



# Zone Creation and Configuration

---

This chapter describes how to create and manage zones.

This chapter includes the following sections:

- [Overview](#) (What is a Zone)
- [The Zone “Home Page”](#)
- [Zone Management](#) (creating zones and basic zone configuration)
- [Zone Status Icons](#)

## Overview

### What is a Zone?

A zone is a network element, which the Detector monitors for DDoS attacks. A zone can be a network server, client or router; a network link or subnet or an entire network; an individual Internet user or a company doing business using the Internet; an Internet Service Provider (ISP), or any combination of or variant on these. Once a DDoS attack is identified, the Detector can activate a remote Guard automatically to protect the zone against the attack or notify the user to activate the Guard manually.

The Detector can analyze the traffic for different zones simultaneously, as long as their network address ranges don't overlap.

A “Zone” on the detector is the definition of a zone element, configured so that the Detector can detect DDoS attacks issued against it. A zone configuration on the Detector includes the following:

- Zone basic configuration—A zone's basic configuration includes the zone's name and description, the zone's network address and operation definitions and basic networking characteristics such as the zone's bandwidth. See the [“Zone Management”](#) section in this chapter for further details.
- The Zone's Detection Policy—The policies are the mechanisms that enable the Detector to analyze a particular traffic flow and take action against the flow as a result of threshold violation. The detection policies are constructed from policy templates that provide the constructing guiding rules, in two learning phases (see [Chapter 7, “Detecting Traffic Anomalies,”](#) for further details). The action taken by the policies could range from merely notifying to activating a remote Guard or Guards to protect the zone against the DDoS attack (see [Chapter 5, “Advanced Zone Procedures,”](#) for further details).
- The Zone's filters—The zone's filters are the mechanism that directs the diverted traffic to the required analysis modules. The Detector enables you to set its preferred filter configurations and thus design a variety of possibilities for customized traffic direction and anti-DDoS detection mechanisms (see [Chapter 5, “Advanced Zone Procedures,”](#) for further details).

## The Zone “Home Page”

The zone's “home page” ([Figure 4-1](#)) provides a summary of the zone's status.

To navigate to this screen perform one of the following:

- From the navigation pane under the **All Zones** list, click the zone's name.
- If the zone is currently in detect mode, from the navigation pane under the **Under detection** list, click the zone's name.
- On the zone pages, select **Zone** from the location view.
- From the zone list (**Detector Summary > Zones > Zone list**), click the zone name.

The zone “home page” is divided into four sections:

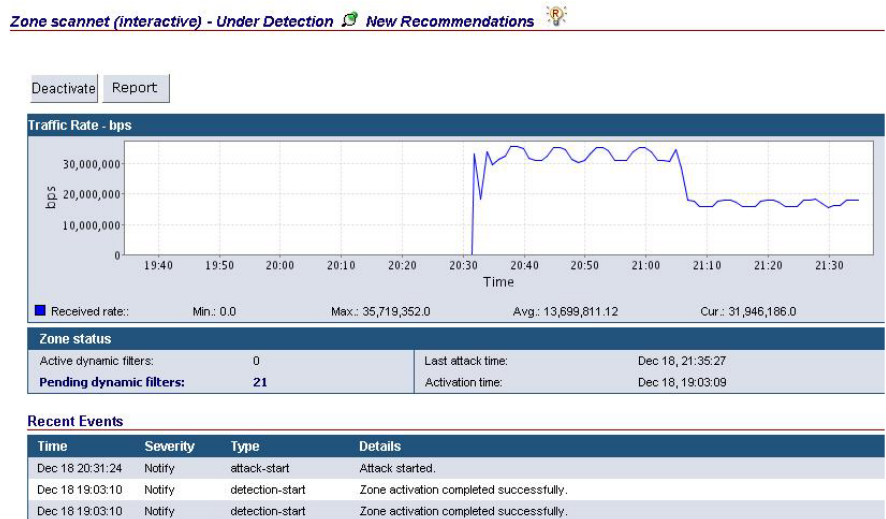
- Zone status bar
- Zone Traffic summary

- Zone status summary
- Zone recent events

In addition, the zone's home page has short cuts, displayed as buttons below the zone status bar.

