CHAPTER 8

Configuring Policies

This chapter describes IPS policies and how to configure the virtual sensor. It contains the following sections:

Understanding 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 6.1 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.

IPS Policies Components

This section describes the various components of IPS Policies, and contains the following sections:

Understanding Analysis Engine

Analysis Engine performs packet analysis and alert detection. It monitors traffic that flows through specified interfaces.

You create virtual sensors in Analysis Engine. Each virtual sensor has a unique name with a list of interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups associated with it. To avoid definition ordering issues, no conflicts or overlaps are allowed in assignments. You assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a specific virtual sensor so that no packet is processed by more than one virtual sensor. Each virtual sensor is also associated with a specifically named signature definition, event action rules, and anomaly detection configuration. Packets from interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups that are not assigned to any virtual sensor are disposed of according to the inline bypass configuration.

Note Cisco IPS 6.1 does not support more than four virtual sensors. You cannot delete the default virtual sensor vs0.

Understanding the Virtual Sensor

The sensor can receive data inputs from one or many monitored data streams. These monitored data streams can either be physical interface ports or virtual interface ports. For example, a single sensor can monitor traffic from in front of the firewall, from behind the firewall, or from in front of and behind the firewall concurrently. And a single sensor can monitor one or more data streams. In this situation a single sensor policy or configuration is applied to all monitored data streams.

A virtual sensor is a collection of data that is defined by a set of configuration policies. The virtual sensor is applied to a set of packets as defined by interface component.

A virtual sensor can monitor multiple segments, and you can apply a different policy or configuration for each virtual sensor within a single physical sensor. You can set up a different policy per monitored segment under analysis. You can also apply the same policy instance, for example, sig0, rules0, or ad0, to different virtual sensors.

You can assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a virtual sensor.

Note The default virtual sensor is vs0. You cannot delete the default virtual sensor. The interface list, the anomaly detection operational mode, the inline TCP session tracking mode, and the virtual sensor description are the only configuration features you can change for the default virtual sensor. You cannot change the signature definition, event action rules, or anomaly detection policies.

Advantages and Restrictions of Virtualization

Virtualization has the following advantages:

- You can apply different configurations to different sets of traffic.
- You can monitor two networks with overlapping IP spaces with one sensor.
- You can monitor both inside and outside of a firewall or NAT device.

Virtualization has the following restrictions:

- You must assign both sides of asymmetric traffic to the same virtual sensor.
- Using VACL capture or SPAN (promiscuous monitoring) is inconsistent with regard to VLAN tagging, which causes problems with VLAN groups.
  - When using Cisco IOS software, a VACL capture port or a SPAN target does not always receive tagged packets even if it is configured for trunking.
  - When using the MSFC, fast path switching of learned routes changes the behavior of VACL captures and SPAN.
- Persistent store is limited.

Virtualization has the following traffic capture requirements:

- The virtual sensor must receive traffic that has 802.1q headers (other than traffic on the native VLAN of the capture port).
- The sensor must see both directions of traffic in the same VLAN group in the same virtual sensor for any given sensor.

The following sensors support virtualization:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS 4270-20
- AIP-SSM

IDSM-2 supports virtualization with the exception of VLAN groups on inline interface pairs. AIM-IPS and NME-IPS do not support virtualization.

Inline TCP Session Tracking Mode

When you choose to modify packets inline, if the packets from a stream are seen twice by the Normalizer engine, it cannot properly track the stream state and often the stream is dropped. This situation occurs most often when a stream is routed through multiple VLANs or interfaces that are being monitored by the IPS. A further complication in this situation is the necessity of allowing asymmetric traffic to merge for proper tracking of streams when the traffic for either direction is received from different VLANs or interfaces. To deal with this situation, you can set the mode so that streams are perceived as unique if they are received on separate interfaces and/or VLANs (or the subinterface for VLAN pairs).

The following inline TCP session tracking modes apply:

- Interface and VLAN—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) and on the same interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.
- VLAN Only—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) regardless of the interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.
- Virtual Sensor—All packets with the same session key (AaBb) within a virtual sensor belong to the same session. This is the default and almost always the best option to choose.

Understanding Normalizer Mode

Normalizer mode only applies when the sensor is operating in inline mode. The default is strict evasion protection, which is full enforcement of TCP state and sequence tracking. The Normalizer enforces duplicate packets, changed packets, out-of-order packets, and so forth, which helps prevent attackers from evading the IPS.

Asymmetric mode disables most of the Normalizer checks. Use asymmetric mode only when the entire stream cannot be inspected, because in this situation, attackers can now evade the IPS.

Understanding Event Action Overrides

You can add an event action override to change the actions associated with an event based on the risk rating of that event. Event action overrides are a way to add event actions globally without having to configure each signature individually. Each event action has an associated risk rating range. If a signature event occurs and the risk rating for that event falls within the range for an event action, that action is added to the event. For example, if you want any event with a risk rating of 85 or more to generate an SNMP trap, you can set the risk rating range for Request SNMP Trap to 85-100. If you do not want to use action overrides, you can disable the entire event action override component.

Calculating the Risk Rating

A risk rating is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network. The calculation takes into account the value of the network asset being attacked (for example, a particular server), so it is configured on a per-signature basis (attack severity rating and signature fidelity rating) and on a per-server basis (target value rating). The risk rating is calculated from several components, some of which are configured, some collected, and some derived.

Note The risk rating is associated with alerts not signatures.

Risk ratings let you prioritize alerts that need your attention. These risk rating factors take into consideration the severity of the attack if it succeeds, the fidelity of the signature, and the overall value of the target host to you. The risk rating is reported in the evIdsAlert.

The following values are used to calculate the risk rating for a particular event:

- Signature fidelity rating (SFR)—A weight associated with how well this signature might perform in the absence of specific knowledge of the target. The signature fidelity rating is configured per signature and indicates how accurately the signature detects the event or condition it describes.

