CHAPTER **10**

Using the Custom Signature Wizard

This chapter describes the Custom Signature Wizard and how to use it to create custom signatures. It contains the following sections:

Understanding the Custom Signature Wizard

> **Note** You must be administrator or operator to create custom signatures.

The Custom Signature Wizard guides you through a step-by-step process for creating custom signatures. There are two possible sequences—using a signature engine to create your custom signature or creating the custom signature without a signature engine.

For More Information

For more information on the individual signature engines, see Appendix B, "Signature Engines."

Using a Signature Engine

The following sequence applies if you use a signature engine to create your custom signature:

Step 1 Choose a signature engine:

- Atomic IP
- Atomic IP Advanced
- Service HTTP
- Service MSRPC

- Service RPC
- State (SMTP, ...)
- String ICMP
- String TCP
- String UDP
- Sweep

Step 2   Assign the signature identification parameters:

- Signature ID
- Subsignature ID
- Signature Name
- Alert Notes (optional)
- User Comments (optional)

Step 3   Assign the engine-specific parameters. The parameters differ for each signature engine, although there is a group of master parameters that applies to each engine.

Step 4   Assign the alert response:

- Signature Fidelity Rating
- Severity of the Alert

Step 5   Assign the alert behavior. You can accept the default alert behavior. To change it, click **Advanced**, which opens the Advanced Alert Behavior wizard. With this wizard you can configure how you want to handle alerts for this signature.

Step 6   Click **Finish**.

Signature Engines Not Supported for the Custom Signature Wizard

The Custom Signature Wizard in Cisco IPS does not support creating custom signatures based on the following signature engines:

- AIC FTP
- AIC HTTP
- Atomic ARP
- Atomic IP6
- Fixed ICMP
- Fixed TCP
- Fixed UDP
- Flood Host
- Flood Net
- Meta

- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H225
- Service IDENT
- Service MSSQL
- Service NTP
- Service P2P
- Service SMB Advanced
- Service SNMP
- Service SSH
- Service TNS
- String XL ICMP
- String XL TCP
- String XL UDP
- Traffic ICMP
- Traffic Anomaly
- Trojan Bo2k
- Trojan Tfn2k
- Trojan UDP

You can create custom signatures based on these existing signature engines by cloning an existing signature from the engine you want.

Note   The IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP support the String XL engines and the Regex accelerator card.

For More Information

- For more information on using the CLI to create custom signatures using these signature engines, refer to *Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.3*.

- For more information on cloning signatures, see .

Not Using a Signature Engine

The following sequence applies if you are not using a signature engine to create your custom signature:

Step 1   Specify the protocol you want to use:

- IP—Go to Step 3.
- ICMP—Go to Step 2.
- UDP—Go to Step 2.
- TCP—Go to Step 2.

Step 2   For ICMP and UDP protocols, select the traffic type and inspect data type. For TCP protocol, select the traffic type.

Step 3   Assign the signature identification parameters:

- Signature ID
- Subsignature ID
- Signature Name
- Alert Notes (optional)
- User Comments (optional)

Step 4   Assign the engine-specific parameters. The parameters differ for each signature engine, although there is a group of master parameters that applies to each engine.

Step 5   Assign the alert response:

- Signature Fidelity Rating
- Severity of the Alert

Step 6   Assign the alert behavior. You can accept the default alert behavior. To change it, click **Advanced**, which opens the Advanced Alert Behavior wizard. With this wizard you can configure how you want to handle alerts for this signature.

Step 7   Click **Finish**.

Creating Custom Signatures

> ⚠ **Caution**   Adding a custom signature can affect sensor performance. To monitor the effect the new signature has on the sensor, choose **Configuration >** *sensor_name* **> Interface Configuration > Traffic Flow Notifications** and configure the Missed Packet Threshold and Notification Interval options to judge how the sensor is handling the new signature.

The Custom Signature Wizard provides a step-by-step procedure for configuring custom signatures.

To create custom signatures using the Custom Signature Wizard, follow these steps:

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

Step 2   Choose **Configuration >** *sensor_name* **> Policies > Signature Definitions > sig0 > Signature Wizard**.

Step 3   If you know the specific signature engine you want to use to create the new signature, click the **Yes** radio button, choose the engine from the Select Engine drop-down list, and then click **Next.** Go to Step 12. If you do not know what engine you should use, click the **No** radio button, and then click **Next**.

Step 4   Click the radio button that best matches the type of traffic you want this signature to inspect, and then click **Next**:

- IP (for IP, go to Step 12.)
- ICMP (for ICMP, go to Step 5.)
- UDP (for UDP, go to Step 6.)
- TCP (for TCP, go to Step 8.)

Step 5   In the ICMP Traffic Type window, click one of the following radio buttons, and then click **Next**:

- Single Packet—You are creating a signature to inspect a single packet for an attack using either the Atomic IP engine (for Header Data) or the String ICMP engine. Go to Step 11.
- Sweeps—You are creating a signature to detect a sweep attack using the sweep engine for your new signature. Go to Step 12.

Step 6   In the UDP Traffic Type window, click one of the following radio buttons, and then click **Next**:

- Single Packet—You are creating a signature to inspect a single packet for an attack using either the Atomic IP engine (for Header Data) or the String UDP engine. Go to Step 11.
- Sweeps—You are creating a signature to detect a sweep attack using the sweep engine for the signature. Go to Step 7.

