Managing Firewall Botnet Traffic Filter Rules

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, and then logs 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. 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.

Related Topics

- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Botnet Traffic Filter Rules Page, page 19-9

Understanding Botnet Traffic Filtering

Botnet Traffic Filter Address Categories

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. To be whitelisted, an address must be 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 graylist.
- **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 graylist generate syslog messages differentiated by type.

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. This section includes the following topics:

- Information About the Dynamic Database
- Information About the Static Database

Information 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.

The security appliance 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, the security appliance sends a syslog message informing you of the suspicious activity.
3. In some cases, the IP address itself is supplied in the dynamic database, and the Botnet Traffic Filter logs any traffic to that IP address without having to inspect DNS requests.

Note To use the database, be sure to configure a domain name server for the security appliance so that it can access the URL.

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

Information 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. You can also enter names or IP addresses in a whitelist, so that names or addresses that appear on both the whitelist and the dynamic blacklist are identified only as whitelist addresses in syslog messages and reports.

You can alternatively enable DNS packet inspection with Botnet Traffic Filter snooping. With DNS snooping, when an infected host sends a DNS request for a name on the static database, the security appliance 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.

Related Topics

- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Botnet Traffic Filter Rules Page, page 19-9

Task Flow for Configuring the Botnet Traffic Filter

To configure the Botnet Traffic Filter, follow these steps:

Step 1 Enable use of a DNS server.

This procedure enables security appliance use of a DNS server. In multiple context mode, enable DNS per context.

For more information, see DNS Page, page 52-14

Step 2 Enable use of the dynamic database.

This procedure enables database updates from the Cisco update server, and also enables use of the downloaded dynamic database by the security appliance. 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.

For more information, see Configuring the Dynamic Database, page 19-4

Step 3 (Optional) Add static entries to the 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.

For more information, see Adding Entries to the Static Database, page 19-5

Step 4 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 security appliance 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 logging function when connections are made to the suspicious address.

For more information, see Enabling DNS Snooping, page 19-6

Step 5 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 for any matching traffic or drops that traffic.

For more information, see Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6

Step 6 Monitor and Mitigate Botnet Activity.

After configuring the Botnet Traffic Filter on a device, the device will begin generating syslog messages to notify you of botnet activity. You should verify the syslog configuration on the device so that messages are appropriately logged and that notifications are sent as needed. As malicious traffic is identified, you will need to perform necessary actions to stop such traffic and to clean any infected computers that are generating the malicious traffic.

For more information, see the following references:

1. Chapter 53, “Configuring Logging Policies on Firewall Devices”
2. Monitoring and Mitigating Botnet Activity, page 68-59
3. Understanding Firewall Summary Botnet Reports, page 69-15

Configuring the Dynamic Database

This procedure enables database updates, and also enables use of the downloaded dynamic database by the security appliance.

In multiple context mode, you enable downloading of the dynamic database on the System context so that it is available to all security contexts. You can then decide, on a per-context basis, whether to enable use of the dynamic database or not.

By default, downloading and using the dynamic database is disabled.

Related Topics

- Dynamic Blacklist Configuration Tab, page 19-10
- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Adding Entries to the Static Database, page 19-5
- Enabling DNS Snooping, page 19-6
- Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6
- Botnet Traffic Filter Rules Page, page 19-9

Before You Begin

Enable security appliance use of a DNS server (see DNS Page, page 52-14). In multiple context mode, enable DNS per context.

Step 1 Do one of the following:

- (Device view) Select **Firewall > Botnet Traffic Filter Rules** from the Policy selector.
- (Policy view) Select **Firewall > Botnet Traffic Filter Rules** from the Policy Type selector. Select an existing policy or create a new one.

Note For devices in multiple context mode, you enable downloading of the dynamic database on the System context and enable use of the dynamic database on each security context, as needed.

This opens the Botnet Traffic Filter Rules Page, page 19-9.

Step 2 On the Dynamic Blacklist Configuration tab, select **Enable Dynamic Blacklist From Server** to enable downloading of the dynamic database.

