Exclusão do tráfego ASA da inspeção CWs com exemplo de configuração FQDN

Índice

Introdução

Este documento descreve como configurar um conector adaptável da ferramenta de segurança de Cisco (ASA) a fim excluir o tráfego da inspeção da Segurança da Web da nuvem (CWs) baseada no nome de domínio totalmente qualificado (FQDN). É frequentemente vantajoso excluir inteiramente sites determinado da inspeção CWs (a fim contornear o serviço e dianteiro os pedidos ao destino) se os locais na pergunta são missão crítica e/ou confiado absolutamente. Isto diminui a carga e as despesas gerais no dispositivo do conector, elimina um ponto da falha, e aumenta a velocidade quando você alcança os locais. Cada tecnologia do conector tem um modo exclusivo configurar exclusões.

Pré-requisitos

Requisitos

Este documento supõe que o ASA está configurado já para a conectividade de rede básica e o serviço CWs.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versões ASA 9.0 e mais atrasado

- Todos os modelos ASA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

1. Antes que você configure exclusões FQDN-baseadas, o ASA deve ser configurado com um Domain Name Server válido (DNS). A fim configurar a consulta de nome, incorpore estes 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>
   ```

   Substitua o campo *<company do domain>* com o domínio em que o ASA reside. *O server IP> <DNS* é o endereço de um server dos DN funcionais que o ASA possa alcançar, e o *<interface-name>* é o nome da relação de que o servidor DNS pode ser encontrado.
2. A fim verificar a funcionalidade da pesquisa de DNS, inscreva o comando ping. O comando ping deve poder resolver o nome fornecido a um endereço IP de Um ou Mais Servidores Cisco ICM NT.

   ```
   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. A fim definir um objeto de rede para cada FQDN que deve ser excluído da inspeção CWs, incorpore estes comandos:
   Note: Este exemplo cria isenções para Google.com, Purple.com, e 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. A fim amarrar junto os objetos em um único grupo de objetos, incorpore estes comandos:
   Note: Este exemplo refere o 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. Adicionar uma extensão do Access Control List (ACLE) ao Access Control List (ACL) provido pelo mapa da classe CWs. Por exemplo, a lista de acessos atual pôde olhar como esta:

   ```
   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
   ```

A fim adicionar as isenções, coloque uma **entrada da negação na** parte superior da lista que provê o grupo de objetos criado em etapa 4:

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

A fim verificar que a lista de acesso esteve construída corretamente, inscreva o **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: A saída do **comando show access-list** expande o grupo de objetos, que permite que você verifique que todo o FQDNs pretendido esta presente na lista terminada.

Configurações

Configuração inicial

Esta configuração contém somente as linhas 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
```

Configuração final

Esta configuração contém somente as linhas 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
```

Verificar

A fim verificar a lista de acesso usou-se a fim definir o tráfego que é inspecionado pelo CWs, incorpora o comando do ***<acl-name> da*** **lista de acesso da mostra**:

```
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: O grupo de objetos e os endereços resolved são expandidos na saída.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.