

CSFのURLカテゴリのトラブルシューティングと確認

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[背景説明](#)

[アーキテクチャ](#)

[ステップ1:FMCでURLカテゴリを検索する](#)

[ステップ2:URLフィルタリング統合設定の確認](#)

[ステップ3：システムサポートトレースを使用して、デバイスのURLカテゴリを確認します。](#)

[ステップ4：カテゴリ番号をカテゴリ名に解決する](#)

[確認](#)

[争議ボタン](#)

[トラブルシューティング](#)

概要

このドキュメントでは、デバイスが同じURL分類を使用していることを確認するために、セキュアファイアウォールとFMCでURLカテゴリの割り当てを確認する方法について説明します。

前提条件

デバイスに対してURLフィルタリングライセンスを有効にし、クラウドサービスを正常な状態で統合し、URLフィルタリングを含み、URL条件の設定後に導入されたアクセスコントロールポリシーを設定する必要があります。

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center(FMC)のURLフィルタリングとカテゴリ検索
- Cisco Secure Firewall(CSF)トラフィックインスペクションおよびポリシー評価
- URLの分類とレピュテーションの動作 (CSFバージョン6.5以降のTalosに基づく)

使用するコンポーネント

このドキュメントでは、Cisco Secure FirewallおよびFMCバージョン6.5以降で使用可能な機能について説明します。このガイドの例では、バージョン7.6.5を使用しています。

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、初期（デフォルト）設定の状態から起動しています。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。

関連製品

このドキュメントは、次の製品とバージョンにも使用できます。

- セキュアファイアウォール管理センター(FMC)
- Cisco Secure Firewall(CSF)
- URLフィルタリングとクラウドサービスの統合

背景説明

URLフィルタリングは、トラフィック検査中に評価されるカテゴリデータベースに依存します。FMCは、宛先のURLカテゴリ情報を格納し、デバイスは、トラフィックが検査されるときにランタイムルックアップを実行します。FMC、デバイス、またはクラウドデータベースの間に不一致があると、アクセスコントロールポリシーが正しく設定されていても、ポリシーの結果が一貫していないように見える場合があります。

検証の重要な部分は、URLカテゴリの割り当てがFMCとデバイスで一貫していることを確認することです。URLカテゴリのルックアップは、クラウドサービスの統合設定とデバイスキャッシュの影響を受けます。キャッシュの更新設定が無効になっているか、エントリの有効期間が長すぎる場合は、Talosが分類を更新した後も、古いカテゴリデータが使用されたままになる可能性があります。

アーキテクチャ

URLフィルタリングが有効な場合、デバイスは最初にローカルURLキャッシュをチェックします。カテゴリがキャッシュに存在しない場合、デバイスはローカルデータベースまたはシスコクラウドに照会できます。デバイスはインスペクション中にローカルURLデータベースとルックアップキャッシュを使用し、beakerdはTaloshと通信してURLフィルタリングデータをダウンロードおよび更新します。FMCで管理されるデバイスでは、beakerdはFMCで実行され、CSFでwaiting状態になります。CSFがローカルで管理されている場合、プロセスはデバイス自体で実行されます。

Talosは複数のサイズでデータベースパッケージ全体を送信します。これらのサイズは/var/sf/cloud_download/ciscoに保存されます。

Talosのデータベースファイルの例を次に示します。

- cisco_uridb_large_1541554243(500 MB)
- cisco_uridb_medium_1541553645(125 MB)
- cisco_uridb_small_1541553061(33 MB)



