Problema del filtro de tráfico de BotNet con el dispositivo de seguridad adaptante

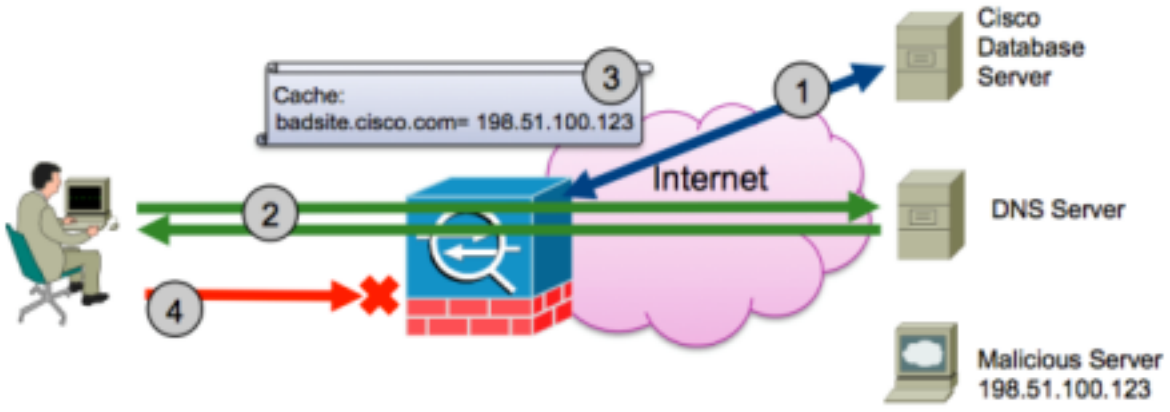
Contenido

Introducción

Este documento describe los pasos para resolver problemas las funciones del filtro de tráfico de BotNet en el dispositivo de seguridad adaptante (ASA). Para la ayuda con la configuración de filtro de tráfico de BotNet, vea esta esta guía de configuración: Configurar el filtro de tráfico de BotNet.

Antecedentes

Las peticiones y las respuestas del Domain Name Server de los monitores del filtro de tráfico de BotNet (DNS) entre los clientes de los DN internos y los servidores DNS externos. Cuando se procesa una respuesta de DNS, el dominio asociado a la respuesta se marca contra la base de datos de los dominios malévolos sabidos. Si hay una coincidencia, cualquier tráfico más otro a la dirección IP presente en la respuesta de DNS se bloquea. Vea este diagrama.



1. **Marque la base de datos dinámica del filtro.** El ASA descarga periódicamente una base de datos actual de los dominios y de los IP address malévolos sabidos. Las operaciones de inteligencia de la Seguridad de Cisco (SIO) determinan que los dominios y los IP Addresses

en esta base de datos sirven el malware o el otro contenido malévolo.
2. **Asegúrese de que el tráfico DNS cruce el ASA.** Un usuario en la red interna o un equipo infectado en la red interna intenta acceder un servidor malévolo para descargar el malware o participar en un BotNet. Para conectar con el servidor malévolo, el equipo del host debe realizar una búsqueda de DNS. En este ejemplo, el acceso de las tentativas de la máquina a badsite.cisco.com. El equipo del host envía una petición DNS a un servidor DNS local o directamente a un servidor DNS externo. En ambas situaciones, una petición DNS debe atravesar el ASA y la respuesta de DNS debe también atravesar el mismo ASA.
3. **Marque el caché del DNS-fisgón.** La función del DNS-fisgón del examen DNS, si está habilitada, monitorea el tráfico DNS y lo determina que una respuesta del Uno-expediente DNS ha vuelto del servidor DNS. La función del DNS-fisgón toma el dominio y los IP Addresses presentes en la respuesta del Uno-expediente y los agrega al caché del DNS-fisgón. El dominio se marca contra la base de datos descargada del paso 1 y se encuentra una coincidencia. La respuesta de DNS no se cae y se permite pasar a través.
4. **Pruebe el filtro de tráfico de BotNet con el tráfico.** Porque había una coincidencia en el paso 3, el ASA agrega una regla interna que indique que todo el tráfico a o desde el IP asociado a badsite.cisco.com está caído. El ordenador infectado entonces intenta acceder el servidor URL badsite.cisco.com y se cae el tráfico.

Flujo de trabajo del Troubleshooting

Utilice estos pasos para resolver problemas y verificar que la característica trabaja.

