



CHAPTER 7

Learning the Zone Traffic Characteristics

This chapter describes how to use the Cisco Traffic Anomaly Detector (Detector) learning process to analyze zone traffic characteristics to create and tune the policies that the Detector uses for zone anomaly detection.

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 the Learning Process and Related Options](#)
- [Synchronizing the Zone Learning Process Results with a Guard](#)
- [Activating the Policy Construction Phase](#)
- [Activating the Threshold Tuning Phase](#)
- [Configuring Learning Parameters](#)
- [Enabling the Detect and Learn Function](#)
- [Using Snapshots to Verify the Results of the Learning Process](#)
- [Backing Up the Zone Policies](#)

Understanding the Learning Process and Related Options

The learning process allows the Detector to analyze normal zone traffic conditions to establish a baseline for determining when traffic is normal and when traffic contains anomalies that indicate an attack on the zone. During the learning process, the Detector creates new zone policies and modifies the policy thresholds based on the normal traffic patterns to produce the reference baseline.

For the learning process to take place, you must configure port mirroring on the switch, or connect the Detector to a router using an optical splitter.

You can enter **learning**-related commands for several zones at the same time. Enter the command in global mode and use an asterisk (*) as a wildcard. For example, to initiate the policy construction phase for all zones, enter the **learning policy-construction *** command in global mode. To accept the results of the policy construction phase for all Detector zones with names that begin with *scan* (such as *scannet* and *scanserver*), enter the **no learning scan* accept** command in global mode.

This section contains the following topics:

- [Understanding the Phases of the Learning Process](#)
- [Verifying the Results of the Learning Process](#)
- [Understanding the Detect and Learn Function](#)

Understanding the Phases of the Learning Process

The learning process consists of these two phases:

- **Policy Construction**—The Detector creates policies for the zone traffic services. The policy templates define the types of zone policies that the Detector creates, the maximum number of services that the Detector monitors closely, and the minimum threshold that triggers the Detector to create new policies. To change the rules for constructing zone policies, you must change the policy template parameters before you initiate the policy construction phase. See [Chapter 6, “Configuring Policy Templates and Policies,”](#) for more information.



Note You cannot perform the policy construction phase for zones that you created using the `GUARD_LINK` or the `DETECTOR_LINK` zone templates.

For more information about using the policy construction phase, see the [“Activating the Policy Construction Phase”](#) section on page 7-4.

- **Threshold Tuning**—The Detector tunes the thresholds of the zone policies to the traffic rates of the zone services. The new thresholds override the existing thresholds.

You can activate the threshold tuning phase and activate zone anomaly detection simultaneously (the detect and learn function) to prevent the Detector from learning malicious traffic thresholds. You can set the Detector to constantly tune the zone policies and define the intervals in which the Detector updates the policy thresholds.

For more information about using the threshold tuning phase, see the [“Activating the Threshold Tuning Phase”](#) section on page 7-6.

During both phases of the learning process, the Detector does not modify the current zone policies until the results of a learning phase are accepted as follows:

- **Manually**—You accept the results of a learning phase.
- **Automatically**—You configure the Detector to automatically accept the learning phase results.

After the policies are created, you can add and delete policies or change policy parameters such as thresholds, services, timeouts, and actions.



Note

The Detector learns new services for worm policies during the threshold tuning phase, rather than during the policy construction phase. You may see new services (ports) added to worm policies during the threshold tuning phase.

Verifying the Results of the Learning Process

You can save the current results of either learning phase at any stage during the learning process and review it later by using the **snapshot** command. Taking a snapshot of the learning process allows you to view the policy information that the Detector has created up to the point of the snapshot and decide

whether or not to accept the results of the learning process. Saving the results of the learning phase in a snapshot does not affect the zone configuration. You can update the zone configuration with the policy information in a snapshot.

For more information about using the `snapshot` command, see the [“Creating Snapshots” section on page 7-12](#).

Understanding the Detect and Learn Function

After the Detector has performed the policy construction phase, you can activate the threshold tuning phase of the learning process and enable zone anomaly detection simultaneously using the detect and learn function. The Detector tunes the policy thresholds while monitoring the traffic for anomalies using the last saved policy thresholds. The detect and learn function enables the Detector to detect zone anomalies, constantly update the policy thresholds based on the zone traffic characteristics, and prevents the Detector from learning malicious traffic thresholds.

