Cisco Secure Firewall ASA Botnet Traffic Filter Guide

First Published: 2021-06-10

Secure Firewall ASA Botnet Traffic Filter Guide

Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses (the blacklist), and then logs or blocks any suspicious activity.

You can also supplement the Cisco dynamic database with blacklisted addresses of your choosing by adding them to a static blacklist; if the dynamic database includes blacklisted addresses that you think should not be blacklisted, you can manually enter them into a static whitelist. Whitelisted addresses still generate syslog messages, but because you are only targeting blacklist syslog messages, they are informational.

Note If you do not want to use the Cisco dynamic database at all, because of internal requirements, you can use the static blacklist alone if you can identify all the malware sites that you want to target.

About the Botnet Traffic Filter

Botnet Traffic Filter Address Types

Addresses monitored by the Botnet Traffic Filter include:

- Known malware addresses—These addresses are on the blacklist identified by the dynamic database and the static blacklist.
- Known allowed addresses—These addresses are on the whitelist. The whitelist is useful when an address is blacklisted by the dynamic database and also identified by the static whitelist.
- Ambiguous addresses—These addresses are associated with multiple domain names, but not all of these domain names are on the blacklist. These addresses are on the *greylist*.
- Unlisted addresses—These addresses are unknown, and not included on any list.

Botnet Traffic Filter Actions for Known Addresses

You can configure the Botnet Traffic Filter to log suspicious activity, and you can optionally configure it to block suspicious traffic automatically.

Unlisted addresses do not generate any syslog messages, but addresses on the blacklist, whitelist, and greylist generate syslog messages differentiated by type. See Botnet Traffic Filter Syslog Messaging.

Botnet Traffic Filter Databases

The Botnet Traffic Filter uses two databases for known addresses. You can use both databases together, or you can disable use of the dynamic database and use the static database alone.

- About the Dynamic Database
- About the Static Database
- About the DNS Reverse Lookup Cache and DNS Host Cache

About the Dynamic Database

The Botnet Traffic Filter can receive periodic updates for the dynamic database from the Cisco update server. This database lists thousands of known bad domain names and IP addresses.

How the ASA Uses the Dynamic Database

The ASA uses the dynamic database as follows:

1. When the domain name in a DNS reply matches a name in the dynamic database, the Botnet Traffic Filter adds the name and IP address to the DNS *reverse lookup cache*.
2. When the infected host starts a connection to the IP address of the malware site, then the ASA sends a syslog message informing you of the suspicious activity and optionally drops the traffic if you configured the ASA to do so.
3. In some cases, the IP address itself is supplied in the dynamic database, and the Botnet Traffic Filter logs or drops any traffic to that IP address without having to inspect DNS requests.

Database Files

The database files are downloaded from the Cisco update server, and then stored in running memory; they are not stored in flash memory. Be sure to identify a DNS server for the ASA so that it can access the Cisco update server URL. In multiple context mode, the system downloads the database for all contexts using the admin context interface; be sure to identify a DNS server in the admin context.

If you need to delete the database, use:

- CLI—the **dynamic-filter database purge** command.
- ASDM—the **Configuration** > **Firewall** > **Botnet Traffic Filter** > **Botnet Database** pane **Purge Botnet Database** button.

Be sure to first disable use of the database by:

- CLI—entering the **no dynamic-filter use-database** command.

- ASDM—unchecking the **Use Botnet data dynamically downloaded from updater server** check box in the **Configuration** > **Firewall** > **Botnet Traffic Filter** > **Botnet Database** > **Dynamic Database Configuration** area.

Note To filter on the domain names in the dynamic database, you need to enable DNS packet inspection with Botnet Traffic Filter snooping; the ASA looks inside the DNS packets for the domain name and associated IP address.

Database Traffic Types

The dynamic database includes the following types of addresses:

- Ads—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.
- Data Tracking—These are sources associated with companies and websites that offer data tracking and metrics services to websites and other online entities. Some of these also run small advertising networks.
- Spyware—These are sources that distribute spyware, adware, greyware, and other potentially unwanted advertising software. Some of these also run exploits to install such software.
- Malware—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.
- Adult—These are sources associated with adult networks/services offering web hosting for adult content, advertising, content aggregation, registration & billing, and age verification. These may be tied to distribution of adware, spyware, and dialers.
- Bot and Threat Networks—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.

About the Static Database

You can manually enter domain names or IP addresses (host or subnet) that you want to tag as bad names in a blacklist. Static blacklist entries are always designated with a Very High threat level. You can also enter names or IP addresses in a whitelist, so that names or addresses that appear on both the *dynamic* blacklist and the whitelist are identified only as whitelist addresses in syslog messages and reports. Note that you see syslog messages for whitelisted addresses even if the address is not also in the dynamic blacklist.

When you add a domain name to the static database, the ASA waits 1 minute, and then sends a DNS request for that domain name and adds the domain name/IP address pairing to the DNS *host cache*. (This action is a background process, and does not affect your ability to continue configuring the ASA). We recommend also enabling DNS packet inspection with Botnet Traffic Filter snooping. The ASA uses Botnet Traffic Filter snooping instead of the regular DNS lookup to resolve static blacklist domain names in the following circumstances:

- The ASA DNS server is unavailable.
- A connection is initiated during the 1 minute waiting period before the ASA sends the regular DNS request.

If DNS snooping is used, when an infected host sends a DNS request for a name on the static database, the ASA looks inside the DNS packets for the domain name and associated IP address and adds the name and IP address to the DNS reverse lookup cache.

If you do not enable Botnet Traffic Filter snooping, and one of the above circumstances occurs, then that traffic will not be monitored by the Botnet Traffic Filter.

About the DNS Reverse Lookup Cache and DNS Host Cache

When you use the dynamic database with DNS snooping, entries are added to the DNS reverse lookup

cache. If you use the static database, entries are added to the DNS host cache (see About the Static Database, about using the static database with DNS snooping and the DNS reverse lookup cache).

