Exclusión del tráfico ASA del examen del CWS con el ejemplo de configuración FQDN

Contenido

Introducción

Este documento describe cómo configurar un conector adaptante del dispositivo de seguridad de Cisco (ASA) para excluir el tráfico del examen de la Seguridad de la red de la nube (CWS) basado en el nombre de dominio completo (FQDN). Es a menudo ventajoso excluir los determinados sitios del examen del CWS totalmente (para desviar el servicio y delantero las peticiones al destino) si los sitios en la pregunta son misión crítica y/o confiado en absolutamente. Esto disminuye la carga y los gastos indirectos en el dispositivo del conector, elimina una punta del error, y aumenta la velocidad cuando usted accede los sitios. Cada tecnología del conector tiene una forma única de configurar las exclusiones.

Prerequisites

Requisitos

Este documento asume que el ASA está configurado ya para la conectividad de red básica y el servicio del CWS.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versiones de ASA 9.0 y posterior
- Todos los modelos ASA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

1. Antes de que usted configure las exclusiones FQDN-basadas, el ASA se debe configurar con un Domain Name Server válido (DNS). Para configurar la búsqueda de nombre, ingrese estos comandos:

   ```
   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>
   ```

   Substituya el campo *<company del domain>* por el dominio en el cual el ASA reside. *<DNS el servidor IP>* es el direccionamiento de un servidor de los DNS funcionales que el ASA pueda alcanzar, y *<interface name>* es el nombre de la interfaz de la cual el servidor DNS puede ser encontrado.
2. Para verificar las funciones de la búsqueda de DNS, ingrese el comando ping. El comando ping debe poder resolver el nombre proporcionado a una dirección 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. Para definir un objeto de red para cada FQDN que se deba excluir del examen del CWS, ingrese estos comandos:
   Note: Este ejemplo crea las exenciones para Google.com, Purple.com, y 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. Para atar los objetos juntos en un solo grupo de objetos, ingrese estos comandos:
   Note: Este ejemplo refiere al grupo como 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. Agregue una extensión de la lista de control de acceso (ACLE) a la lista de control de acceso (ACL) referida por la correspondencia de la clase del CWS. Por ejemplo, la lista de acceso actual pudo parecer esto:

   ```
   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
```

Para agregar las exenciones, ponga una **entrada de la negación** en la cima de la lista que se refiere al grupo de objetos creado en el paso 4:

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

Para verificar que la lista de acceso se haya construido correctamente, ingrese el **comando show access-list**:

```
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 salida del **comando show access-list** amplía el grupo de objetos, que permite que usted verifique que todos los FQDN previstos estén presentes en la lista completada.

Configuraciones

Configuración inicial

Esta configuración contiene solamente las líneas relevantes.

```
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
```

Configuración final

Esta configuración contiene solamente las líneas relevantes.

```
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
```

Verificación

Para verificar la lista de acceso utilizó para definir el tráfico que es examinado por el CWS, ingresa el comando del *<acl-name> de la lista de acceso de la demostración*:

```
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: Amplían al grupo de objetos y los direccionamientos resueltos en la salida.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.