



Configuring Anomaly Detection



Note

Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

This chapter describes how to create multiple security policies and apply them to individual virtual sensors. It contains the following sections:

- [Understanding Security Policies, page 13-1](#)
- [Anomaly Detection Components, page 13-2](#)
- [Configuring Anomaly Detections Policies, page 13-9](#)
- [ad0 Pane, page 13-10](#)
- [Configuring Operation Settings, page 13-11](#)
- [Configuring Learning Accept Mode, page 13-12](#)
- [Configuring the Internal Zone, page 13-15](#)
- [Configuring the Illegal Zone, page 13-22](#)
- [Configuring the External Zone, page 13-29](#)
- [Disabling Anomaly Detection, page 13-35](#)

Understanding Security Policies

You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies. The use of multiple security policies lets you create security policies based on different requirements and then apply these customized policies per VLAN or physical interface.

Anomaly Detection Components

The following section describes the various components of anomaly detection, and contains the following topics:

- [Understanding Anomaly Detection, page 13-2](#)
- [Worms, page 13-2](#)
- [Anomaly Detection Modes, page 13-3](#)
- [Enabling Anomaly Detection, page 13-4](#)
- [Anomaly Detection Zones, page 13-5](#)
- [Anomaly Detection Configuration Sequence, page 13-5](#)
- [Anomaly Detection Signatures, page 13-7](#)

Understanding Anomaly Detection

The anomaly detection component of the sensor detects worm-infected hosts. This enables the sensor to be less dependent on signature updates for protection against worms and scanners, such as Code Red and SQL Slammer and so forth. The anomaly detection component lets the sensor learn normal activity and send alerts or take dynamic response actions for behavior that deviates from what it has learned as normal behavior.

**Note**

Anomaly detection does not detect email-based worms, such as Nimda.

Anomaly detection detects the following two situations:

- When the network starts on the path of becoming congested by worm traffic.
- When a single worm-infected source enters the network and starts scanning for other vulnerable hosts.

Worms

**Caution**

Anomaly detection assumes it gets traffic from both directions. If the sensor is configured to see only one direction of traffic, you should turn off anomaly detection. Otherwise, when anomaly detection is running in an asymmetric environment, it identifies all traffic as having incomplete connections, that is, as scanners, and sends alerts for all traffic flows. Using asymmetric mode protection with anomaly detection enabled causes excessive resource usage and possible false positives for anomaly detection signatures.

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

Anomaly detection identifies worm-infected hosts by their behavior as scanners. To spread, a worm must find new hosts. It finds them by scanning the Internet or network using TCP, UDP, and other protocols to generate unsuccessful attempts to access different destination IP addresses. A scanner is defined as a source IP address that generates events on the same destination port (in TCP and UDP) for too many destination IP addresses.

The events that are important for TCP protocol are nonestablished connections, such as a SYN packet that does not have its SYN-ACK response for a given amount of time. A worm-infected host that scans using TCP protocol generates nonestablished connections on the same destination port for an anomalous number of IP addresses.

The events that are important for UDP protocol are unidirectional connections, such as a UDP connection where all packets are going only in one direction. A worm-infected host that scans using UDP protocol generates UDP packets but does not receive UDP packets on the same quad within a timeout period on the same destination port for multiple destination IP addresses.

The events that are important for other protocols, such as ICMP, are from a source IP address to many different destination IP addresses, that is, packets that are received in only one direction.

**Caution**

If a worm has a list of IP addresses it should infect and does not have to use scanning to spread itself (for example, it uses passive mapping—listening to the network as opposed to active scanning), it is not detected by the anomaly detection worm policies. Worms that receive a mailing list from probing files within the infected host and email this list are also not detected, because no Layer 3/Layer 4 anomaly is generated.

For More Information

- For more information about how worms operate, see [Worms, page 13-2](#).
- For the procedure for turning off anomaly detection, refer to [Disabling Anomaly Detection, page 13-35](#).

Anomaly Detection Modes

**Note**

Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

If you have anomaly detection enabled, it initially conducts a “peacetime” learning process when the most normal state of the network is reflected. Anomaly detection then derives a set of policy thresholds that best fit the normal network.

Anomaly detection has the following modes:

- Learning accept mode—Anomaly detection conducts an initial learning accept mode for the default period of 24 hours. We assume that during this phase no attack is being carried out. Anomaly detection creates an initial baseline, known as a knowledge base (KB), of the network traffic. The default interval value for periodic schedule is 24 hours and the default action is rotate, meaning that a new KB is saved and loaded, and then replaces the initial KB after 24 hours.

**Note**

Anomaly detection does not detect attacks when working with the initial KB, which is empty. After the default of 24 hours, a KB is saved and loaded and now anomaly detection also detects attacks.



Note Depending on your network complexity, you may want to have anomaly detection in learning accept mode for longer than the default 24 hours.

- **Detect mode**—For ongoing operation, the sensor should remain in detect mode. This is for 24 hours a day, 7 days a week. Once a KB is created and replaces the initial KB, anomaly detection detects attacks based on it. It looks at the network traffic flows that violate thresholds in the KB and sends alerts. As anomaly detection looks for anomalies, it also records gradual changes to the KB that do not violate the thresholds and thus creates a new KB. The new KB is periodically saved and takes the place of the old one thus maintaining an up-to-date KB.
- **Inactive mode**—You can turn anomaly detection off by putting it in inactive mode. Under certain circumstances, anomaly detection should be in inactive mode, for example, if the sensor is running in an asymmetric environment. Because anomaly detection assumes it gets traffic from both directions, if the sensor is configured to see only one direction of traffic, anomaly detection identifies all traffic as having incomplete connections, that is, as scanners, and sends alerts for all traffic flows. Having anomaly detection running also lowers performance.

Example

The following example summarizes the default anomaly detection configuration. If you add a virtual sensor at 11:00 pm and do not change the default anomaly detection configuration, anomaly detection begins working with the initial KB and only performs learning. Although it is in detect mode, it cannot detect attacks until it has gathered information for 24 hours and replaced the initial KB. At the first start time (10:00 am by default), and the first interval (24 hours by default), the learning results are saved to a new KB and this KB is loaded and replaces the initial KB. Because the anomaly detection is in detect mode by default, now that anomaly detection has a new KB, the anomaly detection begins to detect attacks.

For More Information

- For the procedure for enabling anomaly detection, see [Enabling Anomaly Detection, page 13-4](#).
- For more information on how worms operate, see [Worms, page 13-2](#).
- For the procedure for configuring the sensor to be in different anomaly detection modes, see [Adding, Editing, and Deleting Virtual Sensors, page 8-12](#).