Before you activate the detect and learn function, you can configure when and how the Detector accepts the results of the threshold tuning phase by configuring the learning parameters.

See the [“Enabling the Detect and Learn Function” section on page 7-11](#) for more information.

Synchronizing the Zone Learning Process Results with a Guard

You can configure the Detector to perform threshold tuning and to update the corresponding zone configuration on a Guard using a process called *zone synchronization*. For example, when you enable the detect and learn function on the Detector and it detects an anomaly, it stops the learning process, updates the Guard with the latest zone configuration using zone synchronization, and then activates the Guard’s attack mitigation services. Zone synchronization enables you to use the Detector to continuously adjust the zone policy thresholds to changes in the normal traffic for both the Detector and the Guard. Because the Detector analyzes a copy of the zone traffic, you avoid having to constantly divert the zone traffic to the Guard for the learning process.

To synchronize the Detector learning process results with a Guard, you must perform the following tasks:

1. Add the Guard to a remote Guard list on the Detector and define the communication method as Secure Sockets Layer (SSL). See the [“Activating Remote Guards Using Remote Guard Lists” section on page 8-5](#).
2. Establish an SSL communication channel with the Guard. See the [“Configuring the SSL Communication Channel Parameters” section on page 3-18](#).
3. Create the zone on the Detector using a Guard zone template. See the [“Creating a New Zone from a Zone Template” section on page 4-4](#).
4. Activate the detect and learn function for the zone. See the [“Enabling the Detect and Learn Function” section on page 7-11](#).

You can synchronize the zone configuration with the Guard manually or configure the Detector to synchronize the zone configuration with the Guard automatically. See the [“Synchronizing Zone Configurations with a Guard” section on page 4-8](#) for more information.

Activating the Policy Construction Phase

Use the policy construction phase after creating a new zone or any time that the zone configuration needs updating with new service policies. When you enable the policy construction phase, the Detector analyzes the traffic to discover the main services (ports and protocols) that the zone uses. The Detector creates the zone policies for the services using the rules established by the policy templates.



Note

You can reconfigure the policy construction rules by modifying the policy templates before you initiate the policy construction phase. For example, you can prevent the Detector from creating policies of a certain type by disabling the relevant policy template. You can also modify the default values for the policy parameters (timeout, action, and threshold). See [Chapter 6, “Configuring Policy Templates and Policies”](#) for information.

The new policies that the Detector creates during the policy construction phase replace the existing policies when you accept the results of the phase.



Note

You cannot perform the policy construction phase of the learning process for zones that are based on these bandwidth-limited link zone templates: DETECTOR_LINK_128K, DETECTOR_LINK_1M, DETECTOR_LINK_4M and GUARD_LINK_512K, GUARD_LINK_128K, GUARD_LINK_1M, GUARD_LINK_4M, and GUARD_LINK_512K.



Caution

Before you activate the policy construction phase, make sure that no attack on the zone is in progress so that the Detector does not construct the policies based on the traffic characteristics of a DDoS attack. If you allow the Detector to learn the traffic characteristics of a DDoS attack and save the results of the attack as a baseline, you may prevent the Detector from detecting future attacks because the Detector may view the attacks as normal traffic conditions.

To construct the zone policies, perform the following steps:

Step 1 Activate the policy construction phase by entering the following command in zone configuration mode:

```
learning policy-construction
```

Step 2 Check that the Detector is receiving a copy of the zone traffic. Wait at least 10 seconds after initiating policy construction or threshold tuning and enter the **show rates** command. Verify that the value of the *Received traffic* rate is greater than zero. A value of zero indicates that the Detector is not receiving a copy of the zone traffic. Check the configuration of the port mirroring on the switch, or use an optical splitter to check the connection of the Detector to the router.

Step 3 (Optional) Display the policies that the Detector is constructing.

You can save a snapshot of the learning parameters (services, thresholds, and other policy-related data) by using the **snapshot** command at any stage during the policy construction phase, and review it later. You can save a single snapshot or save a periodic snapshot at specified intervals.

For more information, see the [“Backing Up the Policy Configuration”](#) section on page 6-25.