Entries in the DNS reverse lookup cache and the DNS host cache have a time to live (TTL) value provided by the DNS server. The largest TTL value allowed is 1 day (24 hours); if the DNS server provides a larger TTL, it is truncated to 1 day maximum.

For the DNS reverse lookup cache, after an entry times out, the ASA renews the entry when an infected host initiates a connection to a known address, and DNS snooping occurs.

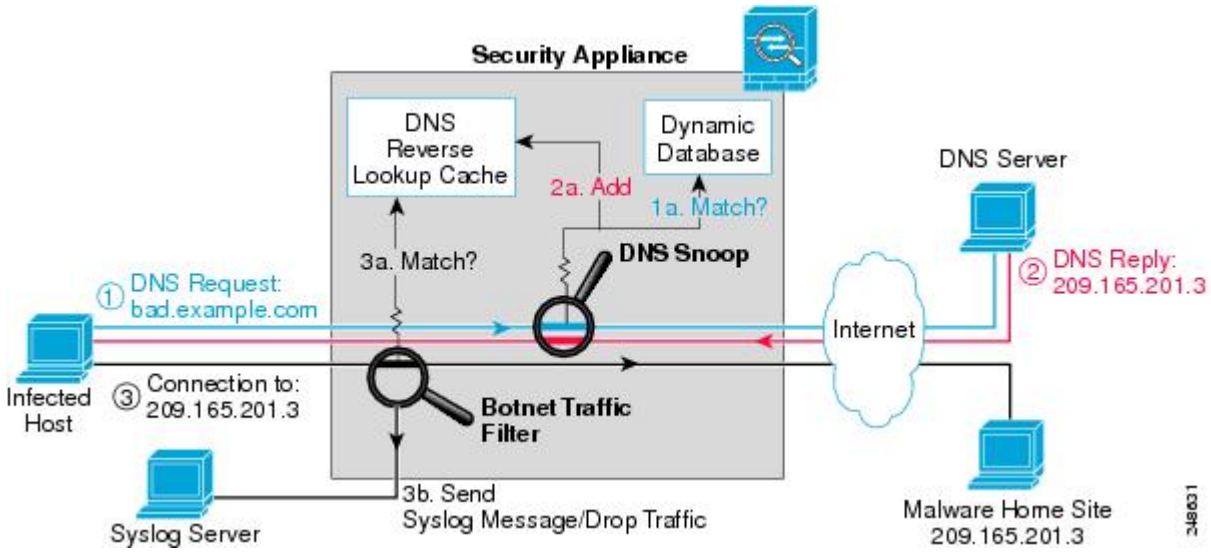
For the DNS host cache, after an entry times out, the ASA periodically requests a refresh for the entry.

For the DNS host cache, the maximum number of blacklist entries and whitelist entries is 1000 each. The number of entries in the DNS reverse lookup cache varies per model.

How the Botnet Traffic Filter Works

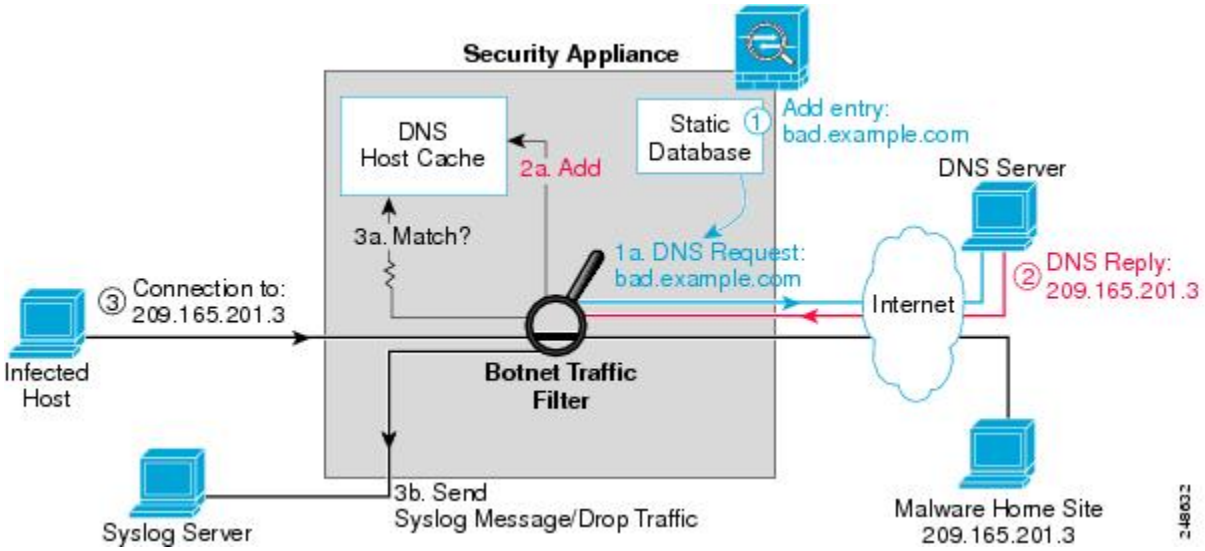
The following figure shows how the Botnet Traffic Filter works with the dynamic database plus DNS inspection with Botnet Traffic Filter snooping.

Figure 1: How the Botnet Traffic Filter Works with the Dynamic Database



The following figure shows how the Botnet Traffic Filter works with the static database.

Figure 2: How the Botnet Traffic Filter Works with the Static Database



Licensing for the Botnet Traffic Filter

Model	License Requirement
ASA Virtual	Standard or Premium License.
All other models	You need the following licenses: • Botnet Traffic Filter License. • Strong Encryption (3DES/AES) License to download the dynamic database.