Step 7   In the UDP Sweep Type window, click one of the following radio buttons, and then click **Next**:

- Host Sweep—You are creating a signature that uses a sweep to search for open ports on a host. The sweep engine is used to create the new signature and the storage key is set to Axxx. Go to Step 12.
- Port Sweep—You are creating a signature that uses a sweep to search for hosts on a network. The sweep engine is used to create the new signature and the storage key is set to AxBx. Go to Step 12.

Step 8   In the TCP Traffic Type window, click one of the following radio buttons, and then click **Next**:

- Single Packet—You are creating a signature to inspect a single packet for an attack. The atomic IP engine is used to create the signature. Go to Step 12.
- Single TCP Connection—You are creating a signature to detect an attack in a single TCP connection. Go to Step 9.
- Multiple Connections—You are creating a signature to inspect multiple connections for an attack. Go to Step 10.

Step 9   In the Service Type window, click one of the following radio buttons, click **Next**, and then go to Step 12:

- HTTP—You are creating a signature to detect an attack that uses the HTTP service. The service HTTP engine is used to create the signature.
- SMTP—You are creating a signature to detect an attack that uses the SMTP service. The SMTP engine is used to create the signature.

- RPC—You are creating a signature to detect an attack that uses the RPC service. The service RPC engine is used to create the signature.

- MSRPC—You are creating a signature to detect an attack that uses the MSRPC service. The service MSRPC engine is used to create the signature.

- Other—You are creating a signature to detect an attack that uses a service other than HTTP, SMTP, or RPC. The string TCP engine is used to create the signature.

Step 10 On the TCP Sweep Type window, click one of the following radio buttons, click **Next**, and then go to Step 12:

- Host Sweep—You are creating a signature that uses a sweep to search for open ports on a host. The sweep engine is used to create the signature and the storage key is set to Axxx.

- Port Sweep—You are creating a signature that uses a sweep to search for hosts on a network. The Sweep engine is used to create the new signature and the storage key is set to AxBx.

Step 11 In the Inspect Data window, for a single packet, click one of the following radio buttons, click **Next**, and then go to Step 12:

- Header Data Only—Specifies the header as the portion of the packet you want the sensor to inspect.

- Payload Data Only—Specifies the payload as the portion of the packet you want the sensor to inspect.

Step 12 In the Signature Identification window, specify the attributes that uniquely identify this signature, and then click **Next**:

   a. In the Signature ID field, enter a number for this signature. Custom signatures range from 60000 to 65000.

   b. In the Subsignature ID field, enter a number for this signature. The default is 0.

      You can assign a subsignature ID if you are grouping signatures together that are similar.

   c. In the Signature Name field, enter a name for this signature. A default name appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

     ✎

     Note The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

   d. (Optional) In the Alert Notes field, enter text to be added to the alert. You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated.

   e. (Optional) In the User Comments field, enter text that describes this signature. You can add any text that you find useful here. This field does not affect the signature or alert in any way.

Step 13 Assign values to the engine-specific parameters, and then click **Next**.

Step 14 In the Alert Response window, specify the following alert response options:

   a. In the Signature Fidelity Rating field, enter a value. The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident.

   b. From the Severity of the Alert drop-down list, choose the severity to be reported by Event Viewer when the sensor sends an alert:

- High

- Informational

- Low

- Medium

Step 15   To accept the default alert behavior, click **Finish** and go to Step 22. To change the default alert behavior, click **Advanced** and continue with Step 16.

> **Note**   You can control how often this signature fires. For example, you may want to decrease the volume of alerts sent out from the sensor. Or you may want the sensor to provide basic aggregation of signature firings into a single alert. Or you may want to counter anti-IPS tools such as "stick," which are designed to send bogus traffic so that the IPS produces thousands of alerts during a very short time.

Step 16   Configure the event count, key, and interval:

a.   In the Event Count field, enter a value for the event count. This is the minimum number of hits the sensor must receive before sending one alert for this signature.

b.   From the Event Count Key drop-down list, choose an attribute to use as the event count key. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the event count key.

c.   If you want to count events based on a rate, check the **Use Event Interval** check box, and then in the Event Interval (seconds) field, enter the number of seconds that you want to use for your interval.

d.   Click **Next** to continue. The Alert Summarization window appears.

Step 17   To control the volume of alerts and configure how the sensor summarizes alerts, click one of the following radio buttons:

- Alert Every Time the Signature Fires—Specifies that you want the sensor to send an alert every time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 18.

- Alert the First Time the Signature Fires—Specifies that you want the sensor to send an alert the first time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 19.

- Send Summary Alerts—Specifies that you want the sensor to only send summary alerts for this signature instead of sending alerts every time the signature fires. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 20.

- Send Global Summary Alerts—Specifies that you want the sensor to send an alert the first time a signature fires on an address set, and then only send a global summary alert that includes a summary of all alerts for all address sets over a given time interval. Go to Step 21.