Step 4 (Optional) After you have run the policy construction phase long enough for the Detector to analyze a complete sample of the network traffic, you can accept the policies that the Detector suggested without stopping the policy construction phase. You can accept the policies once, or define that the Detector automatically accept the suggested policies at specified intervals. You can ensure that the zone has the most updated policies and continues to learn the zone traffic.

To accept the policies that the Detector suggested and continue the policy construction phase, use the following command:

```
learning accept
```

To automatically accept the policies that the Detector suggests at specified intervals, use the following command:

```
learning-params periodic-action auto-accept learn_params_days learn_params_hours  
learn_params_minutes
```

See the “[Configuring Learning Parameters](#)” section on page 7-8 for more information.

Use the **no learning-params periodic-action** command to terminate the periodic action.

Step 5 After allowing the Detector enough time to analyze a complete sample of the network traffic, terminate the policy construction phase and decide how to handle the newly constructed policies.



Note

We recommend that you let the policy construction phase continue for at least 2 hours before terminating it to allow the Detector enough time to discover the main services (ports and protocols) that the zone uses.

You can perform one of the following actions:

- Accept the suggested policies—You can accept the policies that the Detector suggested by entering the following command in zone configuration mode:

```
no learning accept
```

The Detector erases previously learned policies and thresholds.

After accepting the newly constructed policies, you can manually add or remove policies. See [Chapter 6, “Configuring Policy Templates and Policies,”](#) for more information.

- Reject the suggested policies—You can reject the policies that the Detector suggested by entering the following command in zone configuration mode:

```
no learning reject
```

The Detector stops the process and does not save the new policies that it has just learned. The policies of the zone are the policies that the Detector had prior to initiating the learning process or prior to the last time that you accepted the results of the policy construction phase.

After performing the policy construction phase, enable the threshold tuning phase to tune the thresholds of each policy (see the “[Activating the Threshold Tuning Phase](#)” section on page 7-6).

The following example shows how to initiate the policy construction phase and accept the suggested policies at 12-hour intervals. The example also shows how to stop the policy construction phase and accept the suggested policies.

```
user@DETECTOR-conf-zone-scannet# learning policy-construction  
user@DETECTOR-conf-zone-scannet# learning-params periodic-action auto-accept 0 12 0  
user@DETECTOR-conf-zone-scannet# no learning accept
```

Activating the Threshold Tuning Phase

Use the threshold tuning phase to enable the Detector to analyze the zone traffic and define thresholds for the zone policies. We recommend that you run the threshold tuning phase during peak traffic time (the busiest part of the day) for a minimum of 24 hours to allow the Detector enough time to properly tune the policy thresholds.



Note

The following procedure includes the command for enabling the detect and learn function which enables the Detector to perform threshold tuning and anomaly detection simultaneously. We recommend that you enable the detect and learn function when you need to perform the threshold tuning phase (see the [“Understanding the Detect and Learn Function”](#) section on page 7-3).

To activate the threshold tuning phase of the learning process, perform the following steps:

Step 1 Initiate the threshold tuning phase by entering one of the following commands in zone configuration mode:

- **learning threshold-tuning**—Enables the threshold tuning phase only.
- **detect learning**—Enables the detect and learn function in which the threshold tuning phase and anomaly detection perform simultaneously. You can also activate the detect and learn function by entering the **learning threshold-tuning** command and the **detect** command (the order is not important).



Note

If you activate the detect and learn function when traffic to the zone is moderate, the Detector may consider the traffic during peak time as an attack. In this case, you can perform one of the following tasks:

- Set the state of the zone policy thresholds to untuned by entering the **no learning-params threshold-tuned** command in zone configuration mode. See the [“Marking the Policies as Tuned”](#) section on page 7-10 for more information.
- Deactivate zone anomaly detection and continue to learn the zone policy thresholds by entering the **no detect** command in zone configuration mode.

Step 2 Verify that the Detector is receiving a copy of the zone traffic. Wait at least 10 seconds after initiating the policy construction phase or the threshold tuning phase and enter the **show rates** command. Verify that the value of the *Received traffic* rate is greater than zero. A value of zero indicates that the Detector is not receiving a copy of the zone traffic. Check the configuration of the port mirroring on the switch, or use an optical splitter to check the connection of the Detector to the router.

