Проблема фильтра трафика BotNet с устройством адаптивной безопасности

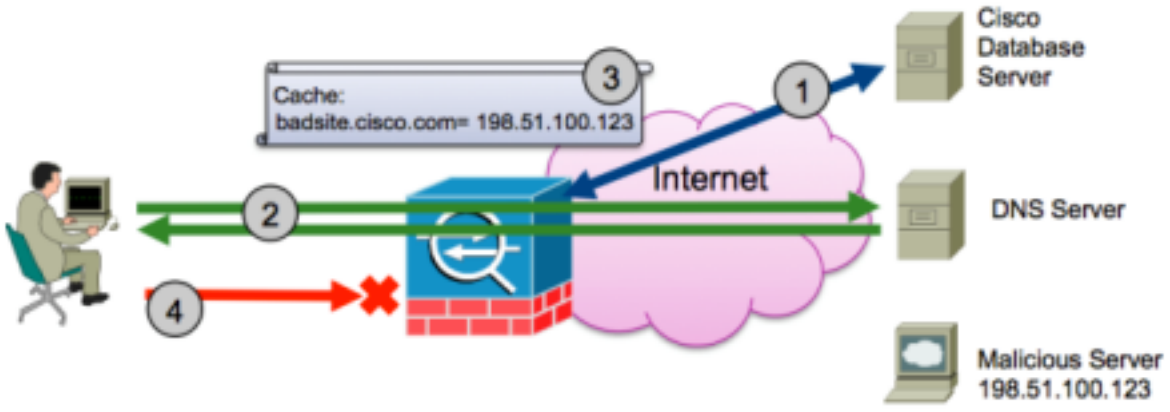
Содержание

Введение

Этот документ описывает шаги для устранения проблем функциональности фильтра трафика BotNet на Устройстве адаптивной защиты (ASA). Для помощи с конфигурацией фильтра трафика BotNet посмотрите это это руководство по конфигурации: Настройка Фильтр трафика BotNet.

Общие сведения

Фильтр трафика BotNet контролирует запросы Сервера доменных имен (DNS) и ответы между клиентами Internal DN и внешними серверами DNS. Когда DNS - ответ обработан, домен, привязанный к ответу, проверен против базы данных известных злонамеренных доменов. Если существует соответствие, дальнейший трафик к подарку IP-адреса в DNS - ответе заблокирован. См. эту схему.



1. **Проверьте базу данных динамического фильтра.** ASA периодически загружает текущую базу данных известных злонамеренных доменов и IP-адресов. Операции интеллектуальной информационной безопасности (SIO) Cisco решают, что домены и

IP-адреса в этой базе данных служат вредоносному ПО или другому злонамеренному содержанию.

2. **Гарантируйте, что трафик DNS пересекает ASA.** Пользователь на внутренней сети или компьютер пораженный вирусом на внутренней сети пытаются обратиться к злонамеренному серверу, чтобы загрузить вредоносное ПО или участвовать в BotNet. Для соединения со злонамеренным сервером главный компьютер должен выполнить Поиск DNS. В данном примере машина делает попытку доступа к badsite. cisco . com. Главный компьютер передает запрос DNS к локальному DNS - серверу или непосредственно к внешнему серверу DNS. В обеих ситуациях запрос DNS должен пересечь ASA, и DNS - ответ должен также пересечь тот же ASA.
3. **Проверьте кэш ищейки DNS.** Функция ищейки DNS проверки DNS, если включено, контролирует трафик DNS и решает, что ответ A-записи DNS возвратился из сервера DNS. Функция ищейки DNS берет домен и подарок IP-адресов в ответе A-записи и добавляет его к кэшу ищейки DNS. Домен проверен против загруженной базы данных от шага 1, и соответствие найдено. DNS - ответ не отброшен и позволен пройти.
4. **Протестируйте фильтр трафика BotNet с трафиком.** Поскольку было соответствие в шаге 3, ASA добавляет внутреннее правило, которое указывает на весь трафик к или от IP, привязанного к badsite. cisco . com отброшен. Зараженный компьютер тогда пытается обратиться к URL badsite. cisco . сервер com и трафик отброшены.

