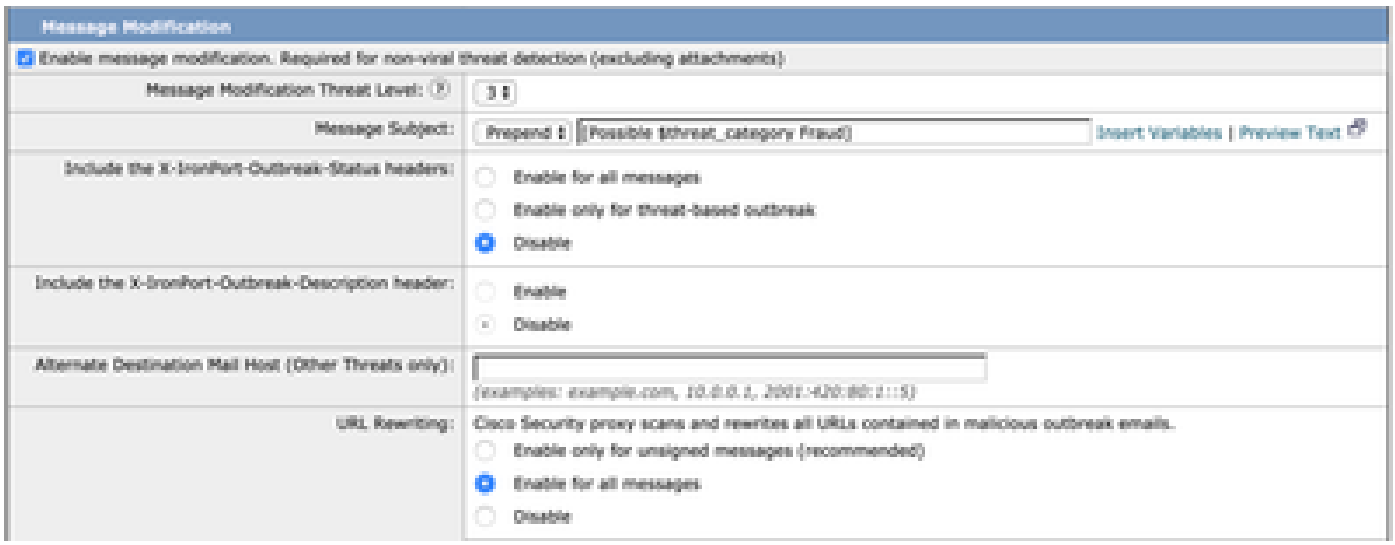


図 13.アウトブレイクフィルタリングでのURLリライトの有効化



レイヤ9:Cisco Secure Email Threat Defense(ETD)によるスプーフィング検出機能の強化

シスコは、Cisco Talosの優れた脅威インテリジェンスを活用するクラウドネイティブソリューションであるEメール脅威対策を提供しています。API対応のアーキテクチャにより、応答時間の短縮、電子メールの完全な可視化（内部Eメールを含む）、状況に応じたより適切な情報を表示するカンバセーションビュー、Microsoft 365メールボックスに潜む脅威の自動または手動による修復を行うツールを提供します。詳細については、『Cisco Secure Email Threat Defense Data Sheet』を参照してください。

Cisco Secure Email Threat Defenseは、送信者認証とBEC検出機能を使用してフィッシングと闘います。機械学習と人工知能エンジンを統合し、ローカルのアイデンティティと関係モデリングをリアルタイムの行動分析と組み合わせて、アイデンティティ詐欺ベースの脅威から保護します。組織内および個人間の信頼できるEメールの動作をモデル化します。Eメール脅威に対する防御には、主に次のような利点があります。

- 高度な脅威検出機能を使用して、既知の脅威、新しい脅威、ターゲットを絞った脅威を検出します。
- 悪意のある手法を特定し、特定のビジネスリスクのコンテキストを把握します。
- 危険な脅威をすばやく検索し、リアルタイムで修復します。
- 検索可能な脅威テレメトリを使用して脅威を分類し、組織のどの部分が攻撃に対して最も脆弱であるかを把握します。

