# Problema do filtro de tráfego BotNet com o Adaptive Security Appliance

## Contents

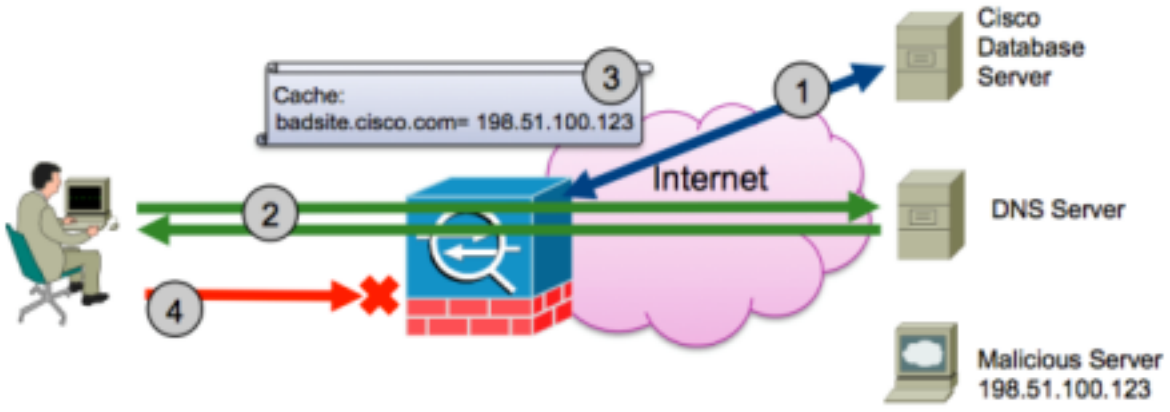


## Introduction

Este documento descreve as etapas para solucionar problemas da funcionalidade do filtro de tráfego BotNet no Adaptive Security Appliance (ASA). Para obter assistência com a configuração do filtro de tráfego BotNet, consulte este guia de configuração: Configurando o filtro de tráfego BotNet.

## Informações de Apoio

O filtro de tráfego BotNet monitora as solicitações e respostas do Servidor de Nomes de Domínio (DNS) entre clientes DNS internos e servidores DNS externos. Quando uma resposta DNS é processada, o domínio associado à resposta é verificado em relação ao banco de dados de domínios mal-intencionados conhecidos. Se houver correspondência, qualquer tráfego adicional para o endereço IP presente na resposta DNS será bloqueado. Veja este diagrama.




1. **Verifique o banco de dados de filtro dinâmico.** O ASA baixa periodicamente um banco de dados atual de domínios mal-intencionados conhecidos e endereços IP. O Security Intelligence Operations (SIO) da Cisco determina que os domínios e endereços IP neste

banco de dados servem malware ou outro conteúdo mal-intencionado.

2. **Certifique-se de que o tráfego DNS atravesse o ASA.** Um usuário na rede interna ou uma máquina infectada na rede interna tenta acessar um servidor mal-intencionado para baixar malware ou participar de um BotNet. Para se conectar ao servidor mal-intencionado, a máquina host deve executar uma pesquisa de DNS. Neste exemplo, a máquina tenta acessar badsite.cisco.com. A máquina host envia uma solicitação DNS a um servidor DNS local ou diretamente a um servidor DNS externo. Em ambas as situações, uma solicitação DNS deve atravessar o ASA e a resposta DNS também deve atravessar o mesmo ASA.
3. **Verifique o cache de snoop DNS.** A função de rastreamento de DNS da inspeção de DNS, se ativada, monitora o tráfego de DNS e determina que uma resposta de registro A de DNS retornou do servidor DNS. A função de rastreamento DNS pega os endereços IP e de domínio presentes na resposta A-Record e os adiciona ao cache de rastreamento DNS. O domínio é verificado em relação ao banco de dados baixado da etapa 1 e uma correspondência é encontrada. A resposta DNS não é descartada e tem permissão para passar.
4. **Teste o filtro de tráfego BotNet com tráfego.** Como houve uma correspondência na etapa 3, o ASA adiciona uma regra interna que indica que todo o tráfego de ou para o IP associado ao badsite.cisco.com foi descartado. Em seguida, o computador infectado tenta acessar o servidor badsite de URL.cisco.com e o tráfego é descartado.

# Solucionar problemas do fluxo de trabalho

Use estes passos para solucionar problemas e verificar se o recurso funciona.