Поток операций устранения неполадок

Используйте эти шаги, чтобы устранить неполадки и проверить, что работает функция.

Шаг 1: Проверьте базу данных динамического фильтра

Проверьте, загрузила ли база данных и вводит **данные динамического фильтра команды show**. Посмотрите этот пример выходных данных:

```
# show dynamic-filter data
Dynamic Filter is using downloaded database version '1404865586'
Fetched at 21:32:02 EDT Jul 8 2014, size: 2097145
Sample contents from downloaded database:
dfgdsfgsdfg.com bulldogftp.com bnch.ru 52croftonparkroad.info
paketoptom.ru lzvideo.altervista.org avtovirag.ru cnner.mobi
Sample meta data from downloaded database:
threat-level: very-high, category: Malware,
description: "These are sources that use various exploits to deliver adware,
spyware and other malware to victim computers. Some of these are associated
with rogue online vendors and distributors of dialers which deceptively
call premium-rate phone numbers." threat-level: high, category: Bot
and Threat Networks, description: "These are rogue systems that
control infected computers. They are either systems hosted on
threat networks or systems that are part of the botnet itself
threat-level: moderate, category: Malware,
description: "These are sources that deliver deceptive or malicious anti-spyware,
anti-malware, registry cleaning, and system cleaning software."
threat-level: low, category: Ads,
description: "These are advertising networks that deliver banner ads,
interstitials, rich media ads, pop-ups, and pop-unders for websites,
spyware and adware. Some of these networks send ad-oriented HTML emails
and email verification services."
Total entries in Dynamic Filter database:
```

```
Dynamic data&colon; 80677 domain names , 4168 IPv4 addresses
Local data&colon; 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
Dynamic data&colon; 0 domain names , 4168 IPv4 addresses
Local data&colon; 0 domain names , 0 IPv4 addresses
```

В этих выходных данных ASA указывает время последней успешной выборки базы данных и выборки содержания в этой базе данных. Если вы выполняете **данные динамического фильтра команды show**, и команда показывает, что никакая база данных не загрузила, устраните неполадки этого шага сначала. Общие проблемы, которые препятствуют тому, чтобы ASA получил базу данных динамического фильтра, включают:

- **Пропавшие без вести или неправильная Конфигурация DNS на ASA.** Клиент средства обновления динамического фильтра должен решить имя хоста сервера обновления. DNS должен быть настроен и функциональный на ASA. Пропингуйте известные домены от командной строки и определите, может ли ASA решить имена хоста.
- **Никакой доступ в Интернет от ASA.** Если ASA находится в сети, которая не имеет доступа к Интернету, или устройство восходящего потока данных блокирует внешний IP - адрес ASA от доступа до Интернета, сбоев обновления.
- **Клиенту средства обновления не включают**. **Клиент средства обновления динамического фильтра** команды **включает**, должен быть настроен так, чтобы ASA мог загрузить базу данных.

