Edição do filtro de tráfego de BotNet com ferramenta de segurança adaptável

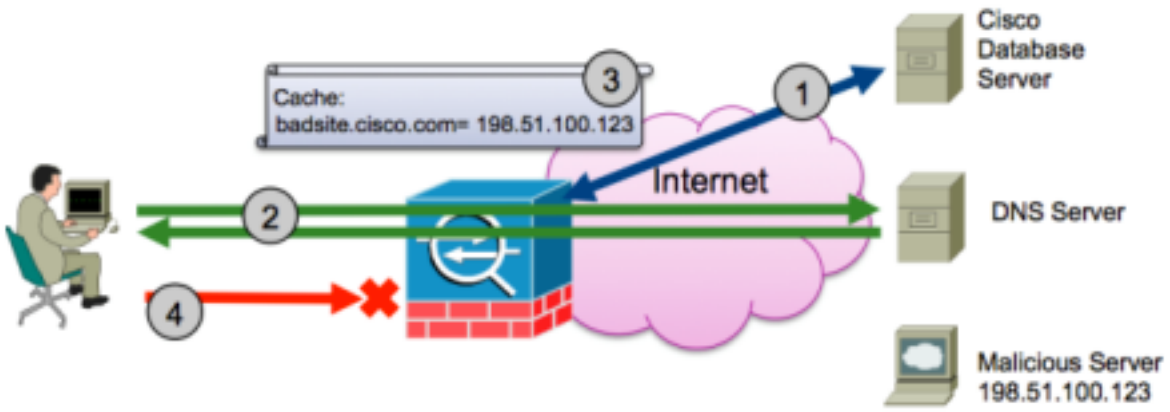
Índice

Introdução

Este documento descreve as etapas para pesquisar defeitos a funcionalidade do filtro de tráfego de BotNet na ferramenta de segurança adaptável (ASA). Para o auxílio com configuração de filtro de tráfego de BotNet, veja este este manual de configuração: Configurando o filtro de tráfego de BotNet.

Informações de Apoio

Os pedidos e as respostas do Domain Name Server dos monitores do filtro de tráfego de BotNet (DNS) entre clientes dos DN internos e servidores DNS externos. Quando uma resposta de DNS é processada, o domínio associado com a resposta está verificado contra o base de dados de domínios maliciosos conhecidos. Se há um fósforo, todo o tráfego mais adicional ao endereço IP de Um ou Mais Servidores Cisco ICM NT atual na resposta de DNS está obstruído. Veja este diagrama.



1. **Verifique o base de dados dinâmico do filtro.** O ASA transfere periodicamente um base de dados atual de domínios e de IP address maliciosos conhecidos. As operações secretas da

Segurança de Cisco (SIO) determinam que os domínios e os endereços IP de Um ou Mais Servidores Cisco ICM NT neste base de dados servem o malware ou o outro índice malicioso.
2. **Assegure-se de que o tráfego DNS cruze o ASA.** Um usuário na rede interna ou em uma máquina infectada na rede interna tenta alcançar um server malicioso a fim transferir o malware ou participar em um BotNet. A fim conectar ao server malicioso, a máquina host deve executar uma pesquisa de DNS. Neste exemplo, a máquina tenta o acesso a badsite.cisco.com. A máquina host envia um pedido DNS a um servidor DNS local ou diretamente a um servidor DNS externo. Em ambas as situações, um pedido DNS deve atravessar o ASA e a resposta de DNS deve igualmente atravessar o mesmo ASA.
3. **Verifique o esconderijo da DNS-espião.** A função da DNS-espião da inspeção DNS, se permitida, monitora o tráfego DNS e determina que uma resposta do Um-registro DNS retornou do servidor DNS. A função da DNS-espião toma o domínio e os endereços IP de Um ou Mais Servidores Cisco ICM NT atuais na resposta do Um-registro e adicionar-los ao esconderijo da DNS-espião. O domínio é verificado contra o base de dados transferido de etapa 1 e um fósforo é encontrado. A resposta de DNS não é deixada cair e é permitida passar completamente.
4. **Teste o filtro de tráfego de BotNet com tráfego.** Porque havia um fósforo em etapa 3, o ASA adiciona uma regra interna que indique que todo o tráfego a ou do IP associado com badsite.cisco.com está deixado cair. O computador contaminado tenta então alcançar o server URL badsite.cisco.com e o tráfego é deixado cair.