Step 3 (Optional) Display the zone policies that the Detector is tuning by using the **snapshot** command (see the [“Using Snapshots to Verify the Results of the Learning Process”](#) section on page 7-12).

Step 4 Accept the suggested thresholds. You can accept the thresholds that the Detector currently suggests and continue the threshold tuning phase, or configure the Detector to automatically accept the suggested policies at specified intervals to ensure that the zone has the most updated thresholds and continues to learn the zone traffic.

To accept the policies that the Detector suggested and continue the threshold tuning phase, use the following command:

```
learning accept [threshold-selection {new-thresholds | max-thresholds | weighted weight}]
```

See [Table 7-2 on page 7-9](#) for a description of the threshold-selection arguments and keywords.

To automatically accept the policies that the Detector suggests at specified intervals, use the following command:

```
learning-params periodic-action auto-accept learn_params_days learn_params_hours
learn_params_minutes
```

See the “[Configuring Learning Parameters](#)” section on [page 7-8](#) for more information.

Use the **no learning-params periodic-action** command to terminate the periodic action.

- Step 5** Terminate the threshold tuning phase and accept or reject the current suggested thresholds after allowing the Detector enough time to properly tune the policy thresholds.



Note If you have the detect and learn function enabled, we recommend that you do not terminate the threshold tuning phase.

You can perform one of the following actions:

- Accept the suggested policies—Terminate the learning process and accept the policy thresholds that the Detector suggests by entering the following command in zone configuration mode:

```
no learning accept [threshold-selection {new-thresholds | max-thresholds | weighted
weight}]
```

See [Table 7-2](#) for a description of the threshold-selection arguments and keywords.

The Detector erases previously learned thresholds.

After accepting the newly tuned policies, you can manually change the policy parameters. See [Chapter 6, “Configuring Policy Templates and Policies,”](#) for more information.

- Reject the suggested policies—Terminate the learning process and reject the policy thresholds that the Detector suggests by entering one of the the following commands in zone configuration mode:

– **no learning reject**

The Detector stops tuning the thresholds and makes no changes to the current thresholds. This process may result in a situation in which new zone policies have thresholds that were obtained based on past traffic characteristics. We recommend that you enable the threshold tuning phase at a later time or that you configure the thresholds manually.

– **deactivate**

If you have the detect and learn function enabled, use the **deactivate** command to terminate anomaly detection and the threshold tuning phase without saving the current suggested thresholds.

The following example shows how to initiate the threshold tuning phase and accept the suggested policies at 1-hour intervals. The Detector then stops the threshold tuning phase and accepts the suggested policies if the threshold values are higher than the current values (the max-thresholds method).

```
user@DETECTOR-conf-zone-scannet# learning threshold-tuning
user@DETECTOR-conf-zone-scannet# learning-params periodic-action auto-accept 0 1 0
user@DETECTOR-conf-zone-scannet# no learning accept threshold-selection max-thresholds
```

After performing the threshold tuning phase, you can perform the following tasks:

- Display the learning process results—Use the **show policies statistics** command to view the results of the threshold tuning phase. See the “[Displaying Policies](#)” section on page 6-22 for more information.
- Modify the learning process results—Change policy parameter values that may not accurately represent normal traffic characteristics. See the “[Configuring Policy Parameters](#)” section on page 6-12 for more information.
- Set the policy threshold as fixed—The next time you enable the threshold tuning phase, the Detector ignores new thresholds and maintains the current ones. See the “[Setting the Threshold as Fixed](#)” section on page 6-14 for more information.
- Set a fixed multiplier for the policy—The next time you enable the threshold tuning phase, the Detector calculates new policy thresholds by multiplying the learned threshold by the specified multiplier and then applying the threshold selection method on the result. See the “[Configuring a Threshold Multiplier](#)” section on page 6-15 for more information.

Configuring Learning Parameters

This section shows how to configure the learning parameters to manage the following functions that affect all of the zone policies:

- Period Detector actions—Configure the Detector to automatically accept the zone policies and save a snapshot of the zone policies at specified intervals.
- Threshold selection method—Configure the default method that the Detector uses to generate new policy thresholds after it accepts the results of the threshold tuning phase.
- Tuned state of the zone policies—Set the state of the current zone policies to tuned or untuned.

