適応型セキュリティ アプライアンスでのボットネット トラフィック フィルタの問題

目次

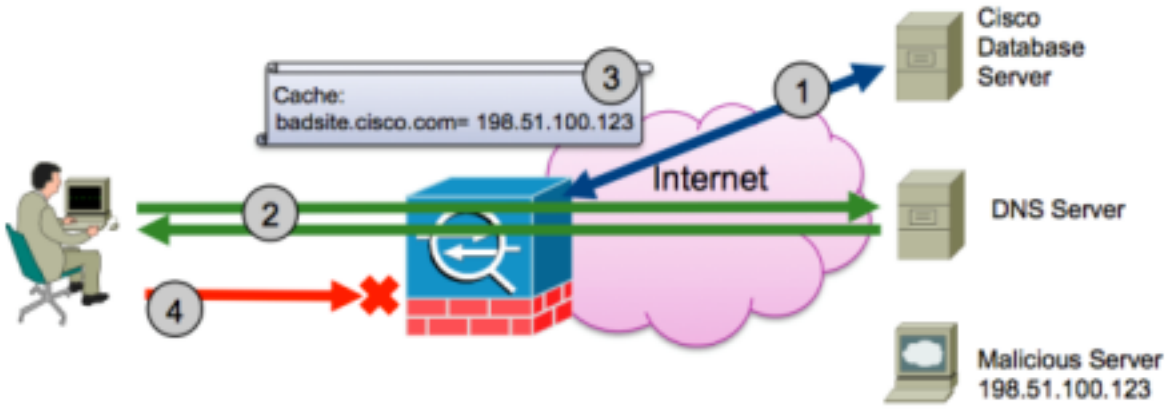
[概要](#)
[背景説明](#)
[作業の流れを解決して下さい](#)
[ステップ 1： 動的フィルター データベースをチェックして下さい](#)
[ステップ 2： DNS トラフィックを交差させますこの ASA を確認して下さい](#)
[ステップ 3： DNS スヌープ キャッシュをチェックして下さい](#)
[ステップ 4： トラフィックの BotNet トラフィック フィルタをテストして下さい](#)

概要

この資料はの BotNet トラフィック フィルタ 機能性を適応型セキュリティ アプライアンス（ASA）ソフトウェア解決するためにステップを記述したものです（ASA）。 BotNet トラフィック フィルタ 設定の支援に関しては、このこのコンフィギュレーション ガイドを参照して下さい: BotNet トラフィック フィルタの設定。

背景説明

ボットネット トラフィック フィルタは、内部 DNS クライアントと外部 DNS サーバとの間で行われるドメイン ネーム サーバ（DNS）のリクエストと応答をモニタします。 DNS 応答を処理する際には、その応答に関連付けられているドメインを、悪意のあるドメインとして既知のドメインのデータベースで照合します。 一致が見つかると、その DNS 応答の IP アドレスへのトラフィックは、それ以降ブロックされます。 このダイアグラムを参照して下さい。



1. **動的フィルター データベースをチェックして下さい。** ASA は定期的に 既知悪意のあるドメインおよび IP アドレスの現在のデータベースをダウンロードします。 このデータベースのドメインおよび IP アドレスが malware か他の悪意のあるコンテンツを機能することを

Cisco の安全保障局オペレーション（SIO）は判別します。
2. **DNS トラフィックが ASA を交差させるようにして下さい。** 内部ネットワークの内部ネットワークまたは感染したマシンのユーザは malware をダウンロードするか、または BotNet に加わるために悪意のあるサーバにアクセスすることを試みます。 悪意のあるサーバに接続するために、ホスト マシンは DNS lookup を行う必要があります。 この例では、マシン試みは badsite.cisco.com にアクセスします。 ホスト マシンはローカルDNSサーバまたは直接外部 DNSサーバに DNS 要求を送信 します。 いずれの場合も、DNS 要求は ASA を横断し、DNS 応答はまた同じ ASA を横断する必要があります。
3. **DNS スヌープ キャッシュをチェックして下さい。** DNS インスペクションの DNS スヌープ機能は、場合有効に された、DNS トラフィックをモニタし、DNS レコード応答が DNSサーバから戻ったことを判別します。 DNS スヌープ 機能はドメインを奪取 し、IP アドレスはレコード応答で示し、DNS スヌープ キャッシュにそれを追加します。 ドメインはステップ 1 からのダウンロードされたデータベースに対してチェックされ、一致はあります。 パススルーへの DNS 応答は廃棄されないし、許可されます。
4. **トラフィックの BotNet トラフィック フィルタをテストして下さい。** ステップ 3 に一致があったので、ASA は badsite.cisco.com と関連付けられる IP に/からのすべてのトラフィックを廃棄されることを示す内部ルールを追加します。 感染させたコンピュータはそれからURL badsite.cisco.com サーバにアクセスすることを試み、トラフィックは廃棄されます。