Войдите команда **отлаживают клиента средства обновления динамического фильтра** для отладки базы данных. Посмотрите этот пример выходных данных от команды:

```
Dynamic Filter: Updater client fetching dataDynamic Filter: update
startingDBG:01:2902417716:7fff2c33ec28:0000: Creating fiber
0x7fff2c4dce90 [ipe_request_fiber], stack(16384) =
0x7fff2c505c60..0x7fff2c509c58 (fc=2),
sys 0x7fff20906038 (FIBERS/fibers.c:fiber_create:544)
DBG:02:2902417779:7fff2c4dce90:0000: Jumpstarting ipe_request_fiber 0x7fff2c4dce90,
sys 0x7fff2c33eba0 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
Dynamic Filter: Created lua machine, launching lua script
DBG:03:2902422654:7fff2c4dce90:0000: Connecting to 00000000:1591947792
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:04:2902422667:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:05:2902422691:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/ssl/CONNECT/3/208.90.58.5/443/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:06:2902422920:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
DBG:07:2902750615:7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
Dynamic Filter: Processing updater server response
Dynamic Filter: update file url1 =
http://updates.ironport.com/threatcast/1.0/blacklist/2mb-1file/1404865586
Dynamic Filter: update file url2 =
http://updates.ironport.com/threatcast/1.0/blacklist/2mb-1file/1404865586
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDBG:08:2902784011:
7fff2c4dce90:0000: Connecting to 00000000:538976288
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:09:2902784026:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:10:2902784051:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/208.90.58.25/80/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:11:2902784241:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
```

```
DBG:12:2902914651:7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
DBG:13:2902914858:7fff2c4dce90:0000: Connecting to 00000000:25465757
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:14:2902914888:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:15:2902914912:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/208.90.58.25/80/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:16:2902915113:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDBG:17:2907804137:
7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
Dynamic Filter: Successfully downloaded the update file from url1
Dynamic Filter: Successfully finished lua script
DBG:18:2907804722:7fff2c4dce90:0000: Fiber 0x7fff2c4dce90 finished leaving 3 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:19:2907804746:7fff2c4dce90:0000: Exiting fiber 0x7fff2c4dce90
(FIBERS/fibers.c:fiber__kill:1287)
DBG:20:2907804752:7fff2c4dce90:0000: Fiber 0x7fff2c4dce90 terminated, 2 more
(FIBERS/fibers.c:fiber__kill:1358)
Dynamic Filter: Downloaded file successfully
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDynamic Filter: read
ramfs bytes 2097152
Dynamic Filter: file MD5 verification check succeeded
Dynamic Filter: decrypt key succeeded
Dynamic Filter: decrypt file succeeded byte = 2097145
Dynamic Filter: updating engine bytes = 2097145
Dynamic Filter: meta data length = 2987
INFO: Dynamic Filter: update succeeded
```

В этих выходных данных вы видите эти шаги, которые делает средство обновления, когда это получает новую базу данных:

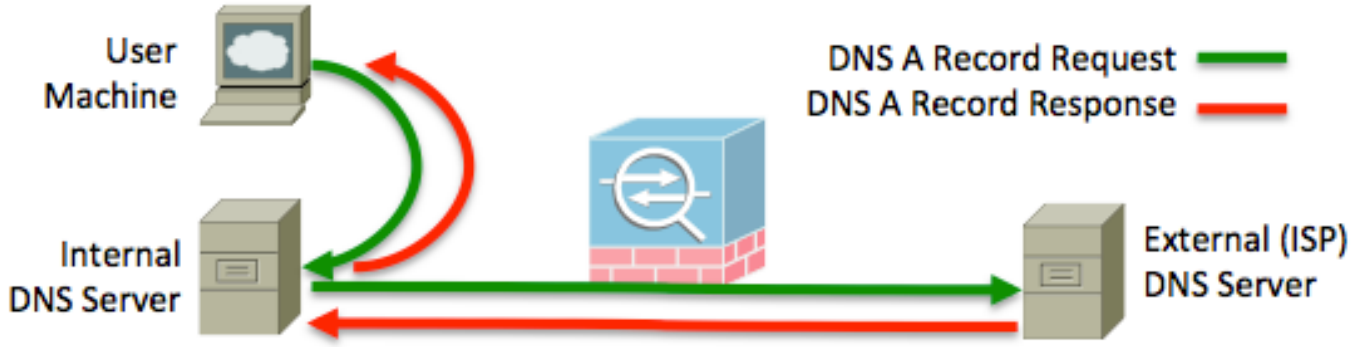
- Средство обновления обращается к URL http://обновление-manifests.ironport.com для определения, какую базу данных это загружает.
- Явный сервер возвращает два возможных URL для загрузки.
- Клиент средства обновления загружает базу данных.
- База данных дешифрована и сохранена в памяти для использования процессом динамического фильтра.