Pesquise defeitos trabalhos

Use estas etapas a fim pesquisar defeitos e verificar que a característica trabalha.

Passo 1: Verifique o base de dados dinâmico do filtro

Verifique se o base de dados transferiu e incorpore os **dados do dinâmico-filtro do** comando show. 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 a época do último esforço bem sucedido do base de dados e uma amostra do índice neste base de dados. Se você é executado os **dados do dinâmico-filtro do** comando show, e o comando mostra que nenhum base de dados transferiu, pesquisam defeitos esta etapa primeiramente. Os problemas comuns que impedem que o ASA obtenha o base de dados dinâmico do filtro incluem:

- **Configuração de DNS faltante ou incorreta no ASA.** O cliente dinâmico do updater do filtro deve resolver o nome de host do server da atualização. O DNS deve ser configurado e funcional no ASA. Sibile domínios conhecidos dos dados da linha de comando e determine se o ASA pode resolver nomes de host.
- **Nenhum acesso ao Internet do ASA.** Se o ASA está em uma rede que não tenha acesso ao Internet, ou um dispositivo ascendente obstrui o endereço IP externo do ASA do acesso ao Internet, a atualização falha.
- **O cliente de Atualizador não é permitido**. **O atualizador-cliente do dinâmico-filtro do** comando **permite** deve ser configurado de modo que o ASA possa transferir o base de dados.

Inscreva o Atualizador-**cliente do dinâmico-filtro do** comando debug a fim debugar o base 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 estas etapas que o updater toma quando obtém um base de dados novo:

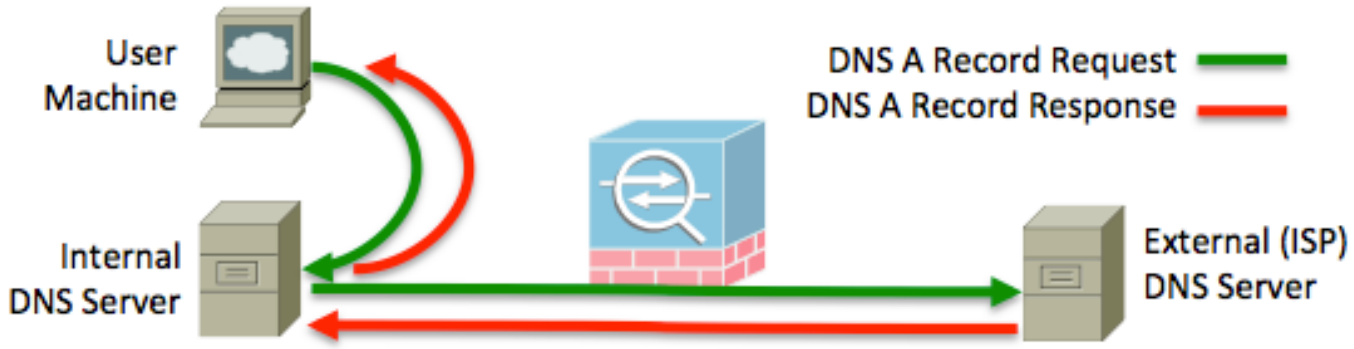
- O updater alcança para fora à URL http://update-manifests.ironport.com a fim determinar que base de dados transfere.
- O server manifesto retorna duas URL possíveis para a transferência.
- O cliente do updater transfere o base de dados.
- O base de dados é decifrado e armazenado na memória para o uso do processo de filtro dinâmico.

Os problemas de conectividade para server diferentes da atualização manifestam como erros nesta saída e ajudam a pesquisar defeitos mais. Force o cliente do updater a ser executado manualmente com o **esforço dinâmico do base de dados do filtro do** comando.

