



CHAPTER 10

Using Interactive Protect Mode

You can activate the Cisco Guard (Guard) to perform zone protection in either one of the following modes of operation:

- Automatic protect mode—Automatically activates the dynamic filters that it creates during an attack.
- Interactive protect mode—Creates dynamic filters during an attack but does not activate them. Instead, the Guard groups the dynamic filters as recommended actions for you to review and decide whether to accept, ignore, or direct these recommendations to automatic activation.

This chapter describes the interactive protect mode and how to switch between the two modes of operation.

This chapter includes the following sections:

- [Understanding Interactive Protect Mode](#)
- [Activating Interactive Protect Mode and Zone Protection](#)
- [Configuring the Zone for Interactive Protect Mode](#)
- [Displaying Recommendations](#)
- [Managing Recommendations](#)
- [Deactivating Interactive Protect Mode](#)

Understanding Interactive Protect Mode

When a Distributed Denial of Service (DDoS) attack on a zone begins, the zone policies create dynamic filters to mitigate the attack. If you configure the zone to operate in interactive protect mode, the Guard does not activate the dynamic filters automatically, but waits for you to decide on what action to take. The filters that await your decision are called *pending dynamic filters*. The Guard groups the pending dynamic filters according to the policy that produced them and presents the groups to you as *Guard recommendations*, which provide the following information:

- A summary of the pending filters, including information about the name of the policy that caused the creation of the pending dynamic filters.
- The data on the traffic anomaly that resulted in the policy activation.
- The number of pending dynamic filters.
- The recommended action.

When you enable interactive protect mode in a zone configuration, you take control over which actions the Guard executes to mitigate an attack in progress. You decide which pending dynamic filters to accept, ignore, or direct to automatic activation. You can configure the zone to operate in interactive protect mode when you define the zone, before you activate zone protection, or after you activate zone protection.

The Guard continues to produce pending dynamic filters as long as it is in interactive protect mode. You can enable the interactive protect mode at any time during zone protection.

The Guard can manage up to 1000 pending dynamic filters and when the number of pending dynamic filters reaches this limit, the Guard performs the following actions:

- Displays an error message instructing you to deactivate the zone and reactivate it in automatic protect mode.
- Records the recommendations in the zone log file and report and then discards them.

You can switch from the interactive protect mode to the automatic protect mode at any time during zone protection, even when the zone is under attack. When you switch to automatic protect mode during an attack, the Guard performs the following actions:

- Retains the dynamic filters that were added as a result of you accepting a recommendation.
- Accepts the pending dynamic filters associated with any recommendations that you did not act upon prior to switching to automatic protect mode.
- Accepts any new dynamic filters automatically as the policies produce them.

Activating Interactive Protect Mode and Zone Protection

This section provides a quick overview of the steps that you need to take to activate the Guard in interactive protect mode. Each step includes the CLI command required to complete the task.

To activate interactive protect mode, perform the following steps:

Step 1 Configure a new or existing zone to operate in interactive protect mode by using the appropriate command as follows:

- New zone—Enter the **zone** *new-zone-name* **interactive** command in zone configuration mode.

```
user@GUARD-conf# zone scannet interactive
```
- Existing zone—Enter the **interactive** command in zone configuration mode.

```
user@GUARD-conf-zone-scannet# interactive
```

See the [“Configuring the Zone for Interactive Protect Mode” section on page 10-3](#) for more information.

Step 2 (Optional) Configure the Guard to display a notification when new recommendations are available by using the **event monitor** command.

```
user@GUARD# event monitor
```

You can also use an external syslog server to receive notification of new pending dynamic filters or manually display the status of the zone by using the **show** command in zone configuration mode.

Step 3 Activate the Guard to learn the zone traffic patterns by using the **learning** command.

If you have created the zone for on-demand protection, you can skip this step (see the [“Activating On-Demand Protection” section on page 9-2](#) for more information about on-demand protection).

See [Chapter 8, “Learning the Zone Traffic Characteristics,”](#) for more information on the learning process.

- Step 4** Activate zone protection by using the **protect** command.

```
user@GUARD-conf-zone-scannet# protect
```

See [Chapter 9, “Protecting Zones,”](#) for more information.