Проблемы с подключением для другой декларации серверов обновления как ошибки в этих выходных данных и справке устраняют неполадки далее. Вынудите клиента средства обновления работать вручную с **выборкой базы данных динамического фильтра** команды.

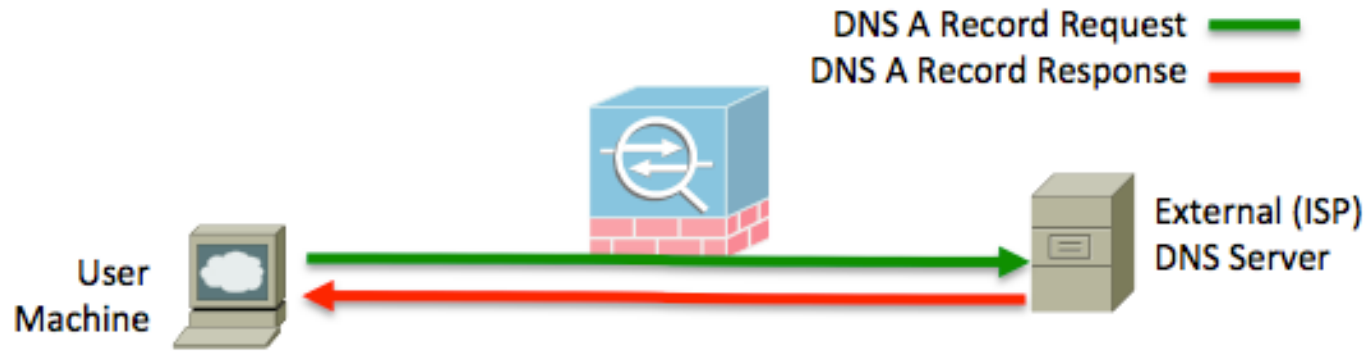
Шаг 2: Гарантируйте Пересечениям Трафика DNS этот ASA

Функциональность фильтра трафика BotNet ASA создана прочь IP-адресов, которые совпадают с доменами, таким образом, ASA должен быть встроен с запросами DNS и ответами, которые пересекают сеть. Некоторая топология могла бы заставить трафик DNS брать путь, который не включает рассматриваемый ASA. Большинство сетей имеет внутренние серверы DNS, которые действуют как DNS - ретрансляторы и кэши для внутренних usr. Пока эти серверы, когда они передают запрос DNS для домена, они не владеют или не могут ответить для, переслать запрос на сервер, который требует пересечения ASA, никакая проблема не должна происходить. Посмотрите эту топологию с и без внутренних серверов DNS:

Этот пример топологии показывает пользователям, которые указывают к внутреннему серверу DNS который вперед к внешнему серверу DNS.



Этот пример топологии показывает пользователям, которые указывают непосредственно к внешнему серверу DNS.



В обоих примерах топологии ключ к функциональным развертываниям фильтра трафика BotNet - то, что DNS, запросы на запись A-для внешних доменов должны пройти через ASA, который выполняет функцию ищейки DNS. В примере внутреннего сервера, если внутренний сервер DNS берет другой сетевой путь для достижения Интернета, чем пользовательская машина, и в процессе не пересекает ASA, таблица ищейки DNS не будет содержать карты IP К ДОМЕНУ, вызванные запросами DNS пользовательской машины, и пользовательская машина не могла бы фильтроваться как ожидалось.

Используйте эти способы, чтобы проверить , что трафик DNS проходит через ASA:

- Проверьте стратегию обслуживания. Посмотрите на выходные данные **show service-policy**, чтобы определить, применена ли проверка DNS, настроила с ключевым словом **ищейки динамического фильтра** и видит трафик. Количество пакетов, привязанное к проверке DNS, должно инкрементно увеличиться, поскольку вы делаете запросы DNS.
- Используйте перехваты. Функция ищейки DNS посмотрела на Пакеты DNS, которые пересекают ASA, таким образом, важно, чтобы вы проверили, что пакеты достигают ASA. Используйте встроенную функцию перехвата ASA, чтобы удостовериться, что трафик DNS вводит и оставляет этот ASA должным образом.