  Signature fidelity rating is calculated by the signature author on a per-signature basis. The signature author defines a baseline confidence ranking for the accuracy of the signature in the absence of qualifying intelligence on the target. It represents the confidence that the detected behavior would produce the intended effect on the target platform if the packet under analysis were allowed to be delivered. For example, a signature that is written with very specific rules (specific regular expression) has a higher signature fidelity rating than a signature that is written with generic rules.

  Note The signature fidelity rating does not indicate how bad the detected event may be.

- Attack severity rating (ASR)—A weight associated with the severity of a successful exploit of the vulnerability.

  The attack severity rating is derived from the alert severity parameter (informational, low, medium, or high) of the signature. The attack severity rating is configured per signature and indicates how dangerous the event detected is.

  Note The attack severity rating does not indicate how accurately the event is detected.

- Target value rating (TVR)—A weight associated with the perceived value of the target.

  The target value rating is a user-configurable value (zero, low, medium, high, or mission critical) that identifies the importance of a network asset (through its IP address). You can develop a security policy that is more stringent for valuable corporate resources and looser for less important resources. For example, you could assign a target value rating to the company web server that is higher than the target value rating you assign to a desktop node. In this example, attacks against the company web server have a higher risk rating than attacks against the desktop node. Target value rating is configured in the Event Action Rules policy.

- Attack relevance rating (ARR)—A weight associated with the relevancy of the targeted OS.

  The attack relevance rating is a derived value (relevant, unknown, or not relevant), which is determined at alert time. The relevant OSes are configured per signature.

- Promiscuous delta (PD)—A weight associated with the promiscuous delta, which can be subtracted from the overall risk rating in promiscuous mode.

  The promiscuous delta is in the range of 0 to 30 and is configured per signature.

  Note If the trigger packet is not inline, the promiscuous delta is subtracted from the rating.

- Watch list rating (WLR)—A weight associated with the CSA MC watch list in the range of 0 to 100 (CSA MC only uses the range 0 to 35).

  If the attacker for the alert is found on the watch list, the watch list rating for that attacker is added to the rating.

Figure 8-1 illustrates the risk rating formula:

Figure 8-1 Risk Rating Formula

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

191016

Understanding Threat Rating

Threat rating is risk rating that has been lowered by event actions that have been taken. Nonlogging event actions have a threat rating adjustment. The largest threat rating from all the event actions taken is subtracted from the risk rating.

The event actions have the following threat ratings:

- Deny attacker inline—45
- Deny attacker victim pair inline—40
- Deny attacker service pair inline—40
- Deny connection inline—35
- Deny packet inline—35
- Modify packet inline—35
- Request block host—20
- Request block connection—20
- Reset TCP connection—20
- Request rate limit—20

Event Action Summarization

Summarization decreases the volume of alerts sent out from the sensor by providing basic aggregation of events into a single alert. Special parameters are specified for each signature and they influence the handling of the alerts. Each signature is created with defaults that reflect a preferred normal behavior. However, you can tune each signature to change this default behavior within the constraints for each engine type.

The nonalert-generating actions (deny, block, TCP reset) go through the filters for each signature event unsummarized. The alert-generating actions are not performed on these summarized alerts; instead the actions are applied to the one summary alert and then put through the filters.

If you select one of the other alert-generating actions and do not have it filtered out, the alert is created even if you do not select Produce Alert. To prevent alerts from being created, you must have all alert-generating actions filtered out.

Summarization and event actions are processed after the Meta engine has processed the component events. This lets the sensor watch for suspicious activity transpiring over a series of events.

Event Action Aggregation

Basic aggregation provides two operating modes. The simple mode involves configuring a threshold number of hits for a signature that must be met before the alert is sent. A more advanced mode is timed-interval counting. In this mode, the sensor tracks the number of hits per second and only sends alerts when that threshold is met. In this example, a hit is a term used to describe an event, which is basically an alert, but it is not sent out of the sensor as an alert until the threshold number of hits has been exceeded.

You can choose from the following summarization options:

- Fire All—Fire All mode fires an alert each time the signature is triggered. If the threshold is set for summarization, alerts are fired for each execution until summarization occurs. After summarization starts only one alert every summary interval fires for each address set. Alerts for other address sets are either all seen or separately summarized. The signature reverts to Fire All mode after a period of no alerts for that signature.
- Summary—Summary mode fires an alert the first time a signature is triggered, and then additional alerts for that signature are summarized for the duration of the summary interval. Only one alert every summary interval should fire for each address set. If the global summary threshold is reached, the signature goes into Global Summarization mode.
- Global Summarization—Global Summarization mode fires an alert for every summary interval. Signatures can be preconfigured for global summarization.
- Fire Once—Fire Once mode fires an alert for each address set. You can upgrade this mode to Global Summarization mode.

Configuring IPS Policies

This section describes IPS Policies and how to configure a virtual sensor. It contains the following topics:

IPS Policies Pane

The IPS Policies pane displays a list of the virtual sensors in the upper half of the pane. In the upper half of this pane you can add, edit, or delete virtual sensors.

For each virtual sensor the following information is displayed:

- Assigned interfaces or pairs
- Signature definition policy
- Event action rules overrides policy
  - Risk rating
  - Actions to add
  - Enabled or disabled

- Anomaly detection policy
- Description of the virtual sensor

Note The default virtual sensor is vs0. You cannot delete the default virtual sensor.

In the lower half of the pane, you can configure the event action rules for each virtual sensor that you select in the upper half of the pane.

Note You can also configure event action rules in the **Configuration > *sensor_name* > Policies > Event Action rules > rules0** pane.

