セキュアアクセスでのDLP経由のTXTアップロードのブロック

内容

はじめに

このドキュメントでは、DLPを使用するCisco Secure Accessで。TXTファイルのアップロードをブロックする手順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。

- Cisco Secure Access管理
- データ損失防止(DLP)。

Cisco では次の前提を満たす推奨しています。

- Cisco Secure Accessへの管理アクセス

使用するコンポーネント

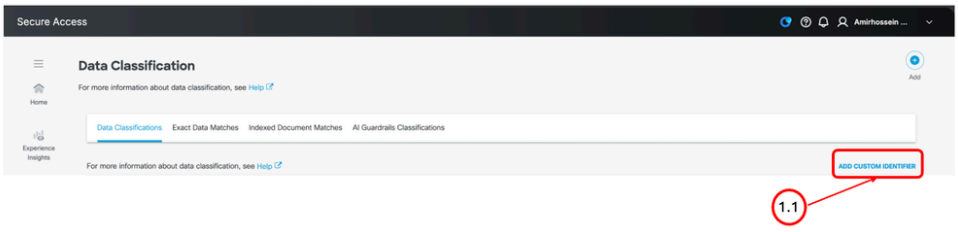
このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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たものです。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。

はじめる前に

1. これらの手順は、DLPプロセスに余分な負荷を与え、パフォーマンスの低下を引き起こす可能性があるため、注意して使用してください。TXTファイルのブロックが利用できるようになるまで、現在サポートされているファイルタイプについては次のリンクを参照してください。Cisco Secure Access - Supported File Types
2. この記事には、参照用に使用できる正規表現の例が含まれています。例を使用する前に、一致条件とそれらが特定するために設計されているパターンを十分に理解してください。必要に応じて、独自の正規表現を作成することもできます。どのような場合でも、目的の一致条件と可能なバリエーションがすべて正しく反映されるように、式を慎重に検証してください。
3. DLPポリシーを適用する前に、トラフィックが復号化されていることを確認します。DLPインスペクションでは、復号化されたコンテンツへのアクセスが必要です。暗号化されたトラフィックをスキャンしてDLPの一致を確認することはできません。

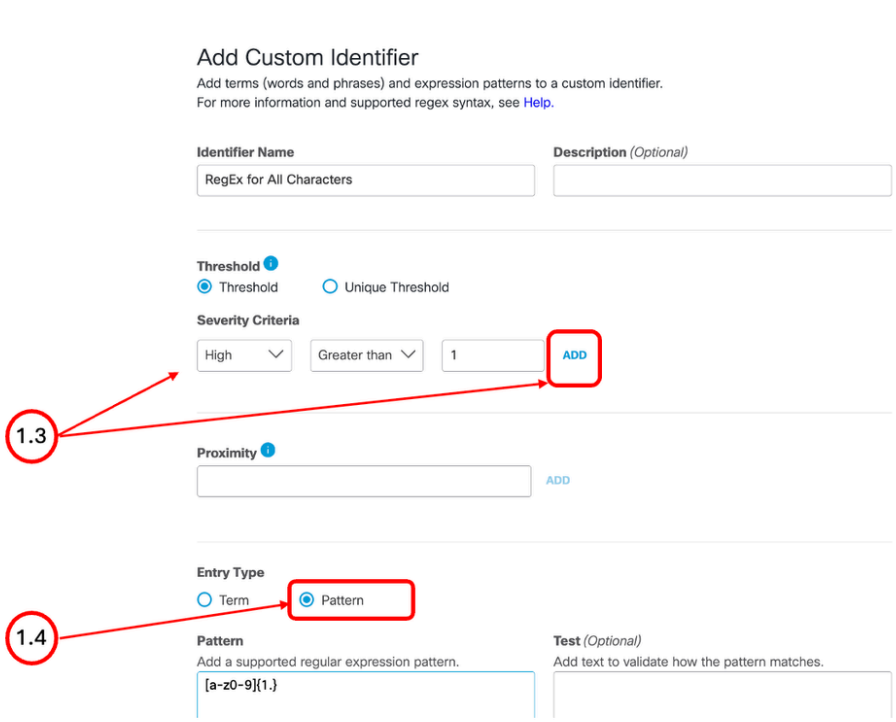
設定手順

[Category]	手順
ステップ 1：データ分類の作成	ステップ 1.1： Cisco Secure Access管理ポータルから、Secure > Data Classificationに移動し、Add Custom Identifierをクリックします。  イメージ – 新しいカスタムIDの作成 ステップ 1.2：新しい識別子の名前を定義します