> **Note**   When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

Step 18   Configure the Alert Every Time the Signature Fires option:

a.   From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

    b. To use dynamic summarization, check the **Use Dynamic Summarization** check box. Dynamic summarization lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.

    c. In the Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a summary alert for this signature.

    d. In the Summary Interval (seconds) field, enter the number of seconds that you want to use for the time interval.

    e. To have the sensor enter global summarization mode, check the **Specify Global Summary Threshold** check box.

    f. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

Step 19   Configure the Alert the First Time the Signature Fires option:

    a. From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

    b. To have the sensor use dynamic global summarization, check the **Use Dynamic Global Summarization** check box.

    c. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

> **Note**   When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

    d. In the Global Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

Step 20   Configure the Send Summary Alerts option:

    a. In the Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

    b. From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

    c. To have the sensor use dynamic global summarization, check the **Use Dynamic Global Summarization** check box.

    d. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

> **Note**   When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

Step 21   In the Global Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

Step 22   Click **Finish** to save your alert behavior changes.

Step 23   Click **Finish** to save your custom signature.

Step 24   Click **Yes** to create the custom signature. The signature you created is enabled and added to the list of signatures.

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

Custom Signature Wizard Field Definitions

This section describes the Custom Signature Wizard windows and lists the field definitions for the Custom Signature Wizard. It also contains procedure for creating three example custom signatures. It contains the following topics:

Welcome Window

The following fields are found in the Welcome window of the Custom Signature Wizard:

- Yes—Activates the Select Engine field and lets you choose from a list of signature engines.
- Select Engine—Displays the list of available signature engines. If you know which signature engine you want to use to create a signature, click **Yes**, and choose one of the following engine types from the drop-down list:
  - Atomic IP—Lets you create an Atomic IP signature.
  - Service HTTP—Lets you create a signature for HTTP traffic.
  - Service MSRPC—Lets you create a signature for MSRPC traffic.
  - Service RPC—Lets you create a signature for RPC traffic.
  - State SMTP—Lets you create a signature for SMTP traffic.
  - String ICMP—Lets you create a signature for an ICMP string.
  - String TCP—Lets you create a signature for a TCP string.
  - String UDP—Lets you create a signature for a UDP string.
  - Sweep—Lets you create a signature for a sweep.
- No—Lets you continue with the advanced engine selection screens of the Custom Signature Wizard.

Protocol Type Window

You can define a signature that looks for malicious behavior in a certain protocol. You can have the following protocols decoded and inspected by your signature:

- IP
- ICMP
- UDP
- TCP

Field Definitions

The following fields are found in the Protocol Type window of the Custom Signature Wizard:

- IP—Creates a signature to decode and inspect IP traffic.
- ICMP—Creates a signature to decode and inspect ICMP traffic.
- UDP—Creates a signature to decode and inspect UDP traffic.
- TCP—Creates a signature to decode and inspect TCP traffic.

Signature Identification Window

The signature identification parameters describe the signature but do not affect the behavior of the signature. You must have a signature ID, subsignature ID, and a signature name. The other fields are optional.

Field Definitions

The following fields are found in the Signature Identification window of the Custom Signature Wizard:

- Signature ID—Identifies the unique numerical value assigned to this signature. The signature ID lets the sensor identify a particular signature. The signature ID is reported to the Event Viewer when an alert is generated. The valid range is between 60000 and 65000.

- SubSignature ID—Identifies the unique numerical value assigned to this subsignature. The subsignature ID identifies a more granular version of a broad signature. The valid value is between 0 and 255. The subsignature is reported to the Event Viewer when an alert is generated.

- Signature Name—Identifies the name assigned to this signature. Reported to the Event Viewer when an alert is generated.

- Alert Notes—(Optional) Specifies the text that is associated with the alert if this signature fires. Reported to the Event Viewer when an alert is generated.

- User Comments—(Optional) Specifies notes or other comments about this signature that you want stored with the signature parameters.

Service MSRPC Engine Parameters Window

The Service MSRPC engine processes MSRPC packets. MSRPC allows for cooperative processing between multiple computers and their application software in a networked environment. It is a transaction-based protocol, implying that there is a sequence of communications that establishes the channel and passes processing requests and replies.

MSRPC is an ISO Layer 5-6 protocol and is layered on top of other transport protocols such as UDP, TCP, and SMB. The MSRPC engine contains facilities to allow for fragmentation and reassembly of the MSRPC PDUs.

This communication channel is the source of recent Windows NT, Windows 2000, and Window XP security vulnerabilities. The Service MSRPC engine only decodes the DCE and RPC protocol for the most common transaction types.

Field Definitions

The following fields are found in the MSRPC Engine Parameters window of the Custom Signature Wizard. These options enable you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

> **Tip** To select more than one action, hold down the **Ctrl** key.

- Specify Regex String—(Optional) Lets you specify an exact match offset, including the minimum and maximum match offset, Regex string, and minimum match length.

- Protocol—Lets you specify TCP or UDP as the protocol.

- Specify Operation—(Optional) Lets you specify an operation.
- Specify UUID—(Optional) Lets you specify a UUID.

ICMP Traffic Type Window

The following fields are found in the ICMP Traffic Type window of the Custom Signature Wizard:

- Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Sweeps—Specifies that you are creating a signature to detect a sweep attack.

Inspect Data Window

The following fields are found in the Inspect Data window of the Custom Signature Wizard:

- Header Data Only—Specifies the header as the portion of the packet you want the sensor to inspect.
- Payload Data Only—Specifies the payload as the portion of the packet you want the sensor to inspect.