The Event Action Rules part of the pane contains the following tabs:

- Event Action Filters—Lets you remove specifications from an event or discard an entire event and prevent further processing by the sensor.
- Target Value Rating—Lets you assign a target value rating to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert.
- OS Identifications—Lets you associate IP addresses with an OS type, which in turn helps the sensor calculate the attack relevance rating.
- Event Variables—Lets you create event variables to use in event action filters. When you want to use the same value within multiple filters, you can use an event variable.
- Risk Category—Lets you create the risk categories you want to use to monitor sensor and network health and to use in event action overrides.
- General Settings—Lets you configure some global settings that apply to event action rules.

IPS Policies Pane Field Definitions

The following fields are found in the IPS Policies pane:

- Name—The name of the virtual sensor. The default virtual sensor is vs0.
- Assigned Interfaces (or Pairs)—The interfaces or interface pairs that belong to this virtual sensor.
- Sig Definition Policy—The name of the signature definition policy for this virtual sensor. The default signature definition policy is sig0.
- Event Action Rules Overrides Policy—The name of the event action rules overrides policy for this virtual sensor. The default event action rules policy is rules0.
  - Risk Rating—Indicates the risk rating range (low, medium, or high risk) that should be used to trigger this event action override.
  - Actions to Add—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
  - Enabled—Indicates whether or not this event action overrides policy is enabled.
- Anomaly Detection Policy—The name of the anomaly detection policy for this virtual sensor. The default anomaly detection policy is ad0.
- Description—The description of this virtual sensor.

Add and Edit Virtual Sensor Dialog Boxes Field Definitions

Note You must be administrator or operator to configure a virtual sensor.

You can apply the same policy, for example, sig0, rules0, and ad0, to different virtual sensors. The Add Virtual Sensor dialog box displays only the interfaces that are available to be assigned to this virtual sensor. Interfaces that have already been assigned to other virtual sensors are not shown in this dialog box.

You can also assign event action overrides to virtual sensors, and configure the following modes:

- Anomaly detection operational mode
- Inline TCP session tracking mode
- Normalizer mode

The following fields are found in the Add and Edit Virtual Sensor dialog boxes:

- Virtual Sensor Name—Name for this virtual sensor.
- Description—Description for this virtual sensor.
- Interfaces—Lets you assign and remove interfaces for this virtual sensor.
  - Assigned—Whether the interfaces or interface pairs have been assigned to the virtual sensor.
  - Name—The list of available interfaces or interface pairs that you can assign to the virtual sensor (GigabitEthernet or FastEthernet).
  - Details—Lists the mode (Inline Interface or Promiscuous) of the interface and the interfaces of the inline pairs.
- Signature Definition Policy—The name of the signature definition policy you want to assign to this virtual sensor. The default is sig0.
- Event Action Rules Policy—The name of the event action rules policy you want to assign to this virtual sensor. The default is rules0.
- Use Event Action Overrides—When checked, lets you configure event action overrides when you click **Add** to open the Add Event Action Override dialog box.
  - Risk Rating—Indicates the level of risk rating for this override.
  - Actions to Add—Indicates the action to add to this override.
  - Enabled—Indicates whether this override is enabled or disabled.
- Anomaly Detection Policy—The name of the anomaly detection policy you want to assign to this virtual sensor. The default is ad0.
- AD Operational Mode—The mode that you want the anomaly detection policy to operate in for this virtual sensor. The default is Detect.
- Inline TCP Session Tracking Mode—The mode used to segregate multiple views of the same stream if the same stream passes through the sensor more than once. The default mode is Virtual Sensor.
  - Interface and VLAN—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) and on the same interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.
  - VLAN Only—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) regardless of the interface belong to the same session.Packets with the same key but on different VLANs are tracked separately.

- Virtual Sensor—All packets with the same session key (AaBb) within a virtual sensor belong to the same session.

- Normalizer Mode—Lets you choose which type of Normalizer mode you need for traffic inspection:
  - Strict Evasion Protection—If a packet is missed for any reason, all packets after the missed packet are not processed. Strict evasion protection provides full enforcement of TCP state and sequence tracking.

    Note Any out-of-order packets or missed packets can produce Normalizer engine signatures 1300 or 1330 firings, which try to correct the situation, but can result in denied connections.

  - Asymmetric Mode Protection—Can only see one direction of bidirectional traffic flow. Asymmetric mode protection relaxes the evasion protection at the TCP layer.

    Note Asymmetric mode lets the sensor synchronize state with the flow and maintain inspection for those engines that do not require both directions. Asymmetric mode lowers security because full protection requires both sides of traffic to be seen.

Add and Edit Event Action Override Dialog Boxes Field Definitions

Note You must be administrator or operator to add or edit event action overrides.

The following fields are found in the Add and Edit Event Action Override dialog boxes:

- Risk Rating—Lets you add the risk rating range, either low, medium, or high risk, that should be used to trigger this event action override.

  If an event occurs with a risk rating that corresponds to the risk you configure, the event action is added to this event.

  In **Add** mode, you can create a numeric range by entering it in to the Risk Rating field. In **Edit** mode, you can select the category that you created.

- Available Actions to Add—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.

- Enabled—Check the check box to enable the action.

Understanding Deny Packet Inline

For signatures that have Deny Packet Inline configured as an action or for an event action override that adds Deny Packet Inline as an action, the following actions may be taken:

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

The deny packet inline action is represented as a dropped packet action in the alert. When a deny packet inline occurs for a TCP connection, it is automatically upgraded to a deny connection inline action and seen as a denied flow in the alert. If the IPS denies just one packet, the TCP continues to try to send that same packet again and again, so the IPS denies the entire connection to ensure it never succeeds with the resends.

