Cisco Secure Accessに関するリアルタイムのDLP問題のトラブルシューティング

内容

概要

このドキュメントでは、Secure Web Gateway(SWG)環境内のインラインまたはリアルタイムデータ損失防止(DLP)の問題のトラブルシューティング手順について説明します。

前提条件と警告

- HTTPSインスペクション：HTTPSインスペクションが有効になっていることを確認します。DLPは暗号化トラフィックをスキャンできません。WebサイトがCisco Secure AccessルートCAまたはカスタムCAで復号化されていることを確認します。
- QUICプロトコル：すべてのブラウザでQUICプロトコルを無効にします。QUICはUDPを使用します。UDPはSWGをバイパスし、DLPスキャンを防止します。
- IPv6:デュアルスタック機能はバイパスを引き起こす必要があるため、トラフィックがSWGに到達しない場合はIPv6を無効にします。
- セキュリティポリシー：アクセスルールで[許可 – セキュリティの上書き]または[分離]が有効になっていないことを確認してください。

概要

インラインDLPは、SWGの拡張スキャン機能です。SWGプロキシを介してアップロードされたファイル内の機密データ、機密データ、または個人を特定できるデータのアップロードを監視またはブロックします。お客様は、シスコが定義した識別子（クレジットカードや社会保障番号など）またはカスタムキーワードを使用してデータ分類を作成します。これらの分類は、特定のIDと宛先に割り当てられたDLPポリシーに適用されます。DLPエンジンは、HTTP POST、PUT、およびPATCHメソッドのみをスキャンします。

一般的なトラブルシューティングのチェックリスト

DLP検出が発生していない場合は、次に示す手順を確認します。

- 接続：http://policy.test.sse.cisco.comにアクセスして、クライアントがSWGを使用していることを確認します。正しいSWGデータセンターが適用され、テスト結果に「protected by Secure Access」と表示されることを確認します。
- Decryption:セキュリティプロファイルでSSL Decryptionが有効になっていることを確認します。選択的な復号化リストまたは「復号化しない」リストの除外がないことを確認します。
- トラフィックのステアリング：インターネットの設定に外部ドメインバイパス(MAB)が設定されていないことを確認します。
- ID:DLPポリシーがActive Directoryグループに依存している場合は、ユーザが正しいグループのメンバであることを確認します。
- アプリケーションの設定：MicrosoftドメインがDLPに使用されている場合、Office 365バイパスまたはM365互換性設定が無効になっていることを確認してください。
- アクティビティ検索：完全なURLが表示（復号化）され、予期されるIDがトラフィックに関連付けられていることを確認するには、レポート>アクティビティ検索を使用します。Reporting > Data Loss Preventionの順にチェックして、モニタアクティビティまたはブロックアクティビティがログに記録されているかどうかを確認します。
- ポリシー設定：DLPポリシーが正しいIDおよび宛先アプリケーション用に設定されていることを確認します。
- テスト：既知の適切な宛先(pastebin.comやdlptest.comなど)と、シスコのドキュメントに記載されている既知の適切なサンプルテスト文字列を使用します。
- サポートデータ：ユーザからHARファイルを収集し、トラフィックがSWG経由でルーティングされることを確認し、SWGヘッダーを確認します。

フォールスネガティブのトラブルシューティング

DLPがアクティブでも特定の分類子のトリガーが失敗する場合は、次の領域を調査します。

分類子、ファイル、文字列

- ファイルステータス：ファイルが暗号化されていないか、スキャン不可能であることを確認します。簡単なテキストファイルでテストします。
- しきい値：Policy > Data Classificationで、しきい値と近接度の設定を確認してください。分類子では、ヒット数を増やしたり、カスタムストリングに近づけたりする必要がある場合があります。
- 正規表現パターン：オンラインツール(regexr.comなど)を使用してパターンを視覚化します。パターンを単純化して、文字列の小さい部分をキャッチし、徐々に拡大します。

ファイルラベル

- 互換性：ファイルラベル検出はConfluenceまたはJIRAでは機能しません。
- メタデータ：Microsoftアプリケーションでドキュメントプロパティを開きます。値はUmbrellaファイルラベルと正確に一致する必要があります。大文字と小文字は区別されます。
- 暗号化：ラベル検出は、パスワードで保護されたファイルや暗号化されたファイルには機能しません。

Webサイトと通知先

- サポートされているアプリケーション：サポートされているアプリケーションのリストを確認します。サポートされていないアプリケーションまたは「すべての宛先」では、特定のMIMEタイプのみがスキャンされます。
- 検査済みアプリケーション：検査済みアプリケーション(dlptest.comなど)がより包括的にスキャンされます。ランダムなWebサイトは、ファイル違反のスキャンのみが可能です。
- ファイル名：検査された特定のアプリケーションのファイル名だけを検索します。

誤検出のトラブルシューティング

DLPがコンテンツと予期せずに一致する場合は、[レポート] > [データ損失防止] で分類子名とDLPルールを確認します。検出は正当であるが望ましくない場合は、しきい値または近接設定を調整してポリシーを調整します。

デスクトップアプリケーションサポート

デスクトップベースのアプリケーション（Outlook、Teams、Google Workspaceなど）のサポートは、ベスト工フォート方式で提供されます。効率はファイルのアップロード時に使用されるメッセージ形式によって異なり、Webベースのバージョンとデスクトップのバージョンでは異なる場合があります。テストされていないアプリケーションの場合、ファイルのアップロードがサポ

ートされているかどうかは保証されません。

DLP分類子Gotcha

- クレジットカード番号：検証にはLuhnアルゴリズムが使用されます。有効なクレジットカード番号でのみテストします。
- 人名：2 ~ 3語を入力する必要があります。また、各単語は大文字を使用する必要があります。
- 名前の組み合わせ：名前と他のデータの間には区切り文字が必要です（たとえば、「Viagra - John Smith」は一致しますが、「Viagra John Smith」は一致しません）。
- 生年月日：「dob」や「生年月日」などのキーワードまたはヘッダーの近くにする必要があります。
- 好ましくないコンテンツ：特定の例外文字列により、テキストがブックやレポートに似ている場合にこの分類子が発行されるのを防ぎます。
- ポストコード：特定の口ケーション関連キーワードの近くになければなりません。

正確なデータ照合(EDM)

EDMを調査する前に、一般的なDLPスキャンが機能していることを確認します。EDM固有の問題については、ダッシュボードの「Last Edit」フィールドが最新であることを確認し、インデックスツールの出力を確認します。

コマンドの使用状況：

`-d`オプションを指定してインデックスツールを実行し、ブルーム(bloom)フィルタファイル(.blm)を生成します。 このコマンドは、EDMインデックスを検証し、レコードをスキップする理由をトラブルシューティングするために使用します。`-d`フラグを使用すると、診断ブルーム・フィルタ・ファイルを出力するようにツールに指示できます。このファイルは、サンプル・ファイルまたはHAR/Web開発者ツール・データとともに、サポートと共有する必要があります。

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。