注：データベースファイルはcisco_uridbで始まり、サイズが表示されます（小、中、大）。サイズは、使用するハードウェアによって異なります。

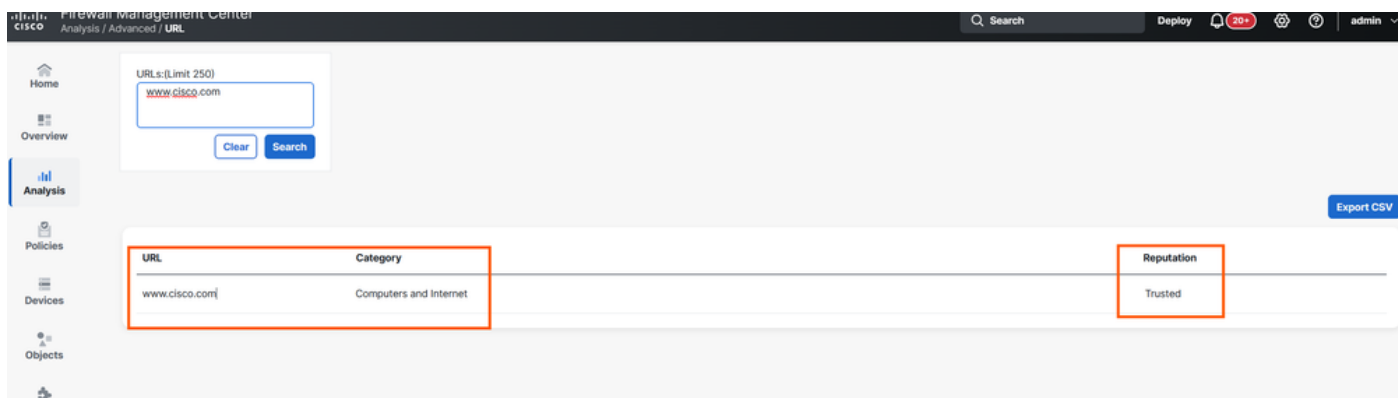
ステップ1:FMCでURLカテゴリを検索する

FMCは、URL宛先を割り当てられたカテゴリにマッピングするローカルURLデータベースを維持します。これは、URLの分類方法を検証する際に推奨される最初のステップです。

FMCで、ロケーションAnalysis > Advanced > URLに移動します。

調査するURLを入力し、割り当てられているカテゴリを確認します。

次の例では、www.cisco.comがComputers and Internetカテゴリの下にリストされています。



ステップ2:URLフィルタリング統合設定の確認

URLフィルタリング統合設定により、FMCとCSFデバイスがURLカテゴリデータベースを送信する場所が決まります。各デバイスは、URLルックアップ用に独自のローカルデータベースを保持し、追加または更新されたURLインテリジェンスについてシスコクラウドに照会できます。

FMCでIntegration > Other Integrations > Cloud Servicesの順に移動して、これらの設定を確認します。

URL Filtering



Last URL Filtering Update: 2026-08-26 10:28:52 [Update Now](#)

☒ Enable Automatic Updates

URL Query Source

- ☐ Local Database Only
- ☒ Local Database and Cisco Cloud
- ☐ Cisco Cloud Only

Cached URLs Expire

After 2 hours



[Dispute URL categories and reputations](#)

Save

統合が正常であり、URL検索キャッシュが予想されるポリシータイミングに従って更新するように設定されていることを確認します。



注意:URLルックアップキャッシュでは、以前に取得したカテゴリおよびレピュテーションの結果を保持できます。キャッシュの有効期限が無効になっているか、または長いライフタイムが設定されている場合、Taloshが分類を更新した後もデバイスはキャッシュされた情報を使用し続けることができるため、デバイスの結果が現在のFMCまたはTalosルックアップと一時的に異なる場合があります。

ステップ3：システムサポートトレースを使用して、デバイスのURLカテゴリを確認します。

CSFデバイスがFMCと同じ方法でURLを分類していることを確認するには、デバイスのCLIでシステムサポートトレースを実行します。これは、Snortインスペクションエンジンがトラフィック

を評価する方法と、接続が検査されたときにどのURLカテゴリが返されるかを示します。

FTD CLIでsystem support traceコマンドを入力し、インタラクティブなプロンプトに応答します。

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 173.37.145.84
Please specify a server port: 443
```



注：この例では、173.37.145.84がwww.cisco.comのIPアドレスです。調査しているURLに対応する宛先IPアドレスを使用します。

出力例：

