



CHAPTER 9

Configuring Anomaly Detection



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. For more information, see [Worms, page 9-2](#). For the procedure for turning off anomaly detection, see [Turning Off Anomaly Detection, page 9-48](#).

This chapter describes anomaly detection (AD) and its features and how to configure them. It contains the following topics:

- [Security Policies, page 9-2](#)
- [Understanding Anomaly Detection, page 9-2](#)
- [Worms, page 9-2](#)
- [Anomaly Detection Modes, page 9-3](#)
- [Anomaly Detection Zones, page 9-4](#)
- [Configuration Sequence, page 9-5](#)
- [Anomaly Detection Signatures, page 9-6](#)
- [Working With Anomaly Detection Policies, page 9-8](#)
- [Configuring Anomaly Detection Operational Settings, page 9-10](#)
- [Internal Zone, page 9-11](#)
- [Illegal Zone, page 9-19](#)
- [External Zone, page 9-28](#)
- [Learning Accept Mode, page 9-36](#)
- [Working With KB Files, page 9-39](#)
- [Displaying Anomaly Detection Statistics, page 9-46](#)
- [Turning Off Anomaly Detection, page 9-48](#)

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. IPS 6.0 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 out per VLAN or physical interface.

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.

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 the 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.

Anomaly Detection Modes

Anomaly detection 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

Although anomaly detection is in detect mode by default, it 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 be 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.

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 information on configuring the sensor to be in learn and detect mode, see [Configuring the Virtual Sensor, page 6-3](#).
- For more information on worms, see [Worms, page 9-2](#).
- For information on configuring the sensor to be in inactive mode, see [Configuring the Virtual Sensor, page 6-3](#).

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 on anomaly detection zones, see [Internal Zone, page 9-11](#), [Illegal Zone, page 9-19](#), and [External Zone, page 9-28](#).

Configuration Sequence

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. Add the anomaly detection policy to your virtual sensors.

You can use the default anomaly detection policy, `ad0`, or you can configure a new one.

2. Configure the anomaly detection zones and protocols.
3. By default, the anomaly detection operational mode is set to Detect, although for the first 24 hours it 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.
4. 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.



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.

After the time period, the sensor saves the initial KB as a baseline of the normal activity of your network.

5. If you manually set anomaly detection to learning accept mode, switch back to detect mode.
6. 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 adding an anomaly detection policy and setting the anomaly detection Operational mode, see [Configuring the Virtual Sensor, page 6-3](#).
- For the procedure for configuring a new anomaly detection policy, see [Working With Anomaly Detection Policies, page 9-8](#).
- For the procedures for configuring anomaly detection zones, see [Configuring the Internal Zone, page 9-11](#), [Configuring the Illegal Zone, page 9-20](#), and [Configuring the External Zone, page 9-28](#).
- For more information on anomaly detection modes, see [Anomaly Detection Modes, page 9-3](#).

- For the procedure for setting the anomaly detection operational mode to Detect, see [Configuring the Virtual Sensor, page 6-3](#).
- For the procedure for configuring scanner thresholds, see [Configuring Anomaly Detection Operational Settings, page 9-10](#).
- For the procedure for enabling automatic KB updates when anomaly detection is in detect mode, see [Configuring Learning Accept Mode, page 9-37](#).
- For more information on anomaly detection worm signatures, see [Anomaly Detection Signatures, page 9-6](#).
- For information on configuring event actions for signatures, see [Assigning Actions to Signatures, page 7-14](#).

Anomaly Detection Signatures

The Traffic Anomaly engine contains nine anomaly detection signatures covering the 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 pairs—Starts IP logging for packets that contain the attacker address.
- Log pair packets—Starts IP logging for packets that contain the attacker and victim address pair.
- Deny attacker service pair inline—Blocks the source IP address and the destination port.
- Request 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).
- You can edit or tune anomaly detection signatures but you cannot create custom anomaly detection signatures.

Table 9-1 lists the anomaly detection worm signatures.

Table 9-1 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.
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 external zone.
13006	1	Illegal 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.

Table 9-1 Anomaly Detection Worm Signatures (continued)

Signature ID	Subsignature ID	Name	Description
13007	0	Illegal UDP Scanner	Identified a single scanner over a UDP protocol in the external zone.
13007	1	Illegal 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.
13008	0	Illegal Other Scanner	Identified a single scanner over an Other protocol in the external zone.
13008	1	Illegal 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.

For More Information

For the procedure for assigning event actions to signatures, see [Assigning Actions to Signatures](#), page 7-14.

Working With Anomaly Detection Policies

Use the **service anomaly-detection name** command in service anomaly detection submode to create an anomaly detection policy. The values of this anomaly detection policy are the same as the default anomaly detection policy, ad0, until you edit them.

Or you can use the **copy anomaly-detection source_destination** command in privileged EXEC mode to make a copy of an existing policy and then edit the values of the new policy as needed.

Use the **list anomaly-detection-configurations** command in privileged EXEC mode to list the anomaly detection policies.

Use the **no service anomaly-detection name** command in global configuration mode to delete an anomaly detection policy. Use the **default service anomaly-detection name** command in global configuration mode to reset the anomaly detection policy to factory settings.

To create, copy, display, edit, and delete anomaly detection policies, follow these steps:

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

Step 2 Create an anomaly detection policy:

```
sensor# configure terminal
sensor(config)# service anomaly-detection MyAD
Editing new instance MyAD.
sensor(config-ano)# exit
Apply Changes?[yes]: yes
sensor(config)# exit
sensor#
```

Step 3 Or copy an existing anomaly detection policy to a new anomaly detection policy:

```
sensor# copy anomaly-detection ad0 ad1
```

```
sensor#
```



Note You receive an error if the policy already exists or if there is not enough space available for the new policy.

Step 4 Accept the default anomaly detection policy values or edit the following parameters:

- a. Configure the operational settings.
- b. Configure the zones.
- c. Configure learning accept mode.
- d. Learn how to work with KBs.

Step 5 To display a list of anomaly detection policies on the sensor:

```
sensor# list anomaly-detection-configurations
Anomaly Detection
  Instance   Size   Virtual Sensor
  -----
  ad0        255   vs0
  temp       707   N/A
  MyAD       255   N/A
  ad1        141   vs1
sensor#
```

Step 6 To delete an anomaly detection policy:

```
sensor# configure terminal
sensor(config)# no service anomaly-detection MyAD
sensor(config)# exit
sensor#
```



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

Step 7 Confirm the anomaly detection instance has been deleted:

```
sensor# list anomaly-detection-configurations
Anomaly Detection
  Instance   Size   Virtual Sensor
  -----
  ad0        204   vs0
  ad1        141   N/A
sensor#
```

Step 8 To reset an anomaly detection policy to factory settings:

```
sensor# configure terminal
sensor(config)# default service anomaly-detection ad1
sensor(config)#
```

For More Information

- For the procedure for configuring operational settings, see [Configuring Anomaly Detection Operational Settings, page 9-10](#).
- For the procedures for configuring anomaly detection zones, see [Internal Zone, page 9-11](#), [Illegal Zone, page 9-19](#), and [External Zone, page 9-28](#).

- For the procedure for configuring learning accept mode, see [Configuring Learning Accept Mode, page 9-37](#).
- For the procedure for working with KBs, see [Working With KB Files, page 9-39](#).