When a deny connection inline occurs, the IPS also automatically sends a TCP one-way reset, which shows up as a TCP one-way reset sent in the alert. When the IPS denies the connection, it leaves an open connection on both the client (generally the attacker) and the server (generally the victim). Too many open connections can result in resource problems on the victim. So the IPS sends a TCP reset to the victim to close the connection on the victim side (usually the server), which conserves the resources of the victim. It also prevents a failover that would otherwise allow the connection to fail over to a different network path and reach the victim. The IPS leaves the attacker side open and denies all traffic from it.

Adding, Editing, and Deleting Virtual Sensors

Note You must assign all interfaces to a virtual sensor and enable them before they can monitor traffic.

To add, edit, and delete virtual sensors, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**, and then click **Add Virtual Sensor**.

Step 3 In the Virtual Sensor Name field, enter a name for the virtual sensor.

Step 4 In the Description field, enter a description of this virtual sensor.

Step 5 To assign the interface to the virtual sensor, check the check box next to the interface you need, and then click **Assign**.

Note Only the available interfaces are listed in the Interfaces list. If other interfaces exist, but have already been assigned to a virtual sensor, they do not appear in this list.

Step 6 Choose a signature definition policy from the drop-down list.

Unless you want to use the default sig0, you must have already added a signature definition policy by choosing **Configuration > *sensor_name* > Policies > Signature Definitions > Add**.

Step 7 Choose an event action rules policy from the drop-down list.

Unless you want to use the default rules0, you must have already added a signature definition policy by choosing **Configuration > *sensor_name* > Policies > Event Action Rules > Add**.

Step 8 To add event action override to this virtual sensor, check the **Use Event Action Overrides** check box, and then click **Add**.

Note You must check the **Use Event Action Overrides** check box or none of the event action overrides will be enabled regardless of the value you set.

a. Choose the risk rating from the Risk Rating drop-down list.

b. Under the Assigned column, check the check boxes next to the actions you want to assign to this event action override.

c. Under the Enabled column, check the check boxes next to the actions you want enabled.

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

d. Click **OK**.

Step 9 Choose an anomaly detection policy from the drop-down list.

Unless you want to use the default ad0, you must have already added a signature definition policy by choosing **Configuration > *sensor_name* > Policies > Anomaly Detections > Add**.

Step 10 Choose the anomaly detection mode (Detect, Inactive, Learn) from the drop-down list. The default is Detect.

Step 11 Click the **Double Arrow** icon to change the default values under Advanced Options:

a. Choose how the sensor tracks inline TCP sessions (by interface and VLAN, VLAN only, or virtual sensor).

The default is virtual sensor. This is almost always the best option to choose.

b. Choose the Normalizer mode (by strict evasion protection or asymmetric mode protection).

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

Step 12 Click **OK**.

The virtual sensor appears in the list in the IPS Policies pane.

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

Step 13 To edit a virtual sensor, select it in the list, and then click **Edit**.

Step 14 Make any changes needed, and then click **OK**.

The edited virtual sensor appears in the list in the upper half of the IPS Policies pane.

Step 15 To remove a virtual sensor, select it, and then click **Delete**.

The virtual sensor no longer appears in the upper half of the IPS Policies pane.

Note You cannot delete the default virtual sensor, vs0.

Step 16 Click **Apply** to apply your changes and save the revised configuration.

Configuring Event Action Filters

This section describes how to configure event action filters, and contains the following topics:

Understanding Event Action Filters

Event action filters are processed as an ordered list and you can move filters up or down in the list.

Filters let the sensor perform certain actions in response to the event without requiring the sensor to perform all actions or remove the entire event. Filters work by removing actions from an event. A filter that removes all actions from an event effectively consumes the event.

Note When filtering sweep signatures, we recommend that you do not filter the destination addresses. If there are multiple destination addresses, only the last address is used for matching the filter.

Event Action Filters Tab

Note You must be administrator or operator to add, edit, enable, disable, or delete event action filters.

You can configure event action filters to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor. You can use the variables that you defined on the Event Variables pane to group addresses for your filters.

Note You must preface the variable with a dollar sign ($) to indicate that you are using a variable rather than a string. Otherwise, you receive the `Bad source and destination` error.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

Event Action Filters Tab Field Definitions

The following fields are found on the Event Action Filters tab:

- Name—Lets you name the filter you are adding. You need to name your filters so that you can move them around in the list and move them to the inactive list if needed.
- Enabled—Indicates whether or not this filter is enabled.

- Sig ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. You can also enter a range of signatures.
- SubSig ID—Identifies the unique numerical value assigned to this subsignature. The subSig ID identifies a more granular version of a broad signature. You can also enter a range of subSig IDs.
- Attacker (address/port)—Identifies the IP address and/or port of the host that sent the offending packet. You can also enter a range of addresses.
- Victim (address/port)—Identifies the IP address and/or port used by the attacker host. This is the port from where the offending packet originated. You can also enter a range of ports.
- Risk Rating—Indicates the risk rating range between 0 and 100 that should be used to trigger this event action filter. If an event occurs with a risk rating that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
- Actions to Subtract—Indicates the actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter.

Add and Edit Event Action Filter Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Event Action Filters dialog boxes:

- Name—Lets you name the filter you are adding. You need to name your filters so that you can move them around in the list and move them to the inactive list if needed.
- Enabled—Lets you enable this filter.
- Signature ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. You can also enter a range of signatures.
- Subsignature ID—Identifies the unique numerical value assigned to this subsignature. The subsignature ID identifies a more granular version of a broad signature. You can also enter a range of subsignature IDs.
- Attacker Address—Identifies the IP address of the host that sent the offending packet. You can also enter a range of addresses.
- Attacker Port—Identifies the port used by the attacker host. This is the port from where the offending packet originated. You can also enter a range of ports.
- Victim Address—Identifies the IP address of the host being attacked (the recipient of the offending packet). You can also enter a range of addresses.
- Victim Port—Identifies the port through which the offending packet was received. You can also enter a range of ports.
- Risk Rating—Indicates the risk rating range between 0 and 100 that should be used to trigger this event action filter. If an event occurs with a risk rating that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
- Actions to Subtract—Opens the Edit Actions dialog box and lets you choose the actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter.
- Active—Lets you add the filter to the filter list so that it takes effect on filtering events.
- OS Relevance—Lets you filter out events where the attack is not relevant to the victim OS.
- Deny Percentage—Determines the percentage of packets to deny for deny attacker features. The valid range is 0 to 100. The default is 100 percent.