UDP Traffic Type Window

The following fields are found in the UDP Traffic Type window of the Custom Signature Wizard:

- Single Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Sweeps—Specifies that you are creating a signature to detect a sweep attack.

UDP Sweep Type Window

The following fields are found in the UDP Sweep Type window of the Custom Signature Wizard:

- Host Sweep—Identifies a sweep that searches for hosts on a network.
- Port Sweep—Identifies a sweep that searches for open ports on a host.

TCP Traffic Type Window

The following fields are found in the TCP Traffic Type window of the Custom Signature Wizard:

- Single Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Single TCP Connection—Specifies that you are creating a signature to inspect a single TCP connection for an attack.
- Multiple Connections—Specifies that you are creating a signature to inspect multiple connections for an attack.

Service Type Window

The following fields are found in the Service Type window of the Custom Signature Wizard:

- HTTP—Specifies you are creating a signature to describe an attack that uses the HTTP service.
- SMTP—Specifies you are creating a signature to describe an attack that uses the SMTP service.
- RPC—Specifies you are creating a signature to describe an attack that uses the RPC service.
- MSRPC—Specifies you are creating a signature to describe an attack that uses the MSRPC service.
- Other—Specifies you are creating a signature to describe an attack that uses a service other than HTTP, SMTP, RPC, or MSRPC.

TCP Sweep Type Window

The following fields are found in the TCP Sweep Type window of the Custom Signature Wizard:

- Host Sweep—Identifies a sweep that searches for hosts on a network.
- Port Sweep—Identifies a sweep that searches for open ports on a host.

Atomic IP Engine Parameters Window

The Atomic IP engine defines signatures that inspect IP protocol headers and associated Layer 4 transport protocols (TCP, UDP, and ICMP) and payloads. The Atomic engines do not store persistent data across packets. Instead they can fire an alert from the analysis of a single packet.

Field Definitions

The following fields are found in the Atomic IP Engine Parameters window of the Custom Signature Wizard. These options let you create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Q

Tip   To select more than one action, hold down the **Ctrl** key.

- Fragment Status—Indicates if you want to inspect fragmented or unfragmented traffic.
- Specify Layer 4 Protocol—(Optional) Lets you choose whether or not a specific protocol applies to this signature. If you choose Yes, you can choose from the following protocols:
  - ICMP Protocol—Lets you specify an ICMP sequence, type, code, identifier, and total length.
  - Other IP Protocols—Lets you specify an identifier.
  - TCP Protocol—Lets you set the TCP flags, window size, mask, payload length, urgent pointer, header length, reserved attribute, and port range for the source and destination.
  - UDP Protocol—Lets you specify a valid UDP length, length mismatch, and port range for the source and destination.
- Specify Payload Inspection—(Optional) Lets you specify the following payload inspection options.
- Specify IP Payload Length—(Optional) Lets you specify the payload length.
- Specify IP Header Length—(Optional) Lets you specify the header length.

- Specify IP Type of Service—(Optional) Lets you specify the type of service.

- Specify IP Time-to-Live—(Optional) Lets you specify the time-to-live for the packet.

- Specify IP Version—(Optional) Lets you specify the IP version.

- Specify IP Identifier—(Optional) Lets you specify an IP identifier.

- Specify IP Total Length—(Optional) Lets you specify the total IP length.

- Specify IP Option Inspection—(Optional) Lets you specify the following IP inspection options:

  - IP Option—Specifies the IP option code to match.

  - IP Option Abnormal Options—Specifies the malformed list of options.

- Specify IP Addr Options—(Optional) Lets you specify the following IP Address options:

  - Address with Localhost—Identifies traffic where the local host address is used as either the source or destination.

  - IP Address—Lets you specify the source or destination address. Use the following syntax: x.x.x.x-z.z.z.z, i.e. 10.10.10.1-10.10.10.254.

  - RFC 1918 Address—Identifies the type of address as RFC 1918.

  - Src IP Equal Dst IP—Identifies traffic where the source and destination addresses are the same.

Example Atomic IP Advanced Engine Signature

Tip   An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution   A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

The following example demonstrates how to create a signature based on the Atomic IP Advanced engine. For example, the following custom signature matches any packets that are IPv6 with a HOP Option Header where the header is type 1 and the length is 8.

To create a signature based on the Atomic IP Advanced engine, follow these steps:

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

Step 2   Choose **Configuration >** *sensor_name* **> Policies > Signature Definitions > sig0 > Active Signatures**, and then click **Add**.

Step 3   In the Signature ID field, enter a unique signature ID for the new signature. Custom signature IDs start at 60000.

Step 4   In the Subsignature field, enter a unique subsignature ID for the new signature.

Step 5   From the Alert Severity drop-down list, choose the severity you want to associate with this signature.

Step 6   In the Signature Fidelity Rating field, enter a value between 1and 100 to represent the signature fidelity rating for this signature.

Step 7   Leave the default value for the Promiscuous Delta field.

Step 8   Complete the signature description fields and add any comments about this signature.

Step 9   From the Engine drop-down list, choose **Atomic IP Advanced**.

Step 10   Configure the Atomic IP Advanced engine-specific parameters:

a.   From the Event Action drop-down list, choose the actions you want the sensor to take when it responds to an event.

