FQDN による CWS 検査からの ASA トラフィックの除外に関する設定例

目次

概要

このドキュメントでは、完全修飾ドメイン名（FQDN）に基づいて Cloud Web Security（CWS）インスペクションからのトラフィックを除外するために、Cisco Adaptive Security Appliance（ASA）コネクタを設定する方法について説明します。 特定のサイトがミッション クリティカルである場合や完全に信頼できる場合には、通常、（サービスをバイパスして要求を宛先に転送するために）それらのサイトを CWS インスペクションから完全に除外することには利点があります。 これにより、コネクタ デバイスの負荷やオーバーヘッドが軽減され、障害ポイントが取り除かれ、サイトにアクセスする際の速度が向上します。 各コネクタ テクノロジーは、それぞれ独自の方法で除外を設定します。

前提条件

要件

このドキュメントでは、基本的なネットワーク接続と CWS サービスに関して ASA がすでに設定されていることを前提とします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ASA バージョン 9.0 以降

- すべての ASA モデル

本書の情報は、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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

1. FQDN ベースの除外を設定する前に、有効なドメイン ネーム サーバ（DNS）を使って ASA を設定しておく必要があります。 名前検索を設定するには、次のコマンドを入力します。

```
asa(config)# domain-name <company domain>
asa(config)# dns server-group DefaultDNS
asa(config-dns-server-group)# name-server <DNS Server IP>
asa(config-dns-server-group)# dns domain-lookup <interface-name>
```

   <company domain> フィールドを、ASA が存在するドメインに置き換えてください。
   <DNS Server IP> は、ASA から到達できる稼働中の DNS サーバのアドレスです。
   <interface-name> は DNS サーバを検出できるインターフェイスの名前です。
2. DNS ルックアップ機能を確認するには、ping コマンドを入力します。 ping コマンドにより、指定した名前が IP アドレスに解決されるはずです。

```
asa# ping www.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.84, timeout is 2 seconds:
!!!!!
```

3. CWS インスペクションから除外する必要がある各 FQDN のネットワーク オブジェクトを定義するには、次のコマンドを入力します。
   注: この例では、Google.com、Purple.com、および M.YouTube.com の除外を作成します。

```
asa(config)# object network google.com-obj
asa(config-network-object)# fqdn google.com
asa(config-network-object)# object network purple.com-obj
asa(config-network-object)# fqdn purple.com
asa(config-network-object)# object network m.youtube.com-obj
asa(config-network-object)# fqdn m.youtube.com
```

4. 複数のオブジェクトを単一のオブジェクト グループにまとめるには、次のコマンドを入力します。
   注: この例では、このグループを CWS_Exclusions と呼びます。

```
asa(config)# object-group network CWS_Exclusions
asa(config-network-object-group)# network-object object google.com-obj
asa(config-network-object-group)# network-object object purple.com-obj
asa(config-network-object-group)# network-object object m.youtube.com-obj
```

5. CWS クラス マップが参照するアクセス コントロール リスト（ACL）に、アクセス コントロール リスト拡張（ACLE）を追加します。 たとえば、現在のアクセス リストが以下のとおりであるとします。

```
asa(config)# object-group network CWS_Exclusions
asa(config-network-object-group)# network-object object google.com-obj
asa(config-network-object-group)# network-object object purple.com-obj
asa(config-network-object-group)# network-object object m.youtube.com-obj
```

   除外を追加するには、ステップ 4 で作成したオブジェクト グループを参照する deny エント

リをリストの先頭に配置します。

```
asa(config)# access-list http-c line 1 extended deny ip any object-group
CWS_Exclusions
```

アクセス リストが正しく作成されたことを確認するには、show access-list コマンドを次のように入力します。

```
asa# show access-list http-c
access-list http-c; 4 elements; name hash: 0xba5a06bc
access-list http-c line 1 extended deny ip any object-group CWS_Exclusions
(hitcnt=0) 0x6161e951
 access-list http-c line 1 extended deny ip any fqdn google.com (unresolved)
(inactive) 0x48f9ca9e
 access-list http-c line 1 extended deny ip any fqdn purple.com (unresolved)
(inactive) 0x1f8c5c7c
 access-list http-c line 1 extended deny ip any fqdn m.youtube.com (unresolved)
(inactive) 0xee068711
access-list http-c line 2 extended permit tcp any any eq www (hitcnt=0)
0xe21092a9
access-list http-c line 3 extended permit tcp any any eq 8080 (hitcnt=0)
0xe218c5a3
```

