



## CHAPTER 6

# Configuring Policy Templates and Policies

---

This chapter describes the Cisco Traffic Anomaly Detector (Detector) zone policies, policy structure, and policy templates, and it describes how to configure the zone policy and the policy template parameters.

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector can also synchronize zone configurations with the Guard. For more information about the Guard, see the *Cisco Anomaly Guard Module Configuration Guide* or the *Cisco Guard Configuration Guide*.

This chapter contains the following sections:

- [Understanding Zone Policies](#)
- [Understanding Policy Templates](#)
- [Understanding the Policy Path](#)
- [Configuring Policy Parameters](#)
- [Understanding Worm Policies](#)
- [Monitoring Policies](#)
- [Backing Up the Policy Configuration](#)

## Understanding Zone Policies

The zone policies enable the Detector to perform a statistical analysis of the zone traffic flow. The zone policies are configured to take action against a particular traffic flow if the flow exceeds the policy thresholds, indicating malicious or abnormal traffic. When a flow exceeds the policy thresholds, the policies configure a set of filters (dynamic filters) dynamically to record the event in its syslog or activate a Guard that you have defined in the remote Guard lists. When activated, the Guard protects the zone by mitigating the attack.

Every zone configuration contains a set of policies. When you create a new zone using a predefined zone template, the Detector configures the new zone with policies associated with the template. When you create a new zone by copying an existing zone, the Detector configures the new zone with the policies of the existing zone.

To create zone-specific policies and tune their thresholds to recognize normal zone traffic, the Detector learns the zone traffic in a two-phase learning process (see “[Understanding the Learning Process](#)” section on page 1-4). The Detector uses predefined policy templates to construct the policies and then learns the policy thresholds as determined by the zone traffic. The Detector uses each policy template to create policies that the Detector requires to protect the zone against a specific Distributed Denial of Service (DDoS) threat. After the Detector creates and tunes the zone policies, you can add and delete policies or change policy parameters.

Policies have cross dependencies and priorities. If two different policies define the same traffic flow, the Detector analyzes the flow using the policy that is more specific. For example, policies relating to TCP services exclude the HTTP services that are handled by the HTTP-related policies.

You can configure the policy triggers and the action that the policy takes once it is activated.

## Understanding Policy Templates

A policy template is a collection of policy construction rules that the Detector uses during the policy construction phase to create the zone policies. The name of the policy template is derived from the characteristics that are common to all the policies that it creates and can be a protocol (such as DNS), an application (such as HTTP), or the objective (such as ip\_scan). For example, the policy template *tcp\_connections* produces policies that relate to a connection, such as the number of concurrent connections. When you create a new zone, the Detector includes a set of policy templates in the zone configuration.

This section contains the following topics:

- [Understanding the Different Policy Template Types](#)
- [Configuring Policy Template Parameters](#)

## Understanding the Different Policy Template Types

[Table 6-1](#) describes the Detector policy templates. The Detector includes these policy templates when you create a new zone using the DETECTOR\_DEFAULT zone template.

**Table 6-1** Policy Templates

Policy Template	Constructs a Group of Policies Relating To
dns_tcp	DNS-TCP protocol traffic.
dns_udp	DNS-UDP protocol traffic.
fragments	Fragmented traffic.
http	HTTP traffic that flows, by default, through port 80 (or other user-configured ports).
ip_scan	<p>IP scanning. A situation in which a client from a specific source IP address tries to access many destination IP addresses in the zone. This policy template is designed primarily for zones in which the IP address definition is a subnet.</p> <p>By default, this policy template is disabled. The default action for this policy template is notify.</p> <p><b>Note</b> The policies that are produced from this policy consume system resources and can affect Detector performance.</p>

**Table 6-1** Policy Templates (continued)

Policy Template	Constructs a Group of Policies Relating To
other_protocols	Non-TCP and non-UDP protocols.
port_scan	<p>Port scanning. A situation in which a client from a specific source IP address tries to access many ports in the zone.</p> <p>By default, this policy template is disabled. The default action for this policy template is notify.</p> <p><b>Note</b> The policies that are produced from this policy template consume system resources and can affect Detector performance.</p>
tcp_connections	TCP connection characteristics.
tcp_not_auth	TCP connections that have not been authenticated by the Detector anti-spoofing functions.
tcp_outgoing	TCP connections initiated by the zone.
tcp_ratio	Ratios between different types of TCP packets, for example, the ratio of SYN packets to FIN/RST packets.
tcp_services	TCP services on ports other than HTTP-related, such as ports 80 and 8080.
udp_services	UDP services.

The Detector includes additional policy templates for zones that were created from zone templates that are designed for specific types of attacks or specific services. [Table 6-2](#) details the policy templates that the Detector adds to a zone configuration based on a specific zone template.

**Table 6-2** Additional Policy Templates

Zone Template	Policy Template
DETECTOR_WORM	<p>worm_tcp—Constructs a group of policies that identify TCP worms. Worm TCP policies manage worm attacks in which one or more source IP addresses create many nonestablished connections on the same port to many destination IP addresses. This policy template is designed primarily for zones in which the IP address definition is a subnet.</p> <p>The Detector adds services to policies that are created from this policy template during the threshold tuning phase of the learning process instead of during the policy construction phase. The policy template parameters, max_services and min_threshold, do not apply to this policy template. See the “<a href="#">Understanding Worm Policies</a>” section on page 6-19 for more information.</p>

If you create a zone from a GUARD\_ zone template, you can configure the parameters of additional policy templates that can be synchronized to a Guard. The Detector uses the policy templates described in [Table 6-3](#) and replaces the policy templates http, tcp\_connections, and tcp\_outgoing with the policy templates http\_ns, tcp\_connections\_ns, and tcp\_outgoing\_ns policies. The http\_ns, tcp\_connections\_ns, and tcp\_outgoing\_ns policy templates do not create policies with actions that require the Guard to apply the strong protection level to the traffic flow.

Table 6-3 details the Detector policy templates for GUARD\_TCP\_NO\_PROXY.

**Table 6-3** GUARD\_TCP\_NO\_PROXY Policy Templates

Policy Template	Replaces Policy Template	Constructs a group of policies relating to
tcp_connections_ns	tcp_connections	TCP connection characteristics.
tcp_outgoing_ns	tcp_outgoing	TCP connections initiated by the zone.
http_ns	http	HTTP traffic flowing, by default, through port 80 (or other user-configured ports).

To view a list of all policy templates, use the **policy-template** command in zone configuration mode and press **Tab** twice.

## Configuring Policy Template Parameters

During the learning process, each active policy template produces a group of policies based on the policy definitions and the zone traffic characteristics. The Detector ranks the services (protocol and port numbers) that the policy template monitors by the level of traffic volume. The Detector then selects the services that have the highest traffic volume and that have exceeded the defined minimum threshold, and it creates a policy for each service. Some of the policy templates create an additional policy to handle all traffic flows for which a specific policy was not added with a service of *any*.

You can configure the following policy template parameters:

- **Maximum Number of Services**—Defines the maximum number of services that the Detector picks up for the policy template to create specific policies.
- **Minimum Threshold**—Defines the minimum threshold that must be exceeded for the Detector to rank the service.
- **Policy Template State**—Defines whether or not the Detector produces policies from the policy template.

The policy template parameters maximum number of services and minimum threshold do not affect the worm\_tcp policy template.

To configure the policy template parameters, enter the policy template configuration mode by entering the following command in zone configuration mode:

```
policy-template policy-template-name
```

The *policy-template-name* argument specifies the name of the policy template. See Table 6-1 for more information.

After executing the command, the Detector enters the policy template configuration mode.

The following example shows how to enter http policy template configuration mode:

```
user@DETECTOR-conf-zone-scannet# policy-template http
user@DETECTOR-conf-zone-scannet-policy_template-http#
```

To display the parameters of a specific policy template, use the **show** command in policy template configuration mode.

This section contains the following topics:

- [Configuring the Maximum Number of Services](#)
- [Configuring the Minimum Threshold](#)
- [Configuring Policy Template States](#)
- [Configuring All Policy Template Parameters Simultaneously](#)

## Configuring the Maximum Number of Services

The maximum number of services parameter defines the maximum number of services (protocol numbers or port numbers) for which the policy template selects and creates policies. The Detector ranks the services by the level of traffic volume for each service. The Detector then selects the services that have the highest traffic volume and that have exceeded the defined minimum threshold (as defined by the *min-threshold* parameter), and it creates policies for each service. The Detector may add an additional policy with a service of **any** to handle all other traffic flows with the characteristics of the policy template.



### Note

---

The higher the maximum number of services, the more Detector memory the zone requires.

---

You can only define the maximum number of services parameter for policy templates that detect services: *tcp\_services*, *tcp\_services\_ns*, *udp\_services*, and other protocols. You cannot configure it for policy templates that monitor a specific service, such as *dns\_tcp*, which monitors service 53, or for policy templates that relate to a specific traffic characteristic, such as *fragments*.

The Detector measures the traffic rate of the service based on the policy traffic characteristics. The traffic characteristic can be the source IP addresses or the destination IP addresses. A policy that monitors the service **any** measures the rate of source IP addresses on all services that are not handled by a specific policy.

By limiting the service number, you can configure the Detector policies to your preferred traffic flow requirements.

To configure the maximum number of services, use the following command in policy template configuration mode:

```
max-services max-services
```

The *max-services* argument is an integer greater than 1 that defines the maximum number of services that the Detector selects. We recommend that you do not exceed the maximum of 10 services.

The following example shows how to configure the maximum number of services that the Detector monitors to 5:

```
user@DETECTOR-conf-zone-scannet-policy_template-tcp_services# max-services 5
```

## Configuring the Minimum Threshold

The minimum threshold parameter defines the minimum traffic volume for a service. When the threshold is exceeded, the Detector constructs policies that relate to the service traffic according to the particular traffic flow that exceeded the threshold. By setting the threshold, you can adapt the anomaly detection operation to the traffic volume of the zone services.

You cannot configure the minimum threshold parameter for policy templates that are essential for proper zone anomaly detection and that always construct a policy such as the following policy templates: tcp\_services, udp\_services, other\_protocols, http, and fragments.

To configure the minimum threshold, use the following command in policy template configuration mode:

```
min-threshold min-threshold
```

The *threshold* argument is a real number (a floating point number with two decimal places), equal to or greater than 0, that defines the minimum threshold rate in packets per second (pps). When measuring concurrent connections and the SYN/FIN ratio, the threshold is an integer that defines the total number of connections.

The following example shows how to configure the minimum threshold of the policy template http:

```
user@DETECTOR-conf-zone-scannet-policy_template-http# min-threshold 12.3
```

## Configuring Policy Template States

The policy template state parameter defines whether the policy template is enabled or disabled. If you disable a policy template, it is prevented from producing policies when the Detector is in the policy construction phase.



### Caution

---

Disabling a policy template may seriously compromise zone anomaly detection. If you disable a policy template, the Detector cannot detect the zone traffic to which the policy template relates. For example, disabling the dns\_udp policy template prevents the Detector from creating zone policies that manage DNS (UDP) attacks.

---

To disable a policy template, use the **disable** command in policy template configuration mode.

To enable a policy template, use the **enable** command in policy template configuration mode.

The following example shows how to disable the policy template http:

```
user@DETECTOR-conf-zone-scannet-policy_template-http# disable
```

## Configuring All Policy Template Parameters Simultaneously

You can configure all policy template operational parameters with a single command by entering the following command in zone configuration mode:

```
policy-template policy-template-name max-services min-threshold {disabled | enabled}
```

Table 6-4 provides the arguments and keywords for the **policy-template** command.

**Table 6-4 Arguments and Keywords for the policy-template Command**

Parameter	Description
<i>policy-template-name</i>	Policy template name. See <a href="#">Table 6-1</a> for more information.
<i>max-services</i>	Maximum number of services for which the Detector selects and constructs policies from the specific policy template.  To prevent the Detector from changing the current value, enter a value of -1.  See the “ <a href="#">Configuring the Maximum Number of Services</a> ” section on page 6-5 for more information.
<i>min-threshold</i>	Minimum threshold that must be exceeded for the Detector to rank the service.  To prevent the Detector from changing the current value, enter a value of -1.  See the “ <a href="#">Configuring the Minimum Threshold</a> ” section on page 6-5 for more information.
<b>disabled</b>	<b>Disables the policy template from producing policies.</b> See the “ <a href="#">Configuring Policy Template States</a> ” section on page 6-6 for more information.
<b>enabled</b>	<b>Enables the policy template.</b> See the “ <a href="#">Configuring Policy Template States</a> ” section on page 6-6 for more information.

The following example shows how to set the parameters of the `tcp_services` policy template. The maximum number of services is set to 3, the policy state is set to **enabled**, and the minimum threshold is unchanged (-1).

```
user@DETECTOR-conf-zone-scannet# policy-template tcp_services 3 -1 enabled
```

## Understanding the Policy Path

The name of a policy, or policy path, is composed of sections that describe the traffic characteristic that it measures. For example, the policy `http/80/analysis/syns/src_ip` measures traffic flows of HTTP SYN packets destined to port 80 that were authenticated by the Detector analysis detection level functions and aggregated according to source IP addresses.

[Figure 6-1](#) provides an example of a zone policy name.

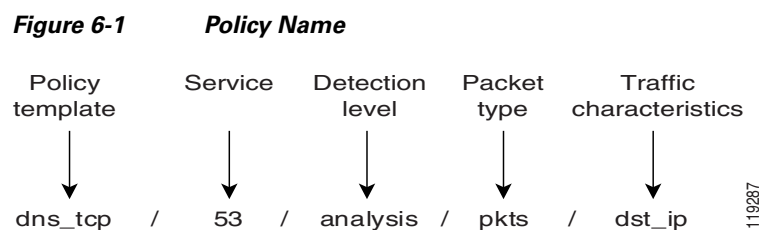


Table 6-5 describes the policy name sections.

**Table 6-5 Policy Name Sections**

Section	Description
Policy template	Policy template that was used to construct the policy. Each policy template deals with the characteristics that the Detector requires to detect a specific DDoS threat. See the “ <a href="#">Understanding Policy Templates</a> ” section on page 6-2 for more information.
Service	Port number or protocol number in the traffic flow that the policy monitors.
Detection level	Detection level that the Detector applies to the traffic flow. Detection levels have a static configuration and cannot be configured manually.
Packet types	Packet types that the Detector monitors.
Traffic characteristics	Traffic characteristics that the Detector uses to aggregate the policy.

The first four sections of the policy name (policy template, service, detection level, and packet type) define the type of traffic that is analyzed. The last section of the policy path (traffic characteristics) defines how to analyze the flow.

This section describes each of the policy path sections as follows:

- [Understanding and Managing the Policy Services](#)
- [Understanding the Packet Types that the Detector Monitors](#)
- [Understanding the Traffic Characteristics that the Detector Monitors](#)

## Understanding and Managing the Policy Services

The service section defines the zone application port or protocol to which each policy relates. Policies have cross dependencies and priorities. If two different policies define the same traffic flow, the Detector analyzes the flow using the policy that is more specific. The service **any** relates to all traffic that does not specifically match other services created from the same policy template.

We recommend that you define specific policies for the zone main services to obtain anomaly detection that is most suited to your individual needs.



### Caution

Do not add the same service (port number) to more than one policy because it may decrease Detector performance.

When you add or delete a service from the zone policies, the Detector marks the zone policies as untuned. If you enabled zone anomaly detection and the learning process, the Detector cannot detect anomalies in the zone traffic until you perform one of the following actions:

- Perform the threshold tuning phase of the learning process and accept the results (see the “[Activating the Threshold Tuning Phase](#)” section on page 7-6).
- Mark the zone policies tuned (see the “[Marking the Policies as Tuned](#)” section on page 7-10).

This section contains the following topics:

- [Adding a Service](#)
- [Deleting a Service](#)

## Adding a Service

You can add services to all policies that were created from a specific policy template. The new service is an addition to the services that were discovered during the policy construction phase and is defined with default values. You can define the threshold manually, but we recommend that you run the threshold tuning phase of the learning process to tune the policies to the zone traffic. See the “[Activating the Threshold Tuning Phase](#)” section on page 7-6 for more information.

You can add a new service to policies that were created from the following policy templates:

- `tcp_services`, `udp_services`, `tcp_services_ns`, or `worm_tcp`

The service designates a port number.

- `other_protocols`

The service designates a protocol number.



### Note

If you activate the policy construction phase after adding a service, new services might override the manually added service.

Unless you enable the policy construction phase, you may need to add a service manually in the following situations:

- A new application or service was added to the zone network.
- The policy construction phase was activated for a short period, so it does not reflect all the network services (for instance, if there are known applications or services that are active only once a week or during the night).

To add a service, use one of the following commands:

- **add-service** *service-num* (in policy template configuration mode)
- **policy-template** *policy-template-name* **add-service** *service-num* (zone configuration mode)

[Table 6-6](#) provides the arguments for the **add-service** command.

**Table 6-6 Arguments for the add-service Command**

Parameter	Description
<code>service-num</code>	Protocol or port number.
<i>policy-template-name</i>	Policy template name. See <a href="#">Table 6-1</a> for more information.

The following example shows how to add a service to all the policies that were created from the policy template `tcp_services`:

```
user@DETECTOR-conf-zone-scannet-policy_template-tcp_services# add-service 25
```

## Deleting a Service

You can delete a specific service for any policy template. The Detector will delete the service from all policies that were created from the specific policy template.

To delete a service, use one of the following commands:

- **remove-service** *service-num* (in policy template configuration mode)
- **policy-template** *policy-template-name* **remove-service** *service-num* (in zone configuration mode)

Table 6-7 provides the arguments for the **remove-service** command.

**Table 6-7 Arguments for the remove-service Command**

Parameter	Description
service-num	Protocol or port number to remove.
policy-template-name	Policy template name. See Table 6-1 for more information.



**Caution**

If you delete a service, the Detector policies cannot monitor the traffic of that service, which may compromise zone anomaly detection.

You can remove services from the following policy templates:

- tcp\_services, udp\_services, or tcp\_services\_ns  
The service is a port number.
- other\_protocols  
The service is a protocol number.

If you do not activate the policy construction phase of the learning process, you may need to remove a service manually in the following situations:

- An application or service was removed from the network.
- An application or service that you do not want to enable (because it is uncommon for the network environment) but was identified during the policy construction phase.



**Note**

If you activate the policy construction phase after removing a service, the same service might be added again.

The following example shows how to delete a service from all policies that were created from the policy template tcp\_services:

```
user@DETECTOR-conf-zone-scanner-policy_template-tcp_services# remove-service 25
```

## Understanding the Packet Types that the Detector Monitors

The Detector monitors packet characteristics, which can be one of the following:

- Packet type (for example, TCP-SYN packets)
- Packet analysis (for example, authenticated packets, which are packets that the Detector has verified their connection by performing a TCP handshake)
- Packet direction (for example, incoming connections)

Table 6-8 describes the packet types that the Detector monitors.

**Table 6-8 Packet Types**

Packet Type	Description
auth_pkts	Packets for which either a TCP handshake or UDP authentication was performed.
auth_tcp_pkts	Packets for which a TCP handshake was performed.
auth_udp_pkts	Packets for which UDP authentication was performed.
in_nodata_conns	Incoming zone connections that have no data transfer on the connection (packets without a data payload).
in_conns	Incoming zone connections.
in_pkts	Incoming zone DNS query packets.
in_unauth_pkts	Incoming zone unauthenticated DNS queries.
non_estb_conns	Nonestablished connections. Incoming zone failed connections, which are TCP connection requests (SYN packets) for which no reply was received.
out_pkts	Incoming zone DNS reply packets.
reqs	Request packets with a data payload.
syms	Synchronization packets (TCP SYN flagged packets).
syn_by_fin	SYN and FIN flagged packets. The Detector verifies the ratio between the number of SYN flagged packets and the number of FIN flagged packets.
unauth_pkts	Packets that did not undergo a TCP handshake.
pkts	All packet types that do not fall under any other category in the same detection level.

## Understanding the Traffic Characteristics that the Detector Monitors

Traffic characteristics define how to analyze the traffic flow and what characteristics were used to aggregate the policies. Different policies can analyze the same traffic flow but measure the rate based on different characteristics, as shown in this example:

`dns_tcp/53/analysis/pkts/dst_ip` and `dns_tcp/53/analysis/pkts/src_ip`.

Table 6-9 describes the traffic characteristics that the Detector monitors.

**Table 6-9 Traffic Characteristics**

Traffic Characteristic	Description
dst_ip	Traffic destined to a zone IP address.
dst_ip_ratio	Ratio of SYN and FIN flagged packets destined to a specific IP address.
dst_port	Traffic destined to a specific zone port.
dst_port_ratio	Ratio of SYN and FIN flagged packets destined to a specific port.
global	Summation of all traffic flow as defined by the other policy sections.
protocol	Traffic destined to the zone aggregated based on the protocol.

**Table 6-9** Traffic Characteristics (continued)

Traffic Characteristic	Description
scanners	Histogram of the number of source IP addresses that scan zone destination IP addresses on a specific destination port. See the “ <a href="#">Understanding Worm Policies</a> ” section on page 6-19 for more information.
src_ip	Traffic destined to the zone aggregated according to the source IP address.
src_ip_many_dst_ips	Traffic from a single IP address that probes a large number of zone IP addresses on the same port. This key is used for IP scanning.
src_ip_many_ports	Traffic from a single IP address that probes a large number of ports on a zone destination IP address. This key is used for port scanning.

## Configuring Policy Parameters

After completing the learning process, you can display specific policy parameters (policy state, policy threshold, policy timeout, policy action, and policy interactive state) to determine if the policy parameters suit the zone traffic. You can configure the policy parameters of a single policy or a group of policies to adapt to zone traffic requirements.

To display the configuration of the policy parameters, use the **show** command in policy configuration mode.

To enter policy configuration mode, use the following command in zone configuration mode:

```
policy policy-path
```

The *policy-path* argument specifies the policy path sections. The path can be a partial path that includes only part of the policy sections. See the “[Understanding Zone Policies](#)” section on page 6-1 for more information.



### Note

To move up one level in the policy path hierarchy, enter **policy ..** at the policy path prompt.

The following example shows how to enter the `dns_tcp/53/analysis/syns/global` policy configuration mode:

```
user@DETECTOR-conf-zone-scannet# policy dns_tcp/53/analysis/syns/global
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global#
```

You can change the policy *action*, *timeout*, *threshold*, and learning parameters at every section of the policy path. However, more policies are affected if you change these parameters at the higher-level policy sections (such as policy template or service sections). If you configure these parameters at a high-level policy path hierarchy, these parameters change in all the subpolicy paths.

You can use an asterisk (\*) as a wildcard character in each policy path section. If you do not specify a policy path section, the Detector relates to the unspecified section as a wildcard (\*). For example, the `tcp_services//analysis//global` policy uses a wildcard for the service and the packet type.

This section contains the following topics:

- [Changing the Policy State](#)
- [Configuring the Policy Threshold](#)
- [Configuring the Policy Timeout](#)

- [Configuring the Policy Action](#)
- [Configuring the Policy Interactive Status](#)

## Changing the Policy State

The zone policies have three possible states as follows:

- Active—The policy monitors the traffic and performs an action once the threshold is exceeded.
- Inactive—The policy monitors the traffic and obtains the threshold, but it takes no action when a threshold is exceeded. You can inactivate a policy to avoid reactivating the threshold-tuning phase of the learning process.
- Disabled—The policy does not monitor the traffic flow, so no threshold is obtained.



### Note

We recommend that you activate the threshold tuning phase of the learning process to ensure that the Detector monitors the correct thresholds for the other policies.



### Caution

When you disable a policy, the active zone policies assume responsibility for the traffic that would normally be monitored by the disabled policy. To adjust the thresholds of the active policies, we recommend that you activate the threshold tuning phase before you activate zone anomaly detection.

To change the policy state, use the following command in policy configuration mode:

```
state {active | disabled | inactive}
```

The following example shows how to set the policy state:

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns# state disabled
```

The following example shows how to set the state of all global policies:

```
user@DETECTOR-conf-zone-scannet-policy-/**/*/global# state inactive
```



### Caution

If you deactivate or disable a policy, the zone policies may not assume their role, and the zone anomaly detection can be compromised.

If you activate the policy construction phase after disabling a zone policy, all zone policies are reconfigured according to the current traffic flow and the policy may be reactivated.

## Configuring the Policy Threshold

The policy threshold defines the threshold traffic rate for a specific policy and is adjusted by the threshold tuning phase. When this threshold is exceeded, the policy performs the action that is defined by the policy action.

The threshold is measured in packets per second except for policies that are constructed from the following policy templates:

- num\_soruces—The threshold is measured in the number of IP addresses or ports.

- `tcp_connections`—The threshold is measured in the number of connections.
- `tcp_ratio`—The threshold is measured as the ratio number.
- `worm_tcp`—The threshold is measured as the maximum number of zone destination IP addresses that a source IP may scan.

You can configure the policy threshold in the following ways:

- Set the threshold—You can set the value of the policy threshold. See the [“Setting the Policy Threshold” section on page 6-14](#).
- Multiply the threshold—The Detector multiplies the current policy thresholds by a factor. The new value may change in subsequent threshold tuning phases if you do not set it as fixed. See the [“Multiplying a Threshold by a Factor” section on page 6-16](#).
- Configure specific IP thresholds—The Detector sets thresholds for specific IP source addresses within the zone address range. See the [“Configuring Specific IP Thresholds” section on page 6-17](#).

The policy threshold may change if you perform additional threshold tuning phases. You can modify how a threshold may change in subsequent threshold tuning phases in the following ways:

- Set the threshold as fixed—The Detector will not change the value of the policy threshold, proxy-threshold, and threshold-list in subsequent threshold tuning phases. See the [“Setting the Threshold as Fixed” section on page 6-14](#).
- Set a fixed multiplier for the policy threshold—The Detector calculates the policy threshold in subsequent threshold tuning phases based on the current policy threshold, the learned threshold, and the fixed multiplier. See the [“Configuring a Threshold Multiplier” section on page 6-15](#).

This section contains the following topics:

- [Setting the Policy Threshold](#)
- [Setting the Threshold as Fixed](#)
- [Configuring a Threshold Multiplier](#)
- [Multiplying a Threshold by a Factor](#)
- [Configuring Specific IP Thresholds](#)

## Setting the Policy Threshold

To configure the policy threshold, use the following command in policy configuration mode:

```
threshold threshold
```

The *threshold* argument is a positive number that specifies the policy threshold.

The following example shows how to set the threshold value of the policy `dns_tcp/53/analysis/syns/global` to 300:

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global# threshold 300
```

## Setting the Threshold as Fixed

You can set a policy threshold, proxy-threshold, and threshold-list as fixed. The Detector ignores new thresholds in the threshold tuning phase of the learning process and maintains the current thresholds. Setting a threshold as fixed enables you to configure the thresholds of a policy but continue learning the thresholds of other policies.

To set a policy threshold as fixed, use the following command in policy configuration mode:

**learning-params fixed-threshold**

The following example shows how to set the threshold of the policy `dns_tcp/53/analysis/syns/global` as fixed:

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global# learning-params fixed-threshold
```

You can set the threshold of several policies as fixed in a single command by entering the command in zone configuration mode. To set a policy threshold as fixed in while zone configuration mode, use the following command:

**policy *policy-path* learning-params fixed-threshold**

The *policy-path* argument specifies the policy path. The path can be a partial path that includes only part of the policy sections. See the “[Understanding Zone Policies](#)” section on page 6-1 for more information.

The following example shows how to set the thresholds of all policies that were created from the `dns_tcp` policy template as fixed:

```
user@DETECTOR-conf-zone-scannet# policy dns_tcp learning-params fixed-threshold
```

To display the policy learning parameters, use the **show learning-params** command in policy configuration mode, or use the **show policies *policy-path* learning-params** command in zone configuration mode.

## Configuring a Threshold Multiplier

You can set a multiplier for a policy threshold. The Detector calculates a new policy threshold by multiplying the learned threshold by the specified multiplier before accepting the results of subsequent threshold tuning phases. The Detector accepts the results of the threshold tuning phase using the configured threshold selection method. See the “[Configuring the Threshold Selection Method](#)” section on page 7-9.

To set a multiplier for the policy threshold, use the following command in zone configuration mode:

**policy *policy-path* learning-params threshold-multiplier *threshold-multiplier***

**Table 6-10** provides the arguments and keywords for the **policy learning-params threshold-multiplier** command.

**Table 6-10 Arguments and Keywords for the policy learning-params threshold-multiplier Command**

Parameter	Description
<i>policy-path</i>	Policy path for which to multiply the thresholds. The path can be a partial path that includes only part of the policy sections. See the “ <a href="#">Understanding Zone Policies</a> ” section on page 6-1 for more information.
<b>learning-params</b>	Configures the learning parameters.
<b>threshold-multiplier</b> <i>threshold-multiplier</i>	Multiplies the policy threshold. The <i>threshold-multiplier</i> is a real positive number (a floating point number with two decimal places) by which the policy threshold is multiplied. Enter a number less than 1 to decrease the policy threshold.

To set a multiplier for the policy threshold in policy configuration mode, use the **learning-params threshold-multiplier** *threshold-multiplier* command.

The following example shows how to configure a threshold multiplier so that the Detector decreases the thresholds of policies that were created from the policy template `dns_tcp` by half in subsequent threshold tuning phases:

```
user@DETECTOR-conf-zone-scannet# policy dns_tcp learning-params threshold-multiplier 0.5
```

To display the policy learning parameters, use the **show learning-params** command in policy configuration mode, or use the **show policies** *policy-path* **learning-params** command in zone configuration mode.

## Multiplying a Threshold by a Factor

You can multiply the thresholds of a policy or a group of policies by a factor, which enables you to increase or decrease the threshold of a policy or a group of policies if the traffic volume does not represent the zone traffic. You can enable the Detector to multiply the policy thresholds, the proxy thresholds, and the thresholds that were defined by the **policy threshold-list** command.

To multiply policy thresholds by a factor, use the following command in zone configuration mode:

```
policy policy-path thresh-mult threshold-multiply-factor
```

Table 6-11 provides the arguments and keywords for the **policy thresh-mult** command.

**Table 6-11 Arguments and Keywords for the policy thresh-mult Command**

Parameter	Description
<i>policy-path</i>	Policy template name. See Table 6-1 for more information.
<b>thresh-mult</b> <i>threshold-multiply-factor</i>	<i>Specifies a real positive number (a floating point number with 4 decimal places) by which to multiply the threshold. Enter a number less than 1 to decrease the policy threshold.</i>

The following example shows how to decrease the thresholds of policies that were created from the policy template `dns_tcp` by half:

```
user@DETECTOR-conf-zone-scannet# policy */*/*/src_ip thresh-mult 0.5
```



### Note

The Detector may change the threshold value in subsequent threshold tuning phases. To prevent the Detector from changing the threshold value, set the threshold value as fixed. See the [“Setting the Threshold as Fixed”](#) section on page 6-14.

To display the policy learning parameters, use the **show learning-params** command in policy configuration mode, or use the **show policies** *policy-path* **learning-params** command in zone configuration mode.

## Configuring Specific IP Thresholds

You can avoid false attack detections by the Detector when traffic increases on a known high traffic source or destination IP address by configuring a policy with a threshold for traffic that is associated with that IP address.

You should consider configuring a specific IP threshold if one of the following situations occurs:

- When there is known high-volume traffic from a source IP address, you can configure a threshold to apply to traffic that originates from the specific source IP address.
- When there is a nonhomogeneous zone (that is, a zone that has more than a single IP address defined) and there is known high-volume traffic flowing to part of the zone only, you can configure a threshold to apply to traffic that targets the specific destination IP address within the zone.

You can configure a specific IP threshold only for policies with traffic characteristics of destination IP (`dest_ip`).

To configure a specific IP threshold, use one of the following commands:

- **policy** *policy-path* **threshold-list** *ip threshold [ip threshold ...]* (in zone configuration mode)
- **threshold-list** *ip threshold [ip threshold ...]* (in policy configuration mode)

Table 6-12 provides the arguments for the **threshold-list** command.

**Table 6-12 Arguments for the policy threshold-list Command**

Parameter	Description
<i>policy-path</i>	Policy template name. See Table 6-1 for more information.
<i>ip</i>	Specific IP address.
<i>threshold</i>	Threshold traffic rate in packets per second, except for policies that measure concurrent connections and SYN-by-FIN ratio, where the threshold is the number of connections.

You can add a maximum of 10 specific IP thresholds for each policy. You can enter all specific IP thresholds in a single command.

The Detector might change the policy thresholds in subsequent threshold tuning phases if the threshold selection method is set to new-thresholds. See the “[Configuring the Threshold Selection Method](#)” section on page 7-9 for more information.

The following example shows how to set specific IP thresholds for IP addresses 10.10.10.2 and 10.10.15.2 for the policy `http/80/analysis/syns/src_ip`:

```
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# threshold-list
10.10.10.2 500 10.10.15.2 500
```

## Configuring the Policy Timeout

The timeout parameter defines the minimum time for dynamic filters that are produced by the policy to apply their action.

To configure the policy timeout, use the following command in policy configuration mode:

```
timeout {forever | timeout}
```

Table 6-13 provides the arguments and keywords for the **timeout** command.

**Table 6-13 Arguments and Keywords for the timeout Command**

Parameter	Description
<b>forever</b>	Specifies an indefinite time span.
<i>timeout</i>	Integer from 1 to 3,000,000 that specifies the minimum time in seconds that the dynamic filters, which are produced by the policy, are active.

The following example shows how to set the timeout of the policy `http/80/analysis/syns/src_ip` to 100 seconds:

```
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# timeout 100
```

To change the timeout of a group of policies simultaneously, use the **policy set-timeout** command in zone configuration mode.

The following example shows how to set the timeout of all policies that were produced from the HTTP policy template and measure source IP addresses to 100:

```
user@DETECTOR-conf-zone-scannet# policy http/*/*/*src_ip set-timeout 100
```

## Configuring the Policy Action

The action parameter defines the type of action that the policy takes once its threshold is exceeded.

To configure the policy action, use the following command in policy configuration mode:

```
action policy-action
```

Table 6-14 describes the policy actions.

**Table 6-14 Policy Actions**

Policy Action	Description
notify	Notifies you when its threshold is exceeded.
remote-activate	Activates remote Guards when its threshold is exceeded. The remote Guards are defined in the remote Guard lists. See the <a href="#">“Activating Remote Guards to Protect a Zone”</a> section on page 8-5 for more information.

The following example shows how to set the action of the policy `http/80/analysis/syns/src_ip`:

```
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# action
remote-activate
```

To change the action of a group of policies simultaneously, use the **policy set-action** command in zone configuration mode.

The following example shows how to set the action of all `dns_tcp` policies:

```
user@DETECTOR-conf-zone-scannet# policy dns_tcp/ set-action remote-activate
set action of dns_tcp/ to remote-activate:
4 policy actions set.
```

## Configuring the Policy Interactive Status

The interactive status parameter defines the interactive status that the pending dynamic filters, which are created by the zone policy, will assume. The interactive status applies only to zones if you enable zone anomaly detection, and the zone is in interactive detect mode. See [Chapter 9, “Using Interactive Detect Mode,”](#) for more information.

To modify the status of the pending dynamic filters that a policy produces after you have set the interactive status of a recommendation to **always-accept** or **always-ignore**, use the **interactive-status** command.

For example, if you have defined the status of a recommendation to **always-accept**, the recommendation and the pending dynamic filters of the recommendation are no longer displayed. To ignore the recommendation or the pending dynamic filters that the recommendation produces, change the policy interactive status to **interactive** or **always-accept**.

To configure the policy interactive status, use the following command in policy configuration mode:

```
interactive-status { always-accept | always-ignore | interactive }
```

[Table 6-15](#) provides the keywords for the **interactive-status** command.

**Table 6-15** Keywords for the *interactive-status* Command

Parameter	Description
<b>always-accept</b>	Accepts the dynamic filters that the policy produces automatically. The action applies automatically whenever the policy produces new recommendations. The Detector does not display <b>these</b> recommendations.
<b>always-ignore</b>	Ignores the dynamic filters that the policy produces automatically. The policy does not produce recommendations when its threshold is exceeded. The Detector does not display <b>these</b> recommendations.
<b>interactive</b>	Waits for you to accept or ignore the dynamic filters that the policy produces. The Detector displays these dynamic filters as part of the recommendations.

The following example shows how to configure the interactive status of policy `dns_tcp/53/analysis/pkts/src_ip` to `always-accept`:

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

## Understanding Worm Policies

Internet worms are automated, self-propagating, intrusion agents that make copies of themselves and facilitate their distribution. Worms attack a vulnerable host, infect it, and then use it as a base to attack other vulnerable targets. They search for other targets by using a form of network inspection, typically a scan, and propagate to the next target. A scanning worm locates vulnerable hosts by generating a list of addresses to probe and then contacting the hosts. Code Red worm, Sasser worm, Blaster worm, and the Slammer worm are all examples of high-profile worms that spread in this manner.

The Detector enables you to detect TCP worm attacks by identifying worms through abnormal traffic patterns that indicate that the zone network is being scanned. The Detector assumes that even if no TCP worm attack is in progress, there may be some scanners in the network. It identifies a scanner as a source IP address that is the initiator of nonestablished connections (an incoming SYN packet for which no SYN/ACK reply packet was identified) to many zone destination IP addresses on a specific port.

To analyze the zone traffic, the Detector uses a table that holds frequency data, which is known as a histogram, of network scanners. The Detector first learns the zone network when no attack is in progress, and then it creates a histogram of concurrent scanners. The histogram describes the number of scanners that concurrently scan specific numbers of zone destination IP addresses. The Detector then measures how many scanners access more than a specific number of zone destination IP addresses.

The Detector uses two types of thresholds to analyze worm traffic characteristics:

- Scanning threshold—Defines the maximum number of zone IP addresses that a single source IP address may scan. This threshold is defined by the policy threshold.
- Histogram threshold—Defines the maximum number of source IP addresses that can scan more than the specified numbers of zone IP addresses.

The Detector identifies a worm attack when there is a deviation from the histogram that it has learned when no attack was in progress (that is, when the number of source IP addresses that concurrently scan more than the defined zone destination IP addresses is exceeded). See the [“Identifying Worm Attacks” section on page 6-21](#) for more information.

Worm policies differ from other policies as follows:

- The Detector learns new services for worm policies during the threshold tuning phase, rather than during the policy construction phase, so you may see new services (ports) added to worm policies during the threshold tuning phase.
- The service **any** relates to ports for which the Detector does not have specific policies. For example, if the Detector has policies for worm\_tcp/80 and worm\_tcp/50, the policy worm\_tcp/any monitors all traffic that is not destined to ports 50 or 80. Unlike other policies, the **any** service does not aggregate the traffic to all unspecified ports. When the Detector monitors the zone traffic, it holds a separate, internal histogram for each port that is scanned. It compares this histogram with the histogram of the **any** service.

This section contains the following topics:

- [Configuring Worm Policies](#)
- [Identifying Worm Attacks](#)

## Configuring Worm Policies

The worm\_tcp policy template is available in the DETECTOR\_WORM zone template only.

The policies that manage TCP worms are constructed from the worm\_tcp policy template, the non\_estb\_conns packet type, and the scanner’s traffic characteristics.

You can configure the histogram and change the scanning thresholds by entering the following command in policy configuration mode:

```
histogram num-dst-ips num-src-ips [num-dst-ips num-src-ips...]
```

Table 6-16 provides the arguments for the **histogram** command.

**Table 6-16 Arguments for the histogram Command**

Parameter	Description
<i>num-dst-ips</i>	Number of scanned zone destination IP addresses. The values of <i>num-dst-ips</i> are 5, 20, and 100 and are system defined. You can modify the value of the <i>num-src-ips</i> that is defined for each <i>num-dst-ips</i> .
<i>num-src-ips</i>	(Optional) Histogram threshold. When the threshold is exceeded, the policy takes the action that is defined by the policy action parameter. The threshold specifies the number of source IP addresses that may scan the specified number of zone destination IP addresses ( <i>num-dst-ips</i> ).

You can enter all the histogram thresholds in a single command.

The following example shows how to set the histogram thresholds for all frequencies:

```
user@DETECTOR-conf-zone-scannet- worm_tcp/445/analysis/non_estb_conns/scanners# histogram
5 99 20 80 50 8 100 1
```

To display the current histogram settings, use the **show policies** command.

You can set the maximum number of zone IP addresses that a single source IP address may scan (scanning threshold). To set this number, use the **threshold** command. See the “[Configuring the Policy Threshold](#)” section on page 6-13 for more information.

To specify the histogram thresholds for a specific port, use the **add-service** command to add a service for the specific port number to all policies that were created from the *worm\_tcp* policy template. See the “[Adding a Service](#)” section on page 6-9 for more information.

## Identifying Worm Attacks

The Detector uses two types of thresholds to analyze worm traffic characteristics: a scanning threshold and a histogram threshold. See the “[Understanding Worm Policies](#)” section on page 6-19 for more information.

When a histogram threshold is exceeded, the Detector produces a dynamic filter with an unspecified source IP address (\*). This dynamic filter indicates that a worm attack is in progress. The dynamic filter policy threshold specifies which histogram threshold was exceeded. The Detector defines a new, internal scanning threshold that is equal to the dynamic filter policy threshold.

The source IP addresses that scan the zone destination IP addresses are those of worm-infected hosts. As long as the zone is under attack, each worm-infected host that scans more zone destination IP addresses than the maximum defined by the new, internal scanning threshold causes the production of a dynamic filter. The Detector acts on these attacking flows as defined by the dynamic filter action.

For example, if the policy threshold (the scanning threshold) is 300, and the policy scanner’s histogram for port 445 is as shown in [Table 6-17](#), then if the Detector identifies a scanner that scans 350 zone destination IP addresses, it produces a dynamic filter indicating that a mass scanner was detected. However, this scanner does not yet imply that a worm attack is in progress.

**Table 6-17 Sample Histogram**

Number of source IP addresses	10	5	2
Number of Destination IP addresses	5	20	100

When the Detector identifies six concurrent source IP addresses that scan more than 50 zone destination IP addresses on port 445, it produces a dynamic filter from the `worm_tcp` policy with an unspecified source IP address (\*) that indicates that the Detector has identified a worm attack on port 445. The dynamic filter policy threshold, 50, specifies the new internal scanning threshold and causes the Detector to lower the threshold definition of a scanner, so that the Detector produces additional dynamic filters for each source IP address that scans more than the new scanning threshold (50).

## Monitoring Policies

You can monitor the policies to see how well they are suited to the zone traffic volume and services.

This section contains the following topics:

- [Displaying Policies](#)
- [Displaying Policy Statistics](#)

## Displaying Policies

You can display the zone policies to verify that they are adapted to the zone traffic characteristics. You might want to view the zone-constructed policies to verify that these policies are customized for the traffic characteristics of the zone. You can configure only policies that appear in this list.

The Detector displays only current zone policies. If a policy template was disabled during the policy construction phase, the Detector does not create policies from that policy template, and you do not see these policies when you enter the **show policies** command.

To display the zone policies, use the following command in zone configuration mode:

```
show policies policy-path
```

The *policy-path* argument specifies a group of policies. You can use an asterisk (\*) as a wildcard character in each policy path section. If you do not specify a policy path section, the Detector considers the unspecified section to be a wildcard (\*). For example, the policy `tcp_services//analysis//global` uses wildcards for the service and the packet type sections.

To display the statistics of all policies, enter an asterisk (\*) for the policy path.

See the “[Understanding Zone Policies](#)” section on page 6-1 for more information about the policy path sections.

The following example shows how to display all the zone policies:

```
user@DETECTOR-conf-zone-scannet# show policies *
```

The following example shows how to display all policies that monitor DNS-over-TCP synchronization packets on port 53:

```
user@DETECTOR-conf-zone-scannet# show policies dns_tcp/53/*/syms/*
```

Table 6-18 describes the fields in the **show policies** command output.

**Table 6-18** *Field Descriptions of the show policies Command Output*

Field	Description
Policy	Policy name. See the “ <a href="#">Understanding Zone Policies</a> ” section on page 6-1 for more information about the policy path sections.
State	Policy state. See the “ <a href="#">Changing the Policy State</a> ” section on page 6-13 for more information. act = active, inact = inactive, disab = disabled
IStatus	Policy interactive status. See the “ <a href="#">Configuring the Policy Interactive Status</a> ” section on page 6-19 for more information. a-accept = always-accept, a-ignor = always-ignore, interac = interactive
Threshold	Policy threshold. When a traffic rate exceeds this threshold, the Detector executes the action associated with the policy. See the “ <a href="#">Configuring the Policy Threshold</a> ” section on page 6-13 for more information.
List	Number of specific IP thresholds defined for the policy. See the “ <a href="#">Configuring Specific IP Thresholds</a> ” section on page 6-17 for more information. Displays H (histogram) for policies that relate to worms. See the “ <a href="#">Understanding Worm Policies</a> ” section on page 6-19 for more information.
Action	Action that the Detector executes when the traffic exceeds the policy threshold. See the “ <a href="#">Configuring the Policy Action</a> ” section on page 6-18 for more information.
Timeout	Minimum time span that the policy action is valid. The Detector determines, according to the filter-termination thresholds, whether or not the dynamic filter that was produced by the policy is to be inactivated. See the “ <a href="#">Configuring the Policy Timeout</a> ” section on page 6-17 for more information.

## Displaying Policy Statistics

You can display the rate of the traffic flowing through a zone policy or a group of zone policies and you can determine whether the type of services and volume represent the zone traffic. The Detector displays the traffic flows forwarded to the zone with the highest rates as measured by the policies. The rate is calculated based on traffic samples.

To display the policy statistics, use the following command in zone configuration mode:

```
show policies policy-path statistics [num-entries]
```

Table 6-19 provides the arguments for the **show policies statistics** command output.

**Table 6-19 Arguments for the show policies statistics Command**

Parameter	Description
<i>policy-path</i>	<p>Group of policies for which to display statistics.</p> <p>You can use an asterisk (*) as a wildcard character in each policy path section. If you do not specify a policy path section, the Detector relates to the unspecified section as a wildcard (*). For example, the policy tcp_services//analysis//global uses wild cards for the service and the packet type sections.</p> <p>To display the statistics of all policies, enter an asterisk (*) for the policy-path.</p> <p>See the “<a href="#">Understanding Zone Policies</a>” section on page 6-1 for more information about the policy path sections.</p>
<i>num-entries</i>	(Optional) Number of entries to display. Enter a number from 1 to 100. The Detector displays the policies with the highest values.

The following example shows how to display the statistics of all the zone policies:

```
user@DETECTOR-conf-zone-scannet# show policies * statistics
```

The following example shows how to display the statistics of all policies that monitor DNS-over-TCP synchronization packets on port 53:

```
user@DETECTOR-conf-zone-scannet# show policies dns_tcp/53/*/syms/*
```

The following example shows how to display the statistics of the zone global traffic:

```
user@DETECTOR-conf-zone-scannet# show policies */**/*global statistics
```

The Detector displays the information in four tables. The information in each table is sorted by value, with the highest values appearing at the top of the table.

Table 6-20 displays the fields in the tables in the **show policies statistics** command output.



**Note**

The Detector does not display tables that contain no data.

**Table 6-20 Field Descriptions of the show policies statistics Command Output Tables**

Column	Description
<b>Fields in all output tables</b>	
Key	<p>Key that is the traffic characteristic used to aggregate the policies.</p> <p>For example, in the tcp_services/any/analysis/syms/dst_ip policy, the key is the destination IP address (dst_ip). If the traffic characteristic that was used to aggregate the policies is global, the key displays N/A.</p> <p>In policies that relate to worms, such as worm_tcp/any/analysis/non_estb_conns/scanners, the key is the the source IP address that scans the zone network addresses, colon, and the destination port that is being scanned, as shown in this example: 192.128.100.3:70.</p> <p>See <a href="#">Table 6-8</a> for more information.</p>

**Table 6-20** *Field Descriptions of the show policies statistics Command Output Tables (continued)*

Column	Description
Policy	Policy name. See the “ <a href="#">Understanding Zone Policies</a> ” section on page 6-1 for more information.
<b>Fields in one of the output tables</b>	
Rate	Rate of the traffic that flows through the policy and is measured in packets per second. The rate is calculated based on traffic samples.
Connection	Number of concurrent connections. This information is available for tcp_connections policies with a packet type of in_nodata_conns.
Ratio	Ratio between the number of SYN flagged packets and the number of FIN/RST flagged packets. This information is available for syn_by_fin policies only.
Dst IPs	Number of zone destination IP addresses that were scanned. This information is available for worm_tcp policies only.

## Backing Up the Policy Configuration

You can back up the current zone policies at any time by using the **snapshot threshold-selection cur-thresholds** command in zone configuration mode.

The following example shows how to create a snapshot to back up the current policy configuration:

```
user@DETECTOR-conf-zone-scannet# snapshot threshold-selection cur-thresholds
```