> **Note**   IPv6 does not support the following event actions: Request Block Host, Request Block Connection, or Request Rate Limit.

> **Tip**   To choose more than one action, hold down the **Ctrl** key.

b.   From the IP Version drop-down list, choose **Yes** to enable the IP version, and then from the IP Version drop-down list, choose **IPv6** to enable IPv6.

c.   From the HOP Options Header drop-down list, choose **Yes** to enable hop-by-hop options, and then from the HOH Present drop-down list, choose **Have HOH**.

d.   From the HOH Options field, choose **Yes**, and then in the HOH Option Type field, enter **1**.

e.   In the HOH Option Length drop-down list, choose **Yes** to enable hop-by-hop length, and then in the HOH Option Length field, enter **8**.

Step 11   Configure Event Counter:

a.   In the Event Count field, enter the number of events you want counted (1 to 65535).

b.   From the Event Count Key drop-down list, choose the key you want to use.

c.   From the Specify Alert Interface drop-down list, choose whether you want to specify the alert interval (Yes or No).

d.   If you chose Yes, enter the alert interval (2 to 1000) in the Alert Interval field.

Step 12   Configure the alert frequency.

Step 13   Leave the default (**Yes**) for the Enabled field.

> **Note**   A signature must be enabled for the sensor to actively detect the attack specified by the signature.

Step 14   Leave the default (**Yes**) for the Retired field. This places the signature in the engine.

> **Note**   A signature must not be retired for the sensor to actively detect the attack specified by the signature.

Step 15   From the Vulnerable OS List drop-down list, choose the operating systems that are vulnerable to this signature.

> **Tip**   To choose more than one action, hold down the **Ctrl** key.

Step 16   From the Mars Category drop-down list, choose the MARS categories you want this signature to identify.

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

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

Step 17　Click **OK**. The new signature appears in the list with the Type set to Custom.

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

Step 18　Click **Apply** to apply your changes and save the revised configuration.

For More Information

For more information on the Atomic IP engines, see Atomic Engine, page B-13.

Service HTTP Engine Parameters Window

The Service HTTP engine is a service-specific string-based pattern-matching inspection engine. The HTTP protocol is one of the most commonly used in networks of today. In addition, it requires the most amount of preprocessing time and has the most number of signatures requiring inspection making it critical to the overall performance of the system.

The Service HTTP engine uses a Regex library that can combine multiple patterns into a single pattern-matching table allowing a single search through the data. This engine searches traffic directed only to web services, or HTTP requests. You cannot inspect return traffic with this engine. You can specify separate web ports of interest in each signature in this engine.

HTTP deobfuscation is the process of decoding an HTTP message by normalizing encoded characters to ASCII equivalent characters. It is also known as ASCII normalization.

Before an HTTP packet can be inspected, the data must be deobfuscated or normalized to the same representation that the target system sees when it processes the data. It is ideal to have a customized decoding technique for each host target type, which involves knowing what operating system and web server version is running on the target. The Service HTTP engine has default deobfuscation behavior for the Microsoft IIS web server.

Field Definitions

The following fields are found in the Service HTTP Engine Parameters window of the Custom Signature Wizard. These options let you create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

**Tip**　To select more than one action, hold down the **Ctrl** key.

- De Obfuscate—Specifies whether or not to apply anti-evasive HTTP deobfuscation before searching. The default is Yes.

- Max Field Sizes—(Optional) Lets you specify maximum URI, Arg, Header, and Request field lengths. The following figure demonstrates the maximum field sizes:

User Input: http://10.20.35.6/cgi-bin/userlist.cgi/user.id=100&user.name=admin

Browser output:
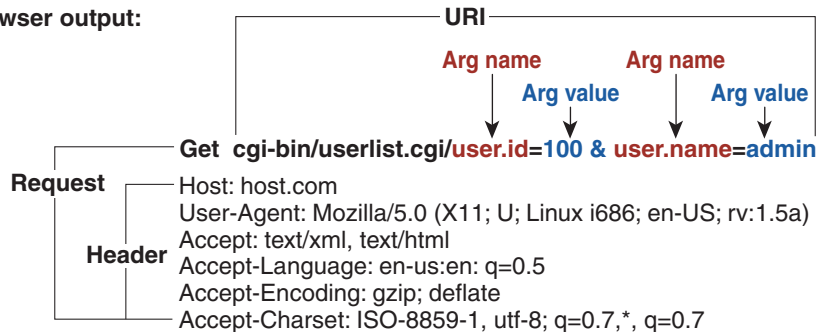
Note*: Individual arguments are separated by '&' Argument name and value are separated by "="

- Regex—Lets you specify a regular expression for the URI, Arg, Header, and Request Regex.
- Service Ports—Identifies the specific service ports used by the traffic. The value is a comma-separated list of ports.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.

Example Service HTTP Engine Signature

Tip   An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution   A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

Use the Custom Signature Wizard to create a custom Service HTTP engine signature.

To create a custom Service HTTP signature, follow these steps:

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

Step 2   Choose **Configuration >** *sensor_name* **> Policies > Signature Definitions > sig0 > Signature Wizard**.