Prerequisites for the Botnet Traffic Filter

To use the dynamic database, identify a DNS server for the ASA so that it can access the Cisco update server URL. In multiple context mode, the system downloads the database for all contexts using the admin context interface; be sure to identify a DNS server in the admin context.

Guidelines for the Botnet Traffic Filter

Failover Guidelines

Does not support replication of the DNS reverse lookup cache, DNS host cache, or the dynamic database in Stateful Failover.

IPv6 Guidelines

Does not support IPv6.

Model Guidelines

The following ASA models support this feature:

- ASA 5505
- ASA 5510, 5520, 5540, 5550
- ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X
- ASA 5580
- ASA 5585-X
- ASASM

Additional Guidelines and Limitations

- TCP DNS traffic is not supported.
- You can add up to 1000 blacklist entries and 1000 whitelist entries in the static database.
- The packet tracer is not supported.

Defaults for the Botnet Traffic Filter

By default, the Botnet Traffic Filter is disabled, as is use of the dynamic database.

For DNS inspection, which is enabled by default, Botnet Traffic Filter snooping is disabled by default.

Configure the Botnet Traffic Filter

To configure the Botnet Traffic Filter, perform the following tasks:

Procedure

Step 1 Configure the Dynamic Database.

This procedure enables database updates from the Cisco update server, and also enables use of the downloaded dynamic database by the ASA. Disallowing use of the downloaded database is useful in multiple context mode so you can configure use of the database on a per-context basis.

Step 2 (Optional)(Optional) Add Entries to the Static Database.

This procedure lets you augment the dynamic database with domain names or IP addresses that you want to blacklist or whitelist. You might want to use the static database instead of the dynamic database if you do not want to download the dynamic database over the Internet.

Step 3 Enable DNS Snooping.

This procedure enables inspection of DNS packets, compares the domain name with those in the dynamic database or the static database (when a DNS server for the ASA is unavailable), and adds the name and IP address to the DNS reverse lookup cache. This cache is then used by the Botnet Traffic Filter when connections are made to the suspicious address.

Step 4 Enable Traffic Classification and Actions for the Botnet Traffic Filter.

This procedure enables the Botnet Traffic Filter, which compares the source and destination IP address in each initial connection packet to the IP addresses in the dynamic database, static database, DNS reverse lookup cache, and DNS host cache, and sends a syslog message or drops any matching traffic.

Configure the Dynamic Database

This procedure enables database updates, and also enables use of the downloaded dynamic database by the ASA. In multiple context mode, the system downloads the database for all contexts using the admin context interface. You can configure use of the database on a per-context basis. By default, downloading and using the dynamic database is disabled.

Before You Begin

Enable ASA use of a DNS server (in the **Device Management** > **DNS** > **DNS Client** > **DNS Lookup** area). In multiple context mode, the system downloads the database for all contexts using the admin context interface; be sure to identify a DNS server in the admin context.

CLI

Procedure

Step 1 Enable downloading of the dynamic database from the Cisco update server:

dynamic-filter updater-client enable

Example:

```
ciscoasa(config)# dynamic-filter updater-client enable
```

In multiple context mode, enter this command in the system execution space. If you do not have a database already installed on the ASA, it downloads the database after approximately 2 minutes. The update server determines how often the ASA polls the server for future updates, typically every hour.

Step 2 (Multiple context mode only) Change to the context so that you can configure use of the database on a per-context basis:

changeto context *context_name*

Example:

```
ciscoasa# changeto context admin
ciscoasa/admin#
```

Step 3 Enable use of the dynamic database:

dynamic-filter use-database

Example:

```
ciscoasa(config)# dynamic-filter use-database
```

ASDM

Procedure

Step 1 Enable downloading of the dynamic database.

- In Single mode, choose the **Configuration** > **Firewall** > **Botnet Traffic Filter** > **Botnet Database** pane, then check the **Enable Botnet Updater Client** check box.
- In multiple context mode in the System execution space, choose the **Configuration** > **Device Management** > **Botnet Database** pane, then check the **Enable Botnet Updater Client** check box.

This setting enables downloading of the dynamic database from the Cisco update server. In multiple context mode, enter this command in the system execution space. If you do not have a database already installed on the ASA, it downloads the database after approximately 2 minutes. The update server determines how often the ASA polls the server for future updates, typically every hour.

Step 2 (Multiple context mode only) In multiple context mode, click **Apply**. Then change to the context where you want to configure the Botnet Traffic Filter by double-clicking the context name in the Device List.

Step 3 In the Configuration > Firewall > Botnet Traffic Filter > Botnet Database > Dynamic Database Configuration area, check the **Use Botnet data dynamically downloaded from updater server** check box.

Step 4 Click **Apply**.

Step 5 (Optional) If you want to later remove the database from running memory, perform the following steps:

a. Disable use of the database by unchecking the **Use Botnet data dynamically downloaded from updater server** check box.

b. Click **Apply**.

c. Click **Purge Botnet Database**.

d. To redownload the database, re-check the **Use Botnet data dynamically downloaded from updater server** check box.

e. Click **Apply**.

Note The **Fetch Botnet Database** button is for testing purposes only; it downloads and verifies the dynamic database, but does not store it in running memory.

For information about the **Search Dynamic Database** area, see Search the Dynamic Database.

Example

The following multiple mode example enables downloading of the dynamic database, and enables use of the database in context1 and context2:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

The following single mode example enables downloading of the dynamic database, and enables use of the database:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

(Optional) Add Entries to the Static Database

The static database lets you augment the dynamic database with domain names or IP addresses that you want to blacklist or whitelist. Static blacklist entries are always designated with a Very High threat level. See About the Static Database for more information.

Before You Begin

- In multiple context mode, perform this procedure in the context execution space.
- Enable ASA use of a DNS server (in the **Device Management** > **DNS** > **DNS Client** > **DNS Lookup** area). In multiple context mode, enable DNS per context.