- **Detect**—Switches the zone to detect mode. This is a shortcut to selecting **Detection > Detect** from the Zone’s main menu.  
This button is present only if the zone is in stand by.
- **Deactivate**—Deactivates the zone’s detection state. This is a shortcut to selecting **Detection > Deactivate** from the Zone's main menu.  
This button is present only if the zone is in detect mode.
- **Report**—Provides a shortcut to the current attack report. This is a shortcut to selecting **Diagnostics > Attack reports** from the Zone’s main menu and clicking on the current attack (the attack with an end time of “attack in progress”). This shortcut is available only if there is a current attack in progress. See [Chapter 8, “Zone Statistics and Diagnostics,”](#) for further details.

**Figure 4-1 Zone “home page”**



119272

## Zone Status Bar

The zone’s status bar provides a quick reference for the zone’s status. It provides details on the following:

- The zone’s name.
- The zone’s operation mode—The operation mode appears in brackets. It indicates whether the zone is in automatic detect mode or in interactive detect mode. The operation mode is displayed only if the zone is active. See the [“Zone Management”](#) section in this chapter for further details.
- The zone’s status—The zone’s status indicates the zone’s detection or learning mode. The zone’s status can be one of the following: under detection, inactive, constructing policy or tuning thresholds. See the [“Zone Status Summary”](#) section in this chapter for further details.
- Indication on new recommendations—If the zone is in interactive mode, the zone’s status bar will include an indication on new recommendations. See the [“Interactive Recommendations Mode”](#) section in [Chapter 7](#), [“Detecting Traffic Anomalies,”](#) for further details.

## Zone Traffic Summary

The zone’s traffic summary graph displays the zone related traffic rate, in bits per second (bps), in the past two hours.

The information is provided on the Received traffic.

Below the graph, the following information is provided:

| Parameter  | Description  |
|------------|--|
| <b>Min</b> | Indicates the minimum traffic rate in bps measured in the past two hours |
| <b>Max</b> | Indicates the maximum traffic rate in bps measured in the past two hours |
| <b>Avg</b> | Indicates the average traffic rate in bps measured in the past two hours |
| <b>Cur</b> | Indicates the current traffic rate in bps                                |

## Zone Status Summary

The zone's status summary provides the following information:

- The number of active Dynamic filters.

**Active dynamic filters** provides a link to the Dynamic filters page. See the “[Dynamic Filters](#)” section in [Chapter 7, “Detecting Traffic Anomalies,”](#) for further details.

- The number of pending Dynamic filters.

The number of pending dynamic filters is greater than 1 when the zone is in interactive detection mode and there are new recommendations.

**Pending dynamic filters** provides a link to the recommendations page. See the “[Dynamic Filters](#)” section in [Chapter 7, “Detecting Traffic Anomalies,”](#) for further details on dynamic filters. See the “[Interactive Recommendations Mode](#)” in [Chapter 7, “Detecting Traffic Anomalies,”](#) for further details on recommendations.

- Last attack time—The date and time of the last attack on the zone.
- Activation time—The date and time detection was activated.

## Zone Recent Events

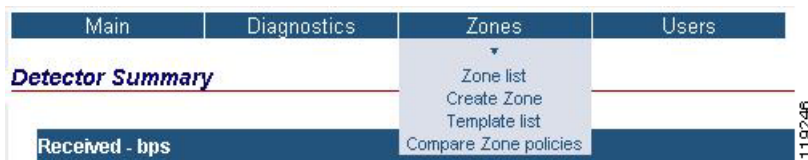
The recent events table displays the recent events issues by the zone. These events are also displayed in the zone event log and the Detector event log. The events displayed in this table have a minimum severity level of *notify*.

# Zone Management

## Creating Zones and Basic Zone Configuration

To stay attuned to the zone's traffic and detect traffic anomalies and DDoS attacks, the zone's network characteristics must be configured on the Detector.

**Figure 4-2 Zones Sub-menu**



To create a new zone, perform one of the following:

- From the Detector's main menu select **Zones > Create Zone**.
- From the Detector's main menu select **Zones > Zone list** and click **Add**.
- From the Zone's main menu select **Main > Create Zone**.
- From the Zone's main menu select **Main > Save as**.

This action copies the current zone basic configuration to a new zone. It is equivalent to the CLI command `zone` with the option `copy-from-this`. Refer to Chapter 4, “Zone Configuration,” in the *Cisco Traffic Anomaly Detector User Guide* for further details.

The Zone Form appears.