- Stop on Match—Determines whether or not this event will be processed against remaining filters in the event action filters list.

  If set to No, the remaining filters are processed for a match until a Stop flag is encountered.

  If set to Yes, no further processing is done. The actions specified by this filter are removed and the remaining actions are performed.
- Comments—Displays the user comments associated with this filter.

Adding, Editing, Deleting, Enabling, Disabling, and Moving Event Action Filters

To add, edit, delete, enable, disable, and move event action filters, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the pane, select the virtual sensor in the list for which you want to add event action filters.

Step 4 In the Event Action Rules half of the pane, click the Event Action Filters tab, and then click **Add**.

Step 5 In the Name field, enter a name for the event action filter.

A default name is supplied, but you can change it to a more meaningful name.

Step 6 In the Enabled field, click the **Yes** radio button to enable the filter.

Step 7 In the Signature ID field, enter the signature IDs of all signatures to which this filter should be applied.

You can use a list (2001, 2004), or a range (2001–2004) or one of the SIG variables if you defined them on the Event Variables tab. Preface the variable with $.

Step 8 In the SubSignature ID field, enter the subsignature IDs of the subsignatures to which this filter should be applied.

Step 9 In the Attacker Address field, enter the IP address of the source host.

You can use one of the variables if you defined them on the Event Variables tab. Preface the variable with $. You can also enter a range of addresses (for example, 0.0.0.0-255.255.255.255).

Step 10 In the Attacker Port field, enter the port number used by the attacker to send the offending packet.

Step 11 In the Victim Address field, enter the IP address of the recipient host.

You can use one of the variables if you defined them on the Event Variables tab. Preface the variable with $. You can also enter a range of addresses (for example, 0.0.0.0-255.255.255.255).

Step 12 In the Victim Port field, enter the port number used by the victim host to receive the offending packet.

Step 13 In the Risk Rating field, enter a risk rating range for this filter.

If the risk rating for an event falls within the range you specify, the event is processed against the criteria of this filter.

Step 14 In the Actions to Subtract field, click the note icon to open the Edit Actions dialog box.

Step 15 Check the check boxes of the actions you want this filter to remove from the event.

Tip To choose more than one event action in the list, hold down the **Ctrl** key.

Step 16 In the Active field, click the **Yes** radio button to add this filter to the list so that it takes effect on filtering events.

Step 17 In the OS Relevance drop-down list, choose whether you want to know if the alert is relevant to the OS that has been identified for the victim.

Step 18 In the Deny Percentage field, enter the percentage of packets to deny for deny attacker features.

The default is 100 percent.

Step 19 In the Stop on Match field, click one of the following radio buttons:

a. **Yes**—If you want the Event Action Filters component to stop processing after the actions of this particular filter have been removed.

   Any remaining filters will not be processed; therefore, no additional actions can be removed from the event.

b. **No**—If you want to continue processing additional filters.

Step 20 In the Comments field, enter any comments that you want to store with this filter, such as the purpose of this filter or why you have configured this filter in a particular way.

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

Step 21 Click **OK**.

The new event action filter now appears in the list on the Event Action Filters tab.

Step 22 To edit an existing event action filter, select it in the list, and then click **Edit**.

Step 23 Make any changes needed.

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

Step 24 Click **OK**.

The edited event action filter now appears in the list on the Event Action Filters tab.

Step 25 To delete an event action filter, select it in the list, and then click **Delete**.

The event action filter no longer appears in the list on the Event Action Filters tab.

Step 26 To move an event action filter up or down in the list, select it, and then click the **Move Up** or **Move Down** arrow icons.

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

Step 27 Click **Apply** to apply your changes and save the revised configuration.

Configuring Target Value Rating

This section describes how to configure the target value rating, and contains the following topics:

Target Value Rating Tab

Note You must be administrator or operator to add, edit, or delete target value ratings.

You can assign a target value rating to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert. You can assign different target value ratings to different targets. Events with a higher risk rating trigger more severe signature event actions.

Target Value Rating Tab Field Definitions

The following fields are found on the Target Value Rating tab:

- Target Value Rating (TVR)—Identifies the value assigned to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IP Address—Identifies the IP address of the network asset you want to prioritize with a target value rating.

Add and Edit Target Value Rating Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Target Value Rating dialog boxes:

- Target Value Rating (TVR)—Lets you assign a value to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IP Address(es)—Identifies the IP address of the network asset you want to prioritize with a target value rating.

Adding, Editing, and Deleting Target Value Ratings

To add, edit, and delete the target value rating for network assets, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure target value ratings.

Step 4 In the Event Action Rules half of the pane, click the Target Value Rating tab, and then click **Add**.

Step 5 To assign a target value rating to a new group of assets, follow these steps:

a. From the Target Value Rating (TVR) drop-down list, choose a rating.

The values are High, Low, Medium, Mission Critical, or No Value.

b. In the Target IP Address(es) field, enter the IP address of the network asset.

To enter a range of IP addresses, enter the lowest address followed by a hyphen and then the highest address in the range. For example: 10.10.2.1-10.10.2.30.

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

Step 6 Click **OK**.

The new target value rating for the new asset appears in the list on the Target Value Rating tab.

Step 7 To edit an existing target value rating, select it in the list, and then click **Edit**.

