Secure Web ApplianceでのカスタムURLカテゴリの設定

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)のカスタムUniform Resource Locator(URL)カテゴリの構造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。

- プロキシの仕組み。
- Secure Web Appliance(SWA)管理

Cisco では次の前提を満たす推奨しています。

- インストールされている物理または仮想Secure Web Appliance(SWA)。
- ライセンスがアクティブ化またはインストールされていること。
- セットアップウィザードが完了しました。

- SWA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。

カスタム URL カテゴリ

URLフィルタエンジンを使用すると、アクセスポリシー、復号ポリシー、およびデータセキュリティポリシーでトランザクションをフィルタリングできます。ポリシーグループのURLカテゴリを設定する場合、カスタムURLカテゴリ（定義されている場合）および定義済みURLカテゴリのアクションを設定できます。

特定のホスト名とインターネットプロトコル(IP)アドレスを記述するカスタムおよび外部のライブフィードURLカテゴリを作成できます。また、URLカテゴリを編集および削除することもできます。

これらのカスタムURLカテゴリを同じAccess、Decryption、またはCisco Data Security Policyグループに含め、各カテゴリに異なるアクションを割り当てると、含まれるカスタムURLカテゴリが上位のもののアクションが優先されます。

注：ドメインネームシステム(DNS)が複数のIPをWebサイトに解決する場合、それらのIPの1つがカスタムブロックリストであれば、カスタムブロックリストになくても、Webセキュリティアプライアンス(WSA)はすべてのIPについてWebサイトをブロックします。

ライブフィードURLカテゴリ

外部ライブフィードカテゴリは、特定のサイトからURLのリストをプルするために使用されます。たとえば、MicrosoftからOffice 365のURLを取得するために使用します。

カスタムURLカテゴリと外部URLカテゴリを作成および編集するときに、カテゴリタイプとして[外部ライブフィードカテゴリ]を選択した場合は、フィード形式（Ciscoフィード形式またはOffice 365フィード形式）を選択し、適切なフィードファイルサーバにURLを指定する必要があります。

各フィードファイルの想定される形式を次に示します。

- Ciscoフィード形式：カンマ区切り値(.csv)ファイル、つまり拡張子が.csvのテキストファイルである必要があります。.csvファイルの各エントリは、アドレス/カンマ/アドレスタイプとしてフォーマットされた個別の行に記述する必要があります
(例：www.cisco.com,siteまたはad2.*\.com,regex) 有効なアドレスタイプはsiteとregexです。

Cisco Feed Format .csvファイルからの抜粋を次に示します。

```
www.cisco.com,site
\.xyz,regex
ad2.*\.com,regex
www.cisco.local,site
1:1:1:11:1:1::200,site
```

- Office 365フィード形式：これは、Microsoft Office 365サーバー、またはファイルの保存先のローカルサーバーにあるXMLファイルです。これはOffice 365サービスによって提供され、変更できません。

ファイル内のネットワークアドレスはXMLタグで囲まれ、この構造はproducts > product > address list > addressです。現在の実装では、「アドレスリストタイプ」はIPv6、IPv4、またはURL [ドメインと正規表現(regex)パターンを含めることができる]です。

Office 365フィードファイルのスニペットを次に示します。

fc00:1040:401::d:80

fc00:1040:401::a

fc00:1040:401::9

10.71.145.72

10.71.148.74

10.71.145.114

**.cisco.com*

**.example.local*

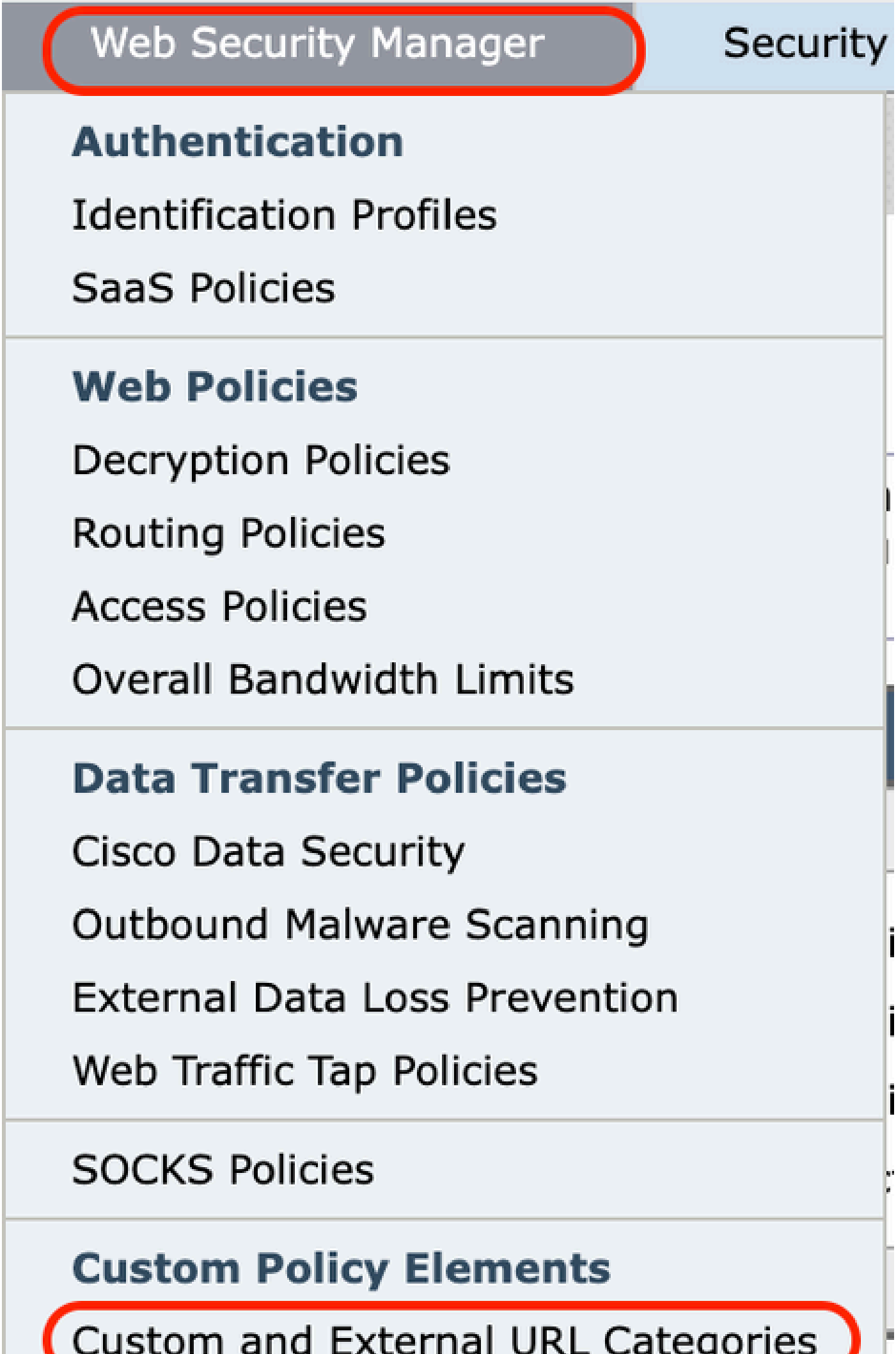
**.subdomain.cisco.com*

**.example.local*

注：ファイル内のサイトエントリの一部としてhttp://またはhttps://を含めないでください。含めると、エラーが発生します。つまり、www.cisco.comは正しく解析されますが、http://www.cisco.comはエラーを生成します

カスタムURLカテゴリを作成する手順

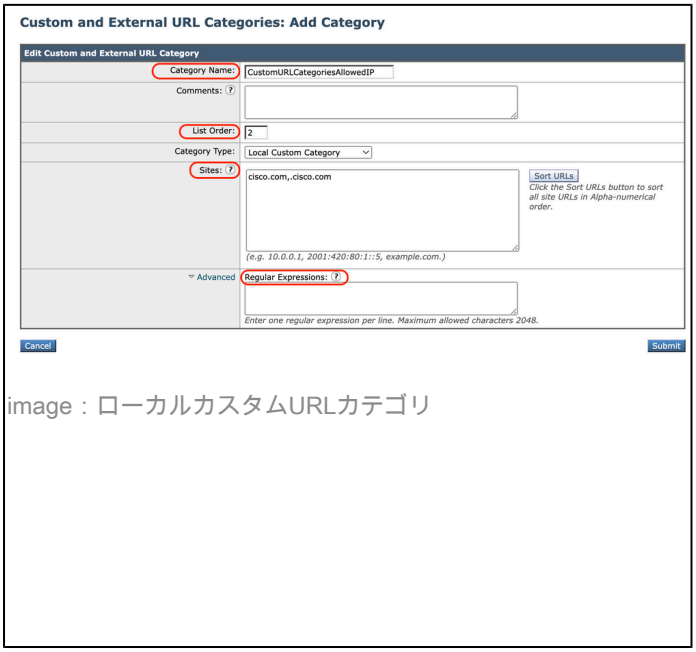
ステップ 1： Web Security Manager > Custom and External URL Categoriesの順に選択します。