- Step 5** Display new recommendations and their pending dynamic filters by using the **show recommendations** command.

```
user@GUARD-conf-zone-scannet# show recommendations
user@GUARD-conf-zone-scannet# show recommendations 135 pending-filters
```

See the [“Displaying Recommendations”](#) section on page 10-4 for more information.

- Step 6** Decide how to manage the new recommendations by using the **recommendation** command. You can decide to accept, ignore, or have the Guard automatically activate the new recommendations.

```
user@GUARD-conf-zone-scannet# recommendation 135 accept
```

See the [“Managing Recommendations”](#) section on page 10-5 for more information.

- Step 7** You can deactivate interactive protect mode at any time by using the **no interactive** command. The Guard activates new dynamic filters automatically.

```
user@GUARD-conf-zone-scannet# no interactive
```

See the [“Deactivating Interactive Protect Mode”](#) section on page 10-7 for more information.

Configuring the Zone for Interactive Protect Mode

You can activate interactive protect mode for an existing zone by using the **interactive** command in zone configuration mode.

The following example shows how to activate interactive protect mode for an existing zone:

```
user@GUARD-conf-zone-scannet# interactive
```

To create a new zone configured for interactive protect mode, use the following command in configuration mode:

```
zone new-zone-name interactive
```

The *new-zone-name* argument specifies the name of the new zone. The zone name is an alphanumeric string that must start with a letter, cannot include any spaces, and can have a maximum of 63 characters.

The following example shows how to create a new zone configured for interactive protect mode:

```
user@GUARD-conf# zone scannew interactive
```

The new zone is created with a default zone template that is configured for interactive protect mode. See the [“Creating a New Zone”](#) section on page 5-3 for more information.

Displaying Recommendations

You can display a list of all recommendations, a list of pending dynamic filters, or a specific recommendation for a zone by entering the following command in zone configuration mode:

```
show recommendations [recommendation-id] [pending-filters]
```

Table 10-1 provides the keywords and arguments for the **show recommendations** command.

Table 10-1 Keywords and Arguments for the **show recommendations** Command

Parameter	Description
<i>recommendation-id</i>	(Optional) ID for a specific recommendation.
pending-filters	(Optional) Displays a list of the pending filters for a specific recommendation.

The following example shows how to display a list of all recommendations:

```
user@GUARD-conf-zone-scanner# show recommendations
```

Table 10-2 describes the fields in the **show recommendations** command output.

Table 10-2 Field Descriptions for the **show recommendations** Command Output

Field	Description
ID	Recommendation identification number.
Policy	Policy that created the recommendation.
Threshold	Policy threshold that was exceeded.
Detection date	Date and time that the recommendation was created.
Attack flow	Characteristics of the attack flow. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. They indicate whether or not the traffic is fragmented. A value of any indicates that there is both fragmented and nonfragmented traffic.
Min current rate	Minimum attack rate measured in packets per second (pps). For recommendations that have several pending dynamic filters, the rate of the lowest pending dynamic filter is displayed.
Max current rate	Maximum attack rate measured in packets per second (pps). For recommendations that have several pending dynamic filters, the rate of the highest pending dynamic filter is displayed.
No. of pending-filters	Number of pending dynamic filters that were created because the policy threshold was exceeded.
Recommended action	Recommended action. This action is taken if you accept the recommendation.

To display a list of all recommendations with recommendation IDs before displaying pending filters for a specific recommendation, use the **show recommendations** command.

Table 10-3 describes the fields in the **show recommendations pending-filters** command output.

Table 10-3 Field Descriptions for the **show recommendations pending-filters** Command

Field	Description
ID	Recommendation identification number.
Policy	Policy that created the recommendation.
Threshold	Policy threshold, in packets per second (pps), that was exceeded.
Pending-filter-id	Pending dynamic filter identification number.
Detection date	Date and time that the recommendation was created.
Attack flow	Flow characteristics of the attack. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. They indicate whether or not the traffic is fragmented. A value of any indicates that there is both fragmented and nonfragmented traffic.
Triggering rate	Attack rate, in packets per second (pps), that triggered the creation of the pending dynamic filter.
Current rate	Current attack rate in packets per second (pps).
Recommended action	Recommended action. This action is taken if you accept the recommendation.
Action flow	Resulting characteristics of the traffic flow to the zone if you accept the pending dynamic filter. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. They indicate whether or not the traffic is fragmented. A value of any indicates that there is both fragmented and nonfragmented traffic.

