Содержание

Введение

Этот документ описывает, как настроить устройство адаптивной защиты Cisco (ASA) Разъём для исключения трафика из контроля Облачной веб-безопасности (CWS) на основе Полного доменного имени (FQDN). Часто выгодно исключить определенные сайты из контроля CWS полностью (чтобы обойти сервис и передать запросы назначению), если рассматриваемые узлы критически важны и/или доверяемы абсолютно. Это уменьшает загрузку и издержки на устройстве Разъёма, устраняет точку сбоя и увеличивает скорость при доступе к узлам. Каждая технология Разъёма имеет уникальный способ для настройки исключений.

Предварительные условия

Требования

Этот документ предполагает, что ASA уже настроен для сервиса CWS и базового сетевого подключения.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версии ASA 9.0 и позже
- Все модели ASA

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Настройка

1. Перед настройкой основанных на FQDN исключений ASA должен быть настроен с допустимым Сервером доменных имен (DNS). Для настройки поиска имени введите эти команды:
```
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>
```
Замените поле *<company domain>* доменом, в котором находится ASA. *<IP Сервера DNS>* является адресом сервера функциональных DN, которого может достигнуть ASA, и *<interface-name>* название интерфейса, от которого может быть найден сервер DNS.
2. Для проверки функциональности Поиска DNS введите **команду ping**. **Команда ping** должна быть в состоянии решить предоставленное название к IP-адресу.
```
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. Для определения сетевого объекта для каждого FQDN, который должен быть исключен из контроля CWS, ввести эти команды:
Примечание: Данный пример создает льготы для **Google.com**, **Purple.com** и **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. Для связывания объектов в группу отдельного объекта введите эти команды:
Примечание: Данный пример обращается к группе как **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. Добавьте Расширение списка контроля доступа (ACLE) к Списку контроля доступа (ACL), на который ссылается карта классов CWS. Например, текущий список доступа мог бы быть похожим на это:
```
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
```
Для добавления льгот разместите **запись deny** наверху списка, который ссылается на групповой объект, созданный в шаге 4:
```
asa(config)# access-list http-c line 1 extended deny ip any object-group
CWS_Exclusions
```
Чтобы проверить, что access-list был создан правильно, введите команду **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
```

Примечание: Выходные данные от команды **show access-list** разворачивают групповой объект, который позволяет вам проверять, что все намеченные FQDNs присутствуют в завершенном списке.

Конфигурации

Начальная конфигурация

Эта конфигурация только содержит соответствующие линии.

```
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
```

Окончательная конфигурация

Эта конфигурация только содержит соответствующие линии.

```
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
```

Проверка

Для проверки access-list, используемого для определения трафика, который осмотрен CWS, введите **show access-list** *<команда name> acl*:

```
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
```

Примечание: Групповой объект и решенные адреса расширены в выходных данных.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.