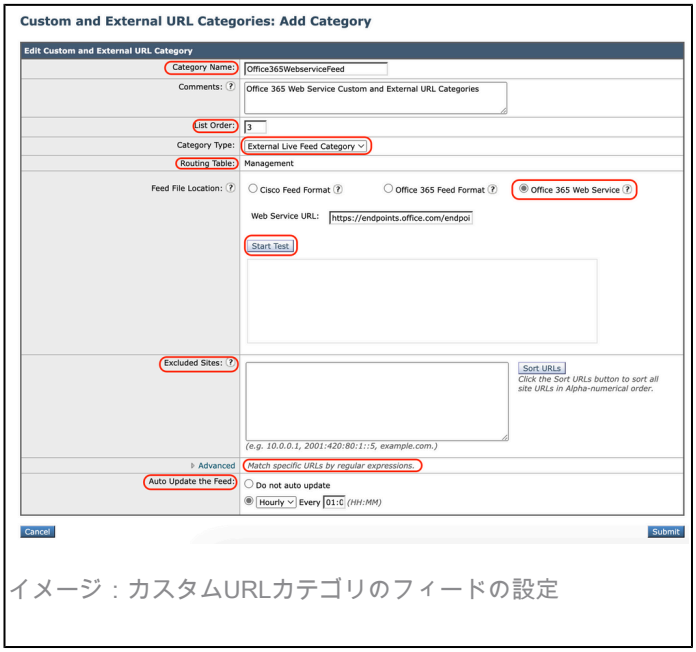

Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

URLフィルタエンジンは、指定された順序でカスタムURLカテゴリに対してクライアント要求を評価します。

注：URLフィルタエンジンは、URLカテゴリとクライアント要求のURLを照合する際、まず、ポリシーグループに含まれるカスタムURLカテゴリに対してURLを評価します。要求のURLが含まれているカスタムカテゴリと一致しない場合、URLフィルタエンジンは定義済みのURLカテゴリと比較します。URLが、含まれているカスタムまたは定義済みのURLカテゴリと一致しない場合、要求はカテゴリ化されません。

- カテゴリタイプ： ローカルカスタムカテゴリまたは外部ライブフィードカテゴリを選択します。
- ルーティングテーブル：管理またはデータを選択します。この選択は、「スプリットルーティング」が有効な場合にのみ使用できます。つまり、ローカルカスタムカテゴリでは使用できません。

<table>
<tr>
<td> 

image：ローカルカスタムURLカテゴリ</td>
<td> 

イメージ：カスタムURLカテゴリのフィードの設定</td>
</tr>
<tr>
<td>ローカルカスタムカテゴリ</td>
<td>外部ライブフィードカテゴリ</td>
</tr>
</table>

正規表現の使用の定義

セキュアWebアプライアンスでは、他のVelocityパターンマッチングエンジンの実装で使用される正規表現の構文とは少し異なる正規表現の構文が使用されます。

さらに、アプライアンスは、スラッシュをエスケープするためのバックスラッシュをサポートしていません。正規表現でスラッシュを使用する必要がある場合は、バックスラッシュを付けずにスラッシュを入力します。

注：技術的には、AsyncOS for WebはFlex正規表現アナライザを使用します

正規表現をテストするには、次のリンクを使用できます。[flex lint - Regex Tester/Debugger]

⚠ 注意:63文字を超える値を返す正規表現は失敗し、invalid-entryエラーが発生します。63文字を超える文字を返す可能性のない正規表現を作成してください

⚠ 注意：広範な文字の照合を実行する正規表現は、リソースを消費し、システムのパフォーマンスに影響を与える可能性があります。このため、正規表現は慎重に適用できます。

正規表現は、次の場所で使用できます。
・ アクセスポリシーのカスタムURLカテゴリ。アクセスポリシーグループで使用するカスタムURLカテゴリを作成する場合は、正規表現を使用して、入力したパターンに一致する複数のWebサーバを指定できます。
・ ブロックするカスタムユーザエージェント。アクセスポリシーグループに対してブロックするアプリケーションを編集する場合、正規表現を使用して、ブロックする特定のユーザエージェントを入力できます。

🔎 ヒント：正規表現にWebプロキシバイパスを設定することはできません。

flex正規表現の文字クラスのリストを次に示します

文字クラス	
.	改行以外の任意の文字
\w \d \s	単語、数字、空白
\W \D \S	単語、数字、空白文字ではない
[abc]	a、b、またはcのいずれか
[^abc]	a、b、またはc以外
【a-g】	aとgの間の文字
アンカー	
^abc$	文字列の先頭/末尾
\b	単語境界
エスケープ文字	
\.* \\	エスケープされた特殊文字
\t \n \r	タブ，改行，復帰
\u00A9	Unicodeエスケープ©
グループとルックアラウンド	
(abc)	キャプチャグループ
\1	グループ#1への逆参照
(?:abc)	非キャプチャグループ
(?=abc)	前向きな将来の展望
(?!abc)	否定的なルックアヘッド

数量詞と変換	
a* a+ a?	0以上、1以上、0又は1
a{5} a{2,}	正確に5つ、2つ以上
a{1,3}	1 ~ 3の間
a+? a{2,}?	できるだけ少ない数に一致させる
ab|cd	abまたはcdに一致

⚠ 注意：長いパターンのエスケープされていないドット、特に長いパターンの途中にあるドットには注意してください。また、このメタ文字（アスタリスク* ）には、特にドット文字と一緒に注意してください。どのパターンにも、ドットが無効になった後に63文字を超える文字を返す、エスケープされていないドットが含まれています。
*(star)および。*や\などの\（バックスラッシュ）を伴う（ドット）。
正規表現で.cisco.localを使用する場合、ドメインXcisco.localも一致します。
エスケープされていない文字はパフォーマンスに影響を与え、Webブラウジング中に速度が低下します。これは、パターンマッチングエンジンは、正しいエントリに一致するエントリを見つけるまで、数千または数百万の可能性を通過する必要があるためです。また、許可されるポリシーの同様のURLに関するセキュリティ上の問題が発生する可能性もあります

コマンドラインインターフェイス(CLI)のadvancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regexオプションを使用すると、大文字と小文字を区別しない一致のためにデフォルトの正規表現変換を小文字に変換するかどうかを指定できます。大文字と小文字の区別に問題がある場合に使用します。

制限および設計上の問題

- これらのURLカテゴリ定義で使用できる外部ライブフィードファイルは30個までで、各ファイルのエントリ数は5000個以下でなければなりません。
- 外部フィードエントリの数が増加すると、パフォーマンスが低下します。
- 複数のカスタムURLカテゴリで同じアドレスを使用することは可能ですが、カテゴリがリストされる順序が関係します。

これらのカテゴリを同じポリシーに含め、それぞれに異なるアクションを定義すると、カスタムURLカテゴリテーブルの最上位にリストされているカテゴリに定義されているアクションが適用されます。

- ネイティブのFile Transfer Protocol（FTP；ファイル転送プロトコル）要求がFTPプロキシに透過的にリダイレクトされる場合、FTPサーバのホスト名情報は含まれず、IPアドレスだけが含まれます。

このため、事前に定義されたURLカテゴリと、ホスト名情報のみを持つWebレピュテーションフィルタの中には、要求の宛先がそれらのサーバであっても、ネイティブFTP要求に一致しないものがあります。

これらのサイトへのアクセスをブロックする場合は、IPアドレスを使用するカスタムURLカテゴリを作成する必要があります。

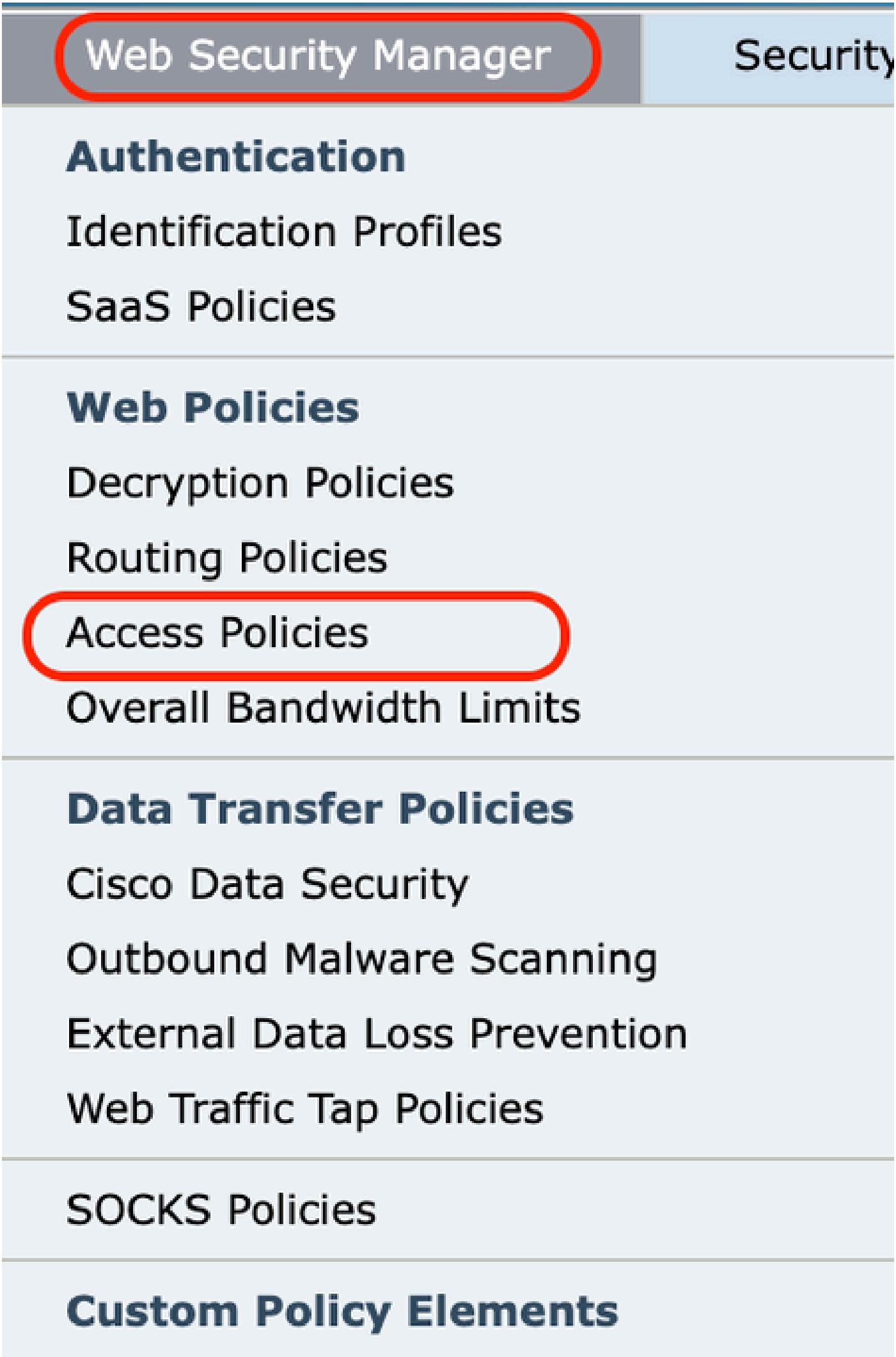
- カテゴリ化されていないURLは、定義済みのURLカテゴリまたは含まれているカスタムURLカテゴリのいずれとも一致しないURLです