Step 3   Click the **Yes** radio button, choose **Service HTTP** from the Select Engine drop-down list, and then click **Next.**

Step 4   To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:

  a. In the Signature ID field, enter a number for the signature. Custom signatures range from 60000 to 65000.

    b. In the Subsignature ID field, enter a number for the signature. The default is 0. You can assign a subsignature ID if you are grouping signatures together that are similar.

    c. In the Signature Name field, enter a name for the signature. A default name, My Sig, appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

       ✎

      Note   The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

    d. (Optional) In the Alert Notes field, enter text to be added to the alert. You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated. The default is My Sig Info.

    e. (Optional) In the User Comments field, enter text that describes this signature, and then click **Next**. You can add any text that you find useful here. This field does not affect the signature or alert in any way. The default is Sig Comment.

Step 5   Assign the event actions. The default is Produce Alert. You can assign more actions, such as deny or block, based on your security policy.

       🔍

      Tip   To select more than one action, hold down the **Ctrl** key.

Step 6   In the De Obfuscate field, choose **Yes** from the drop-down list to configure the signature to apply anti-evasive deobfuscation before searching.

Step 7   (Optional) Under Max Field Sizes you can configure the following optional parameters for maximum field sizes:

- Specify Max URI Field Length—Enables the maximum URI field length.
- Specify Max Arg Field Length—Enables maximum argument field length.
- Specify Max Header Field Length—Enables maximum header field length.
- Specify Max Request Field Length—Enables maximum request field length.

Step 8   Under Regex, configure the Regex parameters:

    a. In the Specify URI Regex field, choose **Yes** from the drop-down list.

    b. In the URI Regex field, enter the URI Regex, for example, [Mm][Yy][Ff][Oo][Oo].

    c. You can specify values for the following optional parameters:

- Specify Arg Name Regex—Enables searching the Arguments field for a specific regular expression.
- Specify Header Regex—Enables searching the Header field for a specific regular expression.
- Specify Request Regex—Enables searching the Request field for a specific regular expression.

Step 9   In the Service Ports field, enter the port number. For example, you can use the web ports variable, $WEBPORTS. The value is a comma-separated list of ports or port ranges where the target service resides.

Step 10   (Optional) In the Swap Attacker Victim field, choose **Yes** from the drop-down list to have the address (and ports) source and destination in the alert message swapped.

Step 11   Click **Next**.

Step 12 (Optional) You can change the following default alert response options:

   a. In the Signature Fidelity Rating field, enter a value. The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident. The default is 75.

   b. In the Severity of the Alert field, choose the severity to be reported by Event Viewer when the sensor sends an alert. The default is Medium.

Step 13 Click **Next**.

Step 14 To change the default alert behavior, click **Advanced**. Otherwise click **Finish** and your custom signature is created. The Create Custom Signature dialog box appears and asks if you want to create and apply this custom signature to the sensor.

> **Tip** To discard your changes, click **Cancel**.

Step 15 Click **Yes** to create the custom signature. The signature you created is enabled and added to the list of signatures.

Service RPC Engine Parameters Window

The Service RPC engine specializes in RPC protocol and has full decode as an anti-evasive strategy. It can handle fragmented messages (one message in several packets) and batch messages (several messages in a single packet).

The RPC portmapper operates on port 111. Regular RPC messages can be on any port greater than 550. RPC sweeps are like TCP port sweeps, except that they only count unique ports when a valid RPC message is sent. RPC also runs on UDP.

Field Definitions

The following fields are found in the Service RPC Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

> **Tip** To select more than one action, hold down the **Ctrl** key.

- Direction—Indicates whether the sensor is watching traffic destined to or coming from the service port. The default is To Service.

- Protocol—Lets you specify TCP or UDP as the protocol.

- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.

- Specify Regex String—Lets you specify a Regex string to search for.

- Specify Port Map Program—Identifies the program number sent to the port mapper of interest for this signature. The valid range is 0 to 999999999.

- Specify RPC Program—Identifies the RPC program number of interest for this signature. The valid range is 0 to 1000000.

- Specify Spoof Src—Fires the alarm when the source address is set to 127.0.0.1.

- Specify RPC Max Length—Identifies the maximum allowed length of the whole RPC message. Lengths longer than this cause an alert. The valid range is 0 to 65535.

- Specify RPC Procedure—Identifies the RPC procedure number of interest for this signature. The valid range is 0 to 1000000.

State Engine Parameters Window

The State engine provides state-based regular expression-based pattern inspection of TCP streams. A state engine is a device that stores the state of an event and at a given time can operate on input to transition from one state to another and/or cause an action or output to take place. State machines are used to describe a specific event that causes an output or alarm. There are three state machines in the State engine: SMTP, Cisco Login, and LPR Format String.

Field Definitions

The following fields are found in the State Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- State Machine—Identifies the name of the state to restrict the match of the regular expression string. The options are: Cisco Login, LPR Format String, and SMTP.

- State Name—Identifies the name of the state. The options are: Abort, Mail Body, Mail Header, SMTP Commands, and Start.

- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match. The valid range is 0 to 65535.

- Regex String—Identifies the regular expression string that triggers a state transition.

- Direction—Identifies the direction of the data stream to inspect for the transition. The default is To Service.

- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.

- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.

- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offset.

String ICMP Engine Parameters Window

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data. There are three String engines: String ICMP, String TCP, and String UDP.

Field Definitions

The following fields are found in the String ICMP Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

$\bigcirc$

Tip   To select more than one action, hold down the **Ctrl** key.

- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to the end of the match. The valid range is 0 to 65535.
- Regex String—Identifies the regular expression string to search for in a single packet.
- Direction—Identifies the direction of the data stream to inspect for the transition. The default is To Service.
- ICMP Type—The ICMP header TYPE value. The valid range is 0 to 18. The default is 0-18.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.
- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offsets.

String TCP Engine Parameters Window

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data. There are three String engines: String ICMP, String TCP, and String UDP.

Field Definitions

The following fields are found in the String TCP Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

$\bigcirc$

Tip   To select more than one action, hold down the **Ctrl** key.

- Strip Telnet Options—Strips the Telnet option control characters from the data stream before the pattern is searched. This is primarily used as an anti-evasion tool. The default is No.

- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match. The valid range is 0 to 65535.

- Regex String—Identifies the regular expression string to search for in a single packet.

- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.

- Direction—Identifies the direction of the data stream to inspect for the transition. The default is To Service.

- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offsets.

- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.

Example String TCP Engine Signature

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

Use the Custom Signature Wizard to create a custom String TCP engine signature. The following procedure also applies to creating custom String ICMP and UDP signatures.

To create a custom String TCP signature, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Signature Wizard**.

Step 3 Click the **Yes** radio button, choose **String TCP** from the Select Engine drop-down list, and then click **Next.** The Signature Identification window appears.

Step 4 To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:

a. In the Signature ID field, enter a number for the signature. Custom signatures range from 60000 to 65000.

b. In the Subsignature ID field, enter a number for the signature. The default is 0. You can assign a subsignature ID if you are grouping signatures together that are similar.

c. In the Signature Name field, enter a name for the signature. A default name, My Sig, appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

Note   The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

---

d. (Optional) In the Alert Notes field, enter text to be added to the alert. You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated. The default is My Sig Info.

e. (Optional) In the User Comments field, enter text that describes this signature. You can add any text that you find useful here. This field does not affect the signature or alert in any way. The default is Sig Comment.

f. Click **Next**. The Engine Specific Parameters window appears.

Step 5   Assign the event actions. The default is Produce Alert. You can assign more actions, such as deny or block, based on your security policy.

Tip   To select more than one action, hold down the **Ctrl** key.

Step 6   (Optional) In the Strip Telnet Options field, choose **Yes** from the drop-down list to strip the Telnet option characters from the data before the pattern is searched.

Step 7   (Optional) In the Specify Min Match Length field, choose **Yes** from the drop-down list to enable minimum match length, and then in the Min Match Length field, enter the minimum number of bytes the regular expression string must match (0 to 65535).

Step 8   In the Regex String field, enter the string this signature will be looking for in the TCP packet.

Step 9   In the Service Ports field, enter the port number, for example, 23. The value is a comma-separated list of ports or port ranges where the target service resides.

Step 10   From the Direction drop-down list, choose the direction of the traffic:

- From Service—Traffic from service port destined to client port.
- To Service—Traffic from client port destined to service port.

Step 11   (Optional) In the Specify Exact Match Offset field, choose **Yes** from the drop-down list to enable exact match offset. The exact match offset is the exact stream offset the regular expression string must report for a match to be valid (0 to 65535).

a. In the Specify Max Match Offset field, enter the maximum value.

b. In the Specify Min Match Offset field, enter the minimum value.

Step 12   In the Swap Attacker Victim field, choose **Yes** from the drop-down list to swap the address (and ports) source and destination in the alert message, and then click **Next**.

Step 13   (Optional) You can change the following default alert response options:

a. In the Signature Fidelity Rating field, enter a value. The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident. The default is 75.

b. In the Severity of the Alert field, choose the severity to be reported by Event Viewer when the sensor sends an alert. The default is Medium.

Step 14   Click **Next**.

Step 15   To change the default alert behavior, click **Advanced**. Otherwise click **Finish** and your custom signature is created. The Create Custom Signature dialog box appears and asks if you want to create and apply this custom signature to the sensor.

$\mathcal{Q}$
Tip   To discard your changes, click **Cancel**.

Step 16   Click **Yes** to create the custom signature. The signature you created is enabled and added to the list of signatures.

For More Information

For more information about regular expression syntax, see Regular Expression Syntax, page B-9.

String UDP Engine Parameters Window

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data. There are three String engines: String ICMP, String TCP, and String UDP.

Field Definitions

The following fields are found in the String UDP Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

$\mathcal{Q}$
Tip   To select more than one action, hold down the **Ctrl** key.

- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match. The valid range is 0 to 65535.
- Regex String—Identifies the regular expression string to search for in a single packet.
- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.
- Direction—Identifies the direction of the data stream to inspect for the transition.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.
- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offset.

Sweep Engine Parameters Window

The Sweep engine analyzes traffic between two hosts or from one host to many hosts. You can tune the existing signatures or create custom signatures. The Sweep engine has protocol-specific parameters for ICMP, UDP, and TCP.

The alert conditions of the Sweep engine ultimately depend on the count of the unique parameter. The unique parameter is the threshold number of distinct hosts or ports depending on the type of sweep. The unique parameter triggers the alert when more than the unique number of ports or hosts is seen on the address set within the time period. The processing of unique port and host tracking is called counting.

⚠

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.