作業の流れを解決して下さい

解決し、機能が動作することを確認するためにこれらのステップを使用して下さい。

ステップ 1： 動的フィルター データベースをチェックして下さい

データベースがダウンロードした確認し、コマンドを**示します動的フィルター データを**かどうか入力して下さい。 次の出力例を参照してください。

```
# 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
```

この出力では、ASA は最後の正常なデータベース フェッチの時およびこのデータベースのコンテンツのサンプルを示します。 コマンドを実行したら**動的フィルター データを示せば**、データベースがダウンロードしなかったことをコマンドは示しましたり、このステップを最初に解決したものです。 ASA は動的フィルター データベースを得ることを防ぐよくある 問題は下記のものを含んでいます:

- **ASA の損失しているか不正 な DNS 設定。** 動的フィルター アップデータ クライアントはアップデート サーバのホスト名を変換する必要があります。 DNS は設定された ASA で機能である必要があります。 よく知られている な ドメインをコマンド ラインから ping し、ASA がホスト名を解決できたかどうか確認して下さい。
- **ASA からインターネットアクセス無し。** ASA がアクセスできないネットワークにインターネットにあるか、またはアップストリーム デバイスがアクセスからインターネットに ASA の外部 IP アドレスをブロックすれば場合、アップデートは失敗します。
- **アップデータ クライアントは有効に なりません。** コマンド**動的フィルター アップデータ クライアント イネーブルは** ASA がデータベースをダウンロードできるように設定する必要があります。

データベースをデバッグするためにコマンド **デバッグ動的フィルター アップデータ クライアントを**入力して下さい。 コマンドからのこの出力例を参照して下さい:

```
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
```

この出力では、新しいデータベースを得るときアップデータが踏むこれらのステップを表示できます:

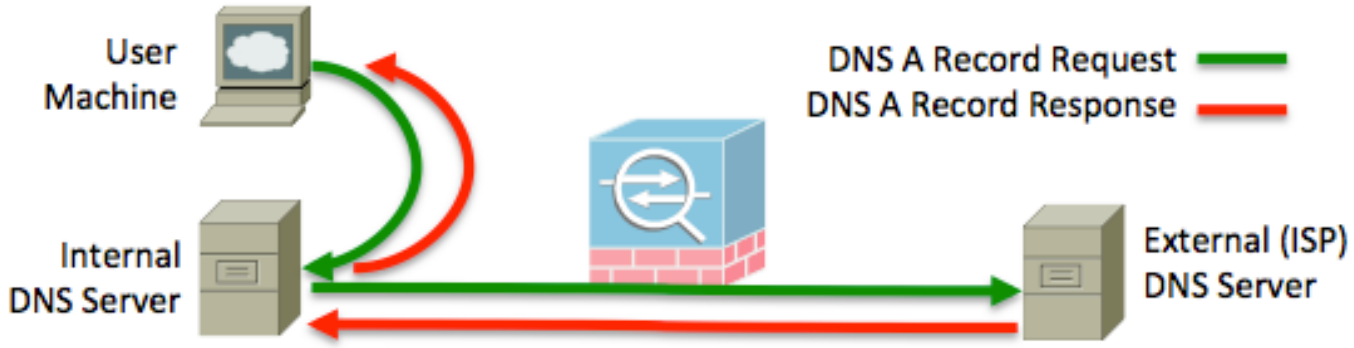
- アップデータは URL http://update-manifests.ironport.com にどのデータベースをダウンロードするか判別するために手を差し伸べます。
- 明らかなサーバはダウンロードのための 2 つの可能性のある URL を戻します。
- アップデータ クライアントはデータベースをダウンロードします。
- データベースは動的フィルター プロセスによって使用のためのメモリで復号化され、保存されます。

異なるアップデート サーバのための接続上の問題はこの出力のエラーとして明示し、更に解決を助けます。 アップデータ クライアントをコマンド**動的フィルター データベース フェッチ**と手動で動作させます。

