Cisco Email Threat Defense(ETD)とCisco Secure Accessを統合する手順：

内容

はじめに

このドキュメントでは、Cisco Email Threat Defense(ETD)とCisco Secure Access(SA) for Email DLPをETD SMTPインラインモードで統合する手順を説明します。これにより、Cisco Secure Access(SA)を使用して、ETDを通過するすべての送信EメールがDLP用にスキャンされます。

概要

今日の分散型の作業環境では、電子メールは依然としてビジネスの主要なコミュニケーションツールであり、サイバー攻撃やデータ漏洩の最も頻繁な標的となっています。これらの進化する課題に対処するため、シスコはEメール脅威対策(ETD)およびセキュアアクセスEメールデータ損失防止(DLP)を通じて、Eメールセキュリティに対する包括的なアプローチを提供します。

Cisco Email Threat Defenseの脅威検出機能とSecure Access Email DLPの堅牢なデータ保護を組み合わせることにより、組織は多層的な防御戦略を確立できます。このアプローチは、外部の利用者からの受信トレイを保護するだけでなく、ユーザの居場所や電子メールへのアクセス方法に関係なく、企業の機密データを厳重に管理できるようにします。

前提条件

以下のコンソールにアクセスします。

1. インラインモードのCisco Email Threat Defense Console(ETD)

   ETDコンソールは、Eメールセキュリティポスチャの中央集中管理プレーンとして機能します。このコンソールへのアクセスは、高度な脅威から環境を保護するための最初のステップです。

   - 「インラインモード」が重要な理由：ETDがインラインモードで設定されている場合、ETDはメール転送エージェント(MTA)または電子メールフローのパスに配置される直接統合として機能します。これにより、メッセージが受信者の受信トレイに配信される前に、メッセージを検査、ブロック、または変更できます。
2. Cisco Secure Access Console(SA)

Cisco Secure Accessは、データ損失防止(DLP)を含むさまざまなセキュリティサービスを1つの緊密なアーキテクチャに統合する、統合されたクラウド提供のセキュリティプラットフォームです。