Enabling Anomaly Detection



Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

To enable anomaly detection, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator or operator privileges.
 - Step 2** Choose **Configuration > sensor_name > Policies > IPS Policies**.
 - Step 3** Select the virtual sensor for which you want to turn on anomaly detection, and then click **Edit**.
 - Step 4** Under Anomaly Detection, choose an anomaly detection policy from the Anomaly Detection Policy drop-down list. Unless you want to use the default ad0, you must have already added a anomaly detection policy by choosing **Configuration > sensor_name > Policies > Anomaly Detections > Add**.

Step 5 Choose Detect as the anomaly detection mode from the AD Operational Mode drop-down list. The default is Inactive.



Tip To discard your changes and close the Edit Virtual Sensor dialog box, click **Cancel**.

Step 6 Click **OK**.



Tip To discard your changes, click **Reset**.

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Anomaly Detection Zones

By subdividing the network into zones, you can achieve a lower false negative rate. A zone is a set of destination IP addresses. There are three zones, internal, illegal, and external, each with its own thresholds.

The external zone is the default zone with the default Internet range of 0.0.0.0-255.255.255.255. By default, the internal and illegal zones contain no IP addresses. Packets that do not match the set of IP addresses in the internal or illegal zone are handled by the external zone.

We recommend that you configure the internal zone with the IP address range of your internal network. If you configure it in this way, the internal zone is all the traffic that comes to your IP address range, and the external zone is all the traffic that goes to the Internet.

You can configure the illegal zone with IP address ranges that should never be seen in normal traffic, for example, unallocated IP addresses or part of your internal IP address range that is unoccupied. An illegal zone can be very helpful for accurate detection, because we do not expect any legal traffic to reach this zone. This allows very low thresholds, which in turn can lead to very quick worm virus detection.

For More Information

For more information about configuring anomaly detection zones, see [Configuring the Internal Zone, page 13-15](#), [Configuring the Illegal Zone, page 13-22](#), and [Configuring the Illegal Zone, page 13-22](#).

Anomaly Detection Configuration Sequence



Note

Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

You can configure the detection part of anomaly detection. You can configure a set of thresholds that override the KB learned thresholds. However, anomaly detection continues learning regardless of how you configure the detection. You can also import, export, and load a KB and you can view a KB for data.

Follow this sequence when configuring anomaly detection:

1. Create an anomaly detection policy to add to the virtual sensors. Or you can use the default anomaly detection policy, ad0.

2. Add the anomaly detection policy to your virtual sensors.
3. Enable anomaly detection.
4. Configure the anomaly detection zones and protocols.
5. For the first 24 hours anomaly detection performs learning to create a populated KB. The initial KB is empty and during the default 24 hours, anomaly detection collects data to use to populate the KB. If you want the learning period to be longer than the default period of 24 hours, you must manually set the mode to learning accept.
6. Let the sensor run in learning accept mode for at least 24 hours (the default). You should let the sensor run in learning accept mode for at least 24 hours so it can gather information on the normal state of the network for the initial KB. However, you should change the amount of time for learning accept mode according to the complexity of your network. After the time period, the sensor saves the initial KB as a baseline of the normal activity of your network.



Note We recommend leaving the sensor in learning accept mode for at least 24 hours, but letting the sensor run in learning accept mode for longer, even up to a week, is better.

7. If you manually set anomaly detection to learning accept mode, switch back to detect mode.
8. Configure the anomaly detection parameters:
 - Configure the worm timeout and which source and destination IP addresses should be bypassed by anomaly detection. After this timeout, the scanner threshold returns to the configured value.
 - Decide whether you want to enable automatic KB updates when anomaly detection is in detect mode.
 - Configure the 18 anomaly detection worm signatures to have more event actions than just the default Produce Alert. For example, configure them to have Deny Attacker event actions.

For More Information

- For the procedure for enabling anomaly detection, see [Enabling Anomaly Detection, page 13-4](#).
- For the procedures for putting anomaly detection in different modes, see [Adding, Editing, and Deleting Virtual Sensors, page 8-12](#).
- For the procedure for configuring a new anomaly detection policy, see [Configuring Anomaly Detections Policies, page 13-9](#).
- For more information on configuring zones, see [Configuring the Internal Zone, page 13-15](#), [Configuring the Illegal Zone, page 13-22](#), and [Configuring the Illegal Zone, page 13-22](#).
- For more information on anomaly detection modes, see [Anomaly Detection Modes, page 13-3](#).
- For more information about configuring learning accept mode, see [Configuring Learning Accept Mode, page 13-12](#).
- For more information on configuring anomaly detection signatures, see [Anomaly Detection Signatures, page 13-7](#).
- For more information on Deny Attacker event actions, see [Event Actions, page 12-7](#).

Anomaly Detection Signatures

The Traffic Anomaly engine contains nine anomaly detection signatures covering three protocols (TCP, UDP, and other). Each signature has two subsignatures, one for the scanner and the other for the worm-infected host (or a scanner under worm attack). When anomaly detection discovers an anomaly, it triggers an alert for these signatures. All anomaly detection signatures are enabled by default and the alert severity for each one is set to high.

When a scanner is detected but no histogram anomaly occurred, the scanner signature fires for that attacker (scanner) IP address. If the histogram signature is triggered, the attacker addresses that are doing the scanning each trigger the worm signature (instead of the scanner signature). The alert details state which threshold is being used for the worm detection now that the histogram has been triggered. From that point on, all scanners are detected as worm-infected hosts.

The following anomaly detection event actions are possible:

- Produce Alert—Writes the event to the Event Store.
- Deny Attacker Inline—(Inline only) Does not transmit this packet and future packets originating from the attacker address for a specified period of time.
- Log Attacker Packets—Starts IP logging for packets that contain the attacker address.
- Deny Attacker Service Pair Inline—Blocks the source IP address and the destination port.
- SNMP Trap—Sends a request to NotificationApp to perform SNMP notification.
- Request Block Host—Sends a request to ARC to block this host (the attacker).

Table 13-1 lists the anomaly detection worm signatures.

Table 13-1 Anomaly Detection Worm Signatures

Signature ID	Subsignature ID	Name	Description
13000	0	Internal TCP Scanner	Identified a single scanner over a TCP protocol in the internal zone.
13000	1	Internal TCP Scanner	Identified a worm attack over a TCP protocol in the internal zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.
13001	0	Internal UDP Scanner	Identified a single scanner over a UDP protocol in the internal zone.
13001	1	Internal UDP Scanner	Identified a worm attack over a UDP protocol in the internal zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13002	0	Internal Other Scanner	Identified a single scanner over an Other protocol in the internal zone.
13002	1	Internal Other Scanner	Identified a worm attack over an Other protocol in the internal zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.