ポリシーでカスタムURLカテゴリを使用する

URLフィルタエンジンを使用すると、アクセスポリシー、復号ポリシー、およびデータセキュリティポリシーでトランザクションをフィルタリングできます。ポリシーグループのURLカテゴリを設定する場合、カスタムURLカテゴリ（定義されている場合）および定義済みURLカテゴリのアクションを設定できます。

アクセスポリシーのURLフィルタを設定する手順

ステップ 1： Web Security Manager > Access Policiesの順に選択します。

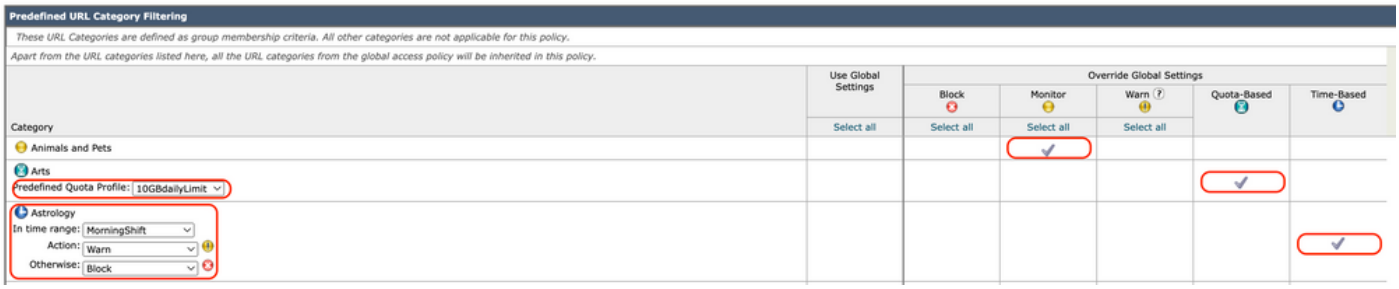

Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements

アクション	説明
Block	Webプロキシは、この設定に一致するトランザクションを拒否します。
リダイレクト（Redirect）	このカテゴリのURL宛てのトラフィックを、指定した場所にリダイレクトします。このアクションを選択すると、「リダイレクト」フィールドが表示されます。すべてのトラフィックのリダイレクト先となるURLを入力します。
プライベート ネットワーク間で	このカテゴリのWebサイトのクライアント要求を常に許可します。 許可された要求は、それ以降のすべてのフィルタとマルウェアスキャンをバイパスします。 この設定は、信頼済みWebサイトにのみ使用します。この設定は内部サイトに使用できます。
モニタ	Webプロキシは要求を許可もブロックもしません。その代わり、Webレピュテーションフィルタなどの他のポリシーグループコントロール設定に対するクライアント要求の評価を続けます。
警告	Webプロキシは最初に要求をブロックし、警告ページを表示しますが、ユーザは警告ページのハイパーテキストリンクをクリックすることで続行できます。
クォータベース	指定したボリュームまたは時間クォータに個々のユーザーが近づくと、警告が表示されます。クォータに達すると、ブロックページが表示されます。
タイムベース	Webプロキシは、指定した時間範囲内で要求をブロックまたは監視します。

ステップ5: [定義済みのURLカテゴリフィルタ]セクションで、各カテゴリに対して次のいずれかのアクションを選択します。

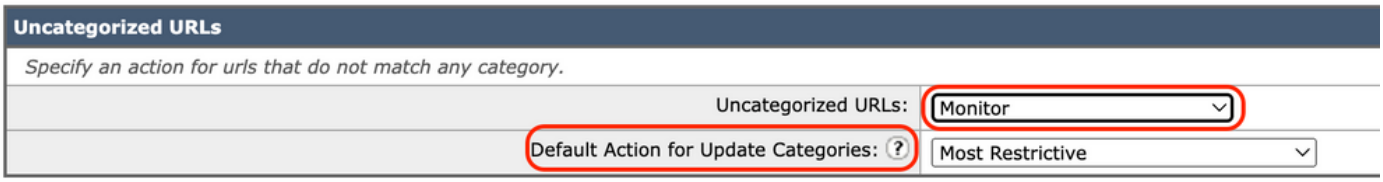
- グローバル設定を使用
- モニタ
- 警告
- Block

- タイムベース
- クォータベース



イメージ – 定義済みカテゴリのアクションの選択

ステップ 6： [未分類のURL]セクションで、定義済みまたはカスタムのURLカテゴリに分類されないWebサイトに対するクライアント要求に対して実行するアクションを選択します。この設定は、URLカテゴリセットの更新から新しいカテゴリの結果とマージされたカテゴリの結果に対する既定のアクションも決定します。

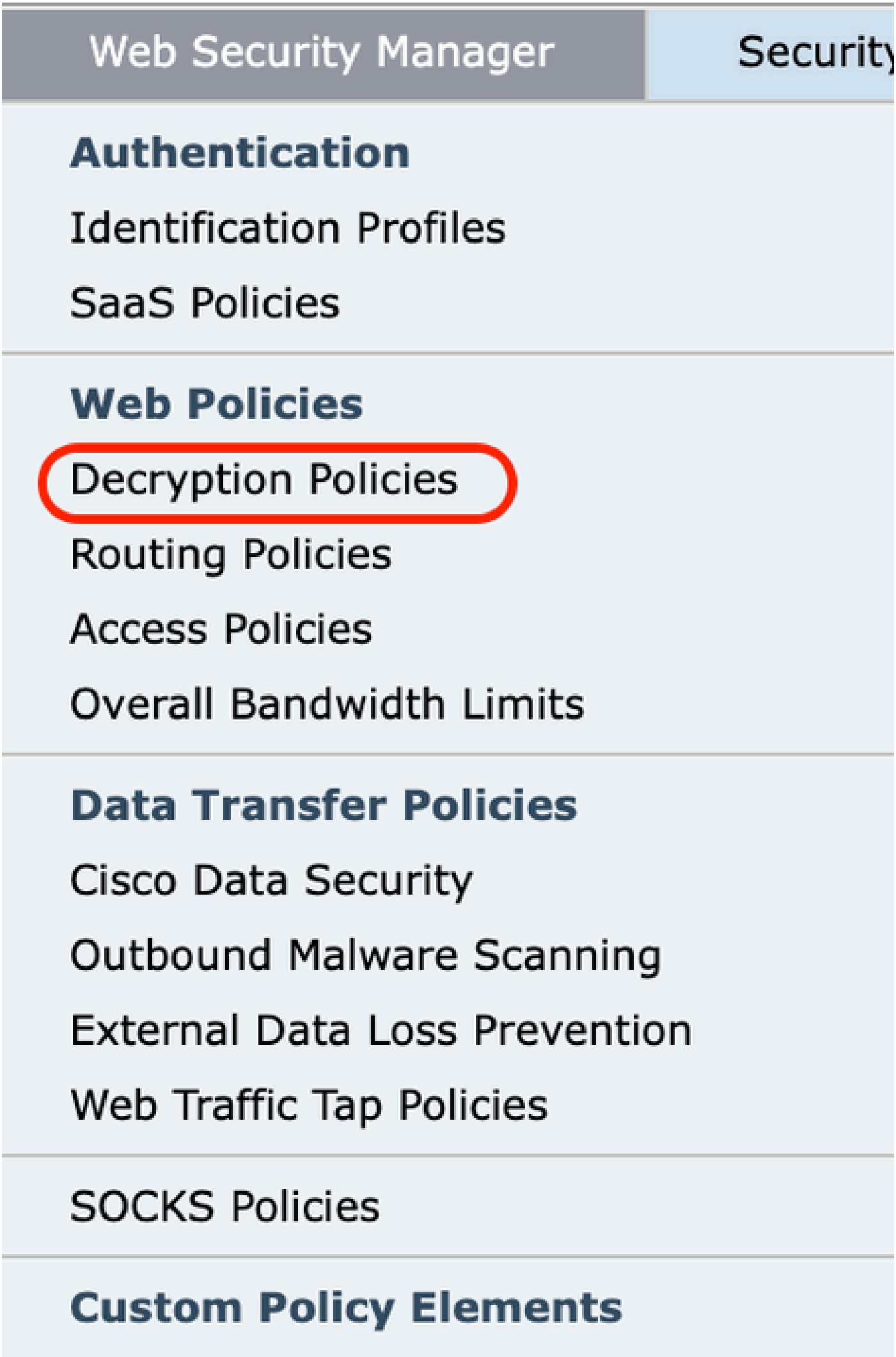


イメージ – 分類されていないURLのアクションを選択

ステップ 7： 送信し、変更を確定します。

復号化ポリシーのURLフィルタを設定する手順

ステップ 1： Web Security Manager > Decryption Policiesの順に選択します。


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements

アクション	説明
パススルー	トラフィックの内容を検査せずに、クライアントとサーバの間の接続を通過します。
モニタ	Webプロキシは要求を許可もブロックもしません。その代わり、Webレピュテーションフィルタなどの他のポリシーグループコントロール設定に対するクライアント要求の評価を続けます。
復号化	接続を許可しますが、トラフィックの内容を検査します。アプライアンスはトラフィックを復号化し、平文のハイパーテキスト転送プロトコル(HTTP)接続であるかのように、復号化されたトラフィックにアクセスポリシーを適用します。接続が復号化され、アクセスポリシーが適用されると、トラフィックをスキャンしてマルウェアを検出できます。
[Drop]	接続をドロップし、接続要求をサーバーに渡しません。アプライアンスは、接続をドロップしたことをユーザに通知しません。