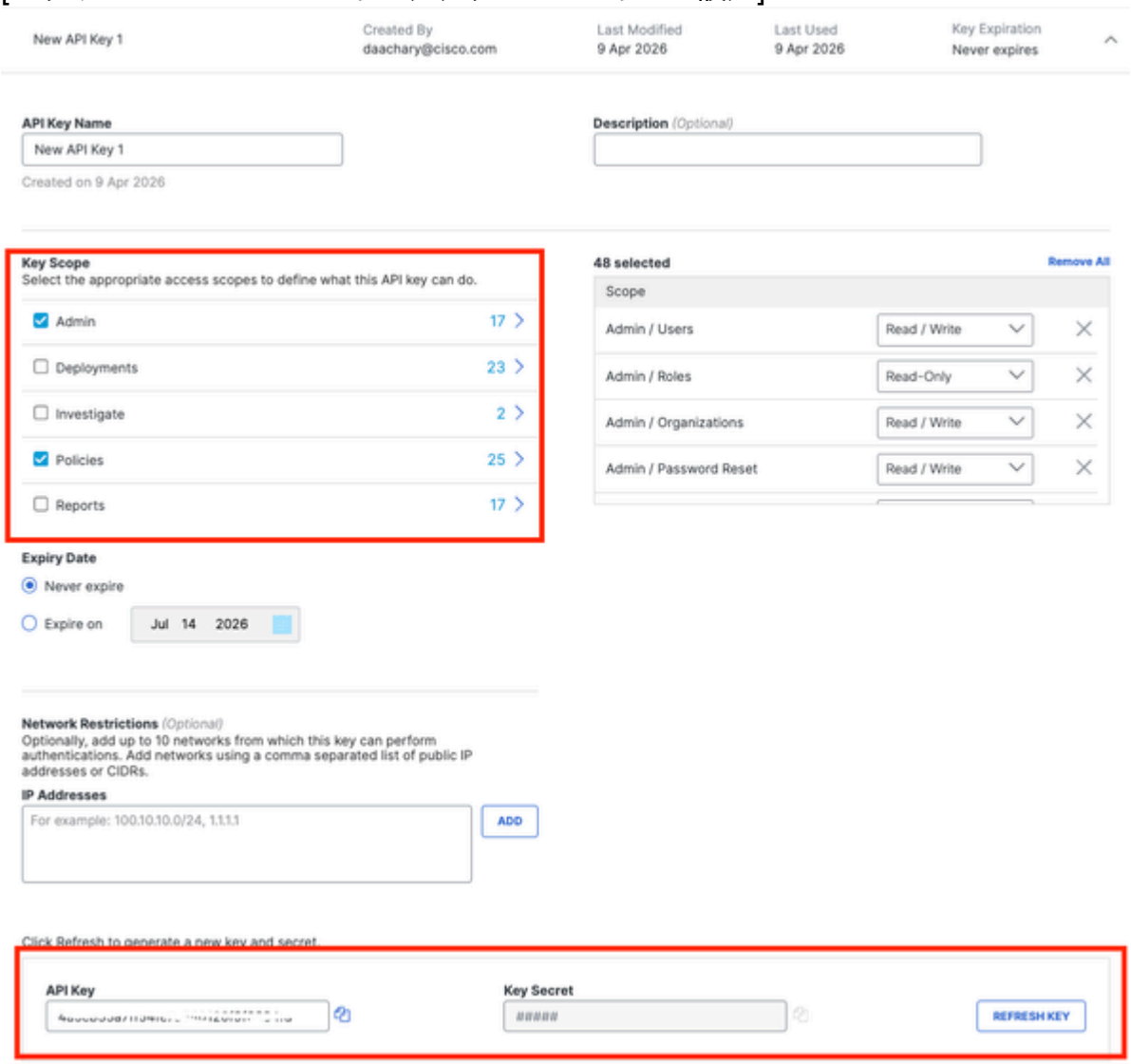
- SAコンソールが必要な理由：セキュアアクセスコンソールは、組織のセキュリティポリシーのオーケストレーションハブです。ETDが脅威固有の電子メールフローを処理する一方で、Secure Access ConsoleではbroaderDLP ポリシーを定義します。このポリシーは、機密データの社内全体での特定方法および処理方法を制御します。
- コンソールロール：このコンソールを使用すると、管理者はデータ分類ルール（PII、クレジットカード番号、内部プロジェクトコードの識別など）を作成および適用できます。SAコンソールにアクセスすることで、電子メールのDLPポリシーを全体的なセキュリティ戦略と同期させることができ、両方の電子メールトラフィックに一貫した適用が可能になります。

設定

統合ステップ

ステップ1:Cisco Secure AccessでAPIクレデンシャルを生成する

開始するには、Secure Accessコンソール内で必要なAPIクレデンシャルを生成し、接続を許可する必要があります。

1. Cisco Secure Accessdashboardにログインします。
2. Admin>API Keysの順に移動します。
3. 新しいAPIキーを作成するオプションを選択します。
4. キーにスコープAdminandPolicyを割り当てます。
    - [スクリーンショット：セキュアアクセスAPIキーの設定]
    - 

ステップ2：キーの有効期限を設定する

組織のセキュリティポリシーに基づいてAPIキーのライフサイクルを定義します。

- オプション1：無期限：手動で交換することなく、中断のないサービスを提供します。
- オプション2：特定の日付 – 定義された有効期限タイムラインを設定します。
    - 重要な注意：有効期限を設定する場合は、ローテーション· プロセスを計画してください。DLPサービスの中断を防ぐために、有効期限の前にETDコンソールでAPIキーを再設定する必要があります。