Note In multiple context mode, you enable downloading of the dynamic database on the System context.

This setting enables downloading of the dynamic database from the Cisco update server. If you do not have a database already installed on the security appliance, it downloads the database after approximately 2 minutes. The update server determines how often the security appliance polls the server for future updates, typically every hour.

Step 3 (Multiple context mode only) Click **Save** to save the changes to the System context. Then change to the context where you want to configure the Botnet Traffic Filter, select **Firewall > Botnet Traffic Filter Rules** for that context, and then proceed to Step 4.

Step 4 On the Dynamic Blacklist Configuration tab, select **Use Dynamic Blacklist** to enable use of the dynamic database.

Note In multiple context mode, these settings are disabled on the System context.

Adding Entries to the Static Database

The static database lets you augment the dynamic database with domain names, IP addresses, or network addresses that you want to blacklist or whitelist. For more information, see Understanding Botnet Traffic Filtering, page 19-1.

Related Topics

- Whitelist/Blacklist Tab, page 19-14
- Device Whitelist or Device Blacklist Dialog Box, page 19-15
- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Configuring the Dynamic Database, page 19-4
- Enabling DNS Snooping, page 19-6
- Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6
- Botnet Traffic Filter Rules Page, page 19-9

Before You Begin

- Enable security appliance use of a DNS server (see DNS Page, page 52-14). In multiple context mode, enable DNS per context.

Step 1 Do one of the following:

- (Device view) Select **Firewall > Botnet Traffic Filter Rules** from the Policy selector.
- (Policy view) Select **Firewall > Botnet Traffic Filter Rules** from the Policy Type selector. Select an existing policy or create a new one.

Note For devices in multiple context mode, you configure the static database on the security context.

This opens the Botnet Traffic Filter Rules Page, page 19-9.

Step 2 On the Whitelist / Blacklist tab, click the **Add Rows** button that corresponds with the type of entry you are adding (Whitelist or Blacklist).

This opens the Device Whitelist or Device Blacklist Dialog Box, page 19-15.

Step 3 In the Domain or IP Address field, enter one or more domain names, IP addresses, and IP address/netmasks. Enter multiple entries separated by commas or on separate lines. You can enter up to 1000 entries for each type.

Step 4 Click **OK**.

Enabling 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 logging function when connections are made to the suspicious address.

The default configuration for DNS inspection inspects all UDP DNS traffic on all interfaces, and does not have Botnet Traffic Filter snooping enabled. We suggest that you enable Botnet Traffic Filter snooping only on interfaces where external DNS requests are going. Enabling Botnet Traffic Filter snooping on all UDP DNS traffic, including that going to an internal DNS server, creates unnecessary load on the security appliance.

Note TCP DNS traffic is not supported.

Related Topics

- Configure DNS Dialog Box, page 17-18
- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Configuring the Dynamic Database, page 19-4
- Adding Entries to the Static Database, page 19-5
- Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6
- Botnet Traffic Filter Rules Page, page 19-9

Step 1 You must first configure DNS inspection for traffic that you want to snoop using the Botnet Traffic Filter. See Chapter 17, "Managing Firewall Inspection Rules".

Step 2 While defining a new inspection rule or editing an existing inspection rule, select DNS as the protocol you want to inspect.

The Configure button to the right of the Selected Protocol field becomes active.

Step 3 Click **Configure**.

This opens the Configure DNS Dialog Box, page 17-18.

Step 4 To enable DNS snooping, select **Enable Dynamic Filter Snooping**.

Step 5 Click **OK**.

Enabling 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 for any matching traffic. The

Botnet Traffic Filter can also drop the connection when matching traffic is encountered. For a particular interface, you can specify only one enable rule that identifies the traffic that is subject to Botnet Traffic Filtering; however, you can specify multiple drop rules to identify traffic that should be dropped by the Botnet Traffic Filter.

The DNS snooping is enabled separately (see Enabling DNS Snooping, page 19-6). Typically, for maximum use of the Botnet Traffic Filter, you need to enable DNS snooping, but you can use Botnet Traffic Filter logging independently if desired. 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.