Table 13-1 *Anomaly Detection Worm Signatures (continued)*

Signature ID	Subsignature ID	Name	Description
13003	0	External TCP Scanner	Identified a single scanner over a TCP protocol in the external zone.
13003	1	External TCP Scanner	Identified a worm attack over a TCP protocol in the external zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.
13004	0	External UDP Scanner	Identified a single scanner over a UDP protocol in the external zone.
13004	1	External UDP Scanner	Identified a worm attack over a UDP protocol in the external zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13005	0	External Other Scanner	Identified a single scanner over an Other protocol in the external zone.
13005	1	External Other Scanner	Identified a worm attack over an Other protocol in the external zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.
13006	0	Illegal TCP Scanner	Identified a single scanner over a TCP protocol in the illegal zone.
13006	1	Illegal TCP Scanner	Identified a worm attack over a TCP protocol in the illegal zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.
13007	0	Illegal UDP Scanner	Identified a single scanner over a UDP protocol in the illegal zone.
13007	1	Illegal UDP Scanner	Identified a worm attack over a UDP protocol in the illegal zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13008	0	Illegal Other Scanner	Identified a single scanner over an Other protocol in the illegal zone.
13008	1	Illegal Other Scanner	Identified a worm attack over an Other protocol in the illegal zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.

For More Information

For the procedure for assigning actions to signatures, see [Assigning Actions to Signatures](#), page 10-23.

Configuring Anomaly Detections Policies

This section describes how to create anomaly detection policies, and contains the following topics:

- [Anomaly Detections Pane, page 13-9](#)
- [Anomaly Detections Pane Field Definitions, page 13-9](#)
- [Add and Clone Policy Dialog Boxes Field Definitions, page 13-9](#)
- [Adding, Cloning, and Deleting Anomaly Detection Policies, page 13-10](#)

Anomaly Detections Pane

**Note**

You must be administrator or operator to add, clone, or delete anomaly detection policies.

**Note**

Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

In the Anomaly Detections pane, you can add, clone, or delete an anomaly detection policy. The default anomaly detection policy is ad0. When you add a policy, a control transaction is sent to the sensor to create the new policy instance. If the response is successful, the new policy instance is added under Anomaly Detections. If the control transaction fails, for example because of resource limitations, an error message appears.

If your platform does not support virtual policies, this means you can only have one instance for each component and you cannot create new ones or delete the existing one. In this case, the Add, Clone, and Delete buttons are disabled.

For More Information

For the procedure for enabling anomaly detection, see [Enabling Anomaly Detection, page 13-4](#).

Anomaly Detections Pane Field Definitions

The following fields are found in the Anomaly Detections pane:

- Policy Name—Identifies the name of this anomaly detection policy.
- Assigned Virtual Sensor—Identifies the virtual sensor to which this anomaly detection policy is assigned.

Add and Clone Policy Dialog Boxes Field Definitions

The following field is found in the Add and Clone Policy dialog boxes:

- Policy Name—Identifies the name of this anomaly detection policy.

Adding, Cloning, and Deleting Anomaly Detection Policies

To add, clone, or delete an anomaly detection policy, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > sensor_name > Policies > Anomaly Detections**, and then click **Add**.
- Step 3** In the Policy Name field, enter a name for the anomaly detection policy.



Tip To discard your changes and close the dialog box, click **Cancel**.

- Step 4** Click **OK**. The anomaly detection policy appears in the list in the Anomaly Detections pane.
- Step 5** To clone an existing anomaly detection policy, select it in the list, and then click **Clone**. The Clone Policy dialog box appears with “_copy” appended to the existing anomaly detection policy name.
- Step 6** In the Policy Name field, enter a unique name.



Tip To discard your changes and close the dialog box, click **Cancel**.

- Step 7** Click **OK**. The cloned anomaly detection policy appears in the list in the Anomaly Detections pane.
- Step 8** To remove an anomaly detection policy, select it, and then click **Delete**. The Delete Policy dialog box appears asking if you are sure you want to delete this policy permanently.



Caution You cannot delete the default anomaly detection policy, ad0.

- Step 9** Click **Yes**. The anomaly detection policy no longer appears in the list in the Anomaly Detections pane.
-

ad0 Pane

The ad0 pane (default) contains the tools to configure anomaly detection. There are five tabs:

- **Operation Settings**—Lets you set the worm timeout and which source and destination IP addresses you want the sensor to ignore during anomaly detection processing.
- **Learning Accept Mode**—Lets you enable the sensor to automatically accept the learning KB, and to configure a schedule for accepting the learned KB.
- **Internal Zone**—Lets you configure the destination IP addresses and the threshold of the internal zone.
- **Illegal Zone**—Lets you configure the destination IP addresses and the threshold of the illegal zone.
- **External Zone**—Lets you configure the threshold of the external zone.

Configuring Operation Settings

This section describes how to configure operation settings, and contains the following topics:

- [Operation Settings Tab, page 13-11](#)
- [Operating Settings Tab Field Definitions, page 13-11](#)
- [Configuring Anomaly Detection Operation Settings, page 13-11](#)

Operation Settings Tab

**Note**

You must be administrator or operator to configure anomaly detection operation settings.

On the Operation Settings tab, you can set the worm detection timeout. After this timeout, the scanner threshold returns to the configured value. You can also configure source and destination IP addresses that you want the sensor to ignore when anomaly detection is gathering information for a KB. Anomaly detection does not track these source and destination IP addresses and the KB thresholds are not affected by these IP addresses.

Operating Settings Tab Field Definitions

The following fields are found on the Operation Settings tab:

- **Worm Timeout**—Lets you enter the time in seconds for the worm termination timeout. The range is 120 to 10,000,000 seconds. The default is 600 seconds.
- **Configure IP address ranges to ignore during anomaly detection processing**—Lets you enter IP addresses that should be ignored while anomaly detection is processing:
 - **Enable ignored IP Addresses**—If checked, enables the list of ignored IP addresses.
 - **Source IP Addresses**—Lets you enter the source IP addresses that you want anomaly detection to ignore.
 - **Destination IP Addresses**—Lets you enter the destination IP addresses that you want anomaly detection to ignore.

Configuring Anomaly Detection Operation Settings

To configure anomaly detection operation settings, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator or operator privileges.
 - Step 2** Choose **Configuration > sensor_name > Policies > Anomaly Detections > ad0 > Operation Settings**.
 - Step 3** In the Worm Timeout field, enter the number of seconds you want to wait for a worm detection to time out. The range is 120 to 10,000,000 seconds. The default is 600 seconds.
 - Step 4** To enable the list of ignored IP addresses, check the **Enable ignored IP Addresses** check box.