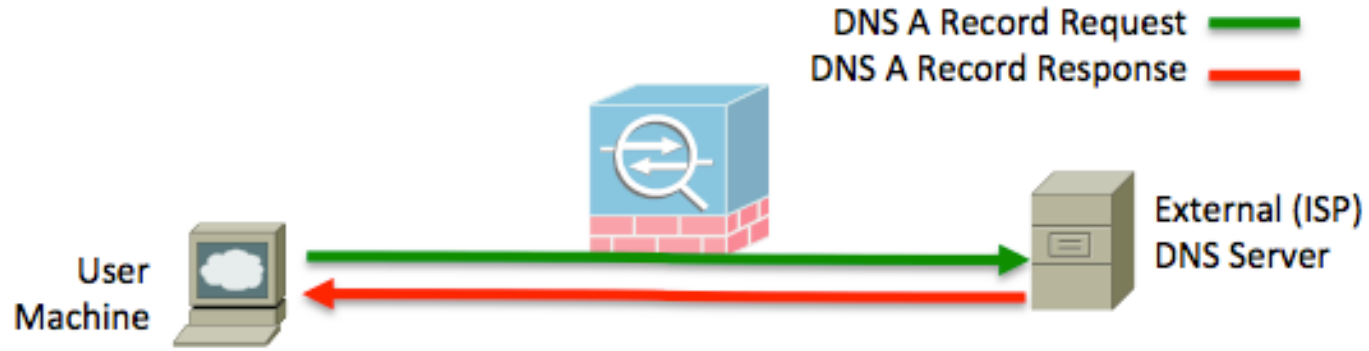
ステップ 2： DNS トラフィックを交差させますこの ASA を確認して下さい

ASA の BotNet トラフィック フィルタ 機能性はドメインを一致する、従って ASA はネットワークを横断する応答および DNS 要求と一直線にある必要があります IP アドレスの構築されます。 いくつかのトポロジーにより DNS トラフィックはパスを選択しますかもしれません疑わしい ASA が含まれていない。 ほとんどのネットワークに内部 usrs のための DNS フォワーダおよびキャッシュとして機能する内部DNSサーバがあります。 これらのサーバがサーバに、ASA を横断することを必要とするドメインのための DNS 要求に転送するとき転送する要求を所有しないし、のために応答できない限り、問題は発生するはずではないです。 内部DNSサーバの有無にかかわらずこれらのトポロジーを参照して下さい:

このサンプルトポロジーは転送するかどれが外部 DNSサーバに内部DNSサーバを指すユーザを示します。



このサンプルトポロジーは外部 DNSサーバを直接指すユーザを示します。



両方のトポロジー例では、機能 BotNet トラフィック フィルタ配備へのキーは外部ドメインのための DNS A-レコード要求がパススルー DNS スヌープ 機能を実行する ASA なることことです。の内部サーバ例ユーザ マシンよりインターネットに達するために内部DNSサーバが別のネットワーク 経路を選択すればとプロセス ASA を横断しません、DNS スヌープ 表はユーザ マシン DNS 要求によって引き起こされた IP にドメイン マップが含まれていないし、ユーザ マシンは予想通りフィルタリングされないかもしれません。

DNS トラフィックが ASA を通ることを確認するためにこれらの手法を使用して下さい:

- サービス ポリシーをチェックして下さい。 DNS インスペクションが適用した、ダイナミック フィルタ **スヌープ** キーワードで設定されて検知 し、トラフィックを見ますかどうか確認するために **show service ポリシー**の出力を。 DNS インスペクションと関連付けられるパケットカウントは DNS 要求をすると同時に増分する必要があります。
- キャプチャを使用して下さい。 パケットが ASA に到着することを確認すること ASA を横断する DNS パケットの DNS スヌープ 機能外観、従ってそれは重要です。 DNS トラフィックがこの ASA をきちんと入力し、出て行くことを確かめるために ASA の組み込みキャプチャ機能を使用して下さい。

手順 3： DNS スヌープ キャッシュをチェックして下さい

DNS スヌープ現金は IP にドメイン マップと読み込む必要があります。 単一 IP アドレスはそれと assocated ドメインの無制限数があるかもしれません。 これは Webサイトをホストする会社がちょうど少数の IP アドレスのドメインの桁をどのように機能できるかです。 コマンドを**示し、動的フィルター dns スヌープ 詳細を**現在見ます DNS スヌープ キャッシュのデータのダンプするを入力して下さい。 これは ASA が DNS インスペクションの DNS スヌープ 機能の使用と得るすべての IP にドメイン マップのレコードです。 次の出力例を参照してください。

```
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
```

この例では、ASA は 3 IP アドレス 4 つのドメインについての情報を学びます。 **magnus.cisco.com** および **raleigh.cisco.com は**両方 198.151.100.91 に解決します。 この例では、ドメインの 2 つはタイプ 1 として、**magnus.cisco.com** および **badsite.cisco.com** リストします。 これはドメインがブラックリストに載せられたドメインとしてデータベースにあることを意味します。 他のドメインはである型 0 としてドメインは示したりちょうど正常なドメイン ブラックリストに載せられないし、または whitelisted、ことをリストされています。