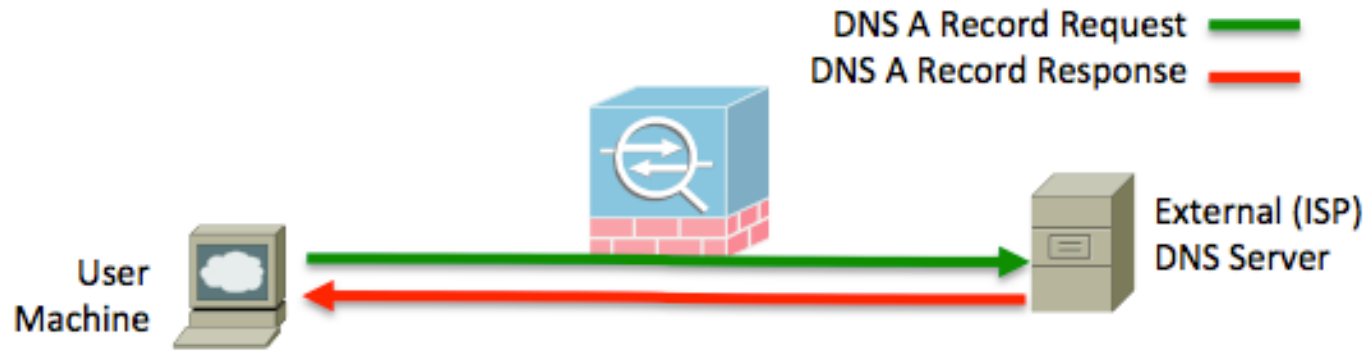
Passo 2: Assegure-se de que tráfego DNS cruze este ASA

A funcionalidade do filtro de tráfego de BotNet do ASA é construída fora dos endereços IP de Um ou Mais Servidores Cisco ICM NT que combinam domínios, assim que o ASA deve ser na linha dos pedidos e das respostas DNS que atravessam a rede. Algumas topologias puderam fazer com que o tráfego DNS tome um trajeto que não incluísse o ASA na pergunta. A maioria de redes têm os servidores internos de DNS que atuam como encaminhadores de DNS e esconderijos para usrs internos. Enquanto estes server, quando os enviam a um pedido DNS para um domínio não possuem nem não podem responder para, enviam o pedido a um server que exija o atravessamento do ASA, nenhum problema deve ocorrer. Veja estas topologias com e sem servidores internos de DNS:

Este exemplo de topologia mostra os usuários que apontam a um servidor interno de DNS qual para a frente a um servidor DNS externo.



Este exemplo de topologia mostra os usuários que apontam diretamente a um servidor DNS externo.



Em ambos os exemplos de topologia, a chave a um desenvolvimento funcional do filtro de tráfego de BotNet é que as solicitações de registro DNS a para domínios externos devem passar com o ASA que executa a característica da DNS-espião. No exemplo do servidor interno, se o servidor interno de DNS toma um caminho de rede diferente a fim alcançar o Internet do que a máquina do usuário, e no processo não atravessa o ASA, a tabela da DNS-espião não conterá os mapas do IP-à-domínio causados por pedidos da máquina DNS do usuário e a máquina do usuário não pôde ser filtrada como esperado.

Use estas técnicas a fim certificar-se do tráfego DNS passe com o ASA:

- Verifique a serviço-política. Olhe a saída da serviço-**política da mostra** a fim determinar se a inspeção DNS é aplicada, configurado com a palavra-chave da dinâmico-filtro-**espião**, e veja o tráfego. O contagem de pacote de informação associado com a inspeção DNS deve incrementar enquanto você faz pedidos DNS.
- Use captações. A característica da DNS-espião olha os pacotes de DNS que atravessam o ASA, assim que é importante que você se certifica dos pacotes alcancem o ASA. Use a função incorporado da captação do ASA a fim certificar-se de que o tráfego DNS incorpora e deixa este ASA corretamente.

Passo 3: Verifique o esconderijo da espião DNS

o dinheiro da DNS-espião deve povoar com mapas do IP-à-domínio. Um único endereço IP de Um ou Mais Servidores Cisco ICM NT pôde ter um número ilimitado de domínios assocated com ele. Isto é como as empresas que hospedam Web site podem servir milhares de domínios com apenas alguns endereços IP de Um ou Mais Servidores Cisco ICM NT. Inscreva o **detalhe da dns-**

espião do dinâmico-filtro do comando show e veja uma descarga dos dados atualmente no esconderijo da DNS-espião. Este é um registro de todos os mapas do IP-à-domínio que o ASA obtém com o uso da função da DNS-espião da inspeção 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 a informação aproximadamente três endereços IP de Um ou Mais Servidores Cisco ICM NT mas quatro domínios. **magnus.cisco.com** e **raleigh.cisco.com** ambos resolvem a 198.151.100.91. Neste exemplo, dois dos domínios, **magnus.cisco.com** e **badsite.cisco.com** alistam como o tipo-1. Isto significa que o domínio está encontrado no base de dados como um domínio põr. Os outros domínios são alistados como o tipo 0, que indica que o domínio não está põr ou whitelisted e é apenas um domínio normal.