Note You must check the **Enable ignored IP Addresses** check box or none of the IP addresses you enter will be ignored.

Step 5 In the Source IP Addresses field, enter the addresses or range of source IP addresses that you want anomaly detection to ignore. The valid form is 10.10.5.5,10.10.2.1-10.10.2.30.

Step 6 In the Destination IP Addresses field, enter the addresses or range of destination IP addresses that you want anomaly detection to ignore.



Tip To discard your changes, click **Reset**.

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Configuring Learning Accept Mode

This section describes how to configure learning accept mode, and contains the following topics:

- [Learning Accept Mode Tab, page 13-12](#)
- [The KB and Histograms, page 13-12](#)
- [Learning Accept Mode Tab Field Definitions, page 13-14](#)
- [Add and Edit Start Time Dialog Boxes Field Definitions, page 13-14](#)
- [Configuring Learning Accept Mode, page 13-14](#)

Learning Accept Mode Tab



Note You must be administrator or operator to configure learning accept mode.

Use the Learning Accept Mode tab to configure whether you want the sensor to create a new KB every so many hours. You can configure whether the KB is created and loaded (Rotate) or saved (Save Only). You can schedule how often and when the KB is loaded or saved.

The default generated filename is *YYYY-Mon-dd-hh_mm_ss*, where *Mon* is a three-letter abbreviation of the current month.

The KB and Histograms

The KB has a tree structure, and contains the following information:

- KB name
- Zone name
- Protocol
- Service

The KB holds a scanner threshold and a histogram for each service. If you have learning accept mode set to auto and the action set to rotate, a new KB is created every 24 hours and used in the next 24 hours. If you have learning accept mode set to auto and the action is set to save only, a new KB is created, but the current KB is used. If you do not have learning accept mode set to auto, no KB is created.

**Note**

Learning accept mode uses the sensor local time.

The scanner threshold defines the maximum number of zone IP addresses that a single source IP address can scan. The histogram threshold defines the maximum number of source IP addresses that can scan more than the specified numbers of zone IP addresses.

Anomaly detection 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 address is exceeded). For example, if the scanning threshold is 300 and the histogram for port 445, if anomaly detection identifies a scanner that scans 350 zone destination IP addresses, it produces an action indicating that a mass scanner was detected. However, this scanner does not yet verify that a worm attack is in progress. [Table 13-2](#) describes this example.

Table 13-2 Example Histogram

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

When anomaly detection identifies six concurrent source IP addresses that scan more than 20 zone destination IP addresses on port 445, it produces an action with an unspecified source IP address that indicates anomaly detection has identified a worm attack on port 445. The dynamic filter threshold, 20, specifies the new internal scanning threshold and causes anomaly detection to lower the threshold definition of a scanner so that anomaly detection produces additional dynamic filters for each source IP address that scans more than the new scanning threshold (20).

You can override what the KB learned per anomaly detection policy and per zone. If you understand your network traffic, you may want to use overrides to limit false positives.

Triggering the High Category Histogram Before the Single-Scanner Threshold

Based on the default histogram (nonlearned knowledge base [KB]) values, histogram-based detection can occur before single-scanner detection.

Single scanner detection is based on the scanner threshold settings. The scanner threshold setting is a single number for that port or protocol and zone. Any single IP address scanning more than that number of hosts of that port or protocol in that zone is alerted as a scanner.

There is a histogram for that port or protocol and zone that tracks how many systems normally scan a smaller number of hosts (10 hosts, 20 hosts, or 100 hosts). When more than that normal number of scanners are seen, then a worm is declared and all IPs scanning more than the associated number of hosts are alerted on as being a worm scanner.

**Note**

An IP source address can be alerted on as being a worm scanner without ever reaching the scanner threshold. The scanner threshold is used to detect single systems scanning a large number of hosts and is tracked separately from the algorithms for detecting worms.

Learning Accept Mode Tab Field Definitions

The following fields are found on the Learning Accept Mode tab:

- Automatically accept learning knowledge base—If checked, the sensor automatically updates the KB. If not checked, anomaly detection does not automatically create a new KB.
- Action—Lets you specify whether to rotate or save the KB. If you choose Save Only, the new KB is created. You can examine it and decide whether to load it into anomaly detection. If you choose Rotate, the new KB is created and loaded according to the schedule you define.
- Schedule—Lets you choose Calendar Schedule or Periodic Schedule:
 - Periodic Schedule—Lets you configure the first learning snapshot time of day and the interval of the subsequent snapshots. The default is the periodic schedule in 24-hour format.
 - Start Time—Enter the time you want the new KB to start. The valid format is hh:mm:ss.
 - Learning Interval—Enter how long you want anomaly detection to learn from the network before creating a new KB.
 - Calendar Schedule—Lets you configure the days and times of the day for the KB to be created.
 - Times of Day—Click **Add** and enter the times of day in the Add Start Time dialog box.
 - Days of the Week—Check the check boxes of the days of the week you want to configure.

Add and Edit Start Time Dialog Boxes Field Definitions

The following field is found in the Add and Edit Start Time dialog boxes:

- Start Time—Lets you enter the start time for learning accept mode in hours, minutes, and seconds. The valid form is hh:mm:ss in 24-hour time.

Configuring Learning Accept Mode

To configure learning accept mode for anomaly detection, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator or operator privileges.
 - Step 2** Choose **Configuration** > *sensor_name* > **Policies** > **Anomaly Detections** > **ad0** > **Learning Accept Mode**.
 - Step 3** To have anomaly detection automatically update the KB, check the **Automatically accept learning knowledge base** check box.
 - Step 4** From the Action drop-down list, choose one of the following action types:
 - Rotate—New KB is created and loaded. This is the default.
 - Save Only—New KB is created but not loaded. You can view it to decide if you want to load it.
 - Step 5** From the Schedule drop-down list, choose one of the following schedule types:
 - Calendar Schedule—Go to Step 6.
 - Periodic Schedule—Go to Step 7.
 - Step 6** To configure the calendar schedule:
 - a. Click **Add** to add the start time.

- b. Enter the start time in hours, minutes, and seconds using the 24-hour time format.



Tip To discard your changes and close the Add Start Time dialog box, click **Cancel**.

- c. Click **OK**.
- d. In the Days of the Week field, check the check boxes of the days you want the anomaly detection module to capture KB snapshots.

Step 7 To configure the periodic schedule (the default):

- a. In the Start Time fields, enter the start time in hours, minutes, and seconds using the 24-hour time format.
- b. In the Learning Interval field, enter the interval of the subsequent KB snapshots.



Tip To discard your changes, click **Reset**.