図 14.Cisco Secure Email Threat Defenseは、お客様の組織がどのように標的とされているかについての情報を提供します。

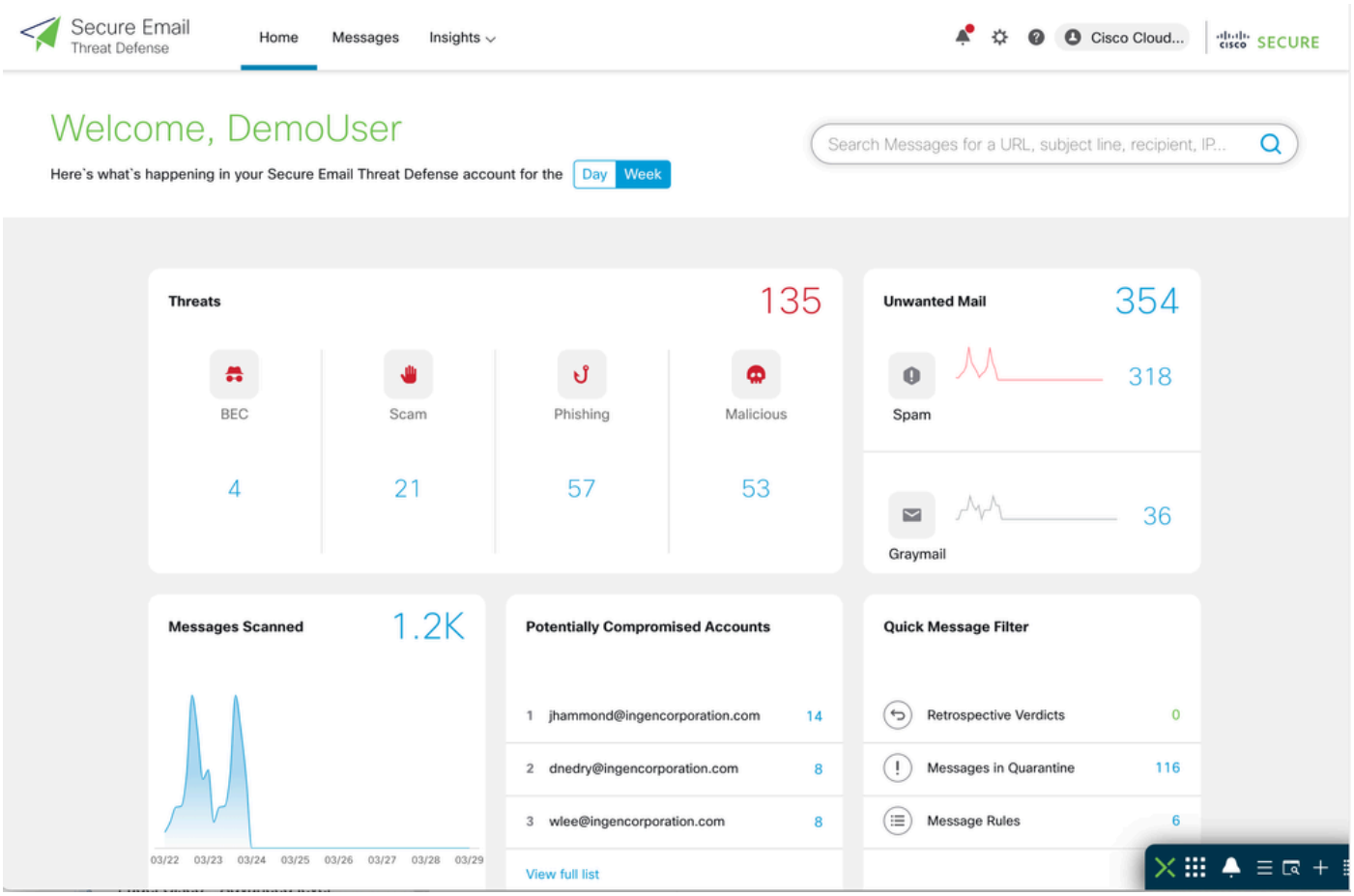
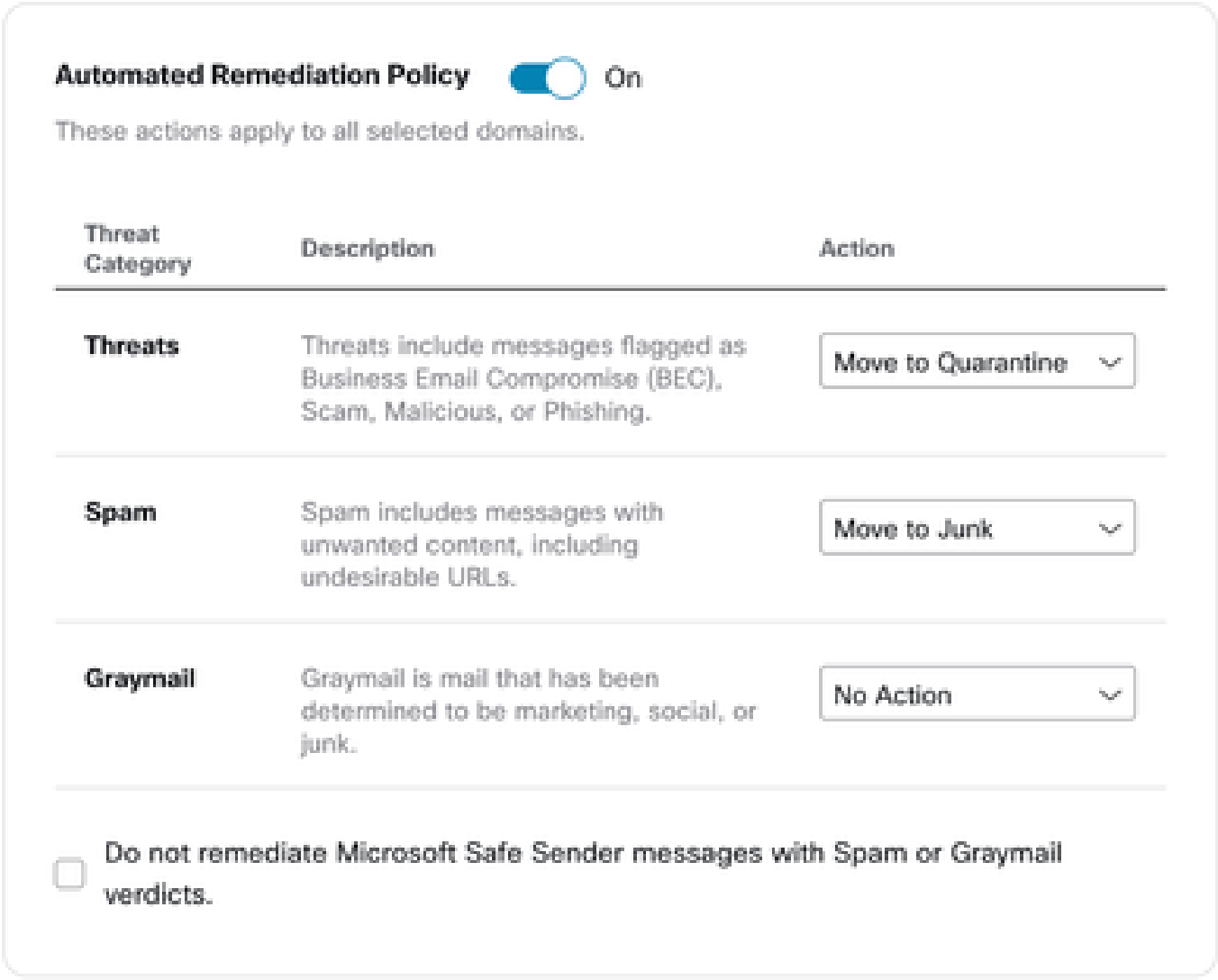