Step 8 Make any changes needed.

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

Step 9 Click **OK**.

The edited network asset now appears in the list on the Target Value Rating tab.

Step 10 To delete a network asset, select in the list, and then click **Delete**.

The network asset no longer appears in the list on the Target Value Rating tab.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring OS Identifications

This section describes how to configure OS maps, and contains the following topics:

Understanding Passive OS Fingerprinting

Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK packets exchanged on the network to determine the OS type.

The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk rating of the alert for the attack and/or the sensor may filter the alert for the attack. You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the victim OS, the source of the OS identification, and the relevance to the victim OS in the alert.

Passive OS fingerprinting consists of three components:

- Passive OS learning

  Passive OS learning occurs as the sensor observes traffic on the network. Based on the characteristics of TCP SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address.

- User-configurable OS identification

  You can configure OS host mappings, which take precedence over learned OS mappings.

- Computation of attack relevance rating and risk rating

  The sensor uses OS information to determine the relevance of the attack signature to the targeted host. The attack relevance is the attack relevance rating component of the risk rating value for the attack alert. The sensor uses the OS type reported in the host posture information imported from the CSA MC to compute the attack relevance rating.

There are three sources of OS information. The sensor ranks the sources of OS information in the following order:

1. Configured OS mappings—OS mappings you enter. Configured OS mappings reside in the Event Action Rules policy and can apply to one or many virtual sensors.

Caution You can specify multiple operating systems for the same IP address. The last one in the list is the operating system that is matched.

2. Imported OS mappings—OS mappings imported from an external data source. Imported OS mappings are global and apply to all virtual sensors.

   Note Currently CSA MC is the only external data source.

3. Learned OS mappings—OS mappings observed by the sensor through the fingerprinting of TCP packets with the SYN control bit set. Learned OS mappings are local to the virtual sensor that sees the traffic.

When the sensor needs to determine the OS for a target IP address, it consults the configured OS mappings. If the target IP address is not in the configured OS mappings, the sensor looks in the imported OS mappings. If the target IP address is not in the imported OS mappings, the sensor looks in the learned OS mappings. If it cannot find it there, the sensor treats the OS of the target IP address as unknown.

Note Passive OS fingerprinting is enabled by default and the IPS contains a default vulnerable OS list for each signature.

Configuring Passive OS Fingerprinting

You do not have to configure passive OS fingerprinting for it to function. IPS provides a default vulnerable OS list for each signature and passive analysis is enabled by default.

You can configure the following aspects of passive OS fingerprinting:

- Define OS mappings

  We recommend configuring OS mappings to define the identity of the OS running on critical systems. It is best to configure OS mappings when the OS and IP address of the critical systems are unlikely to change.

- Limit the attack relevance rating calculation to a specific IP address range

  This limits the attack relevance rating calculations to IP addresses on the protected network.

- Import OS mappings

  Importing OS mappings provides a mechanism for accelerating the learning rate and fidelity of the OS identifications made through passive analysis. If you have an external product interface, such as the CSA MC, you can import OS identifications from it.

- Define event action rules filters using the OS relevancy value of the target

  This provides a way to filter alerts solely on OS relevancy.

- Disable passive analysis

  Stops the sensor from learning new OS mappings.

- Edit signature vulnerable OS lists

  The vulnerable OS list specifies what OS types are vulnerable to each signature. The default, general-os, applies to all signatures that do not specify a vulnerable OS list.

OS Identifications Tab

Note You must be administrator or operator to add, edit, and delete configured OS maps.

Use the OS Identifications tab to configure OS host mappings, which take precedence over learned OS mappings. On the OS Identifications tab you can add, edit, and delete configured OS maps. You can move them up and down in the list to change the order in which the sensor computes the attack relevance rating and risk rating for that particular IP address and OS type combination.

You can also move them up and down in the list to change the order in which the sensor resolves the OS associated with a particular IP address. Configured OS mappings allow for ranges, so for network 192.168.1.0/24 an administrator might define the following (Table 8-1):

Table 8-1 Example Configured OS Mapping

IP Address Range Set	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10,192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

More specific mappings should be at the beginning of the list. Overlap in the IP address range sets is allowed, but the entry closest to the beginning of the list takes precedence.

OS Identifications Tab Field Definitions

The following fields are found on the OS Identifications tab:

- Enable passive OS fingerprinting analysis—When checked, lets the sensor perform passive OS analysis.
- Restrict OS mapping and ARR to these IP addresses—Lets you configure the mapping of OS type to a specific IP address and have the sensor calculate the attack relevance rating for that IP address.
- Configured OS Map—Displays the attributes of the configured OS map.
  - Name—The Name you give the configured OS map.
  - Active—Whether this configured OS map is active or inactive.
  - IP Address—The IP address of this configured OS map.
  - OS Type—The OS type of this configured OS map.

Add and Edit Configured OS Map Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Configured OS Map dialog boxes:

- Name—Lets you name this configured OS map.
- Active—Lets you choose to have the configured OS map active or inactive.
- IP Address—Lets you enter the IP address associated with this configured OS map.

  The IP address for configured OS mappings (and *only* configured OS mappings) can be a set of IP addresses and IP address ranges. The following are all valid IP address values for configured OS mappings:
  - 10.1.1.1,10.1.1.2,10.1.1.15
  - 10.1.2.1
  - 10.1.1.1-10.2.1.1,10.3.1.1
  - 10.1.1.1-10.1.1.5

- OS Type—Lets you choose one of the following OS Types to associate with the IP address:
  - AIX
  - BSD
  - General OS
  - HP UX
  - IOS
  - IRIX
  - Linux
  - Mac OS
  - Netware
  - Other
  - Solaris
  - UNIX
  - Unknown OS
  - Win NT
  - Windows
  - Windows NT/2K/XP

Adding, Editing, Deleting, and Moving Configured OS Maps

To add, edit, delete, and move configured OS maps, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure OS identifications.