The zone's basic configuration includes the following:

| Parameter          | Description                           |
|--------------------|---------------------------------------|
| <b>Name</b>        | The zone name.                        |
| <b>Description</b> | (Optional) A description of the zone. |

| Parameter             | Description   |
|-----------------------|---|
| <b>From Template</b>  | <p>A template that defines the zone configuration. The Template could be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>DEFAULT</b>—The Detector default zone template.</li> <li>• <b>Bandwidth Limited Link Templates</b>—Templates designed and specifically tailored for detection of large subnets segmented according to zones with known bandwidth. Detection on zones defined by these templates can be assumed without undergoing the learning process. It is recommended to define such a zone with protect-ip state of only-dest-ip (See <i>Protect-IP state</i> in this table for further details).</li> </ul> <p>The following Bandwidth Limited Link templates are available for 128K, 1M, 4M, and 512K links respectively:</p> <ul style="list-style-type: none"> <li>- <b>LINK_128K</b></li> <li>- <b>LINK_1M</b></li> <li>- <b>LINK_4M</b></li> <li>- <b>LINK_512K</b></li> </ul> <p><b>Note</b> Learning Phase 1, policy construction, cannot be performed for these templates.</p> |
| <b>Operation mode</b> | <p>Indicates the mode used for zone Dynamic filters activation. The mode can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Automatic</b>—The dynamic filters will be activated automatically.</li> <li>• <b>Interactive</b>—The interactive mode enables you to define the action taken for each Dynamic filter. The Dynamic filters the policies recommend will appear as recommendations. You will specify whether to accept or reject each Dynamic filter.</li> </ul> <p>See the <a href="#">“Interactive Recommendations Mode”</a> section in <a href="#">Chapter 7, “Detecting Traffic Anomalies,”</a> for further details.</p>   |

| Parameter               | Description   |
|-------------------------|---|
| <b>Flex filter</b>      | (Optional) Configure the flex filter. See the “ <a href="#">Flex Filter Configuration</a> ” section in <a href="#">Chapter 5, “Advanced Zone Procedures,”</a> for further details.  |
| <b>Filter Action</b>    | (Optional) Configure the Flex filter action. The following options are available: <ul style="list-style-type: none"> <li>• <b>disable</b>—The Flex filter is disabled.</li> <li>• <b>count</b>—The Flex filter is used to count the specified flow. Choose the action from the drop-down list.</li> </ul>   |
| <b>Protect-IP state</b> | Indicates the Guard-protection form used. The Guard-protection form is designed to save Guard-protection resources and better focus on the zone detection and protection requirements. Choose the state from the drop-down list.<br><br>The state can be one of the following: <ul style="list-style-type: none"> <li>• <b>All-Zone</b>—The Detector activates the Guard to assume protection over the overall zone whenever a traffic anomaly is detected. This strategy is recommended when the overall zone consists of intra-related zones that cannot be risked.</li> <li>• <b>only-dst-ip</b>—The Detector activates the Guard protection over a particular zone once a traffic anomaly can be traced as destined to that particular zone. This is since you may want to assume protection per an attacked zone and not spend valuable protection resources over the overall zone.</li> <li>• <b>policy-type</b>—The Detector activates the Guard protection over a particular zone once a traffic anomaly can be traced as destined to the particular zone. The Detector would also activate the Guard protection over the overall zone once the detected anomaly cannot be traced as destined to a particular zone. This strategy is recommended when the overall zone consists of highly related particular zones. This is since you may want to avoid a situation in which a targeted zone may inflict damage on the overall zone.</li> </ul> |
| <b>Mask</b>             | The zone's address mask. Choose the address mask from the drop-down list.   |

**Note**

After creating a zone, the zone's configuration is displayed in two tables. Additional IP addresses and subnets may be entered by clicking **Add** at the bottom of the IP table. This procedure should repeat per each zone IP address or subnet mask. Additional IP addresses and subnets may be entered or deleted while the zone is active.

## Reconfiguring a Zone

To reconfigure an existing zone:

1. From the Zone's menu select **Configuration > General**.
2. Click **Config**.

## Deleting a Zone





To delete a zone:

1. From the Detector's main menu select **Zones > Zone list**.
2. Select the appropriate zone check box.
3. Click **Delete**.

# Zone Status Icons

For illustration purposes, the zone's status is displayed by different icons. Each status is displayed by a different icon. These icons are used in the navigation pane and in the zone's status bar.

**Table 4-1**      *Zone status icons*

|   |   |
|---|---|
|  | Standby zone.   |
|  | Zone in one of the learning phases.   |
|  | Zone in detect mode.  |
|  | Indicates that new recommendations are available for the zone. This icon is displayed in addition to the zone icon. |