The Guard uses an asterisk (*) as a wildcard for one of the parameters to indicate the following:

- The value is undetermined.
- More than one value was measured for the parameter.



Note

You can display recommendations and their pending dynamic filters only if the Guard is in interactive protect mode and a DDoS attack on the zone is in progress.

The following example shows how to display the pending dynamic filters of recommendation 135:

```
user@GUARD-conf-zone-scannet# show recommendations 135 pending-filters
```

Managing Recommendations

You can decide whether or not to activate recommendations. You can make decisions for all recommendations, a specific recommendation, or for a specific pending dynamic filter. Your decisions determine whether or not the pending dynamic filters in a policy become dynamic filters and for how long.

You can instruct the Guard to automatically activate the pending dynamic filters of a specific policy. You can also instruct the Guard to prevent policies from producing recommendations. The Guard policies continue to produce recommendations if the zone is in interactive protect mode and a DDoS attack is in progress. We recommend that you display the zone status when you manage recommendations in order to verify the zone status and determine whether or not additional actions are required.

**Note**

When you accept a recommendation, you also accept the additional recommendations that contain the same or partial flow with the same action and timeout as the accepted recommendation. The Guard deletes any duplicate recommendations.

To decide on recommendations for a zone, use the following command in zone configuration mode:

```
recommendation recommendation-id [pending-filters pending-filter-id] decision [timeout]
```

Table 10-4 provides the arguments and keywords for the **recommendation** command.

Table 10-4 Arguments and Keywords for the recommendation Command

Parameter	Description
<i>recommendation-id</i>	Identification number of the recommendation. An asterisk (*) is a wildcard, indicating all recommendations.
pending-filters <i>pending-filter-id</i>	(Optional) Specifies the ID of a specific pending dynamic filter.
<i>decision</i>	Action for the recommendation. The following are possible values: <ul style="list-style-type: none"> • accept—Accepts the specific recommendation. The pending dynamic filters become active dynamic filters. • always-accept—Accepts the specific recommendation. The decision applies automatically whenever the recommendation policy produces new recommendations. Pending dynamic filters automatically become active dynamic filters. If you take this action, the Guard no longer displays such recommendations. • always-ignore—Ignores the specific recommendation. No dynamic filter or pending dynamic filters are produced. The decision automatically applies to all future recommendations produced by the policy. If you decide to always ignore a recommendation, the Guard no longer displays it.
<i>timeout</i>	(Optional) Length of time that the decision applies. The following are possible values: <ul style="list-style-type: none"> • forever—Activates the dynamic filters produced by the recommendations for as long as protection is in effect. This timeout is the default. See the “Configuring Dynamic Filters” section on page 6-18 for more information. • new-timeout—Activates the dynamic filters produced by the policies for a period of time that you define. This time is measured in seconds. See the “Configuring Dynamic Filters” section on page 6-18 for more information.

The following example shows how to accept recommendation 135:

```
user@GUARD-conf-zone-scannet# recommendation 135 accept
```

You can configure the interactive status for a specific policy, or any part of it, and decide whether or not that part of the policy should produce recommendations and pending dynamic filters. Configuring the interactive status of a policy gives you control and enables you to improve how policies adapt to traffic flows. See the [“Configuring the Policy Interactive Status” section on page 7-20](#) for more information.

The Guard does not display **always-accept** or **always-ignore** recommendations. When you decide to always ignore or accept a recommendation, your decision becomes part of the interactive status of the policy that created the recommendation.

You can disable or inactivate a policy to prevent the policy from producing recommendations and their pending dynamic filters. Use the **state** command to disable or inactivate a policy. See the [“Changing the Policy State” section on page 7-13](#) for more information.

The following example configures the interactive status for `dns_tcp/53/analysis` to **always-accept**:

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/# interactive-status  
always-accept
```

Deactivating Interactive Protect Mode

To deactivate the interactive protect mode, use the **no interactive** command in zone configuration mode. When you deactivate the interactive protect mode, the Guard activates all new dynamic filters automatically and configures the interactive status of the policies to **always-accept** (see the [“Displaying Policies” section on page 7-21](#) for information on displaying the zone policies).

The following example shows how to deactivate interactive protect mode for the zone scannet:

```
user@GUARD-conf-zone-scannet# no interactive
```