## Passo 1: Verificar o banco de dados de filtro dinâmico

Verifique se o banco de dados foi baixado e digite o comando **show dynamic-filter data**. Veja este exemplo de saída:

```
# 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
```

Nesta saída, o ASA indica o horário da última busca bem-sucedida do banco de dados e um exemplo do conteúdo desse banco de dados. Se você executar o comando **show dynamic-filter data**, e o comando mostrar que nenhum banco de dados foi baixado, solucione esse problema primeiro. Os problemas comuns que impedem o ASA de obter o banco de dados de filtro dinâmico incluem:

- **Configuração de DNS incorreta ou ausente no ASA.** O cliente do atualizador de filtro dinâmico deve resolver o nome de host do servidor de atualização. O DNS deve ser configurado e funcional no ASA. Faça ping em domínios bem conhecidos na linha de comando e determine se o ASA pode resolver nomes de host.
- **Sem acesso à Internet do ASA.** Se o ASA estiver em uma rede que não tem acesso à Internet ou se um dispositivo upstream bloquear o acesso do endereço IP externo do ASA à Internet, a atualização falhará.
- **O cliente do atualizador não está ativado**. O comando **dynamic-filter updater-client enable** deve ser configurado para que o ASA possa baixar o banco de dados.

Insira o comando **debug dynamic-filter updater-client** para depurar o banco de dados. Veja este exemplo de saída do 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
```

Nesta saída, você pode ver estes passos que o atualizador executa quando obtém um novo banco de dados:

- O atualizador acessa o URL http://update-manifests.ironport.com para determinar qual banco de dados é baixado.
- O servidor de manifesto retorna dois URLs possíveis para o download.
- O cliente atualizador faz o download do banco de dados.
- O banco de dados é descriptografado e armazenado na memória para uso pelo processo de filtro dinâmico.

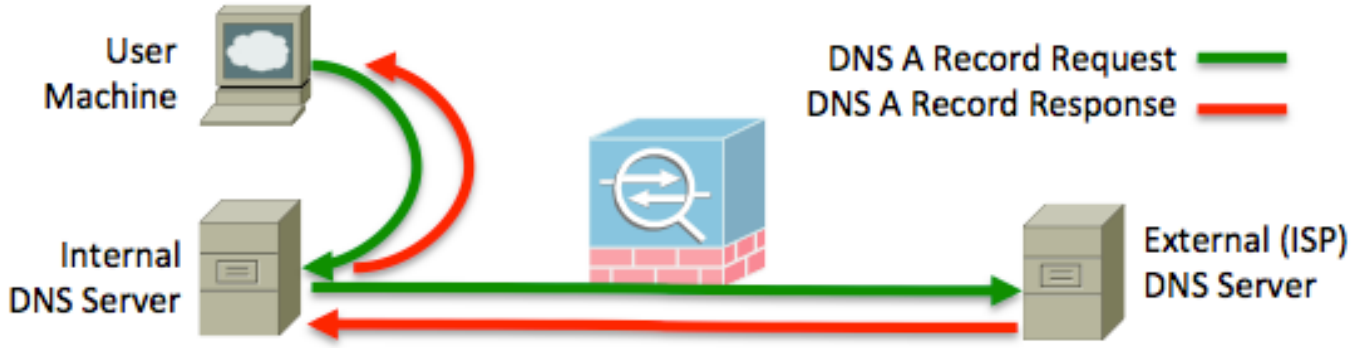
Problemas de conectividade para diferentes servidores de atualização manifestam-se como erros nesta saída e ajudam a solucionar problemas ainda mais. Force o cliente atualizador a ser executado manualmente com o comando **dynamic-filter database fetch**.

## Passo 2: Garanta que o tráfego DNS atravesse este ASA

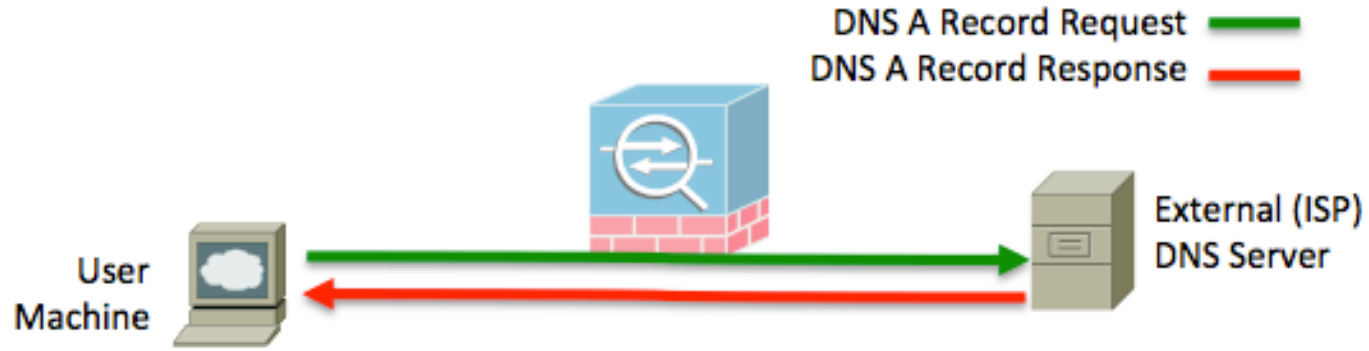