ステップ 1.3：Thresholdセクションで、Severity Criteria を設定し、Addをクリックします。

ステップ 1.4： 各正規表現を個別に定義し、追加をクリックします。

ヒント：この記事で提供されている正規表現は例にすぎません。これらを使用する前に、式がすべての必要な一致条件と可能なバリエーションを正しくカバーしていることを確認します。

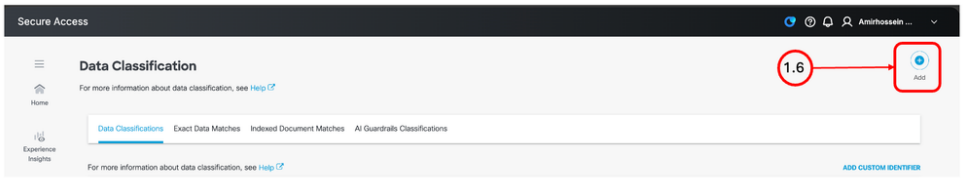


イメージ – カスタムIDの追加

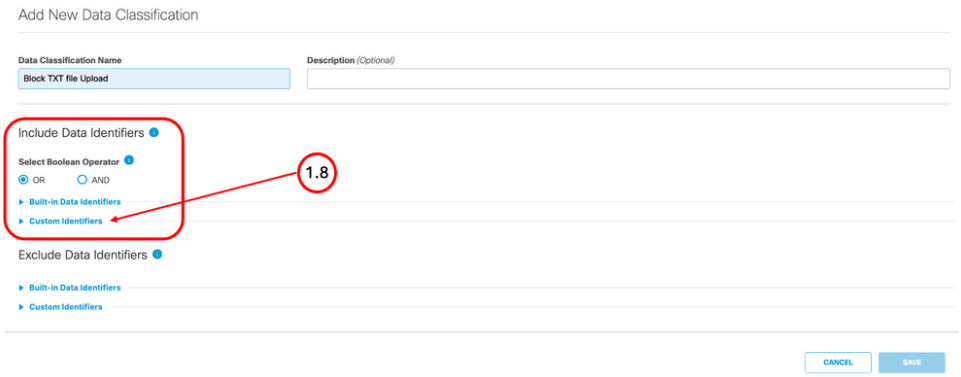
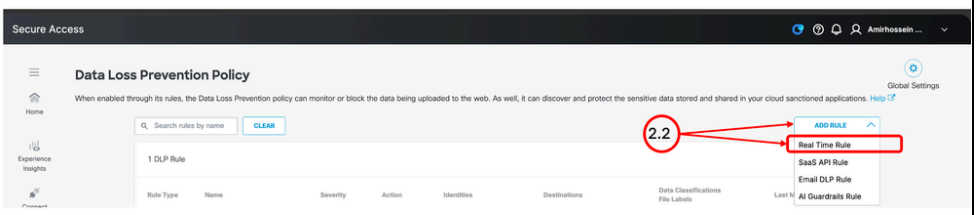
注：正規表現が10を超える場合は、同じ手順を使用して別のカスタム識別子を作成する必要があります。