What You Need To Know About Botnet Traffic Classification ACLs

When you configure the enable and drop rules, you have the option of specifying an extended ACL policy object to limit the traffic to which Botnet Traffic Filtering will be applied. If you do not specify an ACL object, filtering is done for all traffic: this is equivalent to specifying an ACL with the single rule permit IP any any.

If you want to specify an ACL so that filtering is performed on less than all traffic, keep the following in mind:

- Permit rules identify the traffic that is subject to Botnet Traffic Filtering. In drop rules, permit entries identify the traffic that the ASA is allowed to drop.
- Deny rules identify the traffic that should not be subject to filtering. The Botnet Traffic Filter ignores traffic that matches deny entries.
- The ACL that you select for drop rules should be a subset of the ACL used in the enable rules for the interface. For traffic to be dropped, there must not only be a permit rule in the drop rule's ACL, the traffic must also fall under a permit rule in the enable rule's ACL. This is because the drop rule is not considered until traffic permitted in an enable rule has first been identified as blacklisted.

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.

Related Topics

- Traffic Classification Tab, page 19-11
- BTF Enable Rules Editor, page 19-12
- BTF Drop Rules Editor, page 19-13
- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Configuring the Dynamic Database, page 19-4
- Adding Entries to the Static Database, page 19-5
- Enabling DNS Snooping, page 19-6
- Botnet Traffic Filter Rules Page, page 19-9

Step 1 Do one of the following:

- (Device view) Select **Firewall > Botnet Traffic Filter Rules** from the Policy selector.
- (Policy view) Select **Firewall > Botnet Traffic Filter Rules** from the Policy Type selector. Select an existing policy or create a new one.

Note For devices in multiple context mode, you configure traffic classification on the security context.

This opens the Botnet Traffic Filter Rules Page, page 19-9.

Step 2 To enable the Botnet Traffic Filter on specified traffic, follow these steps:

a. On the Traffic Classification tab, click **Add Row** under the Enable Rules table.

This opens the BTF Enable Rules Editor, page 19-12.

b. In the Interfaces field, specify the interface or interfaces on which you want to enable the Botnet Traffic Filter. Normally, you want to enable the Internet-facing interface only. To select the interfaces or interface role objects using the Interfaces Selector, click **Select** (see Understanding Interface Role Objects, page 6-69).

You can configure a global classification that applies to all interfaces by selecting the All Interfaces role object (selected by default). If you configure an interface-specific classification, the settings for that interface overrides the global setting.

c. Do one of the following to identify the traffic that you want to monitor:

- To monitor all traffic, leave the ACL field blank.
- To specify the traffic that you want to monitor, click **Select** to the right of the ACL field to select an Access Control List object that identifies the traffic that you want to monitor. For example, you might want to monitor all port 80 traffic on the outside interface. For more information about Access Control List objects, see Creating Access Control List Objects, page 6-51.

Note You can specify only one enable rule per interface.

d. Click **OK**.

The BTF Enable Rules Editor closes and the rule is added to the Enable Rules table.

Step 3 To automatically drop malware traffic, follow these steps:

Note You must enable the Botnet Traffic Filter for the traffic you want to automatically drop before creating a drop rule for that traffic.

a. On the Traffic Classification tab, click **Add Row** under the Drop Rules table.

This opens the BTF Drop Rules Editor, page 19-13.

b. In the Interfaces field, specify the interface or interfaces on which you want to drop traffic. There must be a corresponding enable rule for the interface. To select the interfaces or interface role objects using the Interfaces Selector, click **Select** (see Understanding Interface Role Objects, page 6-69).

You can configure a global classification that applies to all interfaces by selecting the All Interfaces role object (selected by default). If you configure an interface-specific classification, the settings for that interface overrides the global setting.

c. Do one of the following to identify the traffic that you want to drop:

- To monitor all traffic, leave the ACL field blank.

- To specify the traffic that you want to monitor, click **Select** to the right of the ACL field to select an Access Control List object that identifies the traffic that you want to monitor. For example, you might want to monitor all port 80 traffic on the outside interface. For more information about Access Control List objects, see Creating Access Control List Objects, page 6-51.