Шаг 3: Проверьте кэш ищейки DNS

Наличные деньги ищейки DNS должны заполнить с картами IP К ДОМЕНУ. Один IP-адрес мог бы иметь безграничное количество доменов assocated с ним. Это - то, как компании, которые размещают веб-сайты, могут служить тысячам доменов со всего несколькими IP-адресами. Введите **подробность ищейки dns динамического фильтра команды show** и

посмотрите дамп данных в настоящее время в кэше ищейки DNS. Это - запись всех карт IP К ДОМЕНУ, которые ASA получает с использованием функции ищейки DNS проверки DNS. Посмотрите этот пример выходных данных:

```
DNS Reverse Cache Summary Information: 3 addresses, 3 names
Next housekeeping scheduled at 22:28:01 EDT Jul 8 2014,
DNS reverse Cache Information:
[198.151.100.77] flags=0x1, type=0, unit=0 b:u:w=0:1:0, cookie=0x0
[cisco.com] type=0, ttl=31240
[198.151.100.91] flags=0x23, type=0, unit=0 b:u:w=1:1:0, cookie=0x0
[magnus.cisco.com] type=1, ttl=0
[raleigh.cisco.com] type=0, ttl=0
[198.151.100.1] flags=0x2, type=0, unit=0 b:u:w=1:0:0, cookie=0x0
[badsite.cisco.com] type=1, ttl=0
```

В данном примере ASA изучает информацию приблизительно три IP-адреса, но четыре домена. **magnus. cisco . com** и **raleigh. cisco . com** оба решения к 198.151.100.91. В данном примере, двух из доменов, **magnus. cisco . com** и **badsite. cisco** . список **com** как тип 1. Это означает, что домен найден в базе данных как помещенный в черный список домен. Другие домены перечислены как тип 0, который указывает, что домен не помещен в черный список или добавлен в белый список и является просто обычным доменом.

1. Проверьте, что запросы DNS от пользовательской машины eventially пересекают межсетевой экран и обработаны ищейкой DNS и делают запрос DNS. Проверьте кэш для записи, которая совпадает. Протестируйте и используйте домен, который решает, но достаточно неясен, что он не делали запрос недавно и уже находится в таблице. Например, домен asa. cisco . com выбран. Nslookup инструмента командной строки используется для запроса того имени хоста. Рассмотрим следующий пример:

   ```
   $ nslookup asa.cisco.com

   Name: asa.cisco.com
   Address: 198.151.100.64
   ```

2. Проверьте кэш ищейки DNS. Рассмотрим следующий пример:

   ```
   DNS Reverse Cache Summary Information: 5 addresses, 7 names
   Next housekeeping scheduled at 22:48:01 EDT Jul 8 2014,
   DNS reverse Cache Information:
   [198.151.100.64] flags=0x11, type=0, unit=0 b:u:w=0:1:0, cookie=0x0
   [asa.cisco.com] type=0, ttl=86359
   ```

Запись присутствует в кэше ищейки DNS. Если бы запись не присутствовала то перед тестом nslookup это означало бы, что функция ищейки DNS работает и что ASA работает правильно с запросами DNS и ответами.

Если запись не показывает, гарантирует, что трафик DNS проходит через ASA. Вы, возможно, должны были бы сбросить кэш DNS на главном компьютере или внутренних серверах DNS, если применимо, чтобы гарантировать, что запросы не подаются от кэша.

Функция ищейки DNS не поддерживает EDNS0. Если DNS - клиент или сервер используют EDNS0, ASA не мог бы заполнить кэш ищейки DNS с картами IP К ДОМЕНУ, если ответ имеет подарок записей дополнительного ресурса. Это ограничение отслежено идентификатором ошибки Cisco CSCta36873.

