ASA の正規表現を使った HTTP URL フィルタ機能

内容

概要

このドキュメントでは、HTTP インスペクション エンジンを使用して、適応型セキュリティ アプライアンス（ASA）で URL フィルタを設定する方法について説明します。これは、HTTP 要求の一部が正規表現パターンのリストと一致した時点で完了します。特定の URL をブロック、または選択した URL 以外のすべての URL をブロックできます。

前提条件

要件

このドキュメントに特有の要件はありません。

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的

な影響について確実に理解しておく必要があります。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

> **注**：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定手順

以下は一般的な設定手順です。

1. ブロックまたは許可する必要のあるドメインのショート リストを特定する
2. 問題となっているすべてのドメインと一致する正規表現クラス マップを作成する
3. これらのドメインと一致するトラフィックを廃棄または許可する HTTP インスペクション ポリシー マップを作成する
4. この HTTP インスペクション ポリシー マップをモジュラ ポリシー フレームワーク内の HTTP インスペクションに適用する

一部のドメインをブロックして残りのすべてのドメインを許可するか、またはすべてのドメインをブロックしてほんの一部のドメインを許可するかに関係なく、手順は同じです。ただし HTTP インスペクション ポリシー マップを作成する場合は異なります。

ブロックまたは許可する必要のあるドメインのショート リストを特定する

この設定例では、これらのドメインがブロックまたは許可されます。

- cisco1.com
- cisco2.com
- cisco3.com

これらのドメインの正規表現パターンを、次のように設定します。

```
regex cisco1.com "cisco1.com"regex cisco2.com "cisco2.com"regex cisco3.com "cisco3.com"
```

問題となっているすべてのドメインと一致する正規表現クラス マップを作成する

正規表現パターンと一致する正規表現クラスを、次のように設定します。

```
class-map type regex match-any domain-regex-classmatch regex cisco1.commatch regex
cisco2.commatch regex cisco3.com
```

これらのドメインと一致するトラフィックを廃棄または許可する HTTP インスペクション ポリシー マップを作成する

この設定内容を理解するために、この URL フィルタの目標に最もよく一致する説明を選択してください。上記の手順で作成した正規表現クラスは、許可またはブロックする必要のあるドメインのリストです。

- **リストされているドメイン以外のすべてのドメインを許可する**この設定の重要なポイントは、リストされているドメインと一致する HTTP トランザクションが「blocked-domain-class」として分類される場合にクラス マップが作成される点です。 このクラスと一致する HTTP トランザクションはリセットされ、閉じます。基本的には、これらのドメインと一致する HTTP トランザクションのみがリセットされます。

  ```
  class-map type inspect http match-all blocked-domain-class match request header host regex
  class domain-regex-class!policy-map type inspect http regex-filtering-policy parameters
  class blocked-domain-class  reset log
  ```

- **リストされているドメイン以外のすべてのドメインをブロックする**この設定の重要なポイントは、キーワード「match not」を使用してクラス マップが作成される点です。 これにより、ドメイン リストと一致しないすべてのドメインが「allowed-domain-class」というタイトルのクラスと一致する必要があることがファイアウォールに指示されます。このクラスと一致する HTTP トランザクションはリセットされ、閉じます。基本的には、リストされるドメインと一致する HTTP トランザクションを除くトランザクションがすべてリセットされます。

  ```
  class-map type inspect http match-all allowed-domain-class match not request header host
  regex class domain-regex-class!policy-map type inspect http regex-filtering-policy
  parameters class allowed-domain-class  reset log
  ```

この HTTP インスペクション ポリシー マップをモジュラ ポリシー フレームワーク内の HTTP インスペクションに適用する

HTTP インスペクション ポリシー マップが「regex-filtering-policy」として設定されたため、このポリシー マップを、既存の HTTP インスペクションまたはモジュラ ポリシー フレームワーク内の新しいインスペクションに適用します。これによりたとえば、「global_policy」に設定されている「inspection_default」クラスにインスペクションが追加されます。

```
policy-map global_policy class inspection_default  inspect http regex-filtering-policy
```

一般的な問題

HTTP インスペクション ポリシー マップおよび HTTP クラス マップを設定するときには、必要な目的のために match または match not が設定されていることを確認してください。これはスキップする必要のある単純なキーワードであり、結果として意図しない動作が生じます。また、この形式の正規表現処理は、高度なパケット処理と同様に、ASA の CPU 使用率を増加させるとともに、スループットを低下させる可能性があります。正規表現パターンをさらに追加する場合は注意してください。