注: show access-list コマンドの出力ではオブジェクト グループが展開されます。こうして、完成したリストに目的のすべての FQDN が含まれるかどうか確認できます。

設定

初期設定

この設定には、該当する行のみが含まれています。

```
asa# show access-list http-c
access-list http-c; 4 elements; name hash: 0xba5a06bc
access-list http-c line 1 extended deny ip any object-group CWS_Exclusions
(hitcnt=0) 0x6161e951
 access-list http-c line 1 extended deny ip any fqdn google.com (unresolved)
(inactive) 0x48f9ca9e
 access-list http-c line 1 extended deny ip any fqdn purple.com (unresolved)
(inactive) 0x1f8c5c7c
 access-list http-c line 1 extended deny ip any fqdn m.youtube.com (unresolved)
(inactive) 0xee068711
access-list http-c line 2 extended permit tcp any any eq www (hitcnt=0)
0xe21092a9
access-list http-c line 3 extended permit tcp any any eq 8080 (hitcnt=0)
0xe218c5a3
```

Final Configuration

この設定には、該当する行のみが含まれています。

```
asa# show access-list http-c
access-list http-c; 4 elements; name hash: 0xba5a06bc
```

```
access-list http-c line 1 extended deny ip any object-group CWS_Exclusions
(hitcnt=0) 0x6161e951
 access-list http-c line 1 extended deny ip any fqdn google.com (unresolved)
(inactive) 0x48f9ca9e
 access-list http-c line 1 extended deny ip any fqdn purple.com (unresolved)
(inactive) 0x1f8c5c7c
 access-list http-c line 1 extended deny ip any fqdn m.youtube.com (unresolved)
(inactive) 0xee068711
access-list http-c line 2 extended permit tcp any any eq www (hitcnt=0)
0xe21092a9
access-list http-c line 3 extended permit tcp any any eq 8080 (hitcnt=0)
0xe218c5a3
```

確認

CWS により検査されるトラフィックを定義するために使われるアクセス リストを確認するには、**show access-list *<acl-name>*** コマンドを次のように入力します。

```
asa# show access-list http-c
access-list http-c; 17 elements; name hash: 0xba5a06bc
access-list http-c line 1 extended deny ip any object-group CWS_Exclusions
(hitcnt=0) 0x6161e951
 access-list http-c line 1 extended deny ip any fqdn google.com (resolved)
0x48f9ca9e
 access-list http-c line 1 extended deny ip any fqdn purple.com (resolved)
0x1f8c5c7c
 access-list http-c line 1 extended deny ip any fqdn m.youtube.com (resolved)
0xee068711
 access-list http-c line 1 extended deny ip any host 153.104.63.227 (purple.com)
(hitcnt=0) 0x5b6c3170
 access-list http-c line 1 extended deny ip any host 74.125.228.97 (m.youtube.com)
(hitcnt=0) 0x8f20f731
 access-list http-c line 1 extended deny ip any host 74.125.228.98 (m.youtube.com)
(hitcnt=0) 0x110e4163
 access-list http-c line 1 extended deny ip any host 74.125.228.99 (m.youtube.com)
(hitcnt=0) 0x5a188b6f
 access-list http-c line 1 extended deny ip any host 74.125.228.100 (m.youtube.com)
(hitcnt=0) 0xa27504c4
 access-list http-c line 1 extended deny ip any host 74.125.228.101 (m.youtube.com)
(hitcnt=0) 0x714d36b9
 access-list http-c line 1 extended deny ip any host 74.125.228.102 (m.youtube.com)
(hitcnt=0) 0x158951c0
 access-list http-c line 1 extended deny ip any host 74.125.228.103 (m.youtube.com)
(hitcnt=0) 0x734a5b42
 access-list http-c line 1 extended deny ip any host 74.125.228.104 (m.youtube.com)
(hitcnt=0) 0xeeed1641
 access-list http-c line 1 extended deny ip any host 74.125.228.105 (m.youtube.com)
(hitcnt=0) 0x0b4b1eb3
 access-list http-c line 1 extended deny ip any host 74.125.228.110 (m.youtube.com)
(hitcnt=0) 0x2b0e5275
 access-list http-c line 1 extended deny ip any host 74.125.228.96 (m.youtube.com)
(hitcnt=0) 0x315ed3b2
access-list http-c line 2 extended permit tcp any any eq www
(hitcnt=0) 0xe21092a9
access-list http-c line 3 extended permit tcp any any eq 8080 (hitcnt=0)
0xe218c5a3
```

注: オブジェクト グループおよび解決されたアドレスが出力で展開されます。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。