```
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1: returned from url lookup, url_info is 90 2003
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1 URL lookup for www.cisco.com/ found rep 90, 2003
```

この出力では、URLはカテゴリID 2003を返します。次の手順では、その数値に対応するカテゴリ名に解決する方法について説明します。

ステップ4：カテゴリ番号をカテゴリ名に解決する

デバイスのURLカテゴリルックアップは、数値のカテゴリIDを返します。その番号を人間が読めるカテゴリ名にマッピングするには、デバイスでaup_categories.jsonファイルを開きます。

expertモードでCSFの/var/sf/cloud_download/ディレクトリに移動します。rootユーザモードであることを確認します。

カテゴリ定義ファイルを開きます。

```
root@firepower:/var/sf/cloud_download# less aup_categories.json
```

トレース出力で返されたカテゴリIDを検索します。カテゴリ2003の入力例：

```
{
  "id": 2003,
  "uuid": "abba9b63-bb10-4729-b901-2e2aa0f02003",
  "mnemonic": "comp",
  "name": "Computers and Internet",
  "type": "aup_cats",
  "state": "active"
}
```



注：カテゴリID番号はすべてのCSFデバイスで一貫しています。同じ数値IDがすべてのCSFデバイスで同じカテゴリ名にマッピングされます。

確認

ステップ1 ~ 4の出力を使用して、URLカテゴリの割り当てが、デバイスのFMCデータベースとSnortエンジンの間で一貫していることを確認します。

この例の設定は次のとおりです。

- FMCデータベースに、「Computers and Internet」としてwww.cisco.comがリストされます。
- デバイスのCLIはカテゴリID 2003を返し、コンピュータとインターネットにマッピングされます。

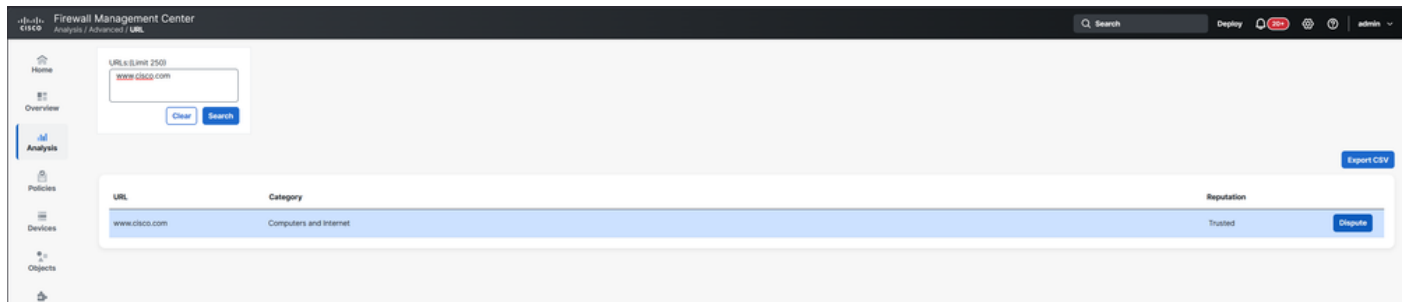
両方のソースが同意し、適用されているURLフィルタリングポリシーがこのURLに対して一貫していることを確認します。

争議ボタン

URLが誤ったカテゴリに分類されたと思われる場合は、Taloshにクレームを送信できます。

FMCで、Analysis > Advanced > URLの順に移動します。

URLを入力してSearchをクリックし、URLエントリの上にマウスポインタを置いてDisputeを選択します。



これにより、Taloshクレームのページが開き、分類を適切なソースで確認および修正できるようになります。

トラブルシューティング

分類が期待値と一致しない場合は、次の領域を確認します。

- URLフィルタリングライセンスが有効になっていて、デバイスに割り当てられていることを確認します。
- クラウドサービスの状態とTaloshへの接続を確認します。
- デバイスキャッシュとキャッシュの更新設定を調べて、古いエントリが再利用されていないことを確認します。
- FMC管理対象デバイスのFMCでbeakerdプロセスが実行されているかどうかを確認します。

FMCによって管理されるデバイスの場合は、FMCエキスパートモードで次のコマンドを実行して、プロセスがアクティブであることを確認します。

```
pmtool status | grep beakerd
```



注:FMCによって管理されているセキュアファイアウォールでこのコマンドを実行すると、プロセスが待機状態になることがあります。Secure Firewallがローカルで管理されている場合、プロセスはRunning状態で表示されます。

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。