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

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

e. Click **OK**.

The BTF Drop Rules Editor closes and the rule is added to the Drop Rules table.

Step 4 To add more rules, repeat steps 2 and 3, as required. When finished adding rules, click **Save** to save your changes.

Step 5 To treat graylisted traffic as blacklisted traffic for action purposes, on the Dynamic Blacklist Configuration tab, check the **Treat Ambiguous traffic as Blacklist** check box.

If you do not enable this option, graylisted traffic will not be dropped if you configure a drop rule for that traffic.

Botnet Traffic Filter Rules Page

You can use the Botnet Traffic Filter Rules page to define rules for identifying malicious traffic passing through your ASA security device.

The Botnet Traffic Filter Rules page is divided into three sections:

- Dynamic Blacklist Configuration Tab, page 19-10
- Traffic Classification Tab, page 19-11
- Whitelist/Blacklist Tab, page 19-14

Navigation Path

To access the Botnet Traffic Filter Rules page, do one of the following:

- (Device view) Select a device, then select **Firewall > Botnet Traffic Filter Rules** from the Policy selector.
- (Policy view) Select **Firewall > Botnet Traffic Filter Rules** from the Policy Type selector. Select an existing policy or create a new one.
- (Map view) Right-click a device and select **Edit Firewall Policies > Botnet Traffic Filter Rules**.

Related Topics

- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Dynamic Blacklist Configuration Tab, page 19-10
- Traffic Classification Tab, page 19-11
- BTF Enable Rules Editor, page 19-12
- BTF Drop Rules Editor, page 19-13
- Whitelist/Blacklist Tab, page 19-14
- Device Whitelist or Device Blacklist Dialog Box, page 19-15
- Configure DNS Dialog Box, page 17-18

Dynamic Blacklist Configuration Tab

Use the Dynamic Blacklist Configuration tab to enable database updates from the Cisco update server and to enable use of the downloaded dynamic database by the security appliance.

Navigation Path

From the Botnet Traffic Filter Rules Page, page 19-9, click the **Dynamic Blacklist Configuration** tab.

Related Topics

- Configuring the Dynamic Database, page 19-4
- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Botnet Traffic Filter Rules Page, page 19-9
- Traffic Classification Tab, page 19-11
- BTF Enable Rules Editor, page 19-12
- BTF Drop Rules Editor, page 19-13
- Whitelist/Blacklist Tab, page 19-14
- Device Whitelist or Device Blacklist Dialog Box, page 19-15
- Configure DNS Dialog Box, page 17-18

Field Reference

Table 19-1 Dynamic Blacklist Configuration Tab

Element	Description
Enable Dynamic Blacklist From Server	Enables downloading of the dynamic database from the Cisco update server. If you do not have a database already installed on the security appliance, it downloads the database after approximately 2 minutes. The update server determines how often the security appliance polls the server for future updates, typically every hour. **Note** If the device is in multiple context mode, configure this option on the System context for that device.

Table 19-1 Dynamic Blacklist Configuration Tab (Continued)

Element	Description
Use Dynamic Blacklist	Enables use of the dynamic database for the Botnet Traffic Filter. **Note** In multiple context mode, you configure use of the database on a per-context basis.
Treat Ambiguous traffic as Blacklist	When selected, graylisted traffic will be treated as blacklisted traffic for action purposes. If you do not enable this option, graylisted traffic will not be dropped if you configure a drop rule for that traffic.

Traffic Classification Tab

Use the Traffic Classification tab to view or to configure the traffic classification definitions for a device or shared policy and to identify malicious traffic that you want automatically dropped. Traffic classification definitions (enable rules) consist of an interface or interface role with an associated ACL that identifies the traffic that is monitored by the Botnet Traffic Filter. You can configure settings for specific interfaces or for interface roles. You can use the All Interfaces role object to enable botnet filtering globally (selected by default). If you configure an interface-specific classification, the settings for that interface override any settings defined for an interface role.