ステップ 5： [未分類のURL]セクションで、定義済みまたはカスタムのURLカテゴリに分類されないWebサイトに対するクライアント要求に対して実行するアクションを選択します。

この設定は、URLカテゴリセットの更新から新しいカテゴリの結果とマージされたカテゴリの結果に対する既定のアクションも決定します。

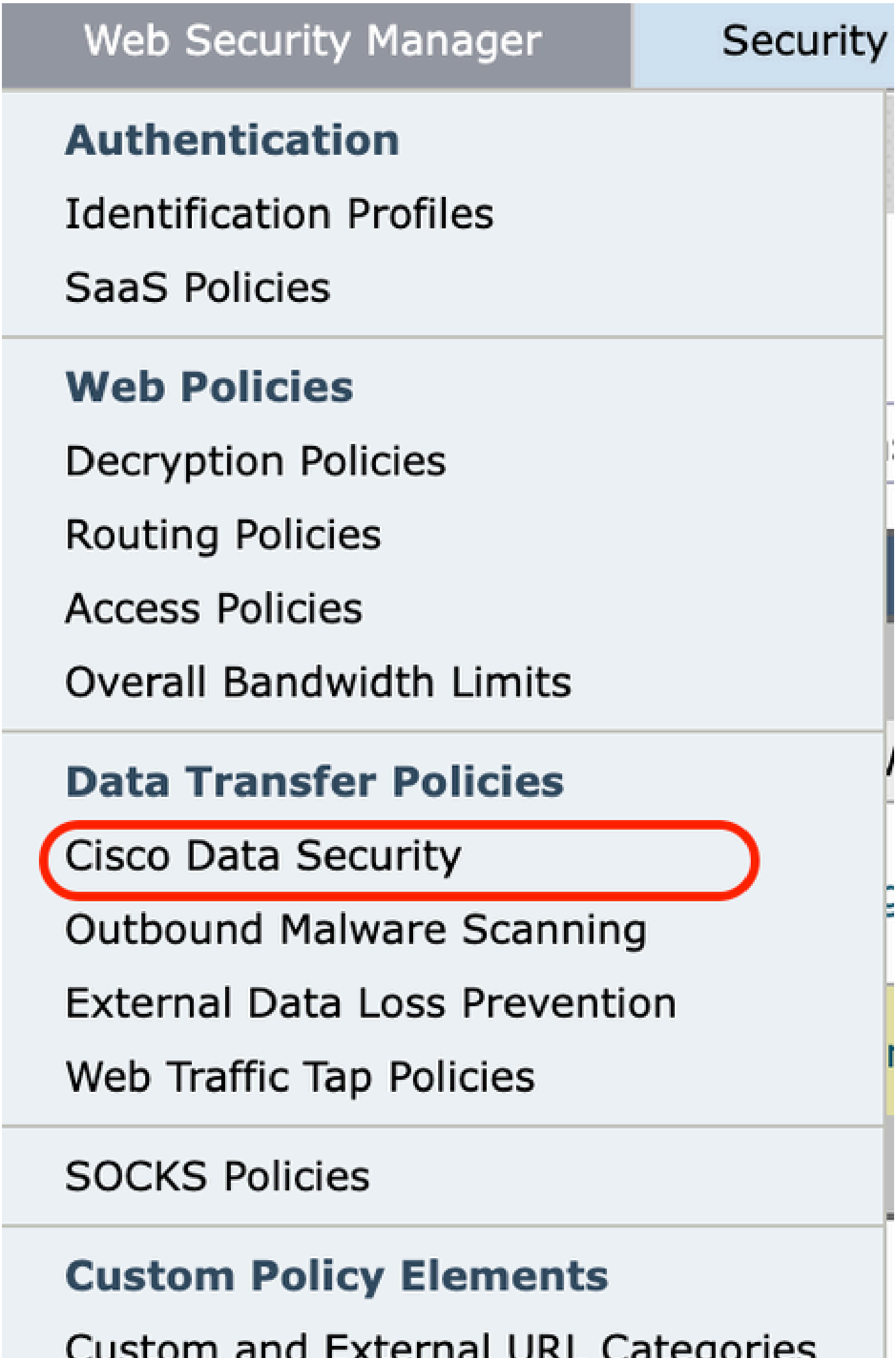
イメージ – 未分類の復号化ポリシー

ステップ 6： 送信し、変更を確定します。

⚠ 注意: Hypertext Transfer Protocol Secure(HTTPS)要求のために特定のURLカテゴリをブロックする場合は、Decryption Policyグループでそのカテゴリの暗号化を解除することを選択してから、Access Policyグループで同じURLカテゴリの暗号化をブロックすることを選択してください。

データセキュリティポリシーグループのURLフィルタを設定する手順

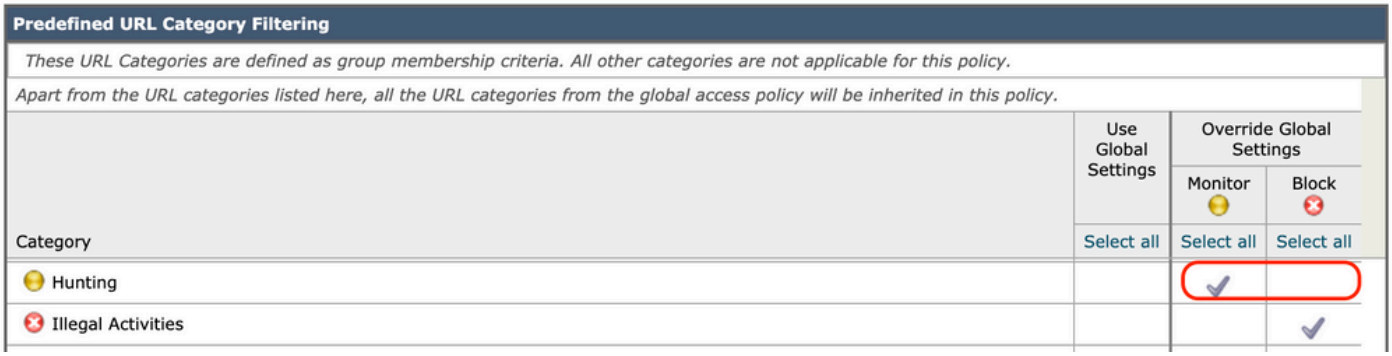
ステップ 1： Web Security Manager > Cisco Data Securityの順に選択します。


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

アクション	説明
プライベート ネットワーク間で	このカテゴリのWebサイトのアップロード要求を常に許可します。カスタムURLカテゴリにのみ適用されます。 許可された要求は、それ以降のデータセキュリティスキャンをすべてバイパスし、アクセスポリシーに対して評価されます。 この設定は、信頼済みWebサイトにのみ使用します。この設定は内部サイトに使用できます。
モニタ	Webプロキシは要求を許可もブロックもしません。その代わり、Webレピュテーションフィルタなどの他のポリシーグループコントロール設定に対するアップロード要求の評価が続行されます。
Block	Webプロキシは、この設定に一致するトランザクションを拒否します。

ステップ5: [定義済みのURLカテゴリフィルタリング]セクションで、各カテゴリに対して次のいずれかのアクションを選択します。

- グローバル設定を使用
- モニタ
- Block



イメージ：データセキュリティの事前定義されたURLアクションの選択

ステップ 6： [未分類のURL]セクションで、定義済みまたはカスタムのURLカテゴリに分類されないWebサイトへのアップロード要求に対して実行するアクションを選択します。

この設定は、URLカテゴリセットの更新から新しいカテゴリの結果とマージされたカテゴリの結果に対する既定のアクションも決定します。

画像 – データセキュリティ未分類

手順 7： 送信し、変更を確定します。

⚠ 注意：最大ファイルサイズ制限を無効にしない場合は、URLフィルタリングで許可オプションまたはモニタオプションが選択されていると、Webセキュリティアプライアンスにより最大ファイルサイズの検証が続行されます。

カスタムURLカテゴリを使用したアップロード要求の制御を設定する手順

各アップロード要求は「アウトバウンドマルウェアスキャン」ポリシーグループに割り当てられ、そのポリシーグループの制御設定を継承します。

Webプロキシがアップロード要求ヘッダーを受信した後、要求本文をスキャンする必要があるかどうかを判断するために必要な情報を取得します。

DVSエンジンは要求をスキャンし、Webプロキシに判定を返します。該当する場合、ブロックページがエンドユーザに表示されます。

<table>
<tr><td>ステップ1</td><td>Web Security Manager > Outbound Malware Scanningの順に選択します。</td></tr>
<tr><td>ステップ2</td><td>Destinations列で、設定するポリシーグループのリンクをクリックします。</td></tr>
<tr><td>ステップ3</td><td>Edit Destination Settingsセクションで、ドロップダウンメニューからDefine Destinations Scanning Custom Settingsを選択します。</td></tr>
<tr><td>ステップ4</td><td>Destinations to Scanセクションで、次のいずれかを選択します。
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>アップロードをスキャンしない</td><td>DVSエンジンはアップロード要求をスキャンしません。すべてのアップロード要求は、アクセスポリシーに照らして評価されます</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>すべてのアップロードをスキャン</td><td>DVSエンジンはすべてのアップロード要求をスキャンします。アップロード要求がブロックされるか、アクセスポリシーに照らして評価されるかは、DVSエンジンスキャンの判定によって決まります</td></tr>
<tr><td>指定したカスタムURLカテゴリへのアップロードをスキャンします</td><td>DVSエンジンは、特定のカスタムURLカテゴリに属するアップロード要求をスキャンします。アップロード要求は、DVSエンジンスキャンの判定に応じて、アクセスポリシーに対してブロックまたは評価されます。