Paso 1: Marque la base de datos dinámica del filtro

Marque si la base de datos ha descargado y ingrese los **datos del dinámico-filtro del** comando show. Vea esta salida de muestra:

```
# 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
```

En esta salida, el ASA indica la época de la búsqueda acertada más reciente de la base de datos y una muestra del contenido en esta base de datos. Si usted se ejecuta los **datos del dinámico-filtro del** comando show, y el comando muestra que ninguna base de datos ha descargado, resuelven problemas este paso primero. Los problemas frecuentes que evitan que el ASA obtenga la base de datos dinámica del filtro incluyen:

- **Configuración de DNS que falta o incorrecta en el ASA.** El cliente dinámico del updater del filtro debe resolver el nombre del host del servidor de actualización. El DNS debe ser configurado y funcional en el ASA. Haga ping los dominios bien conocidos de la línea de comandos y determinelos si el ASA puede resolver los nombres de host.
- **Ningún acceso a internet del ASA.** Si el ASA está en una red que no tenga acceso a Internet, o un dispositivo ascendente bloquea el IP Address externo ASA del acceso a Internet, la actualización falla.
- **No habilitan al cliente del Updater**. **El permiso del Updater-cliente del dinámico-filtro del** comando debe ser configurado de modo que el ASA pueda descargar la base de datos.

Ingrese al Updater-**cliente del dinámico-filtro del** comando debug para hacer el debug de la base de datos. Vea esta salida de muestra del comando:

```
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
```

En esta salida, usted puede ver estas medidas que el updater tome cuando obtiene una nueva base de datos:

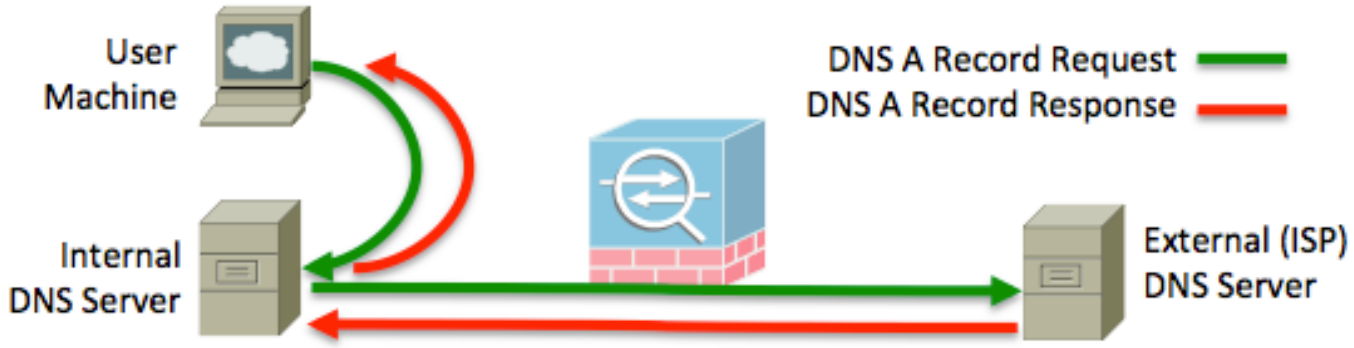
- El updater alcanza hacia fuera al URL http://update-manifests.ironport.com para determinar que la base de datos él descarga.
- El servidor evidente vuelve dos URL posibles para la descarga.
- El cliente del updater descarga la base de datos.
- La base de datos se desencripta y se salva en la memoria para uso del procedimiento de filtrado dinámico.

Los problemas de conectividad para diversos servidores de actualización manifiestan como errores en este Troubleshooting de la salida y de la ayuda más lejos. Fuerce al cliente del updater a ejecutarse manualmente con la **búsqueda dinámica de la base de datos del filtro del** comando.