Configuring Anomaly Detection Operational Settings

Use the **worm-timeout** command in service anomaly detection submode to set the worm detection timeout. After this timeout, the scanner threshold returns to the configured value. Use the **ignore** command in service anomaly detection submode to 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.

The following options apply:

- **worm-timeout**—The amount time in seconds for the worm termination timeout. The range is 120 to 10,000,000 seconds. The default is 600 seconds.
- **ignore**—IP addresses that should be ignored while anomaly detection is processing.
 - **enabled [true | false]**—Enables/disables the list of ignored IP addresses. The default is enabled.
 - **source-ip-address-range**—Source IP addresses that you want anomaly detection to ignore during processing.
 - **dest-ip-address-range**—Destination IP addresses that you want anomaly detection to ignore during processing.



Note IP addresses are in the form of <A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>].

To specify anomaly detection operational settings, follow these steps:

-
- Step 1** Log in to the CLI using an account with Administrator privileges.
- Step 2** Enter anomaly detection submode:
- ```
sensor# configure terminal
sensor(config)# service anomaly-detection ad1
```
- Step 3** Specify the worm timeout:
- ```
sensor(config-ano)# worm-timeout 800
```
- Step 4** Verify the setting:
- ```
sensor(config-ano)# show settings
worm-timeout: 800 seconds default: 600
```
- Step 5** Specify the destination IP addresses that you want to be ignored while anomaly detection is processing:
- ```
sensor(config-ano)# ignore
sensor(config-ano-ign)# dest-ip-address-range 10.10.5.5,10.10.2.1-10.10.2.30
```
- Step 6** Specify the source IP addresses that you want to be ignored while anomaly detection is processing:
- ```
sensor(config-ano-ign)# source-ip-address-range 10.89.30.108-10.89.30.191
```

**Step 7** Verify the settings:

```
sensor(config-ano-ign)# show settings
 ignore

 enabled: true default: true
 source-ip-address-range: 10.89.30.108-10.89.30.191 default: 0.0.0.0
 dest-ip-address-range: 10.10.5.5,10.10.2.1-10.10.2.30 default: 0.0.0.0

sensor(config-ano-ign)#
```

**Step 8** Exit anomaly detection submode:

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

**Step 9** Press **Enter** to apply your changes or enter **no** to discard them.

## Internal Zone

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

You can enable or disable TCP, UDP, and other protocols for the internal zone. You can configure a destination port for the TCP and UDP protocols and a protocol number for the other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

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

- [Configuring the Internal Zone, page 9-11](#)
- [Configuring TCP Protocol for the Internal Zone, page 9-12](#)
- [Configuring UDP Protocol for the Internal Zone, page 9-15](#)
- [Configuring Other Protocols for the Internal Zone, page 9-17](#)

## Configuring the Internal Zone

Use the **internal-zone** {**enabled** | **ip-address-range** | **tcp** | **udp** | **other**} command in service anomaly-detection submode to enable the internal zone, add IP addresses to the internal zone, and specify protocols.

The following options apply:

- **enabled** {**false** | **true**}—Enables/disables the zone.
- **ip-address-range**—The IP addresses of the subnets in the zone. The valid value is <A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>].



**Note** The second IP address in the range must be greater than or equal to the first IP address.

- **tcp**—Lets you configure TCP protocol.
- **udp**—Lets you configure UDP protocol.
- **other**—Lets you configure other protocols besides TCP and UDP.

To configure the internal zone, follow these steps:

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

**Step 2** Enter anomaly detection internal zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# internal-zone
sensor(config-ano-int)#
```

**Step 3** Enable the internal zone:

```
sensor(config-ano-int)# enabled true
```

**Step 4** Configure the IP addresses to be included in the internal zone:

```
sensor(config-ano-int)# ip-address-range 10.89.130.72-10.89.130.108
```

**Step 5** Configure TCP protocol.

**Step 6** Configure UDP protocol.

**Step 7** Configure the other protocols.

#### For More Information

- For the procedure for configuring TCP protocol, see [Configuring TCP Protocol for the Internal Zone, page 9-12](#).
- For the procedure for configuring UDP protocol, see [Configuring UDP Protocol for the Internal Zone, page 9-15](#).
- For the procedure for configuring other protocols, see [Configuring Other Protocols for the Internal Zone, page 9-17](#).

## Configuring TCP Protocol for the Internal Zone

Use the **tcp {enabled | dst-port *number* | default-thresholds}** command in service anomaly detection internal zone submode to enable and configure the TCP service.

The following options apply:

- **enabled {false | true}**—Enables/disables TCP protocol.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram {low | medium | high} num-source-ips *number***—Sets values in the threshold histogram.

- **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **dst-port number**—Defines thresholds for specific destination ports. The valid values are 0 to 65535.
- **enabled {true | false}**—Enables/disables the service.
- **override-scanner-settings {yes | no}**—Lets you override the scanner values.
  - **threshold-histogram {low | medium | high} num-source-ips number**—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure TCP protocol for the internal zone, follow these steps:

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

**Step 2** Enter anomaly detection internal zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# internal-zone
sensor(config-ano-int)#
```

**Step 3** Enable TCP protocol:

```
sensor(config-ano-int)# tcp
sensor(config-ano-int-tcp)# enabled true
```

**Step 4** Associate a specific port with TCP protocol:

```
sensor(config-ano-int-tcp)# dst-port 20
sensor(config-ano-int-tcp-dst)#
```

**Step 5** Enable the service for that port:

```
sensor(config-ano-int-tcp-dst)# enabled true
```

**Step 6** To override the scanner values for that port:

```
sensor(config-ano-int-tcp-dst)# override-scanner-settings yes
sensor(config-ano-int-tcp-dst-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-int-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-int-tcp-dst-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-int-tcp-dst-yes)# exit
sensor(config-ano-int-tcp-dst)# exit
sensor(config-ano-int-tcp)# exit
sensor(config-ano-int-tcp)# default-thresholds
sensor(config-ano-int-tcp-def)# default-thresholds
sensor(config-ano-int-tcp-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-int-tcp-def)# scanner-threshold 120
```

**Step 10** Verify the TCP configuration settings:

```

sensor(config-ano-int-tcp)# show settings
tcp

dst-port (min: 0, max: 65535, current: 4)

number: 20

override-scanner-settings

yes

scanner-threshold: 120 default: 200
threshold-histogram (min: 0, max: 3, current: 1)

dest-ip-bin: low
num-source-ips: 100

enabled: true default: true

number: 23

override-scanner-settings

no

enabled: true <defaulted>

number: 113

override-scanner-settings

no

enabled: true <defaulted>

number: 567

override-scanner-settings

no

enabled: true <defaulted>

default-thresholds

scanner-threshold: 120 default: 200
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium
num-source-ips: 120 default: 1
<protected entry>

```

```

dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

enabled: true <defaulted>

sensor(config-ano-int-tcp)#

```

## Configuring UDP Protocol for the Internal Zone

Use the **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} command in service anomaly detection internal zone submode to enable and configure the UDP service.