For a particular interface, you can specify only one enable rule that identifies the traffic that is subject to Botnet Traffic Filtering; however, you can specify multiple drop rules to identify traffic that should be dropped by the Botnet Traffic Filter.

Note We highly recommend configuring Dynamic Filter Snooping for proper functioning of the Botnet Traffic Filter. When in Device view, Cisco Security Manager provides a link at the bottom of the Traffic Classification tab that will take you directly to the Inspection Rules page so that you can enable Dynamic Filter Snooping. For more information, see Enabling DNS Snooping, page 19-6.

The columns in the tables summarize the settings for an entry and are explained in BTF Enable Rules Editor, page 19-12 and BTF Drop Rules Editor, page 19-13.

To configure traffic classification and actions:

- Click the **Add Row** button to add an interface or interface role to the table, and fill in the BTF Enable Rules Editor, page 19-12 or BTF Drop Rules Editor, page 19-13.
- Select an entry and click the **Edit Row** button to edit an existing entry.
- Select an entry and click the **Delete Row** button to delete it.

Navigation Path

From the Botnet Traffic Filter Rules Page, page 19-9, click the **Traffic Classification** tab.

Related Topics

- BTF Enable Rules Editor, page 19-12
- BTF Drop Rules Editor, page 19-13
- Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6
- Understanding Botnet Traffic Filtering, page 19-1

- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Botnet Traffic Filter Rules Page, page 19-9
- Dynamic Blacklist Configuration Tab, page 19-10
- Whitelist/Blacklist Tab, page 19-14
- Device Whitelist or Device Blacklist Dialog Box, page 19-15
- Configure DNS Dialog Box, page 17-18

BTF Enable Rules Editor

Use the BTF Enable Rules Editor to specify the interfaces on which you want to enable the Botnet Traffic Filter and to identify the traffic that you want to monitor. You can specify only one enable rule per interface.

Navigation Path

To access the BTF Enable Rules Editor, right-click inside the work area of the Enable Rules table on the Traffic Classification tab and then select **Add Row**, or right-click an existing entry and select **Edit Row**.

Related Topics

- Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6
- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Botnet Traffic Filter Rules Page, page 19-9
- Dynamic Blacklist Configuration Tab, page 19-10
- Traffic Classification Tab, page 19-11
- BTF Drop Rules Editor, page 19-13
- Whitelist/Blacklist Tab, page 19-14
- Device Whitelist or Device Blacklist Dialog Box, page 19-15
- Configure DNS Dialog Box, page 17-18

Field Reference

Table 19-2 BTF Enable Rules Editor

Element	Description
Interfaces	The interfaces or interface roles on which you want to enable the Botnet Traffic Filter. Enter the name of the interface or the interface role, or click **Select** to select the interface or role from a list, or to create a new role. An interface must already be defined to appear on the list. You can use the All Interfaces role object to enable botnet filtering globally (selected by default). If you configure an interface-specific classification, the settings for that interface override the global settings. Interface role objects are replaced with the actual interface names when the configuration is generated for each device. See Understanding Interface Role Objects, page 6-69.

Table 19-2 BTF Enable Rules Editor (Continued)

Element	Description
ACL	Specifies the access-list to use for identifying the traffic that you want to monitor. If you do not specify an access list, by default you monitor all traffic. To specify the traffic that you want to monitor, click **Select** to the right of the ACL field to select an Access Control List object that identifies the traffic that you want to monitor. For example, you might want to monitor all port 80 traffic on the outside interface. For more information about Access Control List objects, see Creating Access Control List Objects, page 6-51.

BTF Drop Rules Editor

Use the BTF Drop Rules Editor to identify malware traffic that you want to automatically drop. You can specify multiple drop rules per interface.

Navigation Path

To access the BTF Drop Rules Editor, right-click inside the work area of the Drop Rules table on the Traffic Classification tab and then select **Add Row**, or right-click an existing entry and select **Edit Row**.