Step 4 In the Event Action Rules half of the pane, click the OS Identifications tab, and then click **Add**.

Step 5 In the Name field, enter a name for the configured OS map.

Step 6 In the Active field, click the **Yes** radio button to add this configured OS map to the list so that it takes effect.

Step 7 In the IP Address field, enter the IP address of the host that you are mapping to an OS.

For example, use this format, 10.10.5.5,10.10.2.1-10.10.2.30.

Step 8 From the OS Type drop-down list, choose the OS that will be mapped to the IP address.

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

Step 9 Click **OK**.

The new configured OS map now appears in the list on the OS Identifications tab.

Step 10 Check the **Enable passive OS fingerprinting analysis** check box.

Note You must check the **Enable passive OS fingerprinting analysis** check box on the OS Identifications tab or none of the configured OS maps will be enabled regardless of the value you set in the Add Configured OS Map dialog box.

Step 11 To edit a configured OS map, select it in the list, and then click **Edit**.

Step 12 Make any changes needed.

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

Step 13 Click **OK**.

The edited configured OS map now appears in the list on the OS Identifications tab.

Step 14 Check the **Enable passive OS fingerprinting analysis** check box.

Note You must check the **Enable passive OS fingerprinting analysis** check box on the OS Identifications tab or none of the configured OS maps will be enabled regardless of the value you set in the Edit Configured OS Map dialog box.

Step 15 To delete a configured OS map, select it in the list, and then click **Delete**.

The configured OS map no longer appears in the list on the OS Identifications tab.

Step 16 To move a configured OS map up or down in the list, select it, and then click the **Move Up** or **Move Down** arrows.

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

Step 17 Click **Apply** to apply your changes and save the revised configuration.

Configuring Event Variables

This section describes how to configure event variables, and contains the following topics:

Event Variables Tab

Note You must be administrator or operator to add, edit, or delete event variables.

You can create event variables and then use those variables in event action filters. When you want to use the same value within multiple filters, use a variable. When you change the value of the variable, any filter that uses that variable is updated with the new value.

Note You must preface the variable with a dollar ($) sign to indicate that you are using a variable rather than a string.

Some variables cannot be deleted because they are necessary to the signature system. If a variable is protected, you cannot select it to edit it. You receive an error message if you try to delete protected variables. You can edit only one variable at a time.

When configuring IP addresses, specify the full IP address or ranges or set of ranges. For example:

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 10.89.10.10-10.89.10.23

Timesaver For example, if you have an IP address space that applies to your engineering group and there are no Windows systems in that group, and you are not worried about any Windows-based attacks to that group, you could set up a variable to be the IP address space of the engineering group. You could then use this variable to configure a filter that would ignore all Windows-based attacks for this group.

Event Variables Tab Field Definitions

The following fields are found on the Event Variables tab:

- Name—Lets you assign a name to this variable.
- Type—Identifies the variable as an address.
- Value—Lets you add the value(s) represented by this variable.

Add and Edit Event Variable Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Event Variable dialog boxes:

- Name—Lets you assign a name to this variable.
- Type—Identifies the variable as an address.

  Note This is the only available event variable in Cisco IPS 6.1.

- Value—Lets you add the value(s) represented by this variable.

Adding, Editing, and Deleting Event Variables

To add, edit, and delete event variables, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure event variables.

Step 4 In the Event Action Rules half of the pane, click the Event Variables tab, and then click **Add**.

Step 5 In the Name field, enter a name for this variable.

Note A valid name can only contain numbers or letters. You can also use a hyphen (-) or an underscore (_).

Step 6 In the Value field, enter the values for this variable.

Specify the full IP address or ranges or set of ranges. For example:

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255

Note You can use commas as delimiters. Make sure there are no trailing spaces after the comma. Otherwise, you receive a `Validation failed` error.

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

Step 7 Click **OK**.

The new variable appears in the list on the Event Variables tab.

Step 8 To edit an existing variable, select it in the list, and then click **Edit**.

Step 9 Make any changes needed.

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

Step 10 Click **OK**.

The edited event variable now appears in the list on the Event Variables tab.

Step 11 To delete an event variable, select in the list, and then click **Delete**.

The event variable no longer appears in the list on the Event Variables tab.

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

Step 12 Click **Apply** to apply your changes and save the revised configuration.

Configuring Risk Category

This section describes how to configure them risk categories, and contains the following topics:

Risk Category Tab

Note You must be administrator to add and edit risk levels.

On the Risk Category tab, you can use predefined risk categories (HIGHRISK, MEDIUMRISK, AND LOWRISK) or you can define your own labels. Risk categories link a category name to a numeric range defining the risk rating. You specify the low threshold for the category to make sure that the ranges are contiguous. The upper category is either the next higher category or 100.

You can then group the threats in red, yellow, and green categories. These red, yellow, and green threshold statistics are used in event action overrides and are also shown in the Network Security Gadget on the Home page.

Note You cannot delete a predefined risk category.

The red, yellow, and green threshold statistics represent the state of network security with red being the most critical. If you change a threshold, any event action overrides that had the same range as the risk category are changed to reflect the new range.

The new category is inserted in to the Risk Category list according to its threshold value and is automatically assigned actions that cover its range.

Risk Category Tab Field Definitions

The following fields are found on the Risk Category tab:

- Risk Category Name—Name of this risk level. The predefined categories have the following values:
  - HIGHRISK—90 (means 90 to 100)
  - MEDIUMRISK—70 (means 70-89)
  - LOWRISK—1 (means 1-69)
- Risk Threshold—Threshold number for this risk. The value is a number from 0 to 100.

- Risk Range—Risk Rating range for his risk category.