The following options apply:

- **enabled** {**false** | **true**}—Enables/disables UDP protocol.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **dst-port** *number*—Defines thresholds for specific destination ports. The valid values are 0 to 65535.
- **enabled** {**true** | **false**}—Enables/disables the service.
- **override-scanner-settings** {**yes** | **no**}—Lets you override the scanner values.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure UDP protocol for a zone, follow these steps:

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

**Step 2** Enter anomaly detection internal zone submode:

```

sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# internal-zone
sensor(config-ano-int)#

```

**Step 3** Enable UDP protocol:

```

sensor(config-ano-int)# udp
sensor(config-ano-int-udp)# enabled true

```

**Step 4** Associate a specific port with UDP protocol:

```

sensor(config-ano-int-udp)# dst-port 20
sensor(config-ano-int-udp-dst)#

```

**Step 5** Enable the service for that port:

```

sensor(config-ano-int-udp-dst)# enabled true

```

**Step 6** To override the scanner values for that port:

```
sensor(config-ano-int-udp-dst)# override-scanner-settings yes
sensor(config-ano-int-udp-dst-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-int-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-int-udp-dst-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-int-udp-dst-yes)# exit
sensor(config-ano-int-udp-dst)# exit
sensor(config-ano-int-udp)# default-thresholds
sensor(config-ano-int-udp-def)# default-thresholds
sensor(config-ano-int-udp-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-int-udp-def)# scanner-threshold 120
```

**Step 10** Verify the UDP configuration settings:

```
sensor(config-ano-int-udp)# show settings
udp

dst-port (min: 0, max: 65535, current: 4)

number: 20

override-scanner-settings

yes

scanner-threshold: 100 default: 200
threshold-histogram (min: 0, max: 3, current: 1)

dest-ip-bin: low
num-source-ips: 100

enabled: true default: true

number: 23

override-scanner-settings

no

enabled: true <defaulted>

number: 113

override-scanner-settings

no

```

```


enabled: true <defaulted>

number: 567

override-scanner-settings

no

enabled: true <defaulted>

default-thresholds

scanner-threshold: 120 default: 200
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium
num-source-ips: 120 default: 1
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

enabled: true <defaulted>

sensor (config-ano-int-udp) #

```

## Configuring Other Protocols for the Internal Zone

Use the **other** {**enabled** | **protocol** *number* | **default-thresholds**} command in service anomaly detection internal zone submode to enable and configure the other services.

The following options apply:

- **enabled** {**false** | **true**}—Enables/disables other protocols.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **protocol-number** *number*—Defines thresholds for specific protocols. The valid values are 0 to 255.
- **enabled** {**true** | **false**}—Enables/disables the service.

- **override-scanner-settings** {**yes** | **no**}—Lets you override the scanner values.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure other protocols for a zone, follow these steps:

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

**Step 2** Enter anomaly detection internal zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# internal-zone
sensor(config-ano-int)#
```

**Step 3** Enable the other protocols:

```
sensor(config-ano-int)# other
sensor(config-ano-int-oth)# enabled true
```

**Step 4** Associate a specific number for the other protocols:

```
sensor(config-ano-int-oth)# protocol-number 5
sensor(config-ano-int-oth-pro)#
```

**Step 5** Enable the service for that port:

```
sensor(config-ano-int-oth-pro)# enabled true
```

**Step 6** To override the scanner values for that protocol:

```
sensor(config-ano-int-oth-pro)# override-scanner-settings yes
sensor(config-ano-int-oth-pro-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-int-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-int-oth-pro-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-int-oth-pro-yes)# exit
sensor(config-ano-int-oth-pro)# exit
sensor(config-ano-int-oth)# default-thresholds
sensor(config-ano-int-oth-def)# default-thresholds
sensor(config-ano-int-oth-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-int-oth-def)# scanner-threshold 120
```

**Step 10** Verify the other configuration settings:

```
sensor(config-ano-int-oth)# show settings
other

protocol-number (min: 0, max: 255, current: 1)

number: 5
```

```

override-scanner-settings

 yes

 scanner-threshold: 95 default: 200
 threshold-histogram (min: 0, max: 3, current: 1)

 dest-ip-bin: high
 num-source-ips: 75

 enabled: true default: true

default-thresholds

 scanner-threshold: 200 <defaulted>
 threshold-histogram (min: 0, max: 3, current: 3)

 <protected entry>
 dest-ip-bin: low <defaulted>
 num-source-ips: 10 <defaulted>
 <protected entry>
 dest-ip-bin: medium <defaulted>
 num-source-ips: 1 <defaulted>
 <protected entry>
 dest-ip-bin: high <defaulted>
 num-source-ips: 1 <defaulted>

 enabled: true default: true

sensor(config-ano-int-oth)#

```

## Illegal Zone

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.

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.

You can enable or disable TCP, UDP, and other protocols for the internal zone. You can configure a destination port for the TCP and UDP protocols and a protocol number for the other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

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

- [Configuring the Illegal Zone, page 9-20](#)
- [Configuring TCP Protocol for the Illegal Zone, page 9-21](#)
- [Configuring UDP Protocol for the Illegal Zone, page 9-23](#)
- [Configuring Other Protocols for the Illegal Zone, page 9-26](#)

## Configuring the Illegal Zone

Use the **illegal-zone** {**enabled** | **ip-address-range** | **tcp** | **udp** | **other**} command in service anomaly detection submode to enable the illegal zone, add IP addresses to the illegal zone, and specify protocols.

The following options apply:

- **enabled** {**false** | **true**}—Enables/disables the zone.
- **ip-address-range**—The IP addresses of the subnets in the zone. The valid value is <A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>].



**Note** The second IP address in the range must be greater than or equal to the first IP address.

- **tcp**—Lets you configure TCP protocol.
- **udp**—Lets you configure UDP protocol.
- **other**—Lets you configure other protocols besides TCP and UDP.

To configure the illegal zone, follow these steps:

---

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

**Step 2** Enter anomaly detection illegal zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# illegal-zone
sensor(config-ano-ill)#
```

**Step 3** Enable the illegal zone:

```
sensor(config-ano-ill)# enabled true
```

**Step 4** Configure the IP addresses to be included in the illegal zone:

```
sensor(config-ano-ill)# ip-address-range 10.89.130.72-10.89.130.108
```

**Step 5** Configure TCP protocol.

**Step 6** Configure UDP protocol.

**Step 7** Configure the other protocols.

---

### For More Information

- For the procedure for configuring TCP protocol, see [Configuring TCP Protocol for the Illegal Zone, page 9-21](#).
- For the procedure for configuring UDP protocol, see [Configuring UDP Protocol for the Illegal Zone, page 9-23](#).
- For the procedure for configuring other protocols, see [Configuring Other Protocols for the Illegal Zone, page 9-26](#).

## Configuring TCP Protocol for the Illegal Zone

Use the `tcp {enabled | dst-port number | default-thresholds}` command in service anomaly detection illegal zone submode to enable and configure the TCP service.

