



# Advanced Zone Procedures

---

This chapter describes how to perform advanced configuration tasks for zones on the Cisco Traffic Anomaly Detector using the Web-Based Management (WBM).

This chapter includes the following sections:

- [Overview](#) (What are Policy templates, Policies and Filters)
- [Zone Filter Configuration](#) (configuring the Flex and Bypass filters)
- [Policy Templates](#) (configuring policy template parameters)

## Overview

## Filters

The zone's filters are the mechanism that directs the zone's mirrored traffic to the Detector's detection modules. The Detector enables to set its preferred filter configurations and thus design a variety of possibilities for customized traffic direction and DDoS attack detection mechanisms.

There are three filter types used by the Cisco Traffic Anomaly Detector:

- Bypass filter—Bypass filters are used to prevent specific traffic flows from being handled by the Detector detection mechanisms.
- Flex filter—The Flex filter is used to count a specified packet flow. It is a Berkley Packet filter that facilitates you with extremely flexible filtering capabilities such as filtering according to fields in the IP and TCP headers and filtering according to content bytes. The flex filter enables to use complex Boolean expressions. Only a single flex filter can be configured per zone.
- Dynamic filter—Dynamic filters are created by the Detector as the result of the analysis of traffic flow. The Dynamic filters produce a notification record in the Detector's syslog or activate a remote Guard or Guards. See the “Dynamic Filters” section in [Chapter 7, “Detecting Traffic Anomalies,”](#) for further details.

**Note**

---

Changes in the zone's filter configuration take effect immediately.

---

For detailed information on the Detector's filters, refer to Chapter 6, “Filter Procedures,” in the *Cisco Traffic Anomaly Detector User Guide*.

## Policy Templates and Policies

The Detector policies measure the particular traffic flows. Once suspicious indicators in the form of threshold violations are sensed, the policies assume an action. This action could be either a Guard remote-activation or recording the event in the Detector syslog. The Detector policies enable the Detector to stay tightly attuned to the zone traffic, detect traffic anomalies, and take an action accordingly.

The detection policies are constructed from policy templates.

A policy template is a collection of policy constructing guiding rules that will be used during the learning phases to construct the zone's policies (see [Chapter 6, “Zone Traffic Learning and Policy Construction,”](#) for further details).

# Zone Filter Configuration

## Bypass Filter Configuration

The Bypass filter is used to prevent specific traffic flows from being handled by the Detector. You may configure the Bypass filter to direct trusted traffic away from the Detector's detection mechanisms. The traffic would then be directly dropped.

To configure the Bypass filters:

1. From the Zone's main menu select **Configuration > Bypass filters**.
2. Click **Add**.

No Bypass filter is defined by default.

Enter the following information to configure the Bypass filter:

Parameter	Description
Source IP	Directs traffic coming from a specified IP address to bypass the Detector filter system. Leave blank for 'any'.
Source subnet	Directs traffic coming from a specified subnet to bypass the Detector filter system. Choose the subnet from the drop-down list.
Protocol	Directs traffic from a specified protocol to bypass the Detector filter system. The protocol is denoted by the its well known number. Leave blank for 'any'.
Dst Port	Directs traffic destined to a specified destination port to bypass the Detector filter system.
Fragments	Denotes specified traffic type for the filter to analyze. Choose from the drop-down list one of the following: <ul style="list-style-type: none"> <li>• <b>without</b>—The Bypass filter analyses non-fragmented traffic.</li> <li>• <b>with</b>—The Bypass filter analyses fragmented traffic.</li> <li>• <b>*</b>—The Bypass filter analyses fragmented and non-fragmented traffic.</li> </ul>

In the Bypass filter table, the counter denotes the current Bypass filter traffic rate measured in packets per second (pps) that was filtered by the Bypass filter.

To delete a Bypass filter:

1. Select the check box next to the Bypass filter's description.
2. Click **Delete**.

For a comprehensive explanation on the Bypass filter parameters, and examples, refer to Chapter 6, “Filter Procedures,” in the *Cisco Traffic Anomaly Detector User Guide*.

## Flex Filter Configuration

The Flex filter is a Berkley Packet filter which facilitates you with extremely flexible filtering capabilities. It is used to count a desired packet flow. The Flex filter is useful in upfront detecting a minutely defined malicious source of traffic. This filter is very flexible and easily tailored to a specific traffic flow due to its parameter variety. However, only a single flex filter can be configured and it is resource consuming. Therefore, we recommend to use the Flex filter attentively due to its potential performance penalty.