Шаг 4. : Протестируйте фильтр трафика BotNet с трафиком

В шаге 3 кэш ищейки DNS показывает тот домен badsite. cisco . com находится на черном списке. Пропингуйте рассматриваемый домен для тестирования функциональности ботнета. Чем если бы вы пытаетесь загрузить домен в web-браузере, при прозванивании домена более безопасно. Не тестируйте функцию динамического фильтра при помощи своего web-браузера, потому что ваша машина могла бы поставиться под угрозу, если браузер загружает злонамеренное содержание. Используйте Протокол ICMP, потому что это - более безопасный метод и является допустимым тестом фильтра трафика BotNet, поскольку это блокируется на основе IP и ничего определенного для порта или протокола.

Если вы не знаете о помещенном в черный список узле, можно найти тот легко. Войдите **база данных динамического фильтра** команды **находят <search_term>** находить домены, которые помещены в черный список и совпадают с предоставленным критерием поиска. Рассмотрим следующий пример:

```
ASA# dynamic-filter database find cisco verybadsite.cisco.com
m=44098 acmevirus.cisco.com m=44098Found more than 2 matches,
enter a more specific string to find an exact match
```

Пропингуйте один из доменов, который возвращается. При прозванивании этого домена он заставит эти действия происходить:

1. Хост генерирует запрос DNS для рассматриваемого домена.
2. Запрос DNS пересекает ASA, или непосредственно от главного компьютера или переданный внутренним сервером.
3. DNS - ответ пересекает ASA, или назад к главному компьютеру или к внутреннему серверу.
4. Функция ищейки DNS заполняет эту карту IP К ДОМЕНУ в кэше ищейки DNS.
5. ASA сравнивает домен с базой данных dyanmic-фильтра и определяет соответствие. ASA блокирует дальнейший входящий и исходящий трафик от IP, привязанного к злонамеренному домену.
6. Главный компьютер передает эхо-запрос протокола ICMP, который отбрасывает ASA, потому что это предназначено к IP, привязанному к злонамеренному домену.

Когда ASA отбрасывает трафик теста ICMP, он регистрирует системный журнал (системный журнал), подобный данному примеру:

```
Jul 08 2014 23:14:17: %ASA-4-338006: Dynamic Filter dropped blacklisted
ICMP traffic from inside:192.168.1.100/23599 (203.0.113.99/23599) to
outside:198.151.100.72/0 (198.151.100.72/0), destination 198.151.100.72
resolved from dynamic list: acmevirus.cisco.com, threat-level: very-high,
category: Malware
```

Выходные данные **статистики динамического фильтра команды show** указывают на соединения, которые классифицированы и потенциально отброшены. Рассмотрим следующий пример:

```
ASA(config)# show dynamic-filter statistics
Enabled on interface inside
Total conns classified 163, ingress 163, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 8, dropped 0, ingress 8, egress 0
Total blacklist classified 155, dropped 154, ingress 155, egress 0
Enabled on interface outside
Total conns classified 0, ingress 0, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 0, dropped 0, ingress 0, egress 0
Total blacklist classified 0, dropped 0, ingress 0, egress 0
Enabled on interface management
```

```
Total conns classified 0, ingress 0, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 0, dropped 0, ingress 0, egress 0
Total blacklist classified 0, dropped 0, ingress 0, egress 0
```

Классифицированный счетчик только увеличивается, если попытка подключения сделана к IP-адресу, который помещен в черный список, добавлен в белый список, или greylisted. Весь другой трафик не вызывает классифицированное в противоречии с увеличением. Малое число для классифицированного списка не означает, что ASA не оценил попытки нового соединения против фильтра трафика BotNet. Это малое число вместо этого указывает, что немногие получают, или IP - адреса назначения помещены в черный список, добавлены в белый список, или greylisted. Используйте инструкции в этом документе для подтверждения функций функции должным образом.

Если тестовый поток данных не отброшен, проверьте конфигурацию, чтобы гарантировать, что это настроено для отбрасывания трафика с соответствующим уровнем угрозы. Посмотрите этот пример конфигурации, который включает фильтр трафика BotNet глобально на ASA здесь:

```
dynamic-filter updater-client enable
dynamic-filter use-database
dynamic-filter enable
dynamic-filter drop blacklist
```