The following options apply:

- **enabled** {false | true}—Enables/disables TCP protocol.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram** {low | medium | high} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **dst-port** *number*—Defines thresholds for specific destination ports. The valid values are 0 to 65535.
- **enabled** {true | false}—Enables/disables the service.
- **override-scanner-settings** {yes | no}—Lets you override the scanner values.
  - **threshold-histogram** {low | medium | high} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure TCP protocol for illegal zone, follow these steps:

---

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

**Step 2** Enter anomaly detection illegal zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# illegal-zone
sensor(config-ano-ill)#
```

**Step 3** Enable TCP protocol:

```
sensor(config-ano-ill)# tcp
sensor(config-ano-ill-tcp)# enabled true
```

**Step 4** Associate a specific port with TCP protocol:

```
sensor(config-ano-ill-tcp)# dst-port 20
sensor(config-ano-ill-tcp-dst)#
```

**Step 5** Enable the service for that port:

```
sensor(config-ano-ill-tcp-dst)# enabled true
```

**Step 6** To override the scanner values for that port:

```
sensor(config-ano-ill-tcp-dst)# override-scanner-settings yes
sensor(config-ano-ill-tcp-dst-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-ill-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-ill-tcp-dst-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-ill-tcp-dst-yes)# exit
sensor(config-ano-ill-tcp-dst)# exit
sensor(config-ano-ill-tcp)# exit
sensor(config-ano-ill-tcp)# default-thresholds
sensor(config-ano-ill-tcp-def)# default-thresholds
sensor(config-ano-ill-tcp-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-ill-tcp-def)# scanner-threshold 120
```

**Step 10** Verify the TCP configuration settings:

```
sensor(config-ano-ill-tcp)# show settings
tcp

dst-port (min: 0, max: 65535, current: 4)

number: 20

override-scanner-settings

yes

scanner-threshold: 100 default: 200
threshold-histogram (min: 0, max: 3, current: 1)

dest-ip-bin: low
num-source-ips: 100

enabled: true default: true

number: 23

override-scanner-settings

no

enabled: true <defaulted>

number: 113

override-scanner-settings

no

enabled: true <defaulted>

number: 567

override-scanner-settings

no


```

```

 enabled: true <defaulted>

default-thresholds

scanner-threshold: 120 default: 200
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium
num-source-ips: 120 default: 1
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

enabled: true <defaulted>

sensor(config-ano-ill-tcp)#

```

## Configuring UDP Protocol for the Illegal Zone

Use the **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} command in service anomaly detection illegal zone submode to enable and configure the UDP service.

The following options apply:

- **enabled** {**false** | **true**}—Enables/disables UDP protocol.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **dst-port** *number*—Defines thresholds for specific destination ports. The valid values are 0 to 65535.
- **enabled** {**true** | **false**}—Enables/disables the service.
- **override-scanner-settings** {**yes** | **no**}—Lets you override the scanner values.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure UDP protocol for a zone, follow these steps:

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

**Step 2** Enter anomaly detection illegal zone submode:

```

sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# illegal-zone
sensor(config-ano-ill)#

```

**Step 3** Enable UDP protocol:

```
sensor(config-ano-ill)# udp
sensor(config-ano-ill-udp)# enabled true
```

**Step 4** Associate a specific port with UDP protocol:

```
sensor(config-ano-ill-udp)# dst-port 20
sensor(config-ano-ill-udp-dst)#
```

**Step 5** Enable the service for that port:

```
sensor(config-ano-ill-udp-dst)# enabled true
```

**Step 6** To override the scanner values for that port:

```
sensor(config-ano-ill-udp-dst)# override-scanner-settings yes
sensor(config-ano-ill-udp-dst-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-ill-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-ill-udp-dst-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-ill-udp-dst-yes)# exit
sensor(config-ano-ill-udp-dst)# exit
sensor(config-ano-ill-udp)# exit
sensor(config-ano-ill-udp)# default-thresholds
sensor(config-ano-ill-udp-def)# default-thresholds
sensor(config-ano-ill-udp-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-ill-udp-def)# scanner-threshold 120
```

**Step 10** Verify the UDP configuration settings:

```
sensor(config-ano-ill-udp)# show settings
udp

dst-port (min: 0, max: 65535, current: 4)

number: 20

override-scanner-settings

yes

scanner-threshold: 100 default: 200
threshold-histogram (min: 0, max: 3, current: 1)

dest-ip-bin: low
num-source-ips: 100

enabled: true default: true

```

```
number: 23

override-scanner-settings

no

enabled: true <defaulted>

number: 113

override-scanner-settings

no

enabled: true <defaulted>

number: 567

override-scanner-settings

no

enabled: true <defaulted>

default-thresholds

scanner-threshold: 120 default: 200
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium
num-source-ips: 120 default: 1
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

enabled: true <defaulted>

sensor(config-ano-ill-udp)#
```

---

## Configuring Other Protocols for the Illegal Zone

Use the **other** {**enabled** | **protocol** *number* | **default-thresholds**} command in service anomaly detection illegal zone submode to enable and configure the other services.

The following options apply:

- **enabled** {**false** | **true**}—Enables/disables other protocols.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **protocol-number** *number*—Defines thresholds for specific protocols. The valid values are 0 to 255.
- **enabled** {**true** | **false**}—Enables/disables the service.
- **override-scanner-settings** {**yes** | **no**}—Lets you override the scanner values.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure other protocols for a zone, follow these steps:

---

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

**Step 2** Enter anomaly detection illegal zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# illegal-zone
sensor(config-ano-ill)#
```

**Step 3** Enable the other protocols:

```
sensor(config-ano-ill)# other
sensor(config-ano-ill-oth)# enabled true
```

**Step 4** Associate a specific number for the other protocols:

```
sensor(config-ano-ill-oth)# protocol-number 5
sensor(config-ano-ill-oth-pro)#
```

**Step 5** Enable the service for that port:

```
sensor(config-ano-ill-oth-pro)# enabled true
```

**Step 6** To override the scanner values for that protocol:

```
sensor(config-ano-ill-oth-pro)# override-scanner-settings yes
sensor(config-ano-ill-oth-pro-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-ill-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-ill-oth-pro-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-ill-oth-pro-yes)# exit
sensor(config-ano-ill-oth-pro)# exit
sensor(config-ano-ill-oth)# default-thresholds
sensor(config-ano-ill-oth-def)# default-thresholds
sensor(config-ano-ill-oth-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-ill-oth-def)# scanner-threshold 120
```

**Step 10** Verify the other configuration settings:

```
sensor(config-ano-ill-oth)# show settings
other

protocol-number (min: 0, max: 255, current: 1)

number: 5

override-scanner-settings

yes

scanner-threshold: 95 default: 200
threshold-histogram (min: 0, max: 3, current: 1)

dest-ip-bin: high
num-source-ips: 75

enabled: true default: true

default-thresholds

scanner-threshold: 200 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

enabled: true default: true

sensor(config-ano-ill-oth)#
```

# External Zone

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.

You can enable or disable TCP, UDP, and other protocols for the external zone. You can configure a destination port for the TCP and UDP protocols and a protocol number for the other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

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

- [Configuring the External Zone, page 9-28](#)
- [Configuring TCP Protocol for the External Zone, page 9-29](#)
- [Configuring UDP Protocol for the External Zone, page 9-31](#)
- [Configuring Other Protocols for the External Zone, page 9-34](#)

## Configuring the External Zone

Use the **external-zone {enabled | tcp | udp | other}** command in service anomaly detection submode to enable the external zone and specify protocols.

The following options apply:

- **enabled {false | true}**—Enables/disables the zone.
- **tcp**—Lets you configure TCP protocol.
- **udp**—Lets you configure UDP protocol.
- **other**—Lets you configure other protocols besides TCP and UDP.