CLI

Procedure

Step 1 Edit the Botnet Traffic Filter blacklist:

dynamic-filter blacklist

Example:

```
ciscoasa(config)# dynamic-filter blacklist
```

Step 2 Add to the blacklist. You can add up to 1000 blacklist entries.

- Add a name to the blacklist:

  name *domain_name*

Example:

```
ciscoasa(config-llist)# name bad.example.com
```

You can enter this command multiple times for multiple entries.

- Add an IP address to the blacklist:

  address *ip_address mask*

Example:

```
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.255
```

You can enter this command multiple times for multiple entries. The *mask* can be for a single host or for a subnet.

Step 3 Edit the Botnet Traffic Filter whitelist:

dynamic-filter whitelist

Example:

```
ciscoasa(config)# dynamic-filter whitelist
```

Step 4 Add to the whitelist. You can add up to 1000 whitelist entries.

- Add a name to the whitelist:

  name *domain_name*

Example:

```
ciscoasa(config-llist)# name good.example.com
```

You can enter this command multiple times for multiple entries.

- Add an IP address to the whitelist:

  address *ip_address mask*

Example:

```
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

You can enter this command multiple times for multiple entries. The *mask* can be for a single host or for a subnet.

ASDM

Procedure

Step 1 1Choose the **Configuration** > **Firewall** > **Botnet Traffic Filter** > **Black** or **White List** pane, click **Add** for the Whitelist or Blacklist.

Step 2 In the **Addresses** field, enter one or more domain names, IP addresses, and IP address/netmasks.

Enter multiple entries separated by commas, spaces, lines, or semi-colons. You can enter up to 1000 entries for each type.

Step 3 Click **OK**.

Step 4 Click **Apply**.

Example

The following example creates entries for the blacklist and whitelist:

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

Enable DNS Snooping

This procedure enables inspection of DNS packets and enables Botnet Traffic Filter snooping, which compares the domain name with those on the dynamic database or static database, and adds the name and IP address to the Botnet Traffic Filter DNS reverse lookup cache. This cache is then used by the Botnet Traffic Filter when connections are made to the suspicious address.

The following procedure creates an interface-specific service policy for DNS inspection.

Before You Begin

- In multiple context mode, perform this procedure in the context execution space.
- TCP DNS traffic is not supported.
- Default DNS Inspection Configuration and Recommended Configuration—The default configuration for DNS inspection inspects all UDP DNS traffic on all interfaces, and does not have DNS snooping enabled.

  We suggest that you enable DNS snooping only on interfaces where external DNS requests are going. Enabling DNS snooping on all UDP DNS traffic, including that going to an internal DNS server, creates unnecessary load on the ASA.

  For example, if the DNS server is on the outside interface, you should enable DNS inspection with snooping for all UDP DNS traffic on the outside interface.

CLI

Procedure

Step 1 Create a class map to identify the traffic for which you want to inspect DNS:

class-map *name*

Example:

```
ciscoasa(config)# class-map dynamic-filter_snoop_class
```

Step 2 Specify traffic for the class map:

match *parameters*

Example:

```
ciscoasa(config-cmap)# match port udp eq domain
```

For example, you can specify an ACL for DNS traffic to and from certain addresses, or you can specify all UDP DNS traffic.

Step 3 Add or edit a policy map so you can set the actions to take with the class map traffic:

policy-map *name*

Example:

```
ciscoasa(config)# policy-map dynamic-filter_snoop_policy
```

Step 4 Identify the class map you created in Step 1:

class *name*

Example:

```
ciscoasa(config-pmap)# class dynamic-filter_snoop_class
```

Step 5 Enable DNS inspection with Botnet Traffic Filter snooping:

inspect dns [*map_name*] **dynamic-filter-snoop**

Example:

```
ciscoasa(config)# policy-map dynamic-filter_snoop_policy
```

To use the default DNS inspection policy map for the *map_name*, specify **preset_dns_map** for the map name.

Step 6 Activate the policy map on an interface:

service-policy *policymap_name* **interface** *interface_name*

Example:

```
ciscoasa(config)# service-policy dynamic-filter_snoop_policy interface outside
```

The interface-specific policy overrides the global policy. You can only apply one policy map to each interface.

ASDM

Procedure

Step 1 Configure DNS inspection for traffic that you want to snoop using the Botnet Traffic Filter. See the configuration guide for the DNS inspection procedure. See the Before You Begin section for guidelines on configuring DNS inspection.

Note You can also configure DNS snooping directly in the **Configuration** > **Firewall** > **Service Policy Rules** > **Rule Actions** > **Protocol Inspection** > **Select DNS Inspect Map** dialog box by checking the **Enable Botnet traffic filter DNS snooping** check box.

Step 2 Choose the **Configuration** > **Firewall** > **Botnet Traffic Filter** > **DNS Snooping** pane.

All existing service rules that include DNS inspection are listed in the table.

Step 3 For each rule for which you want to enable DNS snooping, in the **DNS Snooping Enabled** column, check the check box.

Step 4 Click **Apply**.

Example

The following recommended configuration creates a class map for all UDP DNS traffic, enables DNS inspection and Botnet Traffic Filter snooping with the default DNS inspection policy map, and applies it to the outside interface:

```
ciscoasa(config)# class-map dynamic-filter_snoop_class
ciscoasa(config-cmap)# match port udp eq domain
ciscoasa(config-cmap)# policy-map dynamic-filter_snoop_policy
ciscoasa(config-pmap)# class dynamic-filter_snoop_class
```

```
ciscoasa(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
ciscoasa(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

Enable Traffic Classification and Actions for the Botnet Traffic Filter

This procedure enables the Botnet Traffic Filter. The Botnet Traffic Filter compares the source and destination IP address in each initial connection packet to the following:

- Dynamic database IP addresses
- Static database IP addresses
- DNS reverse lookup cache (for dynamic database domain names)
- DNS host cache (for static database domain names)

When an address matches, the ASA sends a syslog message. The only additional action currently available is to drop the connection.