Edit custom categories listをクリックして、スキャンするURLカテゴリを選択します</td></tr>
</table>
</td></tr>
<tr><td>ステップ5</td><td>変更を送信します。</td></tr>
<tr><td>ステップ6</td><td>Anti-Malware Filtering列で、ポリシーグループのリンクをクリックします。</td></tr>
<tr><td>ステップ7</td><td>Anti-Malware Settingsセクションで、Define Anti-Malware Custom Settingsを選択します。</td></tr>
<tr><td>ステップ8：</td><td>Cisco DVSアンチマルウェア設定セクションで、このポリシーグループに対して有効にするアンチマルウェアスキャンエンジンを選択します。</td></tr>
<tr><td>ステップ9：</td><td>Malware Categoriesセクションで、さまざまなマルウェアカテゴリをモニタするかブロックするかを選択します。

このセクションに表示されるカテゴリは、有効にするスキャンエンジンによって異なります。</td></tr>
<tr><td>ステップ10：</td><td>送信し、変更を確定します。</td></tr>
</table>

外部DLPポリシーで制御アップロード要求を設定する手順

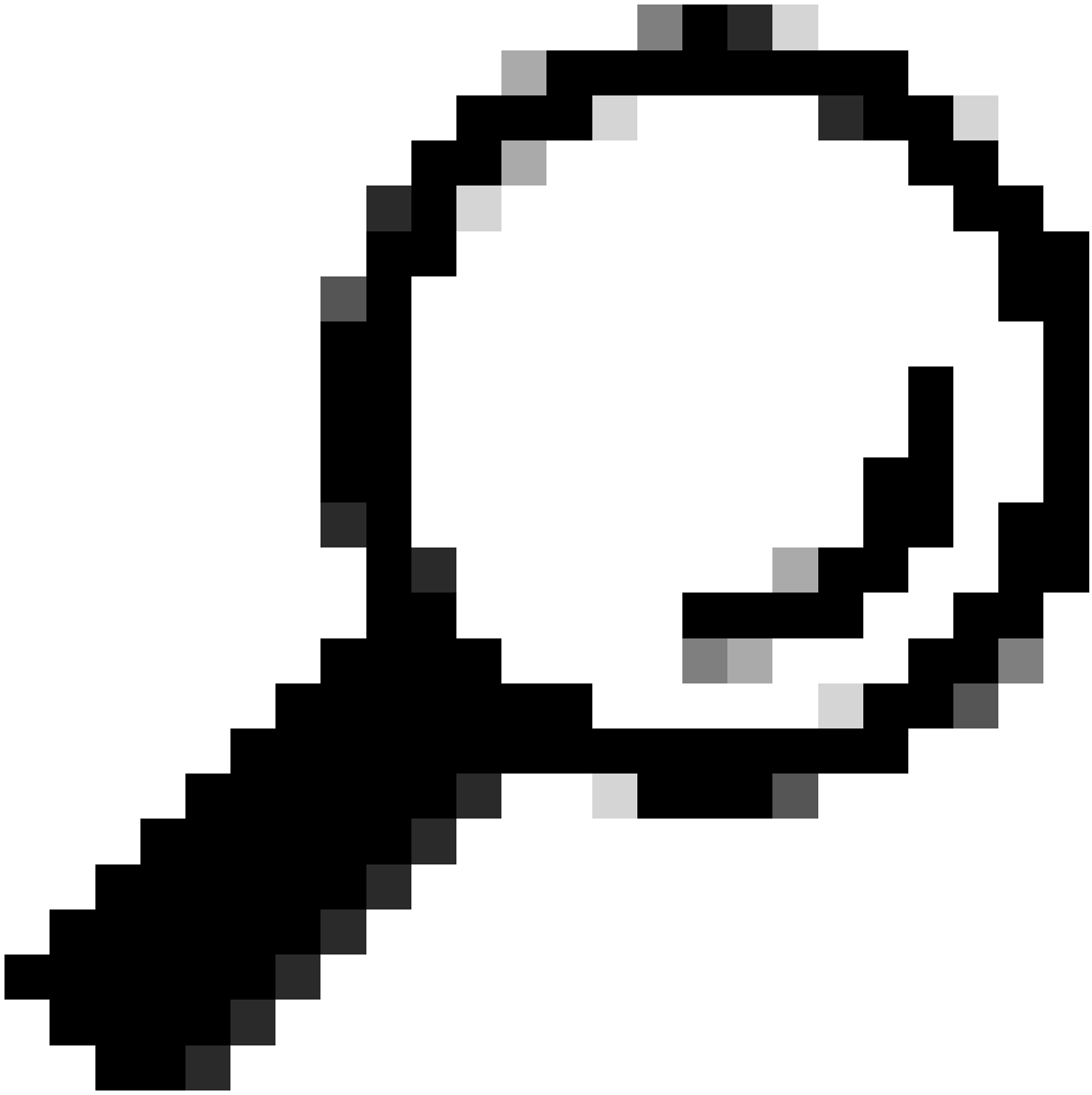
Webプロキシがアップロード要求ヘッダーを受信すると、要求がスキャンのために外部DLPシステムに送信できるかどうかを判断するために必要な情報が得られます。

DLPシステムは要求をスキャンし、ブロックまたはモニタ（アクセスポリシーに対して要求を評価）のいずれかの判定をWebプロキシに返します。

ステップ1	Web Security Manager > External Data Loss Preventionの順に選択します。
ステップ2	設定するポリシーグループのDestinations列の下にあるリンクをクリックします。
ステップ3	Edit Destination Settingsセクションで、Define Destinations Scanning Custom Settingsを選択します。
ステップ4	Destination to scanセクションで、次のいずれかのオプションを選択します。 • アップロードをスキャンしないでください。アップロード要求は、スキャン用に設定されたデータ損失防止(DLP)システムに送信されません。すべてのアップロード要求は、アクセスポリシーに照らして評価されます。 • すべてのアップロードをスキャンします。すべてのアップロード要求は、スキャンのために設定されたDLPシステムに送信されます。アップロード要求がブロックされるか、アクセスポリシーに対して評価されるかは、DLPシステムスキャンの判定によって決まります。 • 指定したカスタムおよび外部URLカテゴリ以外のアップロードをスキャンします。特定のカスタムURLカテゴリに該当するアップロード要求は、DLPスキャンポリシーから除外されます。Edit custom categories listをクリックして、スキャンするURLカテゴリを選択します。
ステップ5	送信し、変更を確定します。

バイパスおよびパススルーURL

トランスペアレントプロキシ実装でセキュアWebアプライアンスを設定して、特定のクライアントからのHTTPまたはHTTPS要求をバイパスしたり、特定の宛先にバイパスしたりできます。



ヒント：パススルーは、トラフィックのパススルーが必要なアプリケーションに使用できます。宛先サーバの修正や証明書チェックは必要ありません

⚠ 注意：ドメインマップ機能は、HTTPSトランスペアレントモードで動作します。 この機能は、ExplicitモードやHTTPトラフィックでは動作しません。

- ローカルカスタムカテゴリは、トラフィックがこの機能を使用できるように設定する必要があります。
- この機能を有効にすると、Server Name Indication(SNI)情報が使用可能な場合でも、ドメインマップで設定されたサーバ名に従ってサーバ名が変更または割り当てられます。
- この機能は、トラフィックがドメインマップに一致し、カスタムカテゴリ、復号化ポリシー、およびパススルーアクションが設定されている場合は、ドメイン名に基づくトラフィック

をブロックしません。

- このパススルー機能では、認証は機能しません。認証には復号化が必要ですが、この場合はトラフィックは復号化されません。
- トラフィックはモニタされません。UDPトラフィックがWebセキュリティアプライアンス(WSA)に到達しないように設定し、代わりにWhatsAppやTelegramなどのアプリケーションのためにファイアウォールからインターネットに直接到達するようにする必要があります。
- WhatsApp、Telegram、およびSkypeはトランスペアレントモードで動作します。ただし、WhatsAppなどの一部のアプリは、アプリの制限のために明示的モードで動作しません。

特定のサーバへのパススルートラフィックを必要とするデバイスに対してIDポリシーが定義されていることを確認します。具体的には、次のことを行う必要があります。

- Exempt from authentication/identificationを選択します。
- このIDプロファイルを適用する必要があるアドレスを指定します。IPアドレス、クラスレスドメイン間ルーティング(CIDR)ブロック、およびサブネットを使用できます。

<table>
<tr><td>ステップ1</td><td>HTTPSプロキシを有効にします。</td></tr>
<tr><td>ステップ2</td><td>Web Security Manager > Domain Mapの順に選択します。
a. Add Domainを選択します。
b. ドメイン名または宛先サーバを入力します。
c. 指定したドメインがある場合は、優先順位を選択します。
d. IPアドレスを入力します。
e. [Submit] をクリックします。</td></tr>
<tr><td>ステップ3</td><td>Web Security Manager > Custom and External URL Categoriesの順に選択します。
a. Add Categoryを選択します。
b. 次の情報を入力します。<table><tr><th>Settings</th><th>説明</th></tr><tr><td>カテゴリ名</td><td>このURLカテゴリの識別子を入力します。この名前は、ポリシー</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th>Settings</th><th>説明</th></tr>
<tr><td></td><td>グループのURLフィルタを設定するときに表示されます。</td></tr>
<tr><td>リストの順序</td><td>カスタムURLカテゴリのリストで、このカテゴリの順序を指定します。リストの最初のURLカテゴリに「1」を入力します。