Step 8 Click **Apply** to apply your changes and save the revised configuration.

Configuring the Internal Zone

This section describes how to configure the internal zone, and contains the following topics:

- [Internal Zone Tab, page 13-15](#)
- [General Tab, page 13-16](#)
- [TCP Protocol Tab, page 13-16](#)
- [Add and Edit Destination Port Dialog Boxes Field Definitions, page 13-17](#)
- [Add and Edit Histogram Dialog Boxes Field Definitions, page 13-17](#)
- [UDP Protocol Tab, page 13-17](#)
- [Other Protocols Tab, page 13-18](#)
- [Add and Edit Protocol Number Dialog Boxes Field Definitions, page 13-18](#)
- [Configuring the Internal Zone, page 13-19](#)

Internal Zone Tab



Note You must be administrator or operator to configure the internal zone.

The Internal Zone tab has four tabs:

- **General**—Lets you enable the internal zone and specify which subnets it contains.
- **TCP Protocol**—Lets you enable TCP protocol and configure your own thresholds and histograms.
- **UDP Protocol**—Lets you enable UDP protocol and configure your own thresholds and histograms.

- Other Protocols—Lets you enable other protocols and your own thresholds and histograms.

The internal zone should represent your internal network. It should receive all the traffic that comes to your IP address range.

General Tab

On the General tab, you enable the zone. If the zone is disabled, packets to this zone are ignored. By default the zone is enabled.

You then add the IP addresses that belong to this zone. If you do not configure IP addresses for all zones, all packets are sent to the default zone, the external zone.

Field Definitions

The following fields are found on the General tab:

- Enable the Internal Zone—If checked, enables the internal zone.
- Service Subnets—Lets you enter the subnets that you want to apply to the internal zone. The valid format is 10.10.5.5,10.10.2.1-10.10.2.30.

TCP Protocol Tab

On the TCP Protocol tab, you enable or disable TCP protocol for the internal zone. You can configure a destination port for the TCP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the TCP Protocol tab:

- Enable the TCP Protocol—If checked, enables TCP protocol.
- Destination Port Map tab—Lets you associate a specific port with the TCP protocol:
 - Port Number—Displays the configured port number.
 - Service Enabled—Whether or not the service is enabled.
 - Scanner Overridden—Whether or not the scanner has been overridden.
 - Overridden Scanner Settings Threshold—Displays the configured threshold settings.
 - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms. Default thresholds are used for services that are not in the KB and were not overridden by the configuration:
 - Scanner Threshold—Lets you change the scanner threshold.
 - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
 - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Destination Port Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Destination Port dialog boxes:

- Destination Port number—Lets you enter the destination port number. The valid range is 0 to 65535.
- Enable the Service—If checked, enables the service.
- Override Scanner Settings—If checked, overrides the default scanner settings and lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
 - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
 - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Add and Edit Histogram Dialog Boxes Field Definitions

The following fields are found on the Add and Edit Histogram dialog boxes:

- Number of Destination IP Addresses—Lets you add a high, medium, or low number of destination IP addresses. Low is 5 destination IP addresses, medium is 20, and high is 100.
- Number of Source IP Addresses—Lets you add the number of source IP addresses. The valid range is 0 to 4096.

UDP Protocol Tab

On the UDP Protocol tab, you enable or disable UDP protocol for the internal zone. You can configure a destination port for the UDP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the UDP Protocol tab:

- Enable the UDP Protocol—If checked, enables UDP protocol.
- Destination Port Map tab—Lets you associate a specific port with the UDP protocol:
 - Port Number—Displays the configured port number.
 - Service Enabled—Whether or not the service is enabled.
 - Scanner Overridden—Whether or not the scanner has been overridden.
 - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
 - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms:
 - Scanner Threshold—Lets you change the scanner threshold.
 - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.

- Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Other Protocols Tab

On the Other Protocols tab, you enable or disable other protocols for the internal zone. You can configure a protocol number map for the other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the Other Protocols tab:

- Enable Other Protocols—If checked, enables the other protocols.
- Protocol Number Map tab—Lets you associate a specific protocol number with the other protocols:
 - Protocol Number—Displays the configured protocol number.
 - Service Enabled—Whether or not the service is enabled.
 - Scanner Overridden—Whether or not the scanner has been overridden.
 - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
 - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms.
 - Scanner Threshold—Lets you change the scanner threshold.
 - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
 - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Protocol Number Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Protocol Number dialog boxes:

- Protocol number—Lets you enter a protocol number.
- Enable the Service—Lets you enable the service.
- Override Scanner Settings—If checked, lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
 - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
 - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Configuring the Internal Zone

To configure the internal zone for anomaly detection, follow these steps:

- Step 1** Log in to the IME using an account with administrator or operator privileges.
- Step 2** Choose **Configuration** > *sensor_name* > **Policies** > **Anomaly Detections** > **ad0** > **Internal Zone**, and then click the **General** tab.
- Step 3** To enable the internal zone, check the **Enable the Internal Zone** check box.



Note You must check the **Enable the Internal Zone** check box or any protocols that you configure will be ignored.

- Step 4** In the Service Subnets field, enter the subnets to which you want the internal zone to apply. The valid format is 10.10.5.5,10.10.2.1-10.10.2.30.
- Step 5** To configure TCP protocol, click the **TCP Protocol** tab.
- Step 6** To enable TCP protocol, check the **Enable the TCP Protocol** check box.



Note You must check the **Enable the TCP Protocol** check box or the TCP protocol configuration will be ignored.

- Step 7** Click the **Destination Port Map** tab, and then click **Add** to add a destination port.
- Step 8** In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.
- Step 9** To enable the service on that port, check the **Enable the Service** check box.
- Step 10** To override the scanner values for that port, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.
- Step 11** To add a histogram for the new scanner settings, click **Add**.
- Step 12** From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).
- Step 13** In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

- Step 14** Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.



Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

- Step 15** Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.
- Step 16** To edit the destination port map, select it in the list, and click **Edit**.
- Step 17** Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

- Step 18** To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list Destination Port Map tab.
- Step 19** To edit the default thresholds, click the **Default Thresholds** tab.
- Step 20** Select the threshold histogram you want to edit, and click **Edit**.
- Step 21** From the Number of Destination IP Addresses the drop down list, change the value (High, Medium, or Low).
- Step 22** In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

- Step 23** To configure UDP protocol, click the **UDP Protocol** tab.
- Step 24** To enable UDP protocol, check the **Enable the UDP Protocol** check box.



Note You must check the **Enable the UDP Protocol** check box or the UDP protocol configuration will be ignored.