Before You Begin

- In multiple context mode, perform this procedure in the context execution space.
- Recommended Configuration—Although DNS snooping is not required, we recommend configuring DNS snooping for maximum use of the Botnet Traffic Filter (see Enable DNS Snooping). Without DNS snooping for the dynamic database, the Botnet Traffic Filter uses only the static database entries, plus any IP addresses in the dynamic database; domain names in the dynamic database are not used.

  We recommend enabling the Botnet Traffic Filter on all traffic on the Internet-facing interface, and enabling dropping of traffic with a severity of moderate and higher.

CLI

Procedure

Step 1 (Optional) Identify the traffic that you want to monitor or drop:

access-list *access_list_name* **extended** {**deny** | **permit**} *protocol source_address mask* [*operator port*] *dest_address mask* [*operator port*]

Example:

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# access-list dynamic-filter_acl_subset extended permit tcp 10.1.1.0
255.255.255.0 any eq 80
```

If you do not create an ACL for monitoring, by default you monitor all traffic. You can optionally use an ACL to identify a subset of monitored traffic that you want to drop; be sure the ACL is a subset of the monitoring ACL. See the general operations configuration guide for more information about creating an ACL.

Step 2 Enable the Botnet Traffic Filter; without any options, this command monitors all traffic:

dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

Example:

```
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
```

We recommend enabling the Botnet Traffic Filter on all traffic on the Internet-facing interface using the **interface** keyword.

You can optionally limit monitoring to specific traffic by using the **classify-list** keyword with an ACL.

You can enter this command one time for each interface and one time for the global policy (where you do not specify the **interface** keyword). Each interface and global command can have an optional **classify-list** keyword. Any interface-specific commands take precedence over the global command.

Step 3 (Optional) Automatically drop malware traffic:

dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** {**eq** *level* | **range** *min max* }]

Example:

```
ciscoasa(config)# dynamic-filter drop blacklist interface outside action-classify-list
dynamic-filter_acl_subset threat-level range moderate very-high
```

To manually drop traffic, see Block Botnet Traffic Manually.

Be sure to first configure a **dynamic-filter enable** command to monitor any traffic you also want to drop.

You can set an interface policy using the **interface** keyword, or a global policy (where you do not specify the **interface** keyword). Any interface-specific commands take precedence over the global command. You can enter this command multiple times for each interface and global policy.

The **action-classify-list** keyword limits the traffic dropped to a subset of monitored traffic. The dropped traffic must always be equal to or a subset of the monitored traffic. For example, if you specify an ACL for the **dynamic-filter enable** command, and you specify the **action-classify-list** for this command, then it must be a subset of the **dynamic-filter enable** ACL.

Make sure you do not specify overlapping traffic in multiple commands for a given interface/global policy. Because you cannot control the exact order that commands are matched, overlapping traffic means you do not know which command will be matched. For example, do not specify both a command that matches all traffic (without the **action-classify-list** keyword) as well as a command with the **action-classify-list** keyword for a given interface. In this case, the traffic might never match the command with the **action-classify-list** keyword. Similarly, if you specify multiple commands with the **action-classify-list** keyword, make sure each ACL is unique, and that the networks do not overlap.

You can additionally limit the traffic dropped by setting the threat level. If you do not explicitly set a threat level, the level used is **threat-level range moderate very-high**.

Note We highly recommend using the default setting unless you have strong reasons for changing the setting.

The *level* and *min* and *max* options are:

- **very-low**
- **low**
- **moderate**
- **high**
- **very-high**

Note Static blacklist entries are always designated with a Very High threat level.

Step 4 (Optional) If you configured the **dynamic-filter drop blacklist** command, then this command treats greylisted traffic as blacklisted traffic for dropping purposes:

dynamic-filter ambiguous-is-black

If you do not enable this command, greylisted traffic will not be dropped. See Botnet Traffic Filter Address Types, for more information about the greylist.

ASDM

Procedure

Step 1 Choose the **Configuration** > **Firewall** > **Botnet Traffic Filter** > **Traffic Settings** pane.

Step 2 To enable the Botnet Traffic Filter on specified traffic, perform the following steps:

a. In the **Traffic Classification** area, check the **Traffic Classified** check box for each interface on which you want to enable the Botnet Traffic Filter.

You can configure a global classification that applies to all interfaces by checking the Traffic Classified check box for Global (All Interfaces). If you configure an interface-specific classification, the settings for that interface overrides the global setting.

b. For each interface, from the **ACL Used** drop-down list choose either **--ALL TRAFFIC--** (the default), or any ACL configured on the ASA.

For example, you might want to monitor all port 80 traffic on the outside interface.

To add or edit ACLs, click **Manage ACL** to bring up the **ACL Manager**. See the general operations configuration guide for more information.

Step 3 (Optional) To treat greylisted traffic as blacklisted traffic for action purposes, in the **Ambiguous Traffic Handling** area, check the **Treat ambiguous (greylisted) traffic as malicious (blacklisted) traffic** check box.

If you do not enable this option, greylisted traffic will not be dropped if you configure a rule in the **Blacklisted Traffic Actions** area. See Botnet Traffic Filter Address Types, for more information about the greylist.

Step 4 (Optional) To automatically drop malware traffic, perform the following steps.

To manually drop traffic, see Block Botnet Traffic Manually.

a. In the **Blacklisted Traffic Actions** area, click **Add**.

The **Add Blacklisted Traffic Action** dialog box appears.

b. From the **Interface** drop-down list, choose the interface on which you want to drop traffic. Only interfaces on which you enabled Botnet Traffic Filter traffic classification are available.

c. In the **Threat Level** area, choose one of the following options to drop traffic specific threat levels. The default level is a range between **Moderate** and **Very High**.

Note We highly recommend using the default setting unless you have strong reasons for changing the setting.

- **Value**—Specify the threat level you want to drop:
  - **Very Low**
  - **Low**
  - **Moderate**
  - **high**
  - **very-high**

    Note Static blacklist entries are always designated with a Very High threat level.

- **Range**—Specify a range of threat levels.

d. In the **ACL Used** area, from the **ACL Used** drop-down list choose either **--ALL TRAFFIC--** (the default), or any ACL configured on the ASA.

Note Be sure the ACL is a subset of the traffic you specified in the Traffic Classification area.

To add or edit ACLs, click **Manage** to bring up the **ACL Manager**. See general operations configuration guide for more information.

e. Click **OK**.

You return to the **Traffic Settings** pane.

f. If you want to apply additional rules to a given interface, repeat steps a through e.

Make sure you do not specify overlapping traffic in multiple rules for a given interface. Because you cannot control the exact order that rules are matched, overlapping traffic means you do not know which command will be matched. For example, do not specify both a rule that matches --ALL TRAFFIC-- as well as a command with and ACL for a given interface. In this case, the traffic might never match the command with the ACL. Similarly, if you specify multiple commands with ACLs, make sure each ACL is unique, and that the networks do not overlap.

Step 5 Click **Apply**.

Example

The following recommended configuration monitors all traffic on the outside interface and drops all traffic at a threat level of moderate or higher:

```
ciscoasa(config)# dynamic-filter enable interface outside
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

If you decide not to monitor all traffic, you can limit the traffic using an ACL. The following example monitors only port 80 traffic on the outside interface, and drops traffic threat level very-high only:

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside threat-level eq
very-high
```

Manage the Botnet Traffic Filter

Block Botnet Traffic Manually

If you choose not to block malware traffic automatically (see Enable Traffic Classification and Actions for the Botnet Traffic Filter), you can block traffic manually by configuring an access rule to deny traffic, or by using the **shun** command to block all traffic to and from a host. For some messages, you can automatically configure access rules in ASDM.

For example, you receive the following syslog message:

```
ASA-4-338002: Dynamic Filter permitted black listed TCP traffic from inside:10.1.1.45/6798
(209.165.201.1/7890) to outside:209.165.202.129/80 (209.165.202.129/80), destination
209.165.202.129 resolved from dynamic list: bad.example.com
```

You can then perform one of the following actions:

- Create an access rule to deny traffic.

  For example, using the syslog message above, you might want to deny traffic from the infected host at 10.1.1.45 to the malware site at 209.165.202.129. Or, if there are many connections to different blacklisted addresses, you can create an ACL to deny all traffic from 10.1.1.45 until you resolve the infection on the host computer. For example, the following commands deny all traffic from 10.1.1.5 to 209.165.202.129, but permits all other traffic on the inside interface:

  ```
  ciscoasa(config)# access-list BLOCK_OUT extended deny ip host 10.1.1.45 host
  209.165.202.129
  ciscoasa(config)# access-list BLOCK_OUT extended permit ip any any
  ciscoasa(config)# access-group BLOCK_OUT in interface inside
  ```

  For the following syslog messages, a reverse access rule can be automatically created from the Real Time Log Viewer:

  – 338001, 338002, 338003, 338004 (blacklist)

  – 338201, 338202 (greylist)

  Note If you create a reverse access rule form a Botnet Traffic Filter syslog message, and you do not have any other access rules applied to the interface, then you might inadvertently block all traffic. Normally, without an access rule, all traffic from a high security to a low security interface is allowed. But when you apply an access rule, all traffic is denied except traffic that you explicitly permit. Because the reverse access rule is a deny rule, be sure to edit the resulting access policy for the interface to permit other traffic.

  ACLs block all future connections. To block the current connection, if it is still active, enter the **clear conn** command. For example, to clear only the connection listed in the syslog message, enter the **clear conn address 10.1.1.45 address 209.165.202.129** command. See the command reference for more information.

- Shun the infected host.

  Shunning blocks all connections from the host, so you should use an ACL if you want to block connections to certain destination addresses and ports. To shun a host, enter the following command (for ASDM, use Tools > Command Line Interface). To drop the current connection as well as blocking all future connections, enter the destination address, source port, destination port, and optional protocol.

  ```
  ciscoasa(config)# shun src_ip [dst_ip src_port dest_port [protocol]]
  ```

  For example, to block future connections from 10.1.1.45, and also drop the current connection to the malware site in the syslog message, enter:

  ```
  ciscoasa(config)# shun 10.1.1.45 209.165.202.129 6798 80
  ```

After you resolve the infection, be sure to remove the ACL or the shun. To remove the shun, enter **no shun** *src_ip*.

Search the Dynamic Database

If you want to check if a domain name or IP address is included in the dynamic database, you can search the database for a string.

CLI

Procedure

Search the dynamic database for a domain name or IP address:

dynamic-filter database find *string*

Example:

```
ciscoasa# dynamic-filter database find bad.example.com
```

The *string* can be the complete domain name or IP address, or you can enter part of the name or address, with a minimum search string of 3 characters. If there are multiple matches, the first two matches are shown. To refine your search for a more specific match, enter a longer string.

Note Regular expressions are not supported for the database search

ASDM

Procedure

Step 1 Go to the **Search Dynamic Database** area:

- In Single mode or within a context, choose the **Configuration** > **Firewall** > **Botnet Traffic Filter** > **Botnet Database Update** pane.
- In multiple context mode in the System execution space, choose the **Configuration** > **Device Management** > **Botnet Database Update** pane.

Step 2 In the **Search** string field, enter a string at least 3 characters in length, and click **Find Now**.

The first two matches are shown. To refine your search for a more specific match, enter a longer string.

Step 3 To clear the displayed matches and the search string, click **Clear**, or you can just enter a new string and click **Find Now** to get a new display.

Example

The following example searches on the string “example.com”, and finds 1 match:

```
ciscoasa# dynamic-filter database find bad.example.com

   bad.example.com
Found 1 matches
```

The following example searches on the string “bad”, and finds more than 2 matches:

```
ciscoasa# dynamic-filter database find bad

   bad.example.com
   bad.example.net
Found more than 2 matches, enter a more specific string to find an exact
match
```

Monitoring the Botnet Traffic Filter

Whenever a known address is classified by the Botnet Traffic Filter, then a syslog message is generated. You can also monitor Botnet Traffic Filter statistics and other parameters by entering commands on the ASA. This section includes the following topics:

- Botnet Traffic Filter Syslog Messaging
- Monitoring Filter Statistics
- Monitoring the Botnet Traffic Filter Server and Dynamic Database
- Monitoring DNS Snooping

Botnet Traffic Filter Syslog Messaging

The Botnet Traffic Filter generates detailed syslog messages numbered 338nnn. Messages differentiate between incoming and outgoing connections, blacklist, whitelist, or greylist addresses, and many other variables. (The greylist includes addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist.)

See the syslog messages guide for detailed information about syslog messages.

For the following syslog messages, a reverse access rule can be automatically created from the Real Time Log Viewer:

- 338001, 338002, 338003, 338004 (blacklist)
- 338201, 338202 (greylist)

Monitoring Filter Statistics

- **Home** > **Firewall Dashboard**

  Shows the Top Botnet Traffic Filter Hits, which shows reports of the top 10 malware sites, ports, and infected hosts. This report is a snapshot of the data, and may not match the top 10 items since the statistics started to be collected. If you right-click an IP address, you can invoke the whois tool to learn more about the botnet site.

  – Top Malware Sites—Shows top malware sites.

  – Top Malware Ports—Shows top malware ports.

  – Top Infected Hosts—Shows the top infected hosts.

- **show dynamic-filter statistics** [**interface** *name*] [**detail**]

  Monitoring > **Botnet Traffic Filter** > **Statistics**

  Shows how many connections were classified as whitelist, blacklist, and greylist connections, and how many connections were dropped. (The greylist includes addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist.) The detail optionshows how many packets at each threat level were classified or dropped.

  To clear the statistics, enter the **clear dynamic-filter statistics** [**interface** *name*] command.

  The following is sample output from the **show dynamic-filter statistics** command:

```
ciscoasa# show dynamic-filter statistics
Enabled on interface outside
 Total conns classified 11, ingress 11, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 11, dropped 5, ingress 11, egress 0
Enabled on interface inside
 Total conns classified 1182, ingress 1182, egress 0
 Total whitelist classified 3, ingress 3, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 1179, dropped 1000, ingress 1179, egress 0
```

- **show dynamic-filter reports top** [**malware-sites** | **malware-ports** | **infected-hosts**]

  Monitoring > **Botnet Traffic Filter** > **Real-time Reports**

  Generates reports of the top 10 malware sites, ports, and infected hosts monitored. The top 10 malware-sites report includes the number of connections dropped, and the threat level and category of each site. This report is a snapshot of the data, and may not match the top 10 items since the statistics started to be collected.

  (ASDM) If you right-click a site IP address, you can invoke the whois tool to learn more about the malware site. Reports can be saved as an HTML file.

  To clear the report data, enter the **clear dynamic-filter reports top** command.

  The following is sample output from the **show dynamic-filter reports top malware-sites** command:

```
ciscoasa# show dynamic-filter reports top malware-sites
Site                              Connections logged dropped Threat Level Category
-------------------------------------------------------------------------------------
bad1.example.com (10.67.22.34)                  11      0         2       Botnet
bad2.example.com (209.165.200.225)               8      8         3       Virus
bad1.cisco.example(10.131.36.158)                6      6         3       Virus
bad2.cisco.example(209.165.201.1)                2      2         3       Trojan
```

```
horrible.example.net(10.232.224.2)                2     2         3      Botnet
nono.example.org(209.165.202.130)                 1     1         3      Virus

Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

The following is sample output from the **show dynamic-filter reports top malware-ports** command:

```
ciscoasa# show dynamic-filter reports top malware-ports
Port                                        Connections logged
------------------------------------------------------------------------
tcp 1000                                                  617
tcp 2001                                                  472
tcp 23                                                     22
tcp 1001                                                   19
udp 2000                                                   17
udp 2001                                                   17
tcp 8080                                                    9
tcp 80                                                      3
tcp >8192                                                   2

Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

The following is sample output from the **show dynamic-filter reports top infected-hosts** command:

```
ciscoasa# show dynamic-filter reports top infected-hosts
Host                                        Connections logged
------------------------------------------------------------------------
10.10.10.51(inside)                                    1190
10.12.10.10(inside)                                      10
10.10.11.10(inside)                                       5