To configure the external zone, follow these steps:

---

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

**Step 2** Enter anomaly detection external zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# external-zone
sensor(config-ano-ext)#
```

**Step 3** Enable the external zone:

```
sensor(config-ano-ext)# enabled true
```

**Step 4** Configure TCP protocol.

**Step 5** Configure UDP protocol.

**Step 6** Configure the other protocols.

---

**For More Information**

- For the procedure for configuring TCP protocol, see [Configuring TCP Protocol for the External Zone, page 9-29](#).
- For the procedure for configuring UDP protocol, see [Configuring UDP Protocol for the External Zone, page 9-31](#).
- For the procedure for configuring other protocols, see [Configuring Other Protocols for the External Zone, page 9-34](#).

## Configuring TCP Protocol for the External Zone

Use the `tcp {enabled | dst-port number | default-thresholds}` command in service anomaly detection external zone submode to enable and configure the TCP service.

The following options apply:

- **enabled {false | true}**—Enables/disables TCP protocol.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram {low | medium | high} num-source-ips number**—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **dst-port number**—Defines thresholds for specific destination ports. The valid values are 0 to 65535.
- **enabled {true | false}**—Enables/disables the service.
- **override-scanner-settings {yes | no}**—Lets you override the scanner values.
  - **threshold-histogram {low | medium | high} num-source-ips number**—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure TCP protocol for the external zone, follow these steps:

---

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

**Step 2** Enter anomaly detection external zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# external-zone
sensor(config-ano-ext)#
```

**Step 3** Enable TCP protocol:

```
sensor(config-ano-ext)# tcp
sensor(config-ano-ext-tcp)# enabled true
```

**Step 4** Associate a specific port with TCP protocol:

```
sensor(config-ano-ext-tcp)# dst-port 20
sensor(config-ano-ext-tcp-dst)#
```

**Step 5** Enable the service for that port:

```
sensor(config-ano-ext-tcp-dst)# enabled true
```

**Step 6** To override the scanner values for that port:

```
sensor(config-ano-ext-tcp-dst)# override-scanner-settings yes
sensor(config-ano-ext-tcp-dst-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-ext-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-ext-tcp-dst-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-ext-tcp-dst-yes)# exit
sensor(config-ano-ext-tcp-dst)# exit
sensor(config-ano-ext-tcp)# exit
sensor(config-ano-ext-tcp)# default-thresholds
sensor(config-ano-ext-tcp-def)# default-thresholds
sensor(config-ano-ext-tcp-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-ext-tcp-def)# scanner-threshold 120
```

**Step 10** Verify the TCP configuration settings:

```
sensor(config-ano-ext-tcp)# show settings
tcp

dst-port (min: 0, max: 65535, current: 4)

number: 20

override-scanner-settings

yes

scanner-threshold: 100 default: 200
threshold-histogram (min: 0, max: 3, current: 1)

dest-ip-bin: low
num-source-ips: 100

enabled: true default: true

number: 23

override-scanner-settings

no

enabled: true <defaulted>

number: 113

override-scanner-settings

no
```

```


enabled: true <defaulted>

number: 567

override-scanner-settings

no

enabled: true <defaulted>

default-thresholds

scanner-threshold: 120 default: 200
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium
num-source-ips: 120 default: 1
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

enabled: true <defaulted>

sensor(config-ano-ext-tcp)#

```

## Configuring UDP Protocol for the External Zone

Use the **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} command in service anomaly detection external zone submode to enable and configure the UDP service.

The following options apply:

- **enabled** {**false** | **true**}—Enables/disables UDP protocol.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **dst-port** *number*—Defines thresholds for specific destination ports. The valid values are 0 to 65535.
- **enabled** {**true** | **false**}—Enables/disables the service.

- **override-scanner-settings** {yes | no}—Lets you override the scanner values.
  - **threshold-histogram** {low | medium | high} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure UDP protocol for a zone, follow these steps:

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

**Step 2** Enter anomaly detection external zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# external-zone
sensor(config-ano-ext)#
```

**Step 3** Enable UDP protocol:

```
sensor(config-ano-ext)# udp
sensor(config-ano-ext-udp)# enabled true
```

**Step 4** Associate a specific port with UDP protocol:

```
sensor(config-ano-ext-udp)# dst-port 20
sensor(config-ano-ext-udp-dst)#
```

**Step 5** Enable the service for that port:

```
sensor(config-ano-ext-udp-dst)# enabled true
```

**Step 6** To override the scanner values for that port:

```
sensor(config-ano-ext-udp-dst)# override-scanner-settings yes
sensor(config-ano-ext-udp-dst-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-ext-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-ext-udp-dst-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-ext-udp-dst-yes)# exit
sensor(config-ano-ext-udp-dst)# exit
sensor(config-ano-ext-udp)# default-thresholds
sensor(config-ano-ext-udp-def)# default-thresholds
sensor(config-ano-ext-udp-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-ext-udp-def)# scanner-threshold 120
```

**Step 10** Verify the UDP configuration settings:

```
sensor(config-ano-ext-udp)# show settings
udp

dst-port (min: 0, max: 65535, current: 4)

number: 20
```

```

override-scanner-settings

 yes

 scanner-threshold: 100 default: 200
 threshold-histogram (min: 0, max: 3, current: 1)

 dest-ip-bin: low
 num-source-ips: 100

enabled: true default: true

number: 23

override-scanner-settings

 no

enabled: true <defaulted>

number: 113

override-scanner-settings

 no

enabled: true <defaulted>

number: 567

override-scanner-settings

 no

enabled: true <defaulted>

default-thresholds

scanner-threshold: 120 default: 200
threshold-histogram (min: 0, max: 3, current: 3)

 <protected entry>
 dest-ip-bin: low <defaulted>
 num-source-ips: 10 <defaulted>
 <protected entry>
 dest-ip-bin: medium
 num-source-ips: 120 default: 1
 <protected entry>
 dest-ip-bin: high <defaulted>
 num-source-ips: 1 <defaulted>

enabled: true <defaulted>

```

```
sensor(config-ano-ext-udp)#
```

---

## Configuring Other Protocols for the External Zone

Use the **other** {**enabled** | **protocol** *number* | **default-thresholds**} command in service anomaly detection external zone submode to enable and configure the other services.

The following options apply:

- **enabled** {**false** | **true**}—Enables/disables other protocols.
- **default-thresholds**—Defines thresholds to be used for all ports not specified in the destination port map.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.
- **protocol-number** *number*—Defines thresholds for specific protocols. The valid values are 0 to 255.
- **enabled** {**true** | **false**}—Enables/disables the service.
- **override-scanner-settings** {**yes** | **no**}—Lets you override the scanner values.
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*—Sets values in the threshold histogram.
  - **scanner-threshold**—Sets the scanner threshold. The default is 200.

To configure other protocols for a zone, follow these steps:

---

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

**Step 2** Enter anomaly detection external zone submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# external-zone
sensor(config-ano-ext)#
```

**Step 3** Enable the other protocols:

```
sensor(config-ano-ext)# other
sensor(config-ano-ext-oth)# enabled true
```

**Step 4** Associate a specific number for the other protocols:

```
sensor(config-ano-ext-oth)# protocol-number 5
sensor(config-ano-ext-oth-pro)#
```

**Step 5** Enable the service for that port:

```
sensor(config-ano-ext-oth-pro)# enabled true
```

**Step 6** To override the scanner values for that protocol:

```
sensor(config-ano-ext-oth-pro)# override-scanner-settings yes
sensor(config-ano-ext-oth-pro-yes)#
```

You can use the default scanner values, or you can override them and configure your own scanner values.