- Step 25** Click the **Destination Port Map** tab, and then click **Add** to add a destination port.
- Step 26** In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.
- Step 27** To enable the service on that port, check the **Enable the Service** check box.
- Step 28** To override the scanner values for that port, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.
- Step 29** To add a histogram for the new scanner settings, click **Add**.
- Step 30** From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).
- Step 31** In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

- Step 32** Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.



Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

- Step 33** Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.
- Step 34** To edit the destination port map, select it in the list, and click **Edit**.
- Step 35** Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.
- Step 36** To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list on the Destination Port Map tab.

- Step 37** To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.
- Step 38** From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).
- Step 39** In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

- Step 40** To configure Other protocols, click the **Other Protocols** tab.
- Step 41** To enable other protocols, check the **Enable Other Protocols** check box.



Note You must check the **Enable Other Protocols** check box or the other protocols configuration will be ignored.

- Step 42** Click the **Protocol Number Map** tab, and then click **Add** to add a protocol number.
- Step 43** In the Protocol Number field, enter the protocol number. The valid range is 0 to 255.
- Step 44** To enable the service of that protocol, check the **Enable the Service** check box.
- Step 45** To override the scanner values for that protocol, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.
- Step 46** To add a histogram for the new scanner settings, click **Add**.
- Step 47** From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).
- Step 48** In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

- Step 49** Click **OK**. The new scanner setting appears in the list in the Add Protocol Number dialog box.



Tip To discard your changes and close the Add Protocol Number dialog box, click **Cancel**.

- Step 50** Click **OK**. The new protocol number map appears in the list on the Protocol Number Map tab.
- Step 51** To edit the protocol number map, select it in the list, and click **Edit**.
- Step 52** Make any changes to the fields and click **OK**. The edited protocol number map appears in the list on the Protocol Number Map tab.
- Step 53** To delete a protocol number map, select it, and click **Delete**. The protocol number map no longer appears in the list on the Protocol Number Map tab.
- Step 54** To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.
- Step 55** From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 56 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.



Tip To discard your changes, click **Reset**.

Step 57 Click **Apply** to apply your changes and save the revised configuration.

Configuring the Illegal Zone

This section describes how to configure the illegal zone, and contains the following topics:

- [Illegal Zone Tab, page 13-22](#)
- [General Tab, page 13-23](#)
- [TCP Protocol Tab, page 13-23](#)
- [Add and Edit Destination Port Dialog Boxes Field Definitions, page 13-23](#)
- [Add and Edit Histogram Dialog Boxes Field Definitions, page 13-24](#)
- [UDP Protocol Tab, page 13-24](#)
- [Other Protocols Tab, page 13-25](#)
- [Add and Edit Protocol Number Dialog Boxes Field Definitions, page 13-25](#)
- [Configuring the Illegal Zone, page 13-25](#)

Illegal Zone Tab



Note You must be administrator or operator to configure the illegal zone.

The Illegal Zone tab has four tabs:

- **General**—Lets you enable the illegal zone and specify which subnets it contains.
- **TCP Protocol**—Lets you enable TCP protocol and configure your own thresholds and histograms.
- **UDP Protocol**—Lets you enable UDP protocol and configure your own thresholds and histograms.
- **Other Protocols**—Lets you enable other protocols and your own thresholds and histograms.

The illegal zone should represent IP address ranges that should never be seen in normal traffic, for example, unallocated IP addresses or part of your internal IP address range that is unoccupied.

General Tab

On the General tab, you enable the zone. If the zone is disabled, packets to this zone are ignored. By default the zone is enabled.

You then add the IP addresses that belong to this zone. If you do not configure IP addresses for all zones, all packets are sent to the default zone, the external zone.

Field Definitions

The following fields are found on the General tab:

- Enable the Internal Zone—If checked, enables the internal zone.
- Service Subnets—Lets you enter the subnets that you want to apply to the internal zone. The valid format is 10.10.5.5,10.10.2.1-10.10.2.30.

TCP Protocol Tab

On the TCP Protocol tab, you enable or disable TCP protocol for the illegal zone. You can configure a destination port for the TCP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the TCP Protocol tab:

- Enable the TCP Protocol—If checked, enables TCP protocol.
- Destination Port Map tab—Lets you associate a specific port with the TCP protocol:
 - Port Number—Displays the configured port number.
 - Service Enabled—Whether or not the service is enabled.
 - Scanner Overridden—Whether or not the scanner has been overridden.
 - Overridden Scanner Settings Threshold—Displays the configured threshold settings.
 - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms. Default thresholds are used for services that are not in the KB and were not overridden by the configuration:
 - Scanner Threshold—Lets you change the scanner threshold.
 - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
 - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Destination Port Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Destination Port dialog boxes:

- Destination Port number—Lets you enter the destination port number. The valid range is 0 to 65535.
- Enable the Service—If checked, enables the service.

- **Override Scanner Settings**—If checked, overrides the default scanner settings and lets you add, edit, delete, and select all histograms.
- **Scanner Threshold**—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- **Threshold Histogram**—Displays the histograms that you added:
 - **Number of Destination IP Addresses**—Displays the number of destination IP addresses that you added.
 - **Number of Source IP Addresses**—Displays the number of source IP addresses that you added.

Add and Edit Histogram Dialog Boxes Field Definitions

The following fields are found on the Add and Edit Histogram dialog boxes:

- **Number of Destination IP Addresses**—Lets you add a high, medium, or low number of destination IP addresses. Low is 5 destination IP addresses, medium is 20, and high is 100.
- **Number of Source IP Addresses**—Lets you add the number of source IP addresses. The valid range is 0 to 4096.

UDP Protocol Tab

On the UDP Protocol tab, you enable or disable UDP protocol for the illegal zone. You can configure a destination port for the UDP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the UDP Protocol tab:

- **Enable the UDP Protocol**—If checked, enables UDP protocol.
- **Destination Port Map tab**—Lets you associate a specific port with the UDP protocol:
 - **Port Number**—Displays the configured port number.
 - **Service Enabled**—Whether or not the service is enabled.
 - **Scanner Overridden**—Whether or not the scanner has been overridden.
 - **Overridden Scanner Settings Threshold**—Displays the configured threshold setting.
 - **Overridden Scanner Settings Histogram**—Displays the configured histogram.
- **Default Thresholds tab**—Displays the default thresholds and histograms:
 - **Scanner Threshold**—Lets you change the scanner threshold.
 - **Threshold Histogram Number of Destination IP Addresses**—Displays the number of destination IP addresses grouped as low, medium, and high.
 - **Threshold Histogram Number of Source IP Addresses**—Displays the number of source IP addresses associated with each group of destination IP addresses.

