ASA从CWS检查的流量排除与FQDN配置示例

目录

简介

本文描述如何配置思科可适应安全工具(ASA)连接器为了从Cloud Web根据完全合格的域名(FQDN)的安全(CWS)检查排除流量。经常是有利的从CWS检查完全地排除某些站点(为了旁路服务和转发请求到目的地)，如果有问题的站点是目标关键并且/或者绝对委托。这减小负载和开销在连接器设备，排除问题的失败，并且增加加速，当您访问站点。每个连接器技术有一个唯一方式配置排除。

先决条件

要求

本文假设， ASA为基本网络连接和CWS服务已经配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA版本9.0和以上
- 所有ASA型号

本文档中的信息都是基于特定实验室环境中的设备编写的。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

1. 在您配置基于FQDN的排除前，必须配置ASA与有效域名服务器(DNS)。为了配置名称查找，请输入这些命令：

```
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>
```

替换*<company domain>*字段与ASA位于的域。*<DNS服务器IP>*是ASA能到达一个功能DNS服务器的地址，并且*<interface-name>*是DNS服务器可以被找到接口的名称。

2. 为了验证DNS查找功能，请输入**ping命令**。**ping命令**应该能解析提供的名称到IP地址。

```
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. 为了定义应该从CWS检查排除的每个FQDN的一个网络对象，请输入这些命令：
Note:此示例创建**Google.com**、**Purple.com**和**M.YouTube.com**的免税。

```
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. 为了配合对象到一个对象组，请输入这些命令：
Note:此示例是指组作为**CWS_Exclusions**。

```
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. 添加一访问控制表分机(ACLE)到CWS类映射参考的访问控制表(ACL)。例如，当前访问列表如下所示：：

```
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
```

为了添加免税，请放置一个**拒绝条目**在参考对象组创建步骤4的列表顶部：

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

为了验证access-list正确地被修建了，请输入**show access-list命令**：

```
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
```

Note:从show access-list命令的输出展开对象组，允许您验证所有打算的FQDN是存在完成列表。

配置

初始配置

此配置只包含相关线路。

```
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
```

最终配置

此配置只包含相关线路。

```
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
```

验证

为了验证access-list用于的为了定义由CWS检查的流量，请输入**show access-list *<acl-name>***命令：

```
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
```

Note:对象组和解决的地址在输出中展开。

故障排除

目前没有针对此配置的故障排除信息。