URLフィルタエンジンは、指定された順序でカスタムURLカテゴリに対してクライアント要求を評価します。</td></tr>
<tr><td>カテゴリタイプ</td><td>Local Custom Categoryを選択します。</td></tr>
<tr><td>詳細</td><td>このセクションに正規表現を入力すると、追加のアドレスセットを指定できます。

正規表現を使用すると、入力したパターンに一致する複数のアドレスを指定できます。</td></tr>
</table>
c. 変更を送信し、保存します。
</td></tr>
<tr><td>ステップ4</td><td>Web Security Manager > Decryption Policiesの順に選択します。
a. 新しい復号化ポリシーを作成します。
b. 特定のアプリケーションのバイパスHTTPSトラフィック用に作成したIDプロファイルを選択します。
c. Advancedパネルで、URL Categoriesへのリンクをクリックします。
d. Add列で、ステップ3で作成したカスタムURLカテゴリをクリックして追加します。
e. Doneを選択します。
f. Decryption Policiesページで、URL Filteringのリンクをクリックします。
g. Pass Throughを選択します。
h. 変更を送信し、保存します。
（オプション）アクセスログ情報を表示するには、%(形式指定子を使用できます。</td></tr>
</table>

Web要求に対するWebプロキシバイパスの設定

カスタムURLカテゴリをプロキシバイパスリストに追加すると、カスタムURLカテゴリのすべてのIPアドレスとドメイン名が、送信元と宛先の両方でバイパスされます。

ステップ1	Web Security Manager > Bypass Settingsの順に選択します。
ステップ2	Edit Bypass Settingsをクリックします。
ステップ3	Webプロキシをバイパスするアドレスを入力します。 注：バイパスリストのいずれかのIPのサブネットマスクとして/0を設定すると、アプライアンスがすべてのWebトラフィックをバイパスします。この場合、アプライアンスは設定を0.0.0.0/0と解釈します。
ステップ4	プロキシバイパスリストに追加するカスタムURLカテゴリを選択します。
ステップ5	変更を送信し、確定します。

⚠ 注意：正規表現にWebプロキシバイパスを設定することはできません。

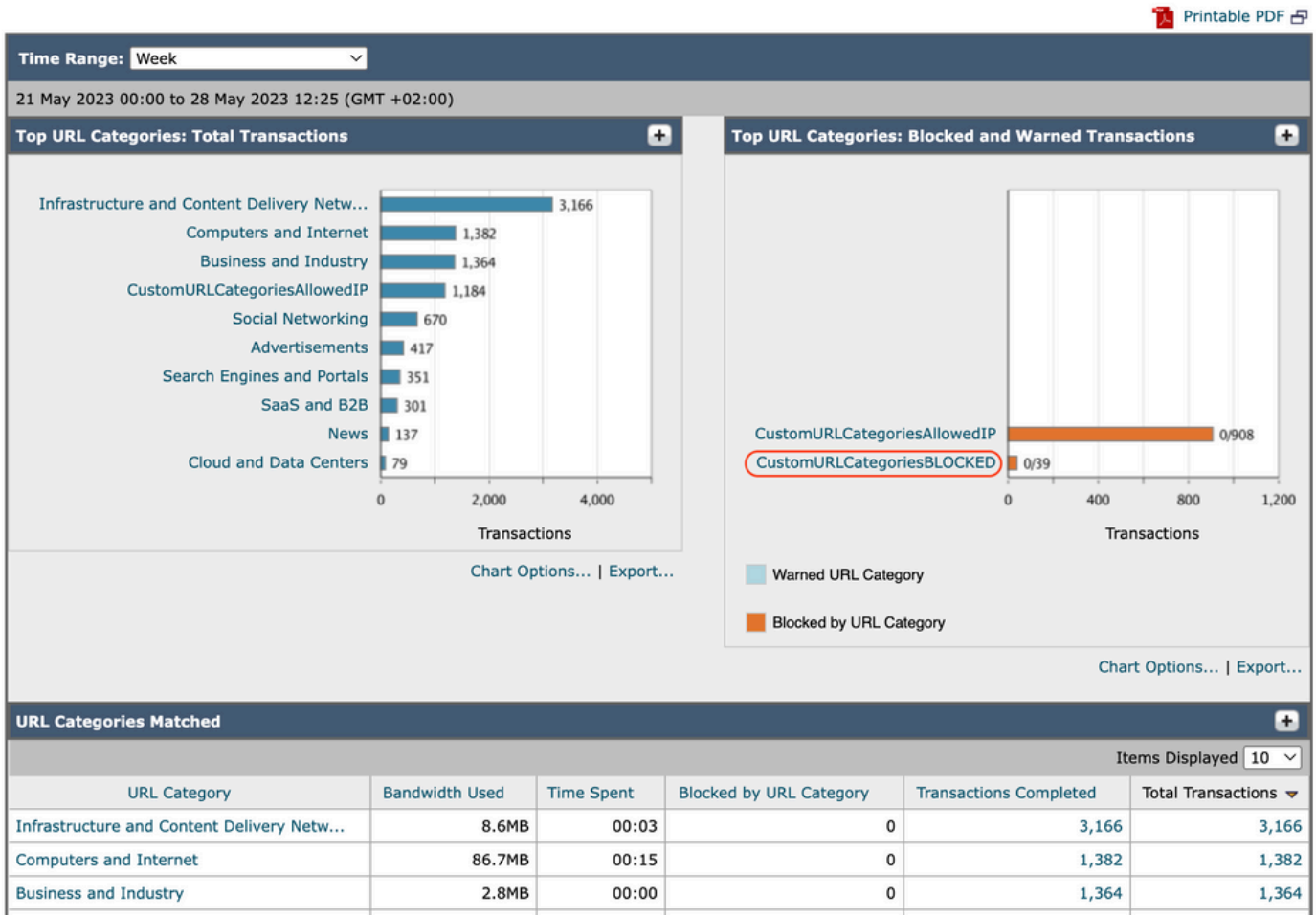
レポート

「Reporting" >> URL Categories'」ページには、一致した上位URLカテゴリとブロックされた上位URLカテゴリに関する情報を含むURL統計情報の集合的な表示が表示されます。

このページには、帯域幅の節約とWebトランザクションに関するカテゴリ固有のデータが表示されます。

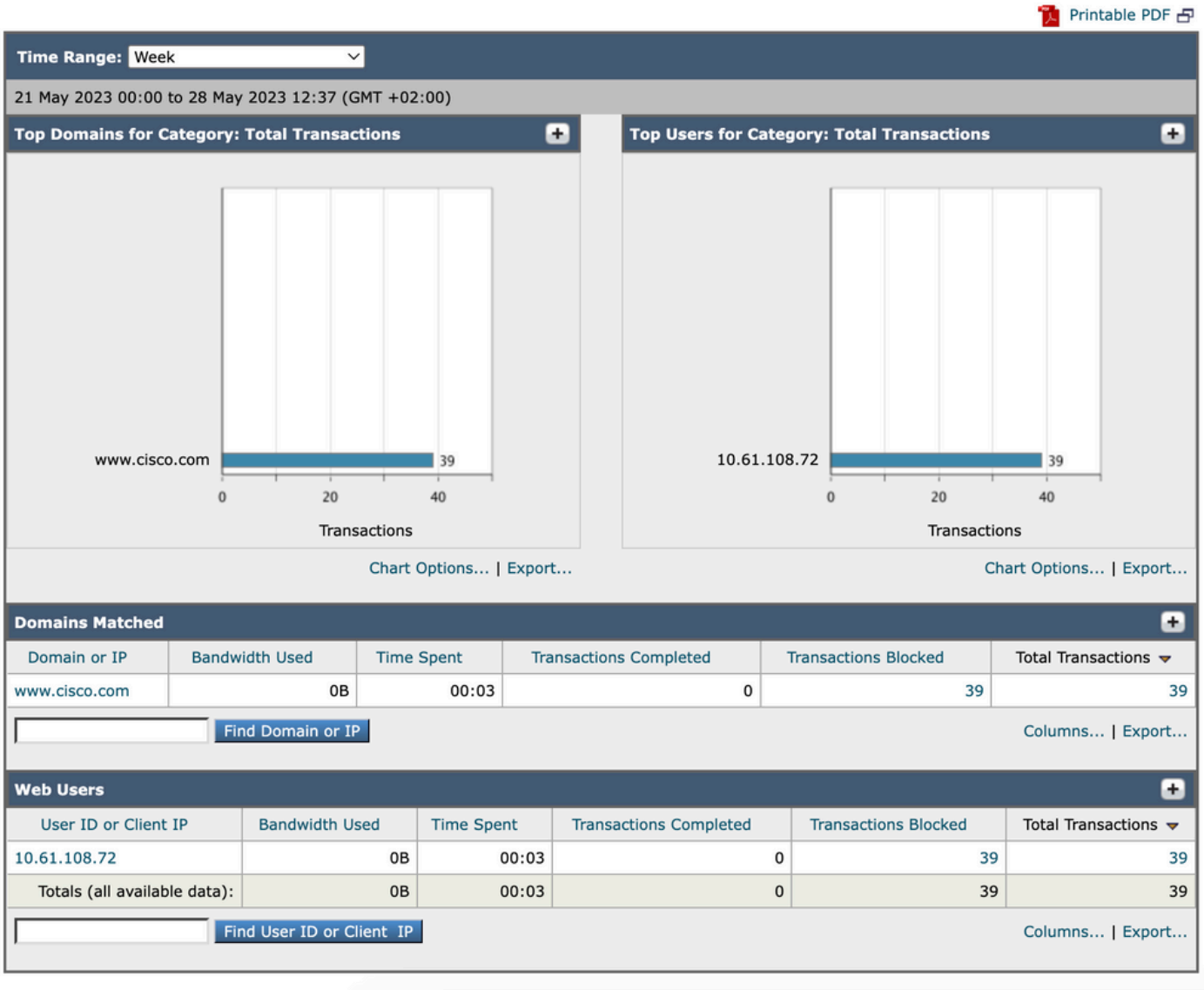
セクション	説明
時間範囲（ドロップダウンリスト）	レポートの時間範囲を選択します。