Other Protocols Tab

On the Other Protocols tab, you enable or disable Other protocols for the illegal zone. You can configure a protocol number map for the Other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the Other Protocols tab:

- Enable Other Protocols—If checked, enables the other protocols.
- Protocol Number Map tab—Lets you associate a specific protocol number with the other protocols:
 - Protocol Number—Displays the configured protocol number.
 - Service Enabled—Whether or not the service is enabled.
 - Scanner Overridden—Whether or not the scanner has been overridden.
 - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
 - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms.
 - Scanner Threshold—Lets you change the scanner threshold.
 - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
 - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Protocol Number Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Protocol Number dialog boxes:

- Protocol number—Lets you enter a protocol number.
- Enable the Service—Lets you enable the service.
- Override Scanner Settings—If checked, lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
 - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
 - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Configuring the Illegal Zone

To configure the illegal zone for anomaly detection, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator or operator privileges.
- Step 2** Choose **Configuration** > *sensor_name* > **Policies** > **Anomaly Detections** > **ad0** > **Illegal Zone**.

Step 3 Click the **General** tab.

Step 4 To enable the illegal zone, check the **Enable the Illegal Zone** check box.



Note You must check the **Enable the Illegal Zone** check box or any protocols that you configure will be ignored.

Step 5 In the Service Subnets field, enter the subnets to which you want the illegal zone to apply. The valid format is 10.10.5.5,10.10.2.1-10.10.2.30.

Step 6 To configure TCP protocol, click the **TCP Protocol** tab.

Step 7 To enable TCP protocol, check the **Enable the TCP Protocol** check box.



Note You must check the **Enable the TCP Protocol** check box or the TCP protocol configuration will be ignored.

Step 8 Click the **Destination Port Map** tab, and then click **Add** to add a destination port.

Step 9 In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

Step 10 To enable the service on that port, check the **Enable the Service** check box.

Step 11 To override the scanner values for that port, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 12 To add a histogram for the new scanner settings, click **Add**.

Step 13 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 14 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 15 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.



Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 16 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 17 To edit the destination port map, select it in the list, and click **Edit**.

Step 18 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 19 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list Destination Port Map tab.

Step 20 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 21 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 22 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the **Default Thresholds** tab.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

Step 23 To configure UDP protocol, click the **UDP Protocol** tab.

Step 24 To enable UDP protocol, check the **Enable the UDP Protocol** check box.



Note You must check the **Enable the UDP Protocol** check box or the UDP protocol configuration will be ignored.

Step 25 Click the **Destination Port Map** tab, and then click **Add** to add a destination port.

Step 26 In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

Step 27 To enable the service on that port, check the **Enable the Service** check box.

Step 28 To override the scanner values for that port, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 29 To add a histogram for the new scanner settings, click **Add**.

Step 30 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 31 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 32 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.



Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 33 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 34 To edit the destination port map, select it in the list, and click **Edit**.

Step 35 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 36 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list on the Destination Port Map tab.

Step 37 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 38 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 39 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

The edited threshold histogram appears in the list on the Default Thresholds tab.

Step 40 To configure Other protocols, click the **Other Protocols** tab.

Step 41 To enable other protocols, check the **Enable Other Protocols** check box.



Note You must check the **Enable Other Protocols** check box or the other protocols configuration will be ignored.

Step 42 Click the **Protocol Number Map** tab, and then click **Add** to add a protocol number.

Step 43 In the Protocol Number field, enter the protocol number. The valid range is 0 to 255.

Step 44 To enable the service of that protocol, check the **Enable the Service** check box.

Step 45 To override the scanner values for that protocol, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 46 To add a histogram for the new scanner settings, click **Add**.

Step 47 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 48 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 49 Click **OK**. The new scanner setting appears in the list in the Add Protocol Number dialog box.



Tip To discard your changes and close the Add Protocol Number dialog box, click **Cancel**.

Step 50 Click **OK**. The new protocol number map appears in the list on the Protocol Number Map tab.

Step 51 To edit the protocol number map, select it in the list, and click **Edit**.

Step 52 Make any changes to the fields and click **OK**. The edited protocol number map appears in the list on the Protocol Number Map tab.

Step 53 To delete a protocol number map, select it, and click **Delete**. The protocol number map no longer appears in the list on the Protocol Number Map tab.

Step 54 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 55 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 56 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

**Tip**

To discard your changes, click **Reset**.

Step 57 Click **Apply** to apply your changes and save the revised configuration.

Configuring the External Zone

This section describes how to configure external zone, and contains the following topics:

- [External Zone Tab, page 13-29](#)
- [TCP Protocol Tab, page 13-29](#)
- [Add and Edit Destination Port Dialog Boxes Field Definitions, page 13-30](#)
- [Add and Edit Histogram Dialog Boxes Field Definitions, page 13-30](#)
- [UDP Protocol Tab, page 13-31](#)
- [Other Protocols Tab, page 13-31](#)
- [Add and Edit Protocol Number Dialog Boxes Field Definitions, page 13-32](#)
- [Configuring the External Zone, page 13-32](#)

External Zone Tab

**Note**

You must be administrator or operator to configure the external zone.

The External Zone tab has three tabs:

- **TCP Protocol**—Lets you enable TCP protocol and configure your own thresholds and histograms.
- **UDP Protocol**—Lets you enable UDP protocol and configure your own thresholds and histograms.
- **Other Protocols**—Lets you enable other protocols and your own thresholds and histograms.

The external zone is the default zone with the default Internet range of 0.0.0.0-255.255.255.255. By default, the internal and illegal zones contain no IP addresses. Packets that do not match the set of IP addresses in the internal or illegal zone are handled by the external zone.

TCP Protocol Tab

On the TCP Protocol tab, you enable or disable TCP protocol for the external zone. You can configure a destination port for the TCP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the TCP Protocol tab:

- Enable the TCP Protocol—If checked, enables TCP protocol.
- Destination Port Map tab—Lets you associate a specific port with the TCP protocol:
 - Port Number—Displays the configured port number.
 - Service Enabled—Whether or not the service is enabled.
 - Scanner Overridden—Whether or not the scanner has been overridden.
 - Overridden Scanner Settings Threshold—Displays the configured threshold settings.
 - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms. Default thresholds are used for services that are not in the KB and were not overridden by the configuration:
 - Scanner Threshold—Lets you change the scanner threshold.
 - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
 - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Destination Port Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Destination Port dialog boxes:

- Destination Port number—Lets you enter the destination port number. The valid range is 0 to 65535.
- Enable the Service—If checked, enables the service.
- Override Scanner Settings—If checked, overrides the default scanner settings and lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
 - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
 - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Add and Edit Histogram Dialog Boxes Field Definitions

The following fields are found on the Add and Edit Histogram dialog boxes:

- Number of Destination IP Addresses—Lets you add a high, medium, or low number of destination IP addresses. Low is 5 destination IP addresses, medium is 20, and high is 100.
- Number of Source IP Addresses—Lets you add the number of source IP addresses. The valid range is 0 to 4096.