  The risk rating is a range between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
- Network Security Health Statistics—Lists the numbers for the red, yellow, and green thresholds. The overall network security value represents the least secure value (green is the most secure and red is the least secure).
  - Red Threat Thresholds
  - Yellow Threat Thresholds
  - Green Threat Thresholds

    These color thresholds refer to the Sensor Health gadget on the Home pane.

Add and Edit Risk Level Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Risk Level dialog boxes:

- Risk Name—Lets you name this risk level.
- Risk Threshold—Lets you assign a risk threshold for this risk level.

  You specify or change only the lower threshold for the category so that the risk categories are contiguous. The upper threshold is either the next higher category or 100.
- Active—Lets you make this risk level active.

Adding, Editing, and Deleting Risk Categories

To add, edit, and delete risk categories, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure risk categories.

Step 4 In the Event Action Rules half of the pane, click the Risk Category tab, and then click **Add**.

Step 5 In the Risk Name field, enter a name for this risk category.

Step 6 In the Risk Threshold field, enter a numerical value for the risk threshold (minimum 0, maximum 100).

This number represents the lower boundary of risk. The range appears in the Risk Range field and in the red, yellow, and green threshold fields.

Step 7 To make this risk category active, click the **Yes** radio button.

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

Step 8 Click **OK**.

The new risk category appears in the list on the Risk Category tab.

Step 9 To edit an existing risk category, select it in the list, and then click **Edit**.

Step 10 Make any changes needed.

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

Step 11 Click **OK**.

The edited risk category now appears in the list on the Risk Category tab.

Step 12 To delete a risk category, select in the list, and then click **Delete**.

The risk category no longer appears in the list on the Risk Category tab.

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

Step 13 Click **Apply** to apply your changes and save the revised configuration.

Configuring General Settings

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

General Tab

Note You must be administrator or operator to configure the general settings for event action rules.

You can configure the general settings that apply globally to event action rules, such as whether you want to use the Summarizer and the Meta Event Generator. The Summarizer groups events into a single alert, thus decreasing the number of alerts the sensor sends out. The Meta Event Generator processes the component events, which lets the sensor watch for suspicious activity transpiring over a series of events.

Caution Do not disable the Summarizer or Meta Event Generator except for troubleshooting purposes. If you disable the Summarizer, every signature is set to Fire All with no summarization. If you disable the Meta Event Generator, all Meta engine signatures are disabled.

You can also use Threat Rating adjustment, Event Action Filters, and you can enable One Way TCP Reset. The one-way TCP reset operates for inline mode only and is an automatic addition to the deny packet inline actions. It sends a TCP reset to the victim of the alert, thus creating a black hole for the attacker and clearing the TCP resources of the victim.

Note An inline sensor now denies packets for any alert with a risk rating of greater than or equal to 90. It also issues a one-way TCP reset on TCP alerts with a risk rating of greater than or equal to 90.

You can configure how long you want to deny attackers, the maximum number of denied attackers, and how long you want blocks to last.

General Tab Field Definitions

The following fields are found the on the General tab:

- Use Summarizer—Enables the Summarizer component.

  By default, the Summarizer is enabled. If you disable it, all signatures are set to Fire All with no summarization. If you configure individual signatures to summarize, this configuration will be ignored if the Summarizer is not enabled.

- Use Meta Event Generator—Enables the Meta Event Generator.

  By default, the Meta Event Generator is enabled. If you disable the Meta Event Generator, all Meta engine signatures are disabled.

- Use Threat Rating Adjustment—Enables threat rating adjustment, which adjusts the risk rating. If disabled, then risk rating is equal to threat rating.
- Use Event Action Filters—Enables the event action filter component. You must check this check box to use any filter that is enabled.
- Enable One Way TCP Reset—(inline mode only) Enables a one-way TCP reset for deny packet inline actions for TCP-based alerts. It sends a TCP reset to the victim of the alert thus clearing the TCP resources of the victim.
- Deny Attacker Duration—Number of seconds to deny the attacker inline. The valid range is 0 to 518400. The default is 3600.
- Block Attack Duration—Number of minutes to block a host or connection. The valid range is 0 to 10000000. The default is 30.
- Maximum Denied Attackers—Limits the number of denied attackers possible in the system at any one time. The valid range is 0 to 100000000. The default is 10000.

Configuring the General Settings

Caution The general settings options operate at a global level, so enabling them affects all sensor processing of these features.

To configure the general settings for event action rules, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure general categories.

Step 4 In the Event Action Rules half of the pane, click the General tab.

Step 5 To enable the summarizer feature, check the **Use Summarizer** check box.

Caution Disable the Summarizer for troubleshooting purposes only. Otherwise, make sure the Summarizer is enabled so that all signatures you configure for summarization will actually summarize.

Step 6 To enable the meta event generator, check the **Use Meta Event Generator** check box.

Caution Disable the Meta Event Generator for troubleshooting purposes only. Otherwise, make sure the Meta Event Generator is enabled so that all Meta engine signatures are functional.

Step 7 To enable threat rating adjustment, check the **Use Threat Rating Adjustment** check box.

Step 8 To enable event action filters, check the **Use Event Action Filters** check box.

Note You must check the Use Event Action Filters check box on the General pane so that any event action filters you configured in the **Configuration > *sensor_name* > Policies > IPS Policies > Event Action Filters** pane are active.

Step 9 To enable one way TCP reset for deny packet inline actions, check the **Enable One Way TCP Reset** check box.

Step 10 In the Deny Attacker Duration field, enter the number of seconds you want to deny the attacker inline.

Step 11 In the Block Action Duration field, enter the number of minutes you want to block a host or connection.

Step 12 In the Maximum Denied Attackers field, enter the maximum number of denied attackers you want at any one time.

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

Step 13 Click **Apply** to apply your changes and save the revised configuration.