1. ユーザ マシンからの DNS 要求が eventially ファイアウォールを横断し、DNS スヌープによって処理され、確認して下さい DNS 要求をことを作って下さい。 一致するエントリがあるようにキャッシュを確認して下さい。 最近問い合わせられなかったし、表に既にあっていること解決が十分に曖昧であるが、ことドメインをテストし、使用して下さい。 たとえば、ドメイン asa.cisco.com は選択されます。 コマンドラインツール nslookup がそのホスト名を問い合わせるのに使用されています。 例：

   ```
   $ nslookup asa.cisco.com

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

2. DNS スヌープ キャッシュをチェックして下さい。 例：

   ```
   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
   ```

エントリは DNS スヌープ キャッシュにあります。 エントリが nslookup テストの前になかった場合、DNS スヌープ 機能が動作すること、そして ASA が DNS 要求および応答を正しく使用することを意味します。

エントリが示さない場合、DNS トラフィックが ASA を通るようにして下さい。 要求がキャッシュから動作されないようにするためにホスト マシンまたは内部DNSサーバの DNS キャッシュを、該当する場合フラッシュする、必要があるかもしれません。

DNS スヌープ 機能は EDNS0 をサポートしません。 DNS クライアントかサーバが EDNS0 を使用する場合、ASA は応答に現在の追加情報レコードがある場合 IP にドメイン マップとの DNS スヌープ キャッシュを読み込まないかもしれません。 この制限は Cisco バグ ID CSCta36873 によってトラッキングされます。

ステップ 4： トラフィックの BotNet トラフィック フィルタをテストして下さい

ステップ 3 では、DNS スヌープ キャッシュはドメイン badsite.cisco.com がブラックリストにあることを示します。 疑わしい botnet 機能性をテストするためにドメインを ping して下さい。 ドメインを ping するとき、それは Webブラウザでドメインをロードすることを試みる場合安全よりです。 Webブラウザの使用によって動的フィルター機能をテストしないで下さいブラウザが悪意のあるコンテンツをロードする場合マシンが妥協されるかもしれませんので。 ポートかプロト

コルに特定の IP および何もに基づいてブロックするのでそれがより安全な方式で、BotNet トラフィック フィルタの有効なテストであるのでインターネット制御メッセージ プロトコル（ICMP）を使用して下さい。

ブラックリストに載せられたサイトの知らない場合、1 つを容易に見つけることができます。 ブラックリストに載せられる入力し、提供される検索したい用語を一致する ドメインを見つけるためにコマンド**動的フィルター データベース検索 <search_term> を**。 例：

```
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
```

戻るドメインの 1 つを ping して下さい。 このドメインを ping する場合、により発生するこれらの操作を引き起こします:

1. ホストは疑わしいドメインのための DNS 要求を生成します。
2. DNS 要求はホスト マシンからの ASA を、直接または内部サーバによって転送されて横断します。
3. DNS 応答はホスト マシンに戻ってまたは内部サーバに ASA を、横断します。
4. DNS スヌープ 機能は DNS スヌープ キャッシュのこの IP にドメイン マップを読み込みます。
5. ASA は dyanmic フィルタ データベースに対してドメインを比較し、一致を判別します。 ASA は悪意のあるドメインと関連付けられる IP からのそれ以上の着信 および 発信 トラフィックをブロックします。
6. ホスト マシンは ASA ドロップ悪意のあるドメインと関連付けられる IP に向かうのでその ICMP**エコー要求を送信 します。**

ASA は ICMP テストトラフィックを廃棄するとき、この例と同じようなシステムログ（syslog）を記録 します:

```
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
```

コマンドの出力は**動的フィルターが統計情報**分類され、可能性としては破棄される接続を示すことを**示します。** 例：

```
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
```

分類されたカウンターはブラックリストに載せられるか、whitelisted か、または greylisted 接続の試みが IP アドレスに試みられる場合その時だけ増えます。 他のトラフィックによりすべて分類されたカウンターは増加しません。 分類されたリストのための低い数字は ASA が BotNet トラ

フィック フィルタに対して新しい接続試みを評価しなかったことを意味しません。 この低い数字は代りに少数がソースをたどるかまたは宛先が IP アドレス ブラックリストに載せられるか、whitelisted か、または greylisted ことを示します。 機能 機能をきちんと確認するためにこの資料で手順を使用して下さい。

テストトラフィックが廃棄されない場合、水平な適切な脅威のトラフィックを廃棄することを設定するようにするために設定をチェックして下さい。 ASA の BotNet トラフィック フィルタをここにグローバルに 有効に するこの設定 例を参照して下さい、:

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