セクション	説明
総トランザクション別の上位URLカテゴリ	このセクションには、サイトでアクセスされる上位のURLカテゴリがグラフ形式で表示されます。
ブロックおよび警告トランザクション別の上位URLカテゴリ	ブロックまたは警告アクションをトリガーした最上位のURLが、トランザクションごとにグラフ形式で表示されます。
一致したURLカテゴリ	指定した時間範囲におけるURLカテゴリ別のトランザクションの処理に加えて、使用された帯域幅と各カテゴリで費やされた時間を表示します。 未分類のURLの割合が15 ~ 20 %を超える場合は、次のオプションを検討してください。 • 特定のローカライズされたURLについては、カスタムURLカテゴリを作成し、特定のユーザまたはグループポリシーに適用できます。 • 未分類のURLや誤って分類されたURLをシスコに報告し、評価やデータベースの更新を行うことができます。 • Webレピュテーションフィルタとマルウェア対策フィルタが有効になっていることを確認します。



イメージURLカテゴリレポート

カテゴリ名をクリックすると、一致したドメインやユーザリストなど、そのカテゴリに関連する詳細を表示できます。



イメージ – 詳細レポートページ

事前定義されたURLカテゴリのセットは、Webセキュリティアプライアンス(WSA)で定期的に自動的に更新できます。

これらの更新が行われると、古いカテゴリに関連付けられているデータが古すぎてレポートに含めなくなるまで、古いカテゴリ名がレポートに表示され続けます。

URLカテゴリセットの更新後に生成されるレポートデータでは、新しいカテゴリが使用されるため、古いカテゴリと新しいカテゴリの両方を同じレポートで確認できます。

レポートのURL Categoriesページの URL統計情報では、これらのデータの解釈方法を理解することが重要です。

データ型	説明
バイパスされたURLフィルタリング	URLフィルタリングの前に発生する、ブロックされたポリシー、ポート、および管理者ユーザエージェントを表します。

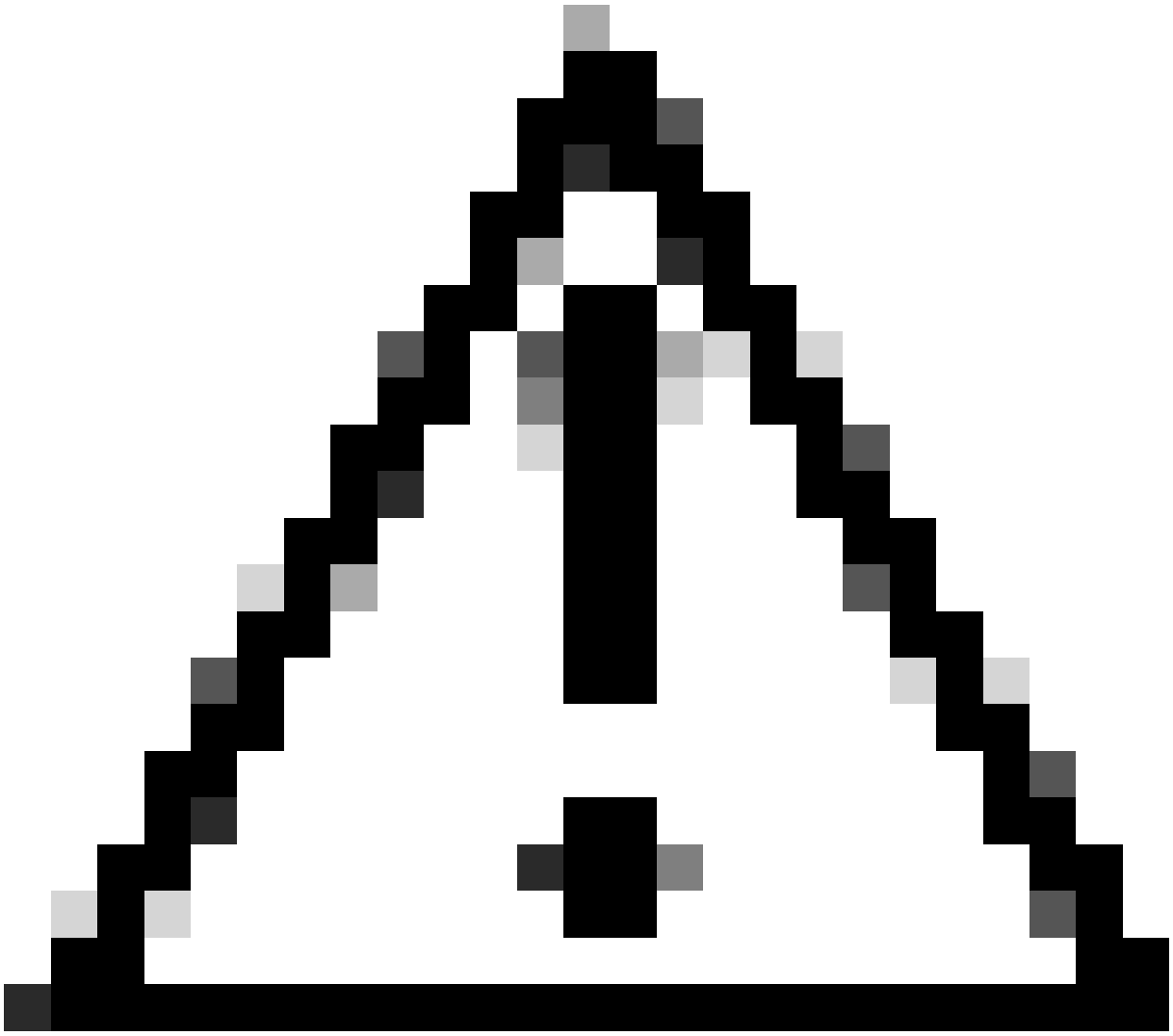
未分類のURL	URLフィルタリングエンジンが照会され、カテゴリが一致しないすべてのトランザクションを表します。

アクセスログのカスタムURLカテゴリの表示

Secure Web Applianceは、アクセスログで、カスタムURLカテゴリ名の最初の4文字にc_を付けて使用します。

この例ではカテゴリ名はCustomURLCategoriesBLOCKEDであり、アクセスログでC_Cust (隠しコマンド) を確認できます。

```
1685269516.853 86 10.61.108.72 TCP_DENIED_SSL/403 0 GET https://www.cisco.com:443/ - NONE/- - DROP_CUSTC
```



注意:Sawmillを使用してアクセスログを解析する場合は、カスタムURLカテゴリ名を検討

してください。カスタムURLカテゴリの最初の4文字にスペースが含まれている場合、Sawmillはアクセスログエントリを正しく解析できません。代わりに、サポートされている文字だけを最初の4文字で使用してください。

ヒント：アクセスログにカスタムURLカテゴリの完全な名前を含める場合は、%XF形式指定子をアクセスログに追加します。

Webアクセスポリシーグループのカスタムカテゴリが Monitor に設定されていて、他のコンポーネント(Web Reputation Filters(WBRF)やDifferent Verdicts Scanning(DVS)エンジンなど)がカスタムURLカテゴリのURLに対する要求を許可またはブロックする最終的な決定を下した場合、要求のアクセスログエントリには、カスタムURLカテゴリではなく、事前定義のURLカテゴリがが表示されます。

アクセスログのカスタムフィールドを設定する方法の詳細については、「アクセスログのパフォーマンスパラメータの設定 – シスコ

トラブルシュート

カテゴリの不一致

アクセスログから、選択が期待どおりではない場合、要求がどのカスタムURLカテゴリに属するかを確認できます。

– 要求が他のカスタムURLカテゴリにカテゴリ化されている場合は、他のカテゴリで重複するURLまたは一致する正規表現を確認するか、カスタムURLカテゴリを先頭に移動してもう一度テストしてください。一致するカスタムURLカテゴリを注意深く調べることをお勧めします。