ステップ3：資格情報を保護する

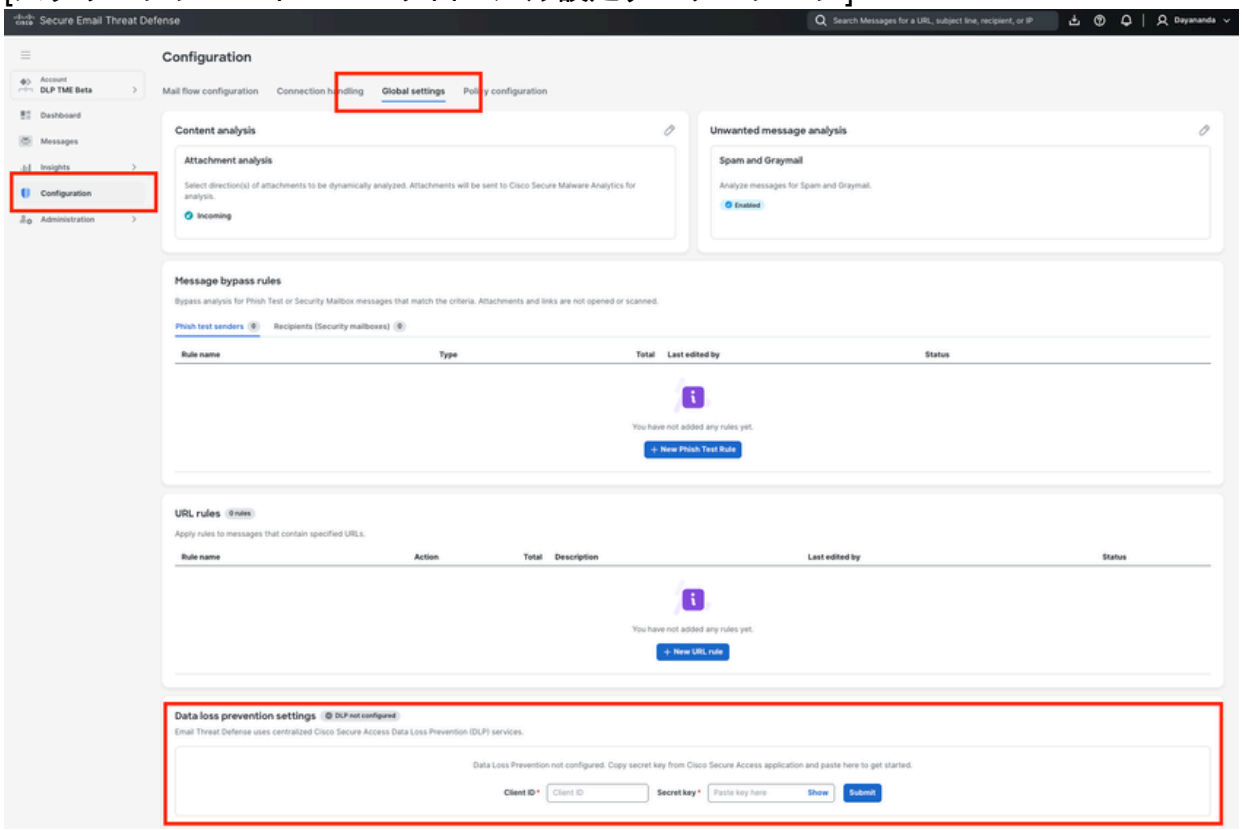
キーが生成されると、API KeyとKey Secretが表示されます。

- 処置：これらのクレデンシャルをコピーし、安全な場所（パスワードマネージャなど）に保存します。
- 警告：この画面から離れると、TheKey Secretは表示されなくなります。紛失した場合は、新しいキーペアを生成する必要があります。