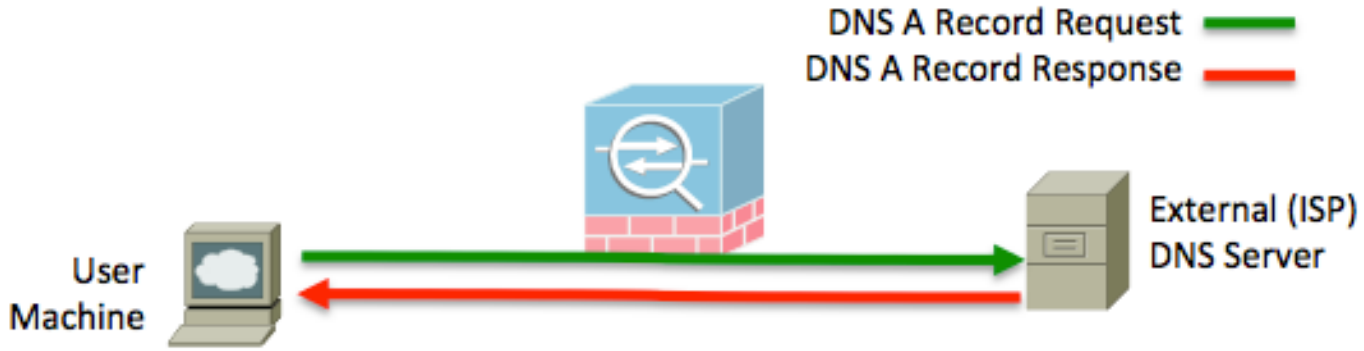
Paso 2: Asegúrese que tráfico DNS cruce este ASA

Las funciones del filtro de tráfico de BotNet del ASA se construyen apagado de los IP Addresses que hace juego los dominios, así que el ASA debe coincidir con las peticiones y las respuestas DNS que atraviesan la red. Algunas topologías pudieron hacer el tráfico DNS tomar una trayectoria que no incluye el ASA en la pregunta. La mayoría de las redes tienen los servidores DNS internos que actúan como los Transmisores de DNS y cachés para los usrs internos. Mientras estos servidores, cuando los remiten a pedido DNS un dominio no posean ni puedan contestar para, transmitan a la petición un servidor que requiera atravesar el ASA, ningún problema debe ocurrir. Vea estas topologías con y sin los servidores DNS internos:

Esta topología de ejemplo muestra a los usuarios que señalan a un servidor DNS interno cuál adelante a un servidor DNS externo.



Esta topología de ejemplo muestra a los usuarios que señalan directamente a un servidor DNS externo.



En ambos ejemplos de topología, la clave a un despliegue funcional del filtro de tráfico de BotNet es que los pedidos de registro DNS a para los dominios externos deben pasar con el ASA que funciona con la característica del DNS-fisgón. En el ejemplo del servidor interno, si el servidor DNS interno toma un diverso trayecto de red para alcanzar Internet que la máquina del usuario, y en el proceso no atraviesa el ASA, la tabla del DNS-fisgón no contendrá las correspondencias del IP-a-dominio causadas por las peticiones de la máquina DNS del usuario y la máquina del usuario no se pudo filtrar como se esperaba.

Utilice estas técnicas para marcar que el tráfico DNS pasa con el ASA:

- Marque la servicio-directiva. Mire la salida de la servicio-**directiva de la demostración** para determinar si el examen DNS es aplicado, configurado con la palabra clave del dinámico-filtro-**fisgón**, y ve el tráfico. La cuenta de paquetes asociada al examen DNS debe incrementar mientras que usted hace las peticiones DNS.
- Utilice las capturas. La característica del DNS-fisgón mira los paquetes DNS que atraviesan el ASA, así que es importante que usted marca que los paquetes alcanzan el ASA. Utilice la función incorporada de la captura ASA para aseegurarse que el tráfico DNS ingresa y deja este ASA correctamente.

Paso 3: Marque el caché del fisgón DNS

el efectivo del DNS-fisgón debe poblar con las correspondencias del IP-a-dominio. Una sola dirección IP pudo tener un número ilimitado de dominios assocated con ella. Éste es cómo las compañías que reciben los sitios web pueden servir los millares de dominios con apenas algunos IP Addresses. Ingrese al **detalle del dns-fisgón del dinámico-filtro del** comando show y vea un vaciado de los datos actualmente en el caché del DNS-fisgón. Éste es un expediente de todas las correspondencias del IP-a-dominio que el ASA obtenga con el uso de la función del DNS-fisgón del examen DNS. Vea esta salida de muestra:

```
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
```

En este ejemplo, el ASA aprende la información cerca de tres IP Addresses pero cuatro dominios. **magnus.cisco.com** y **raleigh.cisco.com** ambos resuelven a 198.151.100.91. En este ejemplo, dos de los dominios, **magnus.cisco.com** y **badsite.cisco.com** enumeran como tipo 1. Esto significa que el dominio está encontrado en la base de datos como dominio puesto. Los otros dominios se enumeran como tipo 0, que indica que el dominio no está puesto o whitelisted y es apenas un dominio normal.