**Step 7** To add a histogram for the new scanner settings:

```
sensor(config-ano-ext-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

Enter the number of destination IP addresses (low, medium, or high) and the number of source IP addresses you want associated with this histogram.

**Step 8** Set the scanner threshold:

```
sensor(config-ano-ext-oth-pro-yes)# scanner-threshold 100
```

**Step 9** Configure the default thresholds for all other unspecified ports:

```
sensor(config-ano-ext-oth-pro-yes)# exit
sensor(config-ano-ext-oth-pro)# exit
sensor(config-ano-ext-oth)# default-thresholds
sensor(config-ano-ext-oth-def)# default-thresholds
sensor(config-ano-ext-oth-def)# threshold-histogram medium num-source-ips 120
sensor(config-ano-ext-oth-def)# scanner-threshold 120
```

**Step 10** Verify the other configuration settings:

```
sensor(config-ano-ext-oth)# show settings
other

protocol-number (min: 0, max: 255, current:1)

number: 5

override-scanner-settings

yes

scanner-threshold: 95 default: 200
threshold-histogram (min: 0, max: 3, current: 1)

dest-ip-bin: high
num-source-ips: 75

enabled: true default: true

default-thresholds

scanner-threshold: 200 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
```

```

num-source-ips: 1 <defaulted>

enabled: true default: true

sensor(config-ano-ext-oth)#

```

## Learning Accept Mode

This section describes KBs and histograms and how to configure learning accept mode. It contains the following topics:

- [The KB and Histograms, page 9-36](#)
- [Configuring Learning Accept Mode, page 9-37](#)
- [Saving and Loading KBs Manually, page 9-40](#)

## 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 9-2](#) describes this example.

**Table 9-2** 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 50 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, 50, 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 (50).

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.

#### For More Information

- For more information on learning accept mode, see [Configuring Learning Accept Mode, page 9-37](#).
- For more information on configuring anomaly detection zones, see [Configuring the Internal Zone, page 9-11](#), [Configuring the Illegal Zone, page 9-20](#), and [Configuring the External Zone, page 9-28](#).

## Configuring Learning Accept Mode

Use the **learning-accept-mode** command in service anomaly detection submode 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 new updated KB file name is the current date and time, *YYYY-Mon-dd-hh\_mm\_ss*, where *Mon* is the three-letter abbreviation of the month.



#### Note

Learning accept mode uses the sensor local time.

The following options apply:

- **learning-accept-mode**—Specifies if and when the KB is saved and loaded.
  - **auto**—Configures the sensor to automatically accept the KB.
  - **manual**—Does not save the KB.



#### Note

You can save and load the KB using the **anomaly-detection [load | save]** commands.

- **action**—Lets you specify whether to rotate or save the KB.
  - **save-only**—Saves the new KB. You can examine it and decide whether to load it into anomaly detection.



#### Note

You can load the KB using the **anomaly-detection load** command.

- **rotate**—Saves the new KB and loads it as the current KB according to the schedule you define.
- **schedule**—Configures a schedule to accept the KB.
  - **calendar-schedule [days-of-week] [times-of-day]**—Starts learning accept mode at specific times on specific days.
  - **periodic-schedule [interval] [start-time]**—Starts learning accept mode at specific periodic intervals.

**Note**

The first saving begins after a full interval between configuration time and start time. For example, if the time is now 16:00 and you configure start time at 16:30 with an interval of one hour, the first KB is saved at 17:30, because there was no one-hour interval between 16:00 and 16:30.

To configure learning accept mode, follow these steps:

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

**Step 2** Enter anomaly detection submode:

```
sensor# configure terminal
sensor(config)# service anomaly-detection ad1
```

**Step 3** Specify how the KB is saved and loaded.

- a. Specify that the KB is automatically saved and loaded:

```
sensor(config-ano)# learning-accept-mode auto
sensor(config-ano-auto)#
```

Go to Step 4.

- b. Specify that the KB is going to be manually saved and loaded:

```
sensor(config-ano)# learning-accept-mode manual
```

**Step 4** Specify how you want the KB automatically accepted.

- a. To save the KB so that you can inspect it and decide whether to load it:

```
sensor(config-ano-aut)# action save-only
```

Go to Step 6.

- b. To have the KB saved and loaded as the current KB according to the schedule you define:

```
sensor(config-ano-aut)# action rotate
```

Continue with Step 5.

**Step 5** Schedule the automatic KB saves and loads:

- For the calendar schedule:

```
sensor(config-ano-aut)# schedule calendar-schedule
sensor(config-ano-aut-cal)# days-of-week monday
sensor(config-ano-aut-cal)# times-of-day time 24:00:00
```

With this schedule the KB is saved and loaded every Monday at midnight.

- For the periodic schedule:

```
sensor(config-ano-aut)# schedule periodic-schedule
sensor(config-ano-aut-per)# start-time 24:00:00
sensor(config-ano-aut-per)# interval 24
```

With this schedule the KB is saved and loaded every 24 hours at midnight.

**Step 6** Verify the settings:

```
sensor(config-ano-aut-per)# exit
sensor(config-ano-aut)# show settings
auto

action: rotate default: rotate
```

```

schedule

periodic-schedule

start-time: 12:00:00 default: 10:00:00
interval: 24 hours default: 24


```

**Step 7** Exit anomaly detection submode:

```

sensor(config-ano-aut)# exit
sensor(config-ano)# exit
Apply Changes?[yes]:

```

**Step 8** Press **Enter** to apply your changes or enter **no** to discard them.

#### For More Information

For the procedures for saving and loading KBs manually, see [Saving and Loading KBs Manually](#), page 9-40.

## Working With KB Files

This section describes how to display, load, save, copy, rename and delete KB files. It also provides the procedures for comparing two KB files and for displaying the thresholds of a KB file. It contains the following topics:

- [Displaying KB Files](#), page 9-39
- [Saving and Loading KBs Manually](#), page 9-40
- [Copying, Renaming, and Erasing KBs](#), page 9-41
- [Displaying the Differences Between Two KBs](#), page 9-43
- [Displaying the Thresholds for a KB](#), page 9-44

## Displaying KB Files

Use the **show ad-knowledge-base [virtual-sensor] files** command in privileged EXEC mode to display the available KB files for a virtual sensor.



#### Note

The \* before the file name indicates that this KB file is the currently loaded KB file.

To display KB files, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Display the KB files for all virtual sensors:

```

sensor# show ad-knowledge-base files
Virtual Sensor vs0
 Filename Size Created

```

```

 initial 84 04:27:07 CDT Wed Jan 29 2003
* 2003-Jan-28-10_00_01 84 04:27:07 CDT Wed Jan 29 2003
Virtual Sensor vs1
 Filename Size Created
 initial 84 14:35:38 CDT Tue Mar 14 2006
 2006-Mar-16-10_00_00 84 10:00:00 CDT Thu Mar 16 2006
 2006-Mar-17-10_00_00 84 10:00:00 CDT Fri Mar 17 2006
 2006-Mar-18-10_00_00 84 10:00:00 CDT Sat Mar 18 2006
 2006-Mar-19-10_00_00 84 10:00:00 CDT Sun Mar 19 2006
 2006-Mar-20-10_00_00 84 10:00:00 CDT Mon Mar 20 2006
 2006-Mar-21-10_00_00 84 10:00:00 CDT Tue Mar 21 2006
 2006-Mar-22-10_00_00 84 10:00:00 CDT Wed Mar 22 2006
 2006-Mar-23-10_00_00 84 10:00:00 CDT Thu Mar 23 2006
 2006-Mar-24-10_00_00 84 10:00:00 CDT Fri Mar 24 2006
 2006-Mar-25-10_00_00 84 10:00:00 CDT Sat Mar 25 2006
 2006-Mar-26-10_00_00 84 10:00:00 CDT Sun Mar 26 2006
 2006-Mar-27-10_00_00 84 10:00:00 CDT Mon Mar 27 2006
 2003-Jan-02-10_00_00 84 10:00:00 CDT Thu Jan 02 2003
 2003-Jan-03-10_00_00 84 10:00:00 CDT Fri Jan 03 2003
 2003-Jan-04-10_00_00 84 10:00:00 CDT Sat Jan 04 2003
 2003-Jan-05-10_00_00 84 10:00:00 CDT Sun Jan 05 2003
 2003-Jan-06-10_00_00 84 10:00:00 CDT Mon Jan 06 2003
sensor#

```

**Step 3** Display the KB files for a specific virtual sensor:

```

sensor# show ad-knowledge-base vs0 files
Virtual Sensor vs0
 Filename Size Created
 initial 84 10:24:58 CDT Tue Mar 14 2006
 2006-Mar-16-10_00_00 84 10:00:00 CDT Thu Mar 16 2006
 2006-Mar-17-10_00_00 84 10:00:00 CDT Fri Mar 17 2006
 2006-Mar-18-10_00_00 84 10:00:00 CDT Sat Mar 18 2006
 2006-Mar-19-10_00_00 84 10:00:00 CDT Sun Mar 19 2006
 2006-Mar-20-10_00_00 84 10:00:00 CDT Mon Mar 20 2006

```

## Saving and Loading KBs Manually

Use these commands in privileged EXEC mode to manually save and load KBs.

The following options apply:

- **show ad-knowledge-base virtual-sensor files**—Displays the available KB files per virtual sensor.
- **anomaly-detection virtual-sensor load {initial | file name}**—Sets the KB file as the current KB for the specified virtual sensor. If anomaly detection is active, the file is loaded as the current KB.
- **anomaly-detection virtual-sensor save [new-name]**—Retrieves the current KB file and saves it locally.

To manually save and load a KB, follow these steps:

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

**Step 2** Locate the KB you want to load:

```

sensor# show ad-knowledge-base vs0 files
Virtual Sensor vs0
 Filename Size Created
 initial 84 10:24:58 CDT Tue Mar 14 2006

```

```

2006-Mar-16-10_00_00 84 10:00:00 CDT Thu Mar 16 2006
2006-Mar-17-10_00_00 84 10:00:00 CDT Fri Mar 17 2006
2006-Mar-18-10_00_00 84 10:00:00 CDT Sat Mar 18 2006
2006-Mar-19-10_00_00 84 10:00:00 CDT Sun Mar 19 2006
2006-Mar-20-10_00_00 84 10:00:00 CDT Mon Mar 20 2006

```

**Step 3** To load the KB file as the current KB file for a specific virtual sensor:

```

sensor# anomaly-detection vs0 load file 2006-Mar-16-10_00_00
sensor#

```

**Step 4** To save the current KB file and store it as a new name:

```

sensor# anomaly-detection vs0 save my-KB
sensor#

```



**Note** An error is generated if anomaly detection is not active when you enter this command. You cannot overwrite the initial file.

## Copying, Renaming, and Erasing KBs

Use these commands in privileged EXEC mode to manually copy, rename, and erase KB files.

The following options apply:

- **copy ad-knowledge-base** *virtual-sensor* { **current** | **initial** | **file name** } *destination-url*—Copies the KB file (current, initial, or the file name you enter) to a specified destination URL.



**Note** Copying a file to a name that already exists overwrites it.

- **copy ad-knowledge-base** *virtual-sensor source-url new-name*—Copies a KB with a new file name to the source URL you specify.



**Note** You cannot use the **current** keyword as a *new-name*. A new current KB file is created with the **load** command.

- **rename ad-knowledge-base** *virtual-sensor* { **current** | **file name** } *new-name*—Renames an existing KB file.
- **erase ad-knowledge-base** [*virtual-sensor [name]*]—Removes all KB files from a virtual sensor, or just one KB file if you use the *name* option.



**Note** You cannot erase the initial KB file or the KB file loaded as the current KB.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- **ftp:**—Source or destination URL for an FTP network server. The syntax for this prefix is:  
ftp:[//[username@] location]/relativeDirectory]/filename  
ftp:[//[username@]location]//absoluteDirectory]/filename
- **scp:**—Source or destination URL for the SCP network server. The syntax for this prefix is:  
scp:[//[username@] location]/relativeDirectory]/filename  
scp:[//[username@] location]//absoluteDirectory]/filename




---

**Note** If you use FTP or SCP protocol, you are prompted for a password. If you use SCP protocol, you must add the remote host to the SSH known hosts list.

---

- **http:**—Source URL for the web server. The syntax for this prefix is:  
http:[//[username@]location]/directory]/filename
- **https:**—Source URL for the web server. The syntax for this prefix is:  
https:[//[username@]location]/directory]/filename




---

**Note** If you use HTTPS protocol, the remote host must be a TLS trusted host.

---

To copy, rename, and remove KB files, follow these steps:

---

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

**Step 2** Locate the KB file you want to copy:

```
sensor# show ad-knowledge-base vs0 files
Virtual Sensor vs0
 Filename Size Created
 initial 84 10:24:58 CDT Tue Mar 14 2006
 2006-Mar-16-10_00_00 84 10:00:00 CDT Thu Mar 16 2006
 2006-Mar-17-10_00_00 84 10:00:00 CDT Fri Mar 17 2006
 2006-Mar-18-10_00_00 84 10:00:00 CDT Sat Mar 18 2006
 2006-Mar-19-10_00_00 84 10:00:00 CDT Sun Mar 19 2006
 2006-Mar-20-10_00_00 84 10:00:00 CDT Mon Mar 20 2006
```

**Step 3** To copy the KB file to a user on a computer with the IP address 10.1.1.1:

```
sensor# copy ad-knowledge-base vs0 file 2006-Mar-16-10_00_00
scp://cidsuser@10.1.1.1/AD/my-KB
password: *****
sensor#
```

**Step 4** To rename a KB file:

```
sensor# rename ad-knowledge-base vs0 2006-Mar-16-10_00_00 My-KB
sensor#
```

**Step 5** To remove a KB file from a specific virtual sensor:

```
sensor# erase ad-knowledge-base vs0 2006-Mar-16-10_00_00
sensor#
```

**Step 6** To remove all KB files except the file loaded as current and the initial KB file from a virtual sensor:

```
sensor# erase ad-knowledge-base vs0
Warning: Executing this command will delete all virtual sensor 'vs0' knowledge bases
except the file loaded as current and the initial knowledge base.
Continue with erase? [yes]: yes
sensor#
```

**Step 7** To remove all KB files except the file loaded as current and the initial KB file from all virtual sensors:

```
sensor# erase ad-knowledge-base
Warning: Executing this command will delete all virtual sensor knowledge bases except the
file loaded as current and the initial knowledge base.
Continue with erase? [yes]: yes
sensor#
```

#### For More Information

- For the procedure for creating KB files, see [Saving and Loading KBs Manually, page 9-40](#).
- For the procedure for adding remote hosts to the SSH known hosts list, see [Adding Hosts to the SSH Known Hosts List, page 4-38](#).
- For the procedure for making a remote host a TLS trusted host, see [Adding TLS Trusted Hosts, page 4-43](#).

## Displaying the Differences Between Two KBs

Use the `show ad-knowledge-base virtual-sensor diff {current | initial | file name1}{current | initial | file name2} [diff-percentage]` command in privileged EXEC mode to display the differences between two KBs.

The following options apply:

- *virtual-sensor*—Name of the virtual sensor that contains the KB files you want to compare.
- *name1*—Name of the first existing KB file to compare.
- *name2*—Name of the second existing KB file to compare.
- **current**—The currently loaded KB.
- **initial**—The initial KB.
- **file**—The name of an existing KB file.
- *diff-percentage*—(Optional) Displays the services where the thresholds differ more than the specified percentage. The valid values are 1 to 100. The default is 10%.

To compare two KBs, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Locate the file you want to compare:

```
sensor# show ad-knowledge-base vs0 files
Virtual Sensor vs0
 Filename Size Created
 initial 84 04:27:07 CDT Wed Jan 29 2003
* 2006-Jun-28-10_00_01 84 04:27:07 CDT Thu Jun 29 2006
sensor#
```

**Step 3** Compare the currently loaded file (the file with the \*) with the initial KB for virtual sensor vs0:

```

sensor# show ad-knowledge-base vs0 diff initial file 2006-Jun-28-10_00_01
Initial Only Services/Protocols
 External Zone
 TCP Services
 Service = 30
 Service = 20
 UDP Services
 None
 Other Protocols
 Protocol = 1
 Illegal Zone
 None
 Internal Zone
 None
2006-Jun-28-10_00_01 Only Services/Protocols
 External Zone
 None
 Illegal Zone
 None
 Internal Zone
 None
Thresholds differ more than 10%
 External Zone
 None
 Illegal Zone
 TCP Services
 Service = 31
 Service = 22
 UDP Services
 None
 Other Protocols
 Protocol = 3
 Internal Zone
 None
sensor#

```

---

## Displaying the Thresholds for a KB

Use the `show ad-knowledge-base virtual-sensor thresholds {current | initial | file name} [zone {external | illegal | internal}] {[protocol {tcp | udp}] [dst-port port] | [protocol other] [number protocol-number]}` command in privileged EXEC mode to display the thresholds in a KB.

The following options apply:

- *virtual-sensor*—Name of the virtual sensor that contains the KB files you want to compare.
- *name*—Name of the existing KB file.
- **current**—The currently loaded KB.
- **initial**—The initial KB.
- **file**—The name of an existing KB file.
- **zone**—(Optional) Displays the thresholds for the specified zone. The default displays information for all zones.
- **external**—Displays the thresholds for the external zone.

- **illegal**—Displays the thresholds for the illegal zone.
- **internal**—Displays the thresholds for the internal zone.
- **protocol**—(Optional) Displays the thresholds for the specified protocol. The default displays information about all protocols.
- **tcp**—Displays the thresholds for the TCP protocol.
- **udp**—Displays the thresholds for the UDP protocol.
- **other**—Displays the thresholds for the other protocols besides TCP or UDP.
- **dst-port**—(Optional) Displays thresholds for the specified port. The default displays information about all TCP and/or UDP ports.
- *port*—The port number. The valid values are 0 to 65535.
- **number**—(Optional) Displays thresholds for the specified other protocol number. The default displays information for all other protocols.
- *protocol-number*—The protocol number. The valid values are 0 to 255.

To display the KB thresholds, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Locate the file for which you want to display thresholds:

```
sensor# show ad-knowledge-base vs1 files
Virtual Sensor vs1
 Filename Size Created
 ----- -
 initial 84 10:24:58 CDT Tue Mar 14 2006
 2006-Mar-16-10_00_00 84 10:00:00 CDT Thu Mar 16 2006
 2006-Mar-17-10_00_00 84 10:00:00 CDT Fri Mar 17 2006
 2006-Mar-18-10_00_00 84 10:00:00 CDT Sat Mar 18 2006
 2006-Mar-19-10_00_00 84 10:00:00 CDT Sun Mar 19 2006
 2006-Mar-27-10_00_00 84 10:00:00 CDT Mon Mar 27 2006
 2006-Apr-24-05_00_00 88 05:00:00 CDT Mon Apr 24 2006
 * 2006-Apr-25-05_00_00 88 05:00:00 CDT Tue Apr 25 2006
```

**Step 3** To display thresholds contained in a specific file for the illegal zone:

```
sensor# show ad-knowledge-base vs0 thresholds file 2006-Nov-11-10_00_00 zone illegal

AD Thresholds
Creation Date = 2006-Nov-11-10_00_00
KB = 2006-Nov-11-10_00_00
Illegal Zone
 TCP Services
 Default
 Scanner Threshold
 User Configuration = 200
 Threshold Histogram - User Configuration
 Low = 10
 Medium = 3
 High = 1
 UDP Services
 Default
 Scanner Threshold
 User Configuration = 200
 Threshold Histogram - User Configuration
 Low = 10
 Medium = 3
 High = 1
 Other Services
```

```

 Default
 Scanner Threshold
 User Configuration = 200
 Threshold Histogram - User Configuration
 Low = 10
 Medium = 3
 High = 1

```

```
sensor#
```

**Step 4** To display thresholds contained in the current KB illegal zone, protocol TCP, and destination port 20:

```
sensor# show ad-knowledge-base vs0 thresholds current zone illegal protocol tcp dst-port 20
```

```

AD Thresholds
Creation Date = 2006-Nov-14-10_00_00
KB = 2006-Nov-14-10_00_00
Illegal Zone
TCP Services
 Default
 Scanner Threshold
 User Configuration = 200
 Threshold Histogram - User Configuration
 Low = 10
 Medium = 3
 High = 1

```

```
sensor#
```

**Step 5** To display thresholds contained in the current KB illegal zone, and protocol other:

```
sensor# show ad-knowledge-base vs0 thresholds current zone illegal protocol other
```

```

AD Thresholds
Creation Date = 2006-Nov-14-10_00_00
KB = 2006-Nov-14-10_00_00
Illegal Zone
Other Services
 Default
 Scanner Threshold
 User Configuration = 200
 Threshold Histogram - User Configuration
 Low = 10
 Medium = 3
 High = 1

```

```
sensor#
```

## Displaying Anomaly Detection Statistics

Use the **show statistics anomaly-detection** *[virtual-sensor-name]* command in privileged EXEC mode to display the statistics for anomaly detection. You can see if an attack is in progress (*Attack in progress* or *No attack*). You can also see when the next KB will be saved (*Next KB rotation at 10:00:00 UTC Wed Apr 26 2006*).



### Note

The **clear** command is not available for anomaly detection statistics.

To display anomaly detection statistics, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Display the anomaly detection statistics for a specific virtual sensor:

```
sensor# show statistics anomaly-detection vs0
Statistics for Virtual Sensor vs0
 No attack
 Detection - ON
 Learning - ON
 Next KB rotation at 10:00:00 UTC Wed Apr 26 2006
 Internal Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
 External Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
 Illegal Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
sensor#
```

**Step 3** To display the statistics for all virtual sensors:

```
sensor# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
 No attack
 Detection - ON
 Learning - ON
 Next KB rotation at 10:00:01 UTC Wed Jun 29 2006
 Internal Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
 External Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
 Illegal Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
Statistics for Virtual Sensor vs1
 No attack
 Detection - ON
 Learning - ON
 Next KB rotation at 10:00:00 UTC Wed Jul 29 2006
 Internal Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
 External Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
```

```

Illegal Zone
 TCP Protocol
 UDP Protocol
 Other Protocol
sensor#

```

---

## Turning Off Anomaly Detection

If 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 submode:
- ```

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.
- 

### For More Information

For more information about worms, see [Worms, page 9-2](#).