Related Topics

- Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6
- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Botnet Traffic Filter Rules Page, page 19-9
- Dynamic Blacklist Configuration Tab, page 19-10
- Traffic Classification Tab, page 19-11
- BTF Enable Rules Editor, page 19-12
- Whitelist/Blacklist Tab, page 19-14
- Device Whitelist or Device Blacklist Dialog Box, page 19-15
- Configure DNS Dialog Box, page 17-18

Field Reference

Table 19-3 BTF Drop Rules Editor

Element	Description
Interfaces	The interfaces or interface roles on which you want to enable the Botnet Traffic Filter. Enter the name of the interface or the interface role, or click **Select** to select the interface or role from a list, or to create a new role. An interface must already be defined to appear on the list. You can use the All Interfaces role object to enable botnet filtering globally (selected by default). If you configure an interface-specific classification, the settings for that interface override the global settings. Interface role objects are replaced with the actual interface names when the configuration is generated for each device. See Understanding Interface Role Objects, page 6-69.
ACL	Specifies the access-list to use for identifying the traffic that you want to monitor. If you do not specify an access list, by default you monitor all traffic. To specify the traffic that you want to monitor, click **Select** to the right of the ACL field to select an Access Control List object that identifies the traffic that you want to monitor. For example, you might want to monitor all port 80 traffic on the outside interface. For more information about Access Control List objects, see Creating Access Control List Objects, page 6-51.
Threat Level	The Threat Level fields identify the threat level of malicious traffic that you want dropped. 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 • Range—Specify a range of threat levels. **Note** Static blacklist entries are always designated with a Very High threat level.

Whitelist/Blacklist Tab

Use the Whitelist/Blacklist tab to view or to configure the static database entries for a device or shared policy. The Device Blacklist contains domain names or IP addresses of malicious or undesirable sites. You can use the static blacklist to supplement the Cisco dynamic database or you can use the static blacklist alone if you can identify all the malware sites that you want to target.

The Device Whitelist contains domain names or IP addresses of sites that are deemed to be acceptable. If the dynamic database includes blacklisted addresses that you think should not be blacklisted, you can manually enter them into a static whitelist. Static whitelist entries take precedence over entries in the static blacklist and the Cisco dynamic database. Whitelisted addresses still generate syslog messages, but because you are only targeting blacklist syslog messages, they are informational.

To configure the static database:

- Click the **Add Row** button to define static database entries using the Device Whitelist or Device Blacklist Dialog Box, page 19-15.
- Select an entry and click the **Edit Row** button to edit an existing entry.

Timesaver Select an entry and press **F2** or double-click on an entry in the Device Whitelist or Device Blacklist to edit that entry in place.

- Select an entry and click the **Delete Row** button to delete it.

Navigation Path

From the Botnet Traffic Filter Rules Page, page 19-9, click the **Whitelist/Blacklist** tab.

Related Topics

- Adding Entries to the Static Database, page 19-5
- Understanding Botnet Traffic Filtering, page 19-1
- Task Flow for Configuring the Botnet Traffic Filter, page 19-2
- Device Whitelist or Device Blacklist Dialog Box, page 19-15
- Botnet Traffic Filter Rules Page, page 19-9
- Dynamic Blacklist Configuration Tab, page 19-10
- Traffic Classification Tab, page 19-11

Device Whitelist or Device Blacklist Dialog Box

Use the Device Whitelist or Device Blacklist dialog box to manually define domain names or IP addresses that you want to add to the whitelisted (safe) or blacklisted (malicious) lists. You can use the static blacklist to supplement the Cisco dynamic database or you can use the static blacklist alone if you can identify all the malware sites that you want to target. Names or addresses that appear on both the whitelist and the dynamic blacklist are identified only as whitelist addresses in syslog messages and reports.

Domain names can be complete (including the host name, such as www.cisco.com), or partial (such as cisco.com). For partial names, all web site hosts on that domain are either whitelisted or blacklisted. You can also enter host IP addresses. Use a comma or new line to separate multiple entries.

Navigation Path

From the Whitelist/Blacklist Tab, page 19-14, click the **Add Rows** button beneath the Device Whitelist or Device Blacklist tables, or select an entry and click the **Edit Row** button.

Related Topics

- Adding Entries to the Static Database, page 19-5