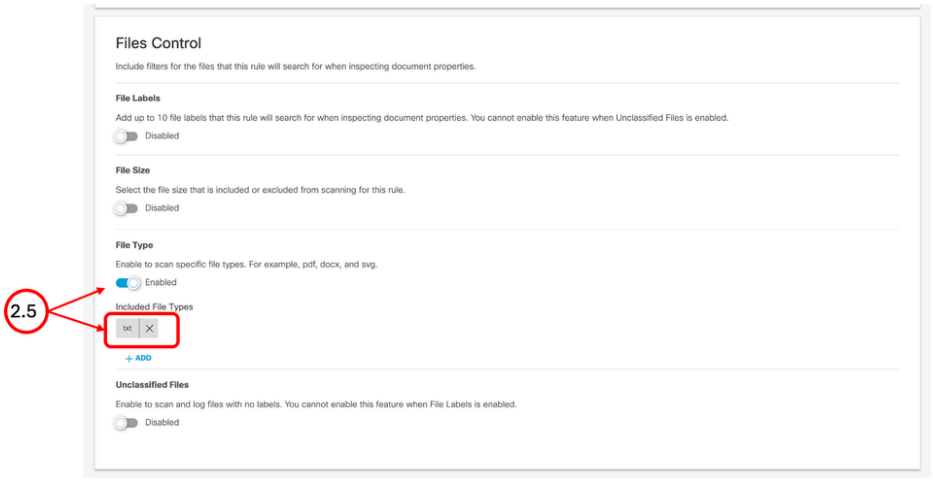
ステップ 1.5：[Save] をクリックします。

ステップ 1.6：Addアイコンをクリックして、新しいデータ分類を作成します



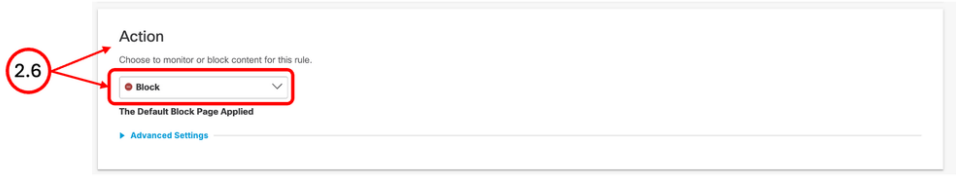
イメージ：新しいデータ分類の作成

	ステップ 1.7：名前を定義します。 ステップ 1.8：Include Data Identifiersセクションから、Custom Identifierをクリックし、前のステップで作成したIDを選択します。  イメージ：データ分類の設定 ステップ 1.9：[Save] をクリックします。
ステップ 2DLPポリシーの設定	ステップ 2.1： Cisco Secure Access管理ポータルから、Secure > Data Loss Prevention Policyの順に移動します。 ステップ 2.2：Add Ruleをクリックして、Real Time Ruleを選択します。  イメージ：新しいリアルタイムDLPポリシーの作成 ステップ 2.3：ポリシー名を定義します。 ステップ 2.4：Data Classificationsセクションで、ステップ1で作成したデータ分類を選択します。 注：新しく作成されたデータ分類がDLPポリシーリストに表示されるようになるまで、最大5分かかります。 ステップ 2.5：Files Controlセクションで、File Typeを有効にし、TXTを選択します。



イメージ – ファイルタイプの設定

ステップ 2.6：Action セクションから、Blockを選択します。



イメージ – アクションをブロックに設定

ステップ 2.7：変更を保存します。

モニタリング

DLPのアクティビティと関連ログを確認するには、Monitor > Data Loss Preventionの順に選択します。使用可能なフィルタを使用して、結果を絞り込み、関連するDLPイベントを特定します。

正規表現の例

日本語のひらがな、カタカナ、漢字に一致する：

```
[ぁ-□ァ-ヺー-□]{1,}
```

大文字の英字に一致：

```
[A-Z]{1,}
```

小文字の英文字と数字に一致：

```
[a-z0-9]{1,}
```

一般的な句読点に一致：

```
[.,;:!?]
```

一重引用符、二重引用符、およびバックチックと一致：

```
['"`]
```

カッコ、角カッコ、および中カッコに一致します。

```
[()\[\]{}]
```

次の一般的な記号と特殊文字に一致します。

```
[@#$%^&*+=|\\/_~-]
```

À-Unicode範囲のラテン文字に一致します。

```
[À-ÿ]
```

キリル文字に一致：

```
[È-ж]
```

ギリシャ文字とコプト文字に一致：

[ヶ-ゞ]

アラビア文字の文字に一致：

[ـ-ۓ]

CJK統合表意文字と一致：

[丄-□]

選択したポーランド語の文字を発音区別符号に一致させます。

[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]

韓国語のハングル音節に一致する：

[가-힣]

関連情報

DLPがサポートされるファイルタイプの完全なリスト
：https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Cisco Secure Access DLPがサポートするファイルタイプ：シスココミュニティ
：https://community.cisco.com/t5/security-knowledge-base/cisco-secure-access-complete-list-of-dlp-supported-file-types/ta-p/5274268

Cisco Secure Access DLPの設定およびポリシーリファレンス
：https://securitydocs.cisco.com/docs/csa/olh/161419.dita

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。