To configure the Flex filter:

1. If the zone is already defined, from the Zone's menu select **Configuration > General**.
2. Click **Config**.

Alternatively, the Flex filter may be configured while creating a new zone (see the “[Creating Zones and Basic Zone Configuration](#)” section in [Chapter 4, “Zone Creation and Configuration](#),” for further details).

For a detailed explanation on the Berkley Packet filter configuration options see: <http://www.freesoft.org/CIE/Topics/56.htm>.

For a comprehensive explanation on the Flex filter parameters, and examples, refer to Chapter 6, “Filter Procedures,” in the *Cisco Traffic Anomaly Detector User Guide*.

# Policy Templates

A policy template is a collection of policy constructing guiding rules and the output of each template is a group of policies. The Detector policy templates consist of the following:


Policy Template	Brief Description
<code>dns_tcp</code>	This policy template produces a group of policies related to DNS-TCP protocol traffic.
<code>dns_udp</code>	This policy template produces a group of policies related to DNS-UDP protocol traffic.
<code>fragments</code>	This policy template produces a group of policies related to fragmented traffic.
<code>http</code>	This policy template produces a group of policies related to HTTP traffic flowing (by default) through port 80 (or other user-configured ports).
<code>ip_scan</code>	<p>This policy template produces a group of policies relating to IP scanning (A situation in which a Src IP tries to access many Dst IPs in the zone). This policy template is relevant when the zone is defined as a subnet. By default this policy template is disabled. The default action for this policy template is “notify”.</p> <p><b>Note</b> The policies created by the <code>ip_scan</code> policy template are resource consuming. Therefore, we recommend to use it attentively due to its potential performance penalty.</p>
<code>other_protocols</code>	This policy template produces a group of policies relating to non TCP or UDP protocols.

Policy Template	Brief Description
<b>port_scan</b>	<p>This policy template produces a group of policies relating to port scanning (A situation in which a Src IP tries to access many ports in the zone). By default, this policy template is disabled. The default action for this policy template is “notify”.</p> <p><b>Note</b> The policies created by the port_scan policy template are resource consuming. Therefore, we recommend to use it attentively due to its potential performance penalty.</p>
<b>tcp_connections</b>	This policy template produces a group of policies related to TCP connection characteristics.
<b>tcp_not_auth</b>	This policy template produces a group of policies related to TCP connections that haven't been authenticated.
<b>tcp_outgoing</b>	This policy template produces sets of policies related to TCP connections initiated by the zone.
<b>tcp_ratio</b>	This policy template produces sets of policies related to ratios between different types of TCP packets. For example, SYN packets versus FIN/RST packets.
<b>tcp_services</b>	This policy template produces a group of policies related to TCP services on ports other than HTTP-related (such as ports 80, 8080, etc.).
<b>udp_services</b>	This template produces a group of policies related to UDP services.

To configure a policy template:

1. From the Zone's main menu, select **Configuration > Policy templates**.
2. Click on the required policy template name.

*Figure 5-1 Policy Templates*

*Victim\_scanner (automatic) - Under Detection* 

Home > Victim > Policy Templates

Policy Template	State	Min Threshold	Max Services
tcp_services		1.0	5
udp_services		1.0	5
tcp_connections			
ip_scan	disabled		

119264

## Configuring the Policy Template Operational Parameters

For each of the policy templates, the following parameters may be configured:

Parameter	Description
State	Specifies the policy template state. The policy template can be enabled or disabled. Disabling a policy template prevents it from producing policies once the Detector undergoes the Policy Construction phase.

Parameter	Description
Min Threshold	Specifies the minimum traffic volume threshold for a service. The Detector denotes the services with traffic volume above the specified threshold and produces policies that relate to the services' traffic according to particular traffic flow criteria (e.g. traffic volume coming from a source IP on a specific service port). Setting the threshold enables to better adopt the Detector detection to the traffic volume of the zone services. This parameter cannot be configured for policy templates that are essential for proper zone detection and therefore always produce a policy, such as fragments.
Max Services	Specifies the maximum number of services the Detector will discover with the aid of a specific policy template. The Detector ranks the services the policy relates to by their level of traffic volume. The Detector will then pick up the services with the highest traffic volume. Limiting the service number would allow to better tailor the Detector detection policies to its preferred traffic flow requirements. This parameter can be configured only for policy templates that detect services, such as tcp_services. It cannot be configured for policy templates that relate to a specified service (such as dns_tcp that relates to service 53), or for policy templates that relate to a specified traffic characteristic (such as fragments).

**Caution**

Disabling a policy template results in the Detector's inability to detect traffic of the kind the policy template relates to, destined to the zone. This may seriously compromise the Detector's detection capabilities.