A unique parameter must be specified for all signatures in the Sweep engine. A limit of 2 through 40 (inclusive) is enforced on the sweeps. 2 is the absolute minimum for a sweep, otherwise, it is not a sweep (of one host or port). 40 is a practical maximum that must be enforced so that the sweep does not consume excess memory. More realistic values for unique range between 5 and 15.

TCP sweeps must have a TCP flag and mask specified to determine which sweep inspector slot in which to count the distinct connections. ICMP sweeps must have an ICMP type specified to discriminate among the various types of ICMP packets.

Data Node

When an activity related to Sweep engine signatures is seen, the IPS uses a data node to determine when it should stop monitoring for a particular host. The data node contains various persistent counters and variables needed for cross-packet reassembly of streams and for tracking the inspection state on a per-stream/per-source/per-destination basis The data node containing the sweep determines when the sweep should expire. The data node stops a sweep when the data node has not seen any traffic for x number of seconds (depending on the protocol).

There are several adaptive timeouts for the data nodes. The data node expires after 30 seconds of idle time on the address set after all of the contained objects have been removed. Each contained object has various timeouts, for example, TCP Stream has a one-hour timeout for established connections. Most other objects have a much shorter expiration time, such as 5 or 60 seconds.

Field Definitions

The following fields are found in the Sweep Engine Parameters window in the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

🔍

Tip   To select more than one action, hold down the **Ctrl** key.

- Unique—Identifies the threshold number of unique host connections. The alarm fires when the unique number of host connections is exceeded during the interval.
- Protocol—Identifies the protocol:
  - ICMP—Lets you specify the ICMP storage type and choose one of these storage keys: attacker address, attacker address and victim port, or attacker and victim addresses.
  - TCP—Lets you choose suppress reverse, inverted sweep, mask, TCP flags, fragment status, storage key, or specify a port range.
  - UDP—Lets you choose a storage key, or specify a port range.
- Src Addr Filter—Processes packets that do not have a source IP address (or addresses) defined in the filter values.

- Dst Addr Filter—Processes packets that do not have a destination IP address (or addresses) defined in the filter values.

- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.

Alert Response Window

The following fields are found in the Alert Response window of the Custom Signature Wizard:

- Signature Fidelity Rating—A weight associated with how well this signature might perform in the absence of specific knowledge of the target.

> **Note** Signature fidelity rating is calculated by the signature author on a per-signature basis. A signature that is written with very specific rules (specific Regex) will have a higher signature fidelity rating than a signature that is written with generic rules.

- Severity of the Alert—The severity at which the alert is reported:

  - High—The most serious security alert.

  - Medium—A moderate security alert.

  - Low—The least security alert.

  - Information—Denotes network activity, not a security alert.

Alert Behavior Window

Normal alert behavior for the sensor is to send the first alert for each address set, and then to send a summary of all the alerts for this address set over the next 15 seconds. Click **Advanced** to change this alert behavior.

This section describes the Advanced Alert Behavior Wizard, and contains the following topics:

Event Count and Interval Window

The following fields are found in the Event Count and Interval window of the Advanced Alert Behavior wizard:

- Event Count—Identifies the minimum number of hits the sensor must receive before sending one alert for this signature.

- Event Count Key—Identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Event Count Key.

- Use Event Interval—Specifies that you want the sensor to count events based on a rate. For example, if set your Event Count to 500 events and your Event Interval to 30 seconds, the sensor sends you one alert if 500 events are received within 30 seconds of one another.

- Event Interval (seconds)—Identifies the time interval during which the sensor counts events for rate-based counting.

Alert Summarization Window

The following fields are found in the Alert Summarization window of the Advanced Alert Behavior wizard:

- Alert Every Time the Signature Fires—Specifies that you want the sensor to send an alert every time the signature detects malicious traffic. You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.

- Alert the First Time the Signature Fires—Specifies that you want the sensor to send an alert the first time the signature detects malicious traffic. You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.

- Send Summary Alerts—Specifies that you want the sensor to only send summary alerts for this signature, instead of sending alerts every time the signature fires. You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.

- Send Global Summary Alerts—Specifies that you want the sensor to send an alert the first time a signature fires on an address set, and then only send a global summary alert that includes a summary of all alerts for all address sets over a given time interval.

Alert Dynamic Response Fire All Window

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Alert Every Time the Signature Fires:

- Summary Key—Identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.

- Use Dynamic Summarization—Lets the sensor dynamically enter summarization mode:

  - Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a summary.

  - Summary Interval (seconds)—Specifies that you want to count events based on a rate and identifies the number of seconds that you want to use for the time interval.

    Note   When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert for each signature to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior. A global summary counts signature firings on all attacker IP addresses and ports and all victim IP addresses and ports.

- Specify Summary Threshold—Lets you choose a summary threshold:

  - Global Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

Alert Dynamic Response Fire Once Window

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Alert the First Time the Signature Fires:

- Summary Key—Identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.

- Use Dynamic Global Summarization—Lets the sensor dynamically enter global summarization mode:

    - Global Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

    Note   When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

    - Global Summary Interval (seconds)—Identifies the time interval during which the sensor counts events for summarization.

Alert Dynamic Response Summary Window

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Summary:

Note   When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

- Summary Interval (seconds)—Identifies the time interval during which the sensor counts events