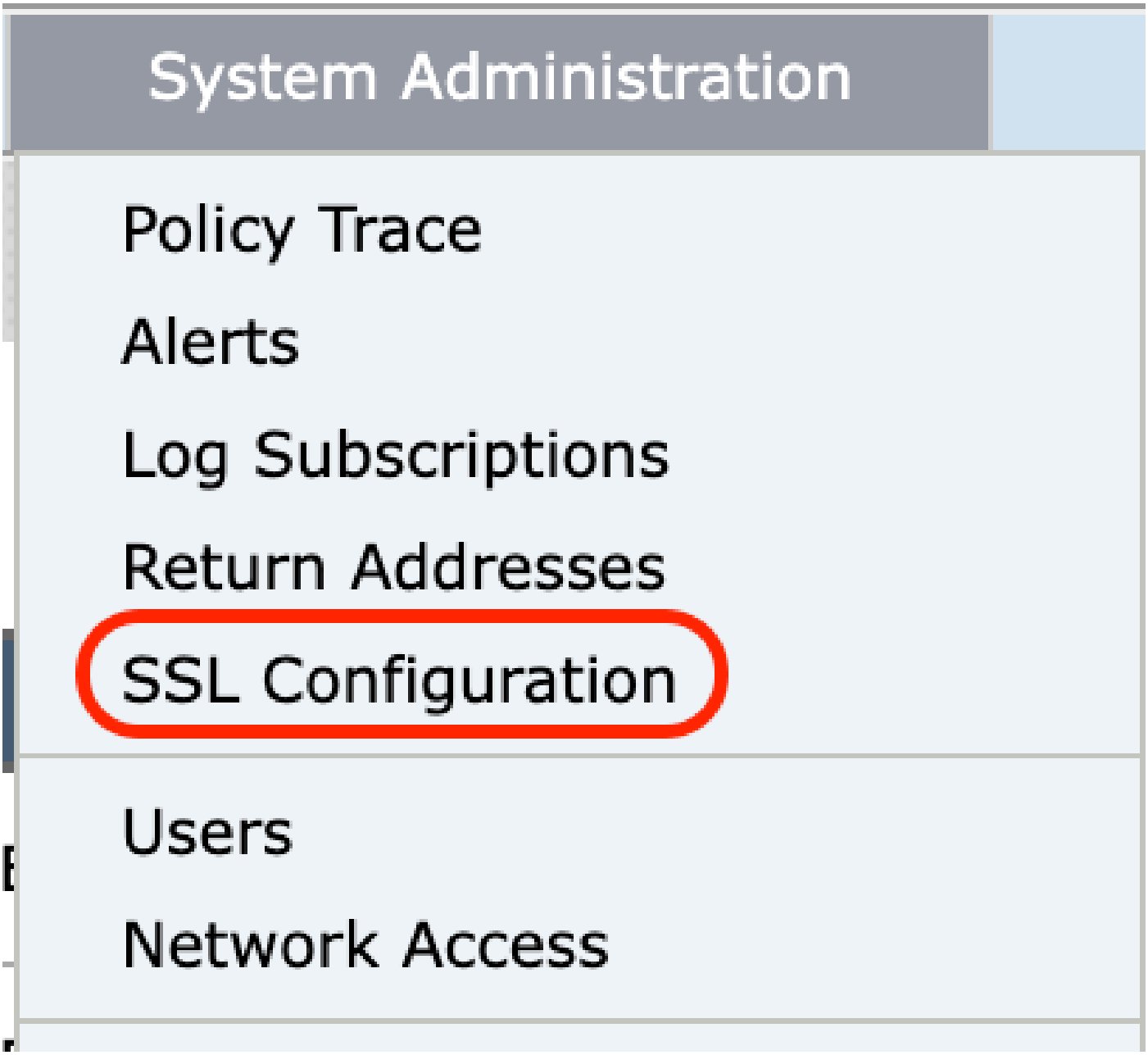
– 要求が定義済みカテゴリに分類されている場合は、既存のカスタムURLカテゴリの条件を確認します。すべての条件が一致する場合は、IPアドレスを追加してテストするか、入力ミスがあり正しい正規表現が使用されていることを確認します。

定義済みカテゴリが最新ではありません

事前定義済みカテゴリが最新でない場合、またはアクセスログのURLカテゴリセクションに「err」と表示される場合は、TLSv1.2がUpdaterに対して有効になっていることを確認します。

Updater SSLの設定を変更するには、GUIから次の手順を実行します。

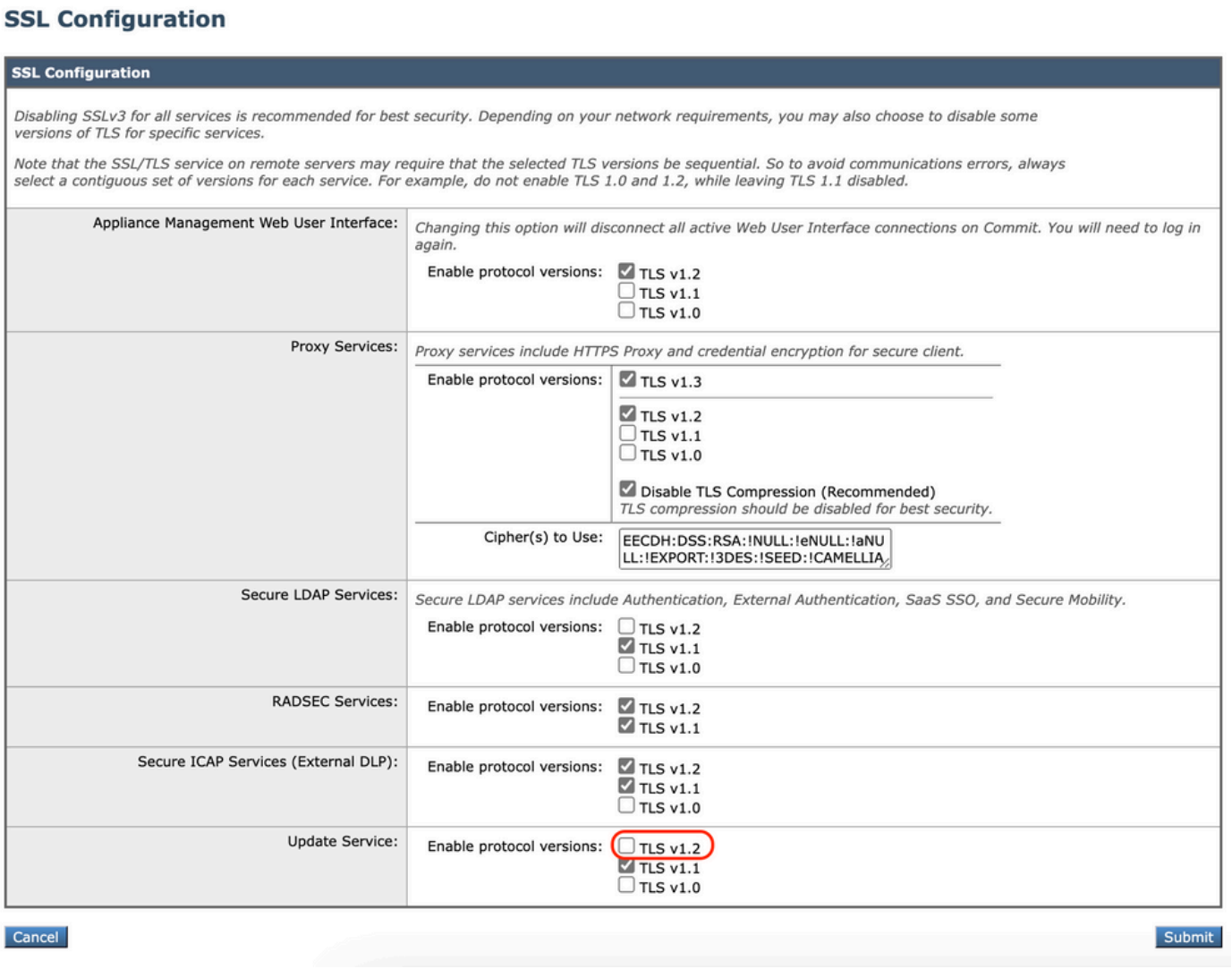
ステップ 1：System Administrationで、SSL Configurationを選択します



イメージ – ssl設定

ステップ 2：Edit Settingsを選択します。

ステップ 3：Update serviceセクションで、TLSv1.2を選択します



イメージ：サービスTLSv1.2の更新

ステップ 4：変更を送信して確定します。

Updater SSLの設定を変更するには、CLIから次の手順を実行します。

ステップ 1：CLIから、sslcofig

ステップ 2：versionと入力してEnterを押す。

ステップ 3：Updaterを選択します

ステップ 4：TLSv1.2を選択します。

ステップ 5：Enterを押してウィザードを終了します

ステップ6：変更を確定します。

```
SWA_CLI> sslconfig

Disabling SSLv3 is recommended for best security.
```

```
Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequentia
1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
- COMPRESS - Enable or disable TLS compression for Proxy Service
- CIPHERS - Set ciphers for services in Secure Web Appliance
- FALLBACK - Enable or disable SSL/TLS fallback option
- ECDHE - Enable or disable ECDHE Authentication.
[]> versions

SSL/TLS versions may be enabled or disabled for the following services:

        LDAPS - Secure LDAP Services (including Authentication, External Authentication, SaaS SSO, Secu
        Updater - Update Service
        WebUI - Appliance Management Web User Interface
        RADSEC - Secure RADSEC Services (including Authentication, External Authentication)
        SICAP - Secure ICAP Service
        Proxy - Proxy Services (including HTTPS Proxy, Credential Encryption for Secure Client)

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

         LDAPS  Updater  WebUI   RADSEC  SICAP   Proxy
TLSv1.0    N       N       N      N/A      N       N
TLSv1.1    Y       Y       N       Y       Y       N
TLSv1.2    N       N       Y       Y       Y       Y
TLSv1.3   N/A     N/A     N/A     N/A     N/A      Y

Select the service for which to enable/disable SSL/TLS versions:

1. LDAPS
2. Updater
3. Proxy
4. RADSEC
5. SICAP
6. WebUI
7. All Services
[]> 2


Currently enabled protocol(s) for Updater are TLSv1.1.


To change the setting for a specific protocol, select an option below:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2
[]> 3

TLSv1.2 support for Update Service is currently disabled. Do you want to enable it? [N]> Y


Currently enabled protocol(s) for Updater are TLSv1.1, TLSv1.2.
```

参考

Cisco Webセキュリティアプライアンスのベストプラクティスガイドライン – Cisco

BRKSEC-3303(ciscolive)

AsyncOS 14.5 for Cisco Secure Web Applianceユーザガイド – GD（一般導入）- [Cisco Secure Web Appliance]の接続、インストール、および設定 – シスコ

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。