Exclusion du trafic ASA d'inspection CWS avec l'exemple de configuration FQDN

Contenu

Introduction

Ce document décrit comment configurer un connecteur de l'appliance de sécurité adaptable Cisco (ASA) afin d'exclure le trafic de l'inspection de la sécurité Web de nuage (CWS) basée sur le nom de domaine complet (FQDN). Il est souvent avantageux d'exclure certains sites de l'inspection CWS entièrement (afin de sauter le service et en avant les demandes à la destination) si les sites en question sont critiques et/ou faits confiance absolument. Ceci diminue le chargement et le temps système sur le périphérique de connecteur, élimine un point de panne, et augmente la vitesse quand vous accédez aux sites. Chaque technologie de connecteur a une façon unique de configurer des exclusions.

Conditions préalables

Conditions requises

Ce document suppose que l'ASA est déjà configurée pour la connexion réseau de base et le service CWS.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Versions 9.0 et ultérieures ASA
- Tous les modèles ASA

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

1. Avant que vous configuriez des exclusions basées sur FQDN, l'ASA doit être configurée avec un Domain Name Server valide (DN). Afin de configurer la recherche de noms, sélectionnez ces commandes :

   ```
   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>
   ```

   Remplacez le champ *<company de domain>* par le domaine dans lequel l'ASA réside. *Le serveur IP> <DNS* est l'adresse d'un serveur DNS fonctionnel que l'ASA peut atteindre, et le *<interface-name>* est le nom de l'interface de laquelle le serveur DNS peut être trouvé.
2. Afin de vérifier la fonctionnalité de consultation de DN, sélectionnez la **commande ping**. **La commande ping** devrait pouvoir résoudre le nom fourni à une adresse IP.

   ```
   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. Afin de définir un objet de réseau pour chaque FQDN qui devrait être exclu de l'inspection CWS, sélectionnez ces commandes :
   Note: Cet exemple crée des exemptions pour **Google.com**, **Purple.com**, et **M.YouTube.com**.

   ```
   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. Afin d'attacher les objets ensemble dans un seul groupe d'objets, sélectionnez ces commandes :
   Note: Cet exemple se rapporte au groupe comme **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. Ajoutez une extension de liste de contrôle d'accès (ACLE) à la liste de contrôle d'accès (ACL) référencée par le class map CWS. Par exemple, la liste d'accès en cours pourrait ressembler à ceci :

   ```
   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
```

Afin d'ajouter les exemptions, placez une **entrée de refuser** en haut de la liste qui met en référence le groupe d'objets créé dans l'étape 4 :

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

Afin de vérifier que la liste d'accès a été construite correctement, sélectionnez la **commande access-list d'exposition** :

```
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: La sortie de la **commande access-list d'exposition** développe le groupe d'objets, qui te permet pour vérifier que tous les FQDN destinés sont présents dans la liste terminée.

Configurations

Configuration initiale

Cette configuration contient seulement les lignes appropriées.

```
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
```

Configuration finale

Cette configuration contient seulement les lignes appropriées.

```
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
```

Vérifiez

Afin de vérifier la liste d'accès utilisée afin de définir le trafic qui est examiné par CWS, sélectionnez la commande de *<acl-name> de liste d'accès d'exposition* :

```
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: Le groupe d'objets et les adresses résolues sont développés dans la sortie.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.