UDP Protocol Tab

On the UDP Protocol tab, you enable or disable UDP protocol for the external zone. You can configure a destination port for the UDP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the UDP Protocol tab:

- Enable the UDP Protocol—If checked, enables UDP protocol.
- Destination Port Map tab—Lets you associate a specific port with the UDP protocol:
 - Port Number—Displays the configured port number.
 - Service Enabled—Whether or not the service is enabled.
 - Scanner Overridden—Whether or not the scanner has been overridden.
 - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
 - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms:
 - Scanner Threshold—Lets you change the scanner threshold.
 - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
 - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Other Protocols Tab

On the Other Protocols tab, you enable or disable Other protocols for the external zone. You can configure a protocol number map for the Other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the Other Protocols tab:

- Enable Other Protocols—If checked, enables the other protocols.
- Protocol Number Map tab—Lets you associate a specific protocol number with the other protocols:
 - Protocol Number—Displays the configured protocol number.
 - Service Enabled—Whether or not the service is enabled.
 - Scanner Overridden—Whether or not the scanner has been overridden.
 - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
 - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms:
 - Scanner Threshold—Lets you change the scanner threshold.
 - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.

- **Threshold Histogram Number of Source IP Addresses**—Displays the number of source IP addresses associated with each group of destination IP addresses.



Add and Edit Protocol Number Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Protocol Number dialog boxes:

- **Protocol number**—Lets you enter a protocol number.
- **Enable the Service**—Lets you enable the service.
- **Override Scanner Settings**—If checked, lets you add, edit, delete, and select all histograms.
- **Scanner Threshold**—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- **Threshold Histogram**—Displays the histograms that you added:
 - **Number of Destination IP Addresses**—Displays the number of destination IP addresses that you added.
 - **Number of Source IP Addresses**—Displays the number of source IP addresses that you added.

Configuring the External Zone

To configure the external zone for anomaly detection, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > sensor_name > Policies > Anomaly Detections > ad0 > External Zone**.
- Step 3** To enable the external zone, check the **Enable the External Zone** check box.
-
-  **Note** You must check the **Enable the External Zone** check box or any protocols that you configure will be ignored.
-
- Step 4** To configure TCP protocol, click the **TCP Protocol** tab.
- Step 5** To enable TCP protocol, check the **Enable the TCP Protocol** check box.
-
-  **Note** You must check the **Enable the TCP Protocol** check box or the TCP protocol configuration will be ignored.
-
- Step 6** Click the **Destination Port Map** tab, and then click **Add** to add a destination port.
- Step 7** In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.
- Step 8** To enable the service on that port, check the **Enable the Service** check box.
- Step 9** To override the scanner values for that port, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.
- Step 10** To add a histogram for the new scanner settings, click **Add**.
- Step 11** From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

- Step 12** In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

- Step 13** Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.



Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

- Step 14** Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

- Step 15** To edit the destination port map, select it in the list, and click **Edit**.

- Step 16** Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

- Step 17** To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list Destination Port Map tab.

- Step 18** To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

- Step 19** From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

- Step 20** In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

- Step 21** To configure UDP protocol, click the **UDP Protocol** tab.

- Step 22** To enable UDP protocol, check the **Enable the UDP Protocol** check box.



Note You must check the **Enable the UDP Protocol** check box or the UDP protocol configuration will be ignored.

- Step 23** Click the **Destination Port Map** tab, then click **Add** to add a destination port.

- Step 24** In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

- Step 25** To enable the service on that port, check the **Enable the Service** check box.

- Step 26** To override the scanner values for that port, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.

- Step 27** To add a histogram for the new scanner settings, click **Add**.

- Step 28** From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

- Step 29** In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 30 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.



Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 31 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 32 To edit the destination port map, select it in the list, and click **Edit**.

Step 33 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 34 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list on the Destination Port Map tab.

Step 35 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 36 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 37 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

Step 38 To configure Other protocols, click the **Other Protocols** tab.

Step 39 To enable other protocols, check the **Enable Other Protocols** check box.



Note You must check the **Enable Other Protocols** check box or the other protocols configuration will be ignored.

Step 40 Click the **Protocol Number Map** tab, and then click **Add** to add a protocol number.

Step 41 In the Protocol Number field, enter the protocol number. The valid range is 0 to 255.

Step 42 To enable the service of that protocol, check the **Enable the Service** check box.

Step 43 To override the scanner values for that protocol, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 44 To add a histogram for the new scanner settings, click **Add**.

Step 45 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 46 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.



Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 47 Click **OK**. The new scanner setting appears in the list in the Add Protocol Number dialog box.



Tip To discard your changes and close the Add Protocol Number dialog box, click **Cancel**.

Step 48 Click **OK**. The new protocol number map appears in the list on the Protocol Number Map tab.

Step 49 To edit the protocol number map, select it in the list, and click **Edit**.

Step 50 Make any changes to the fields and click **OK**. The edited protocol number map appears in the list on the Protocol Number Map tab.

Step 51 To delete a protocol number map, select it, and click **Delete**. The protocol number map no longer appears in the list on the Protocol Number Map tab.

Step 52 To edit the default thresholds, click the **Default Thresholds** tab.

Step 53 Select the threshold histogram you want to edit, and click **Edit**.

Step 54 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 55 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.



Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.



Tip To discard your changes, click **Reset**.

Step 56 Click **Apply** to apply your changes and save the revised configuration.

Disabling Anomaly Detection



Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

If you have anomaly detection enabled and you have your sensor configured to see only one direction of traffic, you should disable anomaly detection. Otherwise, you will receive many alerts, because anomaly detection sees asymmetric traffic as having incomplete connections, that is, like worm scanners, and fires alerts.

To disable anomaly detection, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter analysis engine submode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Enter the virtual sensor name that contains the anomaly detection policy you want to disable.

```
sensor(config-ana)# virtual-sensor vs0  
sensor(config-ana-vir)#
```

Step 4 Disable anomaly detection operational mode.

```
sensor(config-ana-vir)# anomaly-detection  
sensor(config-ana-vir-ano)# operational-mode inactive  
sensor(config-ana-vir-ano)#
```

Step 5 Exit analysis engine submenu.

```
sensor(config-ana-vir-ano)# exit  
sensor(config-ana-vir)# exit  
sensor(config-ana-)# exit  
Apply Changes:[yes]:
```

Step 6 Press **Enter** to apply your changes or enter **no** to discard them.