Last clearing of the top infected-hosts report: at 13:41:06 UTC Jul 15 2009
```

- **show dynamic-filter reports infected-hosts** {**max-connections** | **latest-active** | **highest-threat** | **subnet** *ip_address netmask* | **all**}

  Monitoring > **Botnet Traffic Filter** > **Infected Hosts**

  Generates reports about infected hosts. These reports contain detailed history about infected hosts, showing the correlation between infected hosts, visited malware sites, and malware ports. The **max-connections** option shows the 20 infected hosts with the most number of connections. The **latest-active** option shows the 20 hosts with the most recent activity. The **highest-threat** option shows the 20 hosts that connected to the malware sites with the highest threat level. The **subnet** option shows up to 20 hosts within the specified subnet. The **all** keyword shows all buffered infected-hosts information. This display might include thousands of entries. You might want to use ASDM to generate an HTML file instead of using the CLI.

  (ASDM) Reports can be saved as an HTML file, as either the Current View or the Whole Buffer. The Whole Buffer option shows all buffered infected-hosts information.

  To clear the report data, enter the **clear dynamic-filter reports infected-hosts** command.

Monitoring the Botnet Traffic Filter Server and Dynamic Database

- **show dynamic-filter updater-client**

  Monitoring > **Botnet Traffic Filter** > **Updater Client**

  Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.

- **show dynamic-filter data**

Monitoring > **Botnet Traffic Filter** > **Dynamic Database**

Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.

Monitoring DNS Snooping

show dynamic-filter dns-snoop [detail]

Monitoring > **Botnet Traffic Filter** > **DNS Snooping**

Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names. All inspected DNS data is included in this output, and not just matching names in the blacklist. DNS data from static entries are not included.

To clear the DNS snooping data, enter the **clear dynamic-filter dns-snoop** command.

Viewing Botnet Traffic Rules

show asp table dynamic-filter [hits]

Monitoring > **Botnet Traffic Filter** > **ASP Table Hits**

Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.

Examples for the Botnet Traffic Filter

This section includes the recommended configuration for single and multiple context mode, as well as other possible configurations. This section includes the following topics:

- Recommended Configuration Example
- Other Examples

Recommended Configuration Example

The following recommended example configuration for single context mode enables downloading of the dynamic database, and enables use of the database. It creates a class map for all UDP DNS traffic, enables DNS inspection and Botnet Traffic Filter snooping with the default DNS inspection policy map, and applies it to the outside interface, the Internet-facing interface.

Example1-1 Single Mode Botnet Traffic Filter Recommended Example

```
dynamic-filter updater-client enable
dynamic-filter use-database
class-map dynamic-filter_snoop_class
  match port udp eq domain
policy-map dynamic-filter_snoop_policy
  class dynamic-filter_snoop_class
    inspect dns preset_dns_map dynamic-filter-snoop
service-policy dynamic-filter_snoop_policy interface outside
dynamic-filter enable interface outside
dynamic-filter drop blacklist interface outside
```

The following recommended example configuration for multiple context mode enables the Botnet Traffic Filter for two contexts:

Example 1-2 Multiple Mode Botnet Traffic Filter Recommended Example

```
dynamic-filter updater-client enable
changeto context context1
dynamic-filter use-database
class-map dynamic-filter_snoop_class
  match port udp eq domain
policy-map dynamic-filter_snoop_policy
  class dynamic-filter_snoop_class
    inspect dns preset_dns_map dynamic-filter-snoop
service-policy dynamic-filter_snoop_policy interface outside
dynamic-filter enable interface outside
dynamic-filter drop blacklist interface outside
changeto context context2
dynamic-filter use-database
class-map dynamic-filter_snoop_class
  match port udp eq domain
policy-map dynamic-filter_snoop_policy
  class dynamic-filter_snoop_class
    inspect dns preset_dns_map dynamic-filter-snoop
service-policy dynamic-filter_snoop_policy interface outside
dynamic-filter enable interface outside
dynamic-filter drop blacklist interface outside
```

Other Examples

The following sample configuration adds static entries are to the blacklist and to the whitelist. Then, it monitors all port 80 traffic on the outside interface, and drops blacklisted traffic. It also treats greylist addresses as blacklisted addresses.

```
dynamic-filter updater-client enable
changeto context context1
dynamic-filter use-database
class-map dynamic-filter_snoop_class
  match port udp eq domain
policy-map dynamic-filter_snoop_policy
  class dynamic-filter_snoop_class
    inspect dns preset_dns_map dynamic-filter-snoop
service-policy dynamic-filter_snoop_policy interface outside
dynamic-filter blacklist
  name bad1.example.com
  name bad2.example.com
  address 10.1.1.1 255.255.255.0
dynamic-filter whitelist
  name good.example.com
  name great.example.com
  name awesome.example.com
  address 10.1.1.2 255.255.255.255
access-list dynamic-filter_acl extended permit tcp any any eq 80
dynamic-filter enable interface outside classify-list dynamic-filter_acl
dynamic-filter drop blacklist interface outside
dynamic-filter ambiguous-is-black
changeto context context2
dynamic-filter use-database
class-map dynamic-filter_snoop_class
  match port udp eq domain
```

```
policy-map dynamic-filter_snoop_policy
  class dynamic-filter_snoop_class
    inspect dns preset_dns_map dynamic-filter-snoop
service-policy dynamic-filter_snoop_policy interface outside
dynamic-filter blacklist
  name bad1.example.com
  name bad2.example.com
  address 10.1.1.1 255.255.255.0
dynamic-filter whitelist
  name good.example.com
  name great.example.com
  name awesome.example.com
  address 10.1.1.2 255.255.255.255
access-list dynamic-filter_acl extended permit tcp any any eq 80
dynamic-filter enable interface outside classify-list dynamic-filter_acl
dynamic-filter drop blacklist interface outside
dynamic-filter ambiguous-is-black
```

Feature History for the Botnet Traffic Filter

Feature Name	Platform Release	Description
Botnet Traffic Filter	8.2(1)	This feature was introduced.
Automatic blocking, and blacklist category and threat level reporting.	8.2(2)	The Botnet Traffic Filter now supports automatic blocking of blacklisted traffic based on the threat level. You can also view the category and threat level of malware sites in statistics and reports. The 1 hour timeout for reports for top hosts was removed; there is now no timeout. The following commands were introduced or modified: **dynamic-filter ambiguous-is-black**, **dynamic-filter drop blacklist**, **show dynamic-filter statistics**, show **dynamic-filter reports infected-hosts**, and **show dynamic-filter reports top**. The following screens were introduced or modified: **Configuration** > **Firewall** > **Botnet Traffic Filter** > **Traffic Settings** **Monitoring** > **Botnet Traffic Filter** > **Infected Hosts**.
ASDM can save Botnet Traffic Filter reports as HTML instead of PDF	ASDM 7.3(1)	ASDM can no longer save Botnet Traffic Filter reports as PDF files; it can instead save them as HTML. The following screen was modified: **Monitoring** > **Botnet Traffic Filter**