1. Certifique-se dos pedidos DNS de uma máquina do usuário atravessem o Firewall e estejam processados eventially pela DNS-espião e faça-se um pedido DNS. Verifique o esconderijo para ver se há uma entrada que combine. Teste e use um domínio que as resoluções mas sejam obscuras bastante que não esteve perguntado recentemente e está já na tabela. Por exemplo, o domínio asa.cisco.com é escolhido. O nslookup do ferramenta comando-linha é usado para perguntar esse hostname. Veja este exemplo:

   ```
   $ nslookup asa.cisco.com

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

2. Verifique o esconderijo da DNS-espião. 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 esta presente no esconderijo da DNS-espião. Se a entrada não estava atual antes do teste do nslookup, significaria que a característica da DNS-espião trabalha e que o ASA trabalha corretamente com pedidos e respostas DNS.

Se a entrada não mostra, assegure-se de que o tráfego DNS passe com o ASA. Você pôde precisar de nivelar o esconderijo DNS na máquina host ou nos servidores internos de DNS, se aplicável, a fim assegurar-se de que os pedidos não estivessem servidos de um esconderijo.

A característica da DNS-espião não apoia EDNS0. Se o cliente de DNS ou o server usam EDNS0, o ASA não pôde povoar o esconderijo da DNS-espião com mapas do IP-à-domínio se a resposta tem os registros dos recursos adicionais atuais. Esta limitação é seguida pela identificação de bug Cisco CSCta36873.

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

Em etapa 3, o esconderijo da DNS-espião mostra que o domínio badsite.cisco.com está na lista negra. Sibile o domínio na pergunta a fim testar a funcionalidade do botnet. Quando você sibila o o domínio, é mais seguro do que se você tenta carregar o domínio em um navegador da Web. Não teste a característica dinâmica do filtro usando seu navegador da Web porque sua máquina pôde ser comprometida se o navegador carrega o índice malicioso. Use o Internet Control Message Protocol (ICMP) porque é um método mais seguro e é um teste válido do filtro de tráfego de BotNet porque obstrui baseado no IP e o nada específicos para mover ou o protocolo.

Se você não sabe de um local põr, você pode encontrar um facilmente. Incorpore o **<search_term> do achado do base de dados do dinâmico-filtro do** comando para encontrar os domínios que são põr e para combinar o termo da busca 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
```

Sibile um dos domínios que retorna. Quando você sibila este domínio, fará com que estas ações ocorram:

1. O host gerencie um pedido DNS para o domínio na pergunta.
2. O pedido DNS atravessa o ASA, diretamente da máquina host ou enviado por um servidor interno.
3. A resposta de DNS atravessa o ASA, de volta à máquina host ou ao servidor interno.
4. A função da DNS-espião povoa este mapa do IP-à-domínio no esconderijo da DNS-espião.
5. O ASA compara o domínio contra o base de dados do dyanmic-filtro e determina um fósforo. O ASA obstrui um tráfego de entrada e de saída mais adicional do IP associado com o domínio malicioso.
6. A máquina host envia a uma requisição de eco ICMP essa as gotas ASA porque é destinada a um IP associado com um domínio malicioso.

Quando o ASA deixa cair o tráfego de teste ICMP, registra um log de sistema (Syslog) similar 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 das **estatísticas do dinâmico-filtro do** comando show indica as conexões que são classificadas e deixadas cair potencialmente. 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 aumenta somente se uma tentativa de conexão é feita a um endereço IP de Um ou Mais Servidores Cisco ICM NT que esteja põr, whitelisted, ou greylisted. Todo tráfego restante não causa classificado ao contrário do aumento. Um número baixo para a lista classificada não significa que o ASA não avaliou tentativas da nova conexão contra o filtro de tráfego de BotNet. Este número baixo indica pelo contrário que pouco a fonte ou os endereços IP de destino estão põr, whitelisted, ou greylisted. Use as instruções neste documento a fim confirmar corretamente as funções da característica.

Se o tráfego de teste não é deixado cair, verifique a configuração a fim assegurar-se de que esteja configurada para deixar cair o tráfego com um nível apropriado da ameaça. Veja esta configuração de exemplo, que permite o filtro de tráfego de BotNet globalmente no ASA aqui:

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