図 15.Cisco Eメール脅威に対する防御ポリシー設定により、メッセージが選択された脅威カテゴリに一致するかどうかが自動的に判断されます



スプーフィング防止でできること

多くのスプーフィングは、次のような簡単な予防策を講じて修復できます（ただし、これに限定されるわけではありません）。

- ホストアクセステーブル(HAT)にリストされているドメインの許可を、ごく少数のコアビジネスパートナーに制限します。
- SPOOF_ALLOW送信者グループを作成し、ベストプラクティスリンクに示されている手順を使用している場合は、送信者グループのメンバーを継続的に追跡および更新します。
- グレイメール検出を有効にして、スパム検疫にも配置します。

しかし、最も重要なことは、SPF、DKIM、およびDMARCをイネーブルにして、適切に実装することです。ただし、SPF、DKIM、およびDMARCレコードの公開に関するガイダンスは、このドキュメントの範囲外です。詳細については、ホワイトペーパー『Eメール認証のベストプラクティス：SPF、DKIM、およびDMARCを導入する最適な方法』を参照してください。

ここで説明するスプーフィングキャンペーンのように、電子メール攻撃を修復する際の課題を理解します。これらのベストプラクティスの実装に関して質問がある場合は、シスコテクニカルサポートに連絡してサービスリクエストをオープンしてください。または、ソリューションと設計

ガイダンスについてシスコアカウントチームにお問い合わせください。Cisco Secure Emailの詳細については、Cisco Secure Email のWebサイトを参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。