A funcionalidade do filtro de tráfego BotNet do ASA é incorporada dos endereços IP que correspondem aos domínios, de modo que o ASA deve estar em linha com as solicitações e respostas DNS que atravessam a rede. Algumas topologias podem fazer com que o tráfego DNS siga um caminho que não inclua o ASA em questão. A maioria das redes tem servidores DNS internos que atuam como encaminhadores de DNS e caches para usuários internos. Desde que esses servidores, ao encaminharem uma solicitação de DNS para um domínio para o qual não possuem ou não podem responder, encaminhem a solicitação para um servidor que exija atravessar o ASA, nenhum problema deverá ocorrer. Veja estas topologias com e sem servidores

DNS internos:

Essa topologia de exemplo mostra os usuários que apontam para um servidor DNS interno que encaminha para um servidor DNS externo.




Esta topologia de exemplo mostra os usuários que apontam diretamente para um servidor DNS externo.




Em ambos os exemplos de topologia, a chave para uma implantação de filtro de tráfego BotNet funcional é que as solicitações de registro A de DNS para domínios externos devem passar pelo ASA que executa o recurso de rastreamento de DNS. No exemplo do servidor interno, se o servidor DNS interno pegar um caminho de rede diferente para acessar a Internet do que a máquina do usuário, e no processo não atravessar o ASA, a tabela de rastreamento DNS não conterá mapas de IP para domínio causados por solicitações DNS da máquina do usuário e a máquina do usuário pode não ser filtrada como esperado.

Use estas técnicas para verificar se o tráfego DNS passa pelo ASA:

- Verifique a política de serviço. Examine a saída de **show service-policy** para determinar se a inspeção de DNS é aplicada, configurada com a palavra-chave **dynamic-filter-snoop** e vê o tráfego. A contagem de pacotes associada à inspeção de DNS deve aumentar à medida que você faz solicitações de DNS.
- Usar capturas. O recurso de rastreamento de DNS examina os pacotes de DNS que atravessam o ASA, portanto, é importante verificar se os pacotes chegam ao ASA. Use a função de captura integrada do ASA para garantir que o tráfego DNS entre e saia adequadamente desse ASA.

## Passo 3: Verifique o cache de snoop DNS

O dinheiro do snoop DNS deve ser preenchido com mapas IP para domínio. Um único endereço

IP pode ter um número ilimitado de domínios associados a ele. É assim que as empresas que hospedam sites podem atender a milhares de domínios com apenas alguns endereços IP. Digite o comando **show dynamic-filter dns-snoop detail** e veja um dump dos dados atualmente no cache DNS-snoop. Esse é um registro de todos os mapas IP para domínio obtidos pelo ASA com o uso da função de rastreamento DNS da inspeção de DNS. Veja este exemplo de saída:

```
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
```

Neste exemplo, o ASA aprende informações sobre três endereços IP, mas quatro domínios. **magnus.cisco.com** e **raleigh.cisco.com** resolvem para 198.151.100.91. Neste exemplo, dois dos domínios, **magnus.cisco.com** e **badsite.cisco.com** listam como tipo 1. Isso significa que o domínio é encontrado no banco de dados como um domínio da lista negra. Os outros domínios são listados como tipo 0, o que indica que o domínio não está na lista negra ou na lista branca e é apenas um domínio normal.

1. Verifique se as solicitações de DNS de uma máquina de usuário atravessam o firewall de maneira evencial e são processadas pelo snoop de DNS e fazem uma solicitação de DNS. Verifique se há uma entrada correspondente no cache. Teste e use um domínio que seja resolvido, mas que seja obscuro o suficiente para que não tenha sido consultado recentemente e já esteja na tabela. Por exemplo, o domínio asa.cisco.com é escolhido. A ferramenta de linha de comando nslookup é usada para consultar esse nome de host. Veja este exemplo:

   ```
   $ nslookup asa.cisco.com

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

2. Verifique o cache de snoop DNS. Veja este exemplo:

   ```
   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
   ```

A entrada está presente no cache DNS-snoop. Se a entrada não estivesse presente antes do teste de nslookup, isso significaria que o recurso de snoop de DNS funciona e que o ASA funciona corretamente com solicitações e respostas de DNS.

Se a entrada não for exibida, certifique-se de que o tráfego DNS passe pelo ASA. Talvez seja necessário limpar o cache DNS na máquina host ou nos servidores DNS internos, se aplicável, para garantir que as solicitações não sejam atendidas de um cache.

O recurso de rastreamento DNS não suporta EDNS0. Se o cliente ou servidor DNS usa EDNS0, o ASA pode não preencher o cache de snoop DNS com mapas de IP para domínio se a resposta

tiver registros de recursos adicionais presentes. Essa limitação é controlada pela ID de bug da Cisco CSCta36873.

## Passo 4: Teste o filtro de tráfego BotNet com tráfego

Na etapa 3, o cache de snoop DNS mostra que domain badsite.cisco.com está na lista negra. Faça ping no domínio em questão para testar a funcionalidade de botnet. Quando você efetua ping no domínio, é mais seguro do que se tentar carregar o domínio em um navegador da Web. Não teste o recurso de filtro dinâmico usando o navegador da Web porque sua máquina pode estar comprometida se o navegador carregar conteúdo mal-intencionado. Use o Internet Control Message Protocol (ICMP) porque é um método mais seguro e é um teste válido do filtro de tráfego BotNet à medida que ele bloqueia com base no IP e nada específico da porta ou do protocolo.

Se você não conhece um site na lista negra, você pode encontrá-lo facilmente. Digite o comando **dynamic-filter database find <search_term>** para localizar domínios que estão na lista negra e que correspondam ao termo de pesquisa fornecido. Veja este exemplo:

```
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
```

Faça ping em um dos domínios que retornar. Ao fazer ping neste domínio, isso fará com que estas ações ocorram:

1. O host gera uma solicitação DNS para o domínio em questão.
2. A solicitação DNS atravessa o ASA, diretamente da máquina host ou encaminhada por um servidor interno.
3. A resposta DNS atravessa o ASA, seja de volta para a máquina host ou para o servidor interno.
4. A função DNS-snoop preenche esse mapa IP para domínio no cache DNS-snoop.
5. O ASA compara o domínio com o banco de dados de filtro dinâmico e determina uma correspondência. O ASA bloqueia mais tráfego de entrada e saída do IP associado ao domínio mal-intencionado.
6. A máquina host envia uma solicitação de eco ICMP que o ASA descarta porque é destinado a um IP associado a um domínio mal-intencionado.

Quando o ASA descarta o tráfego de teste do ICMP, ele registra um registro do sistema (syslog) semelhante a este exemplo:

```
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
```

A saída do comando **show dynamic-filter statistics** indica conexões que são classificadas e potencialmente descartadas. Veja este exemplo:

```
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
```

O contador classificado só aumenta se uma tentativa de conexão for feita a um endereço IP que esteja na lista negra, na lista branca ou na lista cinza. Nenhum outro tráfego faz com que o contador classificado aumente. Um número baixo para a lista classificada não significa que o ASA não avaliou novas tentativas de conexão contra o filtro de tráfego BotNet. Esse número baixo indica que poucos endereços IP origem ou destino estão na lista negra, na lista branca ou na lista cinza. Use as instruções neste documento para confirmar se o recurso funciona corretamente.

Se o tráfego de teste não for descartado, verifique a configuração para garantir que ela esteja configurada para descartar o tráfego com um nível de ameaça apropriado. Veja este exemplo de configuração, que ativa o filtro de tráfego BotNet globalmente no ASA aqui:

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