1. Marque que las peticiones DNS de una máquina del usuario eventially atraviesan el Firewall y son procesadas por el DNS-fisgón y hacen una petición DNS. Marque el caché para una entrada que haga juego. Pruebe y utilice un dominio que las resoluciones pero sean bastante indeterminadas que no fue preguntado recientemente y está ya en la tabla. Por ejemplo, se elige el dominio asa.cisco.com. Comando line tool el nslookup se utiliza para preguntar ese nombre de host. Observe este ejemplo:

   ```
   $ nslookup asa.cisco.com

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

2. Marque el caché del DNS-fisgón. Observe este ejemplo:

   ```
   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
   ```

La entrada está presente en el caché del DNS-fisgón. Si la entrada no estuviera presente antes de la prueba del nslookup, significaría que la característica del DNS-fisgón trabaja y que el ASA trabaja correctamente con las peticiones y las respuestas DNS.

Si la entrada no muestra, asegúrese de que el tráfico DNS pase con el ASA. Usted puede ser que necesite vaciar el caché DNS en el equipo del host o los servidores DNS internos, si procede, para asegurarse de que las peticiones no están servidas de un caché.

La característica del DNS-fisgón no soporta EDNS0. Si el cliente DNS o el servidor utiliza EDNS0, el ASA no pudo poblar el caché del DNS-fisgón con las correspondencias del IP-a-dominio si la respuesta tiene expedientes del recurso adicional presentes. Esta limitación es seguida por el Id. de bug Cisco CSCta36873.

Paso 4: Pruebe el filtro de tráfico de BotNet con el tráfico

En el paso 3, el caché del DNS-fisgón muestra que el dominio badsite.cisco.com está en la lista negra. Haga ping el dominio en la pregunta para probar las funciones del botnet. Cuando usted hace ping el dominio, es más seguro que si usted intenta cargar el dominio en un buscador Web. No pruebe la característica dinámica del filtro usando su buscador Web porque su máquina pudo

ser comprometida si el navegador carga el contenido malévolo. Utilice el Internet Control Message Protocol (ICMP) porque es un método más seguro y es una prueba válida del filtro de tráfico de BotNet pues bloquea basado en el IP y nada específicos para virar hacia el lado de babor o protocolo.

Si usted no sabe de un sitio puesto, usted puede encontrar uno fácilmente. Ingrese el **<search_term> del hallazgo de la base de datos del dinámico-filtro del** comando para encontrar los dominios se ponen que y para corresponder con el término de la búsqueda proporcionado. Observe este ejemplo:

```
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
```

Haga ping uno de los dominios que vuelva. Cuando usted hace ping este dominio, hará estas acciones ocurrir:

1. El host genera un pedido DNS el dominio en la pregunta.
2. La petición DNS atraviesa el ASA, directamente del equipo del host o remitido por un servidor interno.
3. La respuesta de DNS atraviesa el ASA, de nuevo al equipo del host o al servidor interno.
4. La función del DNS-fisgón puebla esta correspondencia del IP-a-dominio en el caché del DNS-fisgón.
5. El ASA compara el dominio contra la base de datos del dyanmic-filtro y determina un emparejamiento. El ASA bloquea el tráfico entrante y saliente adicional del IP asociado al dominio malévolo.
6. El equipo del host envía un pedido de eco ICMP ese los descensos ASA porque se destina a un IP asociado a un dominio malévolo.

Cuando el ASA cae el tráfico de prueba ICMP, registra un registro del sistema (Syslog) similar a este ejemplo:

```
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
```

La salida de las **estadísticas del dinámico-filtro del** comando show indica las conexiones se clasifican y potencialmente se caen que. Observe este ejemplo:

```
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
```

El contador clasificado aumenta solamente si un intento de conexión se hace a una dirección IP

se ponga, whitelisted, o greylisted que. El resto del tráfico no causa clasificado en dirección contraria el aumento. Un número bajo para la lista clasificada no significa que el ASA no evaluó las tentativas de la nueva conexión contra el filtro de tráfico de BotNet. Este número bajo en lugar de otro indica que poco la fuente o los IP Address de destino está puesta, whitelisted, o greylisted. Utilice las instrucciones en este documento para confirmar las funciones de la característica correctamente.

Si el tráfico de prueba no se cae, marque la configuración para asegurarse de que está configurada para caer el tráfico con un nivel apropiado de la amenaza. Vea esta configuración de muestra, que habilita el filtro de tráfico de BotNet global en el ASA aquí:

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