To display the current configuration of the learning parameters, use the **show learning-params** command in zone configuration mode.

This section contains the following topics:

- [Configuring Periodic Actions](#)
- [Configuring the Threshold Selection Method](#)
- [Marking the Policies as Tuned](#)

Configuring Periodic Actions

You can configure the Detector to perform one of the following actions at specified intervals:

- Automatically accept the zone policies and save a snapshot of the policies
- Save a snapshot of the zone policies only

See the “[Verifying the Results of the Learning Process](#)” section on page 7-2 for more information about snapshots.

To set the periodic action that the Detector performs, use the following command in zone configuration mode:

```
learning-params periodic-action { auto-accept | snapshot-only } learn_params_days
learn_params_hours learn_params_minutes
```

Table 7-1 provides the arguments and keywords for the **learning-params** command.

Table 7-1 Arguments and Keywords for the learning-params periodic-action Command

Parameter	Description
auto-accept	Accepts the policies that the Detector suggested at the specified interval. The Detector saves a snapshot of the zone policies after accepting the newly suggested ones.
snapshot-only	Saves a snapshot of the policies at the specified interval. The Detector does not accept the new policies and does not modify the policy thresholds.
<i>learn_params_days</i>	Interval in days. Enter an integer from 0 to 1000.
<i>learn_params_hours</i>	Interval in hours. Enter an integer from 0 to 1000.
<i>learn_params_minutes</i>	Interval in minutes. Enter an integer from 0 to 1000.

The value of the interval is the sum of the *learn_params_days* value, the *learn_params_hours* value, and the *learn_params_minutes* value.

The following example shows how to set the Detector to accept the policies at 1-hour intervals:

```
user@DETECTOR-conf-zone-scannet# learning-params periodic-action auto-accept 0 1 0
```

Configuring the Threshold Selection Method

You can define the default method that the Detector uses to generate new thresholds to accept during the threshold tuning phase. You can accept the results of the threshold tuning phase manually, or configure the Detector to automatically accept the results of the threshold tuning phase at specified intervals.

To configure the threshold selection method, use the following command in zone configuration mode:

```
learning-params threshold-selection {new-thresholds | max-thresholds | weighted weight}
```

Table 7-2 provides the arguments and keywords for the **learning-params threshold-selection** command.

Table 7-2 Arguments and Keywords for the learning-params threshold-selection Command

Parameter	Description
new-thresholds	Saves the results of the learning process to the zone configuration.
max-thresholds	Compares the current policy threshold to the learned threshold and saves the higher threshold to the zone configuration. This method is the default.
weighted <i>weight</i>	Calculates the policy thresholds to save based on the following formula: $\text{new-threshold} = (\text{learned-threshold} * \text{weight} + \text{current-threshold} * (100 - \text{weight})) / 100$

This example shows how to configure the Detector to accept the suggested policies if the learned threshold values are higher than the current policy threshold values:

```
user@DETECTOR-conf-zone-scannet# learning-params threshold-selection max-thresholds
```

Marking the Policies as Tuned

The Detector marks the policy threshold status that defines if the policy thresholds are tuned or not and relates to this status when you enable the protect and learn function. The policy threshold status specifies if the Detector identifies an attack on the zone when the policy threshold is exceeded.

When a new zone is created, or after you accept the policy construction phase results for a zone, the Detector marks the zone policy thresholds as untuned. The default thresholds of the zone templates are tuned so that the Detector activates the anti-spoofing functions quickly if it identifies traffic anomalies in the zone traffic. When you enable the protect and learn function, the learning process might stop if the current zone traffic is higher than the current policy threshold values. To avoid this situation, if the zone policies are not tuned, the Detector does not detect attacks in the zone traffic when you enable the detect and learn function until the zone policy thresholds are accepted once.

If the zone policies are untuned, the Detector activates only a threshold selection method of accept-new and ignores previous threshold values when accepting the new policies. If the Detector accepts the threshold tuning phase results of the learning process for a zone with a threshold selection method other than accept-new, bad policy threshold values may result. See the [“Configuring the Threshold Selection Method” section on page 7-9](#) for more information about the threshold selection method.