ステップ4:ETD設定にアクセスする

認証情報を保護した状態で、ETDコンソールに進み、リンクを確定します。

1. Cisco ETDconsoleにログインします。
2. Configuration>Global Settingsの順に移動します。
   - [スクリーンショット：ETDグローバル設定ナビゲーション]
   -



ステップ5：統合の完了

セキュアアクセスから取得したクレデンシャルを入力して、ハンドシェイクを完了します。

1. グローバル設定メニューで、データ損失防止(DLP)セクションを見つけます。
2. ステップ3で保存したクライアントID（APIキー）と秘密キー（キーシークレット）を入力します。
3. 変更を保存します。

検証が成功すると、Cisco ETDとCisco Secure Accessの統合が完了し、DLPポリシーを電子メールトラフィック全体に適用する準備が整います。

これで、ETDとセキュアアクセスの統合が完了しました。
注:Cisco Secure Access for Email DLPでDLPポリシーを作成するには、「Cisco Secure Access(SA)およびCisco Email Threat Defense(ETD)でのEメールDLPポリシーの設定方法」を参照してください。

トラブルシューティングに関する注意

統合プロセスの実行中または実行後に問題が発生した場合は、次の一般的なシナリオと修復手順を確認してください。

1. APIクレデンシャルがETDで受け入れられない

- 症状：ETDにクライアントIDと秘密鍵を入力すると、システムから認証エラーが返されます。
- 解決策：
  - APIキーが正確な必須スコープ「Admin」および「Policy」で作成されたことを確認します。他のスコープが選択されている場合、またはこれらが欠落している場合、接続は失敗します。
  - クライアントIDまたは秘密鍵をETDコンソールに貼り付ける際に、先頭または末尾に誤ってコピーされたスペースがないことを確認します。

2. キーシークレットの紛失または紛失

- 症状：Secure Access APIの作成画面から移動したところ、キーシークレットが表示されなくなってしまいました。
- 解決策：セキュリティ上の理由から、キーシークレットは作成時に1回だけ表示されます。安全に保存しなかった場合は、セキュアアクセスで不完全なAPIキーを削除し、新しいキーを生成する必要があります。

3. DLPポリシーがEメールトラフィックに対して適用されない

- 症状：統合は成功しましたが、設定されたDLPポリシーが機密の電子メールを取得またはブロックしていないと表示されます。
- 解決策：
    - API有効期限の確認：APIキーの有効期限に「特定の日付を選択する」（ステップ2）を選択した場合は、キーが期限切れになっていないことを確認します。キーペアがある場合は、新しいキーペアを生成して適用する必要があります。
    - ETD導入モードの確認：Cisco ETDがインラインモードで導入されていることを確認します。ETDは、Secure Access DLPの判定に基づいてメッセージをアクティブにブロックまたは変更するために、ダイレクトメールフローパスに存在する必要があります。
    - 同期時間：初期統合後、バックエンドシステムがポリシーを同期するまで数分かかります。その後でDLPルールをテストします。

4. 安定期間後のサービス停止

- 症状：DLPの適用が、数ヵ月間正しく機能した後、突然停止します。
- 解決策：これは通常、有効期限が切れたAPIキーが原因で発生します。Cisco Secure AccessでAdmin -> API Keysinに移動し、ETDに使用するキーのステータスを確認します。キーローテーションプロセスを実装して、有効期限に達する前にETDのクレデンシャルを更新します。

要約

Cisco Eメール脅威対策(ETD)とCisco Secure Access(SA)の統合は、統合データ損失防止(DLP)戦略を確立するうえで重要なステップです。Secure Accessコンソールで「Admin」および「Policy」スコープを使用してセキュアAPIキーを生成し、ETDのグローバル設定でこれらのクレデンシャルを設定することで、管理者は2つのプラットフォーム間にシームレスな通信ブリッジを作成できます。

このハンドシェイクが完了すると、ETDは電子メールメタデータをSecure Access DLPエンジンにアクティブにハンドオフできます。これにより、組織はEメールトラフィック(ETD)に対する高度な可視性と適用を維持しながら、1つの一元化されたダッシュボード（セキュアアクセス）からすべてのデータ保護ポリシーを管理できます。

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。