The Detector marks the zone policies as untuned in the following situations:

- When creating a new zone
- After accepting the policy construction phase results
- After removing a service or adding a new service to the zone policies

The Detector marks the zone policies as tuned after accepting the threshold tuning phase results.

You can modify the settings of the zone policies. To mark the zone policies as tuned, use the following command in zone configuration mode:

learning-params threshold-tuned

To mark the zone policies as untuned, use the **no** form of this command.

You may want to change the status of the zone policies to tuned when one of the following applies:

- The new zone was duplicated from an existing zone or snapshot that has similar traffic characteristics.
- You have manually configured all policy thresholds.

You may want to change the status of the zone policies to untuned when one of the following applies:

- A major change was made in the zone network.
- The zone IP address or subnet was modified.
- You have not initiated the detect and learn function during the peak traffic time. Change the status of the zone policies to untuned to prevent the Detector from identifying the traffic during the peak time as an attack.

When the zone policies are marked as untuned, the Detector does not monitor the current policy thresholds and does not detect attacks on the zone if the policy thresholds are exceeded.



Caution

Do not change the status of the zone policies to untuned if there is an attack on the zone because that prevents the Detector from detecting the attack and causes the Detector to learn malicious traffic thresholds.

The following example shows how to mark the status of the zone policies as tuned:

```
user@DETECTOR-conf-zone-scannet# learning-params threshold-tuned
```

Enabling the Detect and Learn Function

You can enable the threshold tuning phase of the learning process and zone anomaly detection simultaneously by using the detect and learn function. The Detector continuously tunes the policy thresholds and at the same time monitors the traffic for anomalies using the last saved policy thresholds. If the Detector detects an attack on the zone, it stops the learning process to prevent it from learning malicious traffic thresholds. If you have the Detector configured to activate a Guard to mitigate the attack, it activates the Guard and then constantly polls the Guard. When the Detector determines that the Guard has deactivated zone protection, it verifies that additional traffic anomalies do not exist before reactivating the detect and learn function.

Perform the following actions before you activate the detect and learn function:

- Activate the policy construction phase of the learning process to construct zone-specific policies (see the [“Activating the Policy Construction Phase”](#) section on page 7-4).
- Display the current tuned state of the zone policies by using the **show learning-params** command in zone configuration mode. If the policies are tuned, then the Detector is ready to perform the detect and learn operation.



Caution

If the zone policies are untuned when you enable the detect and learn function, the Detector is unable to detect zone anomalies until the first time that you accept the results of the threshold tuning phase.

If the policies are untuned, the Detector functions as follows until the first time that you accept results of threshold tuning phase:

- Performs the threshold tuning phase of the learning process only. The Detector does not detect anomalies because it does not monitor the traffic for policy threshold violations. After the first time that you accept the results of the threshold tuning phase, the Detector marks the policies as tuned and begins monitoring the traffic for anomalies.
- The Detector activates a threshold selection method of **accept-new** even if you have the threshold selection method configured for **max-threshold** or **weighted** (see the [“Configuring the Threshold Selection Method”](#) section on page 7-9). After the first time that you accept the results of the threshold tuning phase, the Detector uses the threshold selection method that you have configured.

See the [“Marking the Policies as Tuned”](#) section on page 7-10 for more information.

You can accept the results of the threshold tuning phase manually or configure the Detector to accept the results automatically. You can also configure when and how the Detector accepts the results of the learning process (see the [“Configuring Learning Parameters”](#) section on page 7-8.)

To activate the learning process and zone anomaly detection simultaneously, use the **detect learning** command or enter both the **learning threshold-tuning** command and the **detect** command (the order is not important).

For more information about the threshold tuning phase, see the [“Activating the Threshold Tuning Phase”](#) section on page 7-6. For more information about enabling anomaly detection, see Chapter 8, [“Detecting Zone Traffic Anomalies.”](#)

Using Snapshots to Verify the Results of the Learning Process

The snapshot function allows you to save a copy of the learning parameters (services, thresholds, and other policy-related data) at any stage of the learning process. You can use snapshots to perform the following tasks:

- Compare the learning parameters of two zones.
- Compare two of the zone snapshots to verify the outcome of the learning process and trace the differences in policies, services, and thresholds.
- Use the policies of a snapshot taken during normal traffic conditions to provide anomaly detection if an attack occurs during the learning process.
- Copy zone policies from a snapshot to configure the zone according to previous learning results.

We recommend that you save a snapshot every few hours during the learning process. You can take the snapshot manually or configure the Detector to automatically take a snapshot at specified intervals. The Detector can save up to 100 snapshots for each zone. New snapshots replace the previous ones.

This section contains the following topics:

- [Creating Snapshots](#)
- [Comparing Learning Results](#)
- [Displaying Snapshots](#)
- [Deleting Snapshots](#)
- [Copying Policies to the Zone Configuration](#)

Creating Snapshots

You can save a single snapshot of the zone learning parameters or configure the Detector to automatically take a snapshot at specified intervals. The Detector continues the learning process while taking a snapshot.

To configure the Detector to automatically take a snapshot at specified intervals, see the “[Configuring Periodic Actions](#)” section on page 7-8 for more information.

To save a single snapshot of the zone learning parameters, use the following command in zone configuration mode:

```
snapshot [threshold-selection {new-thresholds | max-thresholds | cur-thresholds | weighted
calc-weight}]
```

[Table 7-3](#) provides the arguments and keywords for the **snapshot** command.

Table 7-3 Arguments and Keywords for the snapshot Command

Parameter	Description
threshold-selection	(Optional) Specifies the method that the Detector uses to calculate the snapshot thresholds. By default, the Detector uses the zone threshold-selection method that is defined by the learning-params threshold-selection command. The default zone threshold-selection method is max-thresholds .
new-thresholds	Saves the results of the leaning process to the zone configuration.

Table 7-3 Arguments and Keywords for the snapshot Command (continued)

Parameter	Description
max-thresholds	Compares the current policy threshold to the learned threshold and saves the higher threshold to the zone configuration. This is the default method.
cur-thresholds	Ignores the new thresholds of the learning process and saves the current policy thresholds to the snapshot. You can use this method to create a backup of the current zone policies and policy thresholds.
weighted <i>calc-weight</i>	Calculates the policy thresholds to save based on the following formula: $\text{threshold} = (\text{new-threshold} * \text{calc-weight} + \text{current-threshold} * (100 - \text{calc-weight})) / 100$

The following example shows how to create a snapshot in which the thresholds are the highest value between the current policy threshold and the new threshold of the learning process:

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

To save a single snapshot in global mode, use the following command:

```
snapshot zone-name [threshold-selection {new-thresholds | max-thresholds | cur-thresholds | weighted weight}]
```

Comparing Learning Results

You can compare the learning results of two snapshots or two zones to trace the differences in policies, services, and thresholds.

This section contains the following topics:

- [Comparing Snapshots](#)
- [Comparing Zones](#)

Comparing Snapshots

To compare two snapshots, use the following command in zone configuration mode:

```
diff snapshots snapshot-id1 snapshot-id2 [percent]
```

Table 7-4 provides the arguments for the **diff** command.

Table 7-4 Arguments for the diff Command

Parameter	Description
snapshot-id1	Identifier of the first snapshot to compare. To display a list of the zone snapshots, use the show snapshots command.

Table 7-4 Arguments for the diff Command (continued)

Parameter	Description
<i>snapshot-id2</i>	Identifier of the second snapshot to compare. To display a list of the zone snapshots, use the show snapshots command.
<i>percent</i>	(Optional) Percentage of difference. The Detector compares the two snapshots and displays only the differences in policy thresholds that are greater than the specified value. The default percentage is 100%, which means that the Detector displays all the differences between the two snapshots.

The following example shows how to display the zone snapshots and compare the two most recent snapshots:

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
3    Feb 10 11:01:50
user@DETECTOR-conf-zone-scannet# diff 2 3
```

To compare snapshots in global mode, use the following command:

```
diff zone-name snapshots snapshot-id1 snapshot-id2 [percent]
```

Comparing Zones

You can compare the learning parameters of two zones by using the following command in global mode or in configuration mode:

```
diff zone-name1 zone-name2 [percent]
```

Table 7-5 provides the arguments for the **diff** command.

Table 7-5 Arguments for the diff Command

Parameter	Description
<i>zone-name1</i>	Name of the first zone with learning parameters that is to be compared.
<i>zone-name2</i>	Name of the second zone with learning parameters that is to be compared.
<i>percent</i>	(Optional) Percentage of difference. The Detector compares the two zones and displays only differences in policy thresholds that are higher than the specified value. The default percentage is 100%, which means that the Detector displays all differences between the two zones.

The following example shows how to compare the learning parameters of two zones:

```
user@DETECTOR# diff scannet scannet-mailserver
```

Displaying Snapshots

You can display a list of the zone snapshots or the snapshot parameters to get a comprehensive view of the zone learning results by entering the following command in zone configuration mode:

```
show snapshots [snapshot-id [policies policy-path]]
```

Table 7-6 provides the arguments and keywords for the **show snapshots** command.

Table 7-6 Arguments and Keywords for the show snapshots Command

Parameter	Description
<i>snapshot-id</i>	(Optional) Identifier of the snapshot to display. If you do not specify policies, the default is to display a list of all the zone snapshots. To view the snapshot ID, use this command with no arguments.
policies <i>policy-path</i>	(Optional) Specifies a group of policies to display. See the “ Understanding Zone Policies ” section on page 6-1 for more information.

To compare snapshots in global mode, use the the following command:

```
show zone zone-name snapshots [snapshot-id [policies policy-path]]
```

The fields of the **show zone zone-name snapshots snapshot-id policies policy-path** command output are identical to the fields in the output of the **show policies** command. See the “[Displaying Policies](#)” section on page 6-22 for more information.

Table 7-7 describes the fields in the **show snapshots** command output.

Table 7-7 Field Descriptions for show snapshots Command Output

Field	Description
ID	Snapshot identifier.
Time	Date and time that the snapshot was taken.

The following example shows how to display a list of the zone snapshots and the policies that are related to dns_tcp in snapshot 2:

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
user@DETECTOR-conf-zone-scannet# show snapshots 2 policies dns_tcp
```

Deleting Snapshots

You can delete old snapshots to free disk space by using the following command in zone configuration mode:

```
no snapshot snapshot-id
```

The *snapshot-id* argument specifies the identifier of an existing snapshot. Enter an asterisk (*) to delete all the zone snapshots. To view the details of a snapshot, use the **show snapshots** command.

The following example shows how to delete all the zone snapshots:

```
user@DETECTOR-conf-zone-scannet# no snapshot *
```

Copying Policies to the Zone Configuration

You can copy a complete policy configuration or a partial configuration to the current zone.

You can copy the following information:

- Copy services—You can copy services from a source zone to the zone, which allows you to configure the zone policies without applying the policy construction phase to discover these services. Before you copy services to the zone, verify that the zones have similar traffic patterns.
- Copy policy parameters—You can replace the zone policy parameters with the policy parameters of one of the zone snapshots, which allows you to revert to prior learning results. The Detector copies parameters of existing policies only.

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

```
copy-policies { snapshot-id | src-zone-name [service-path] }
```

Table 7-8 provides the arguments and keywords for the **copy-policies** command.

Table 7-8 Arguments and Keywords for the copy-policies Command

Parameter	Description
<i>snapshot-id</i>	Identifier of the snapshot from which the policies are copied. To view the snapshot ID, use the show snapshots command.
<i>src-zone-name</i>	Name of the zone for which service policies are copied.
<i>service-path</i>	(Optional) Service to be copied. A service path can have one of the following formats: <ul style="list-style-type: none"> • policy-template—Copies all policies that relate to the policy template. • policy-template/service-num—Copies all policies that relate to the policy template and the specified service. The default is to copy all policies and services.

The following example shows how to copy all services that relate to the policy template tcp_connections from the zone webnet to the current zone, scannet:

```
user@DETECTOR-conf-zone-scannet# copy-policies webnet tcp_connections/
```

The following example shows how to display a list of the zone snapshots and then copy the policies from the snapshot with ID 2:

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
user@DETECTOR-conf-zone-scannet# copy-policies 2
```

Backing Up the Zone Policies

You can create a backup the current zone policies at any time by using the following command in zone configuration mode:

```
snapshot threshold-selection cur-thresholds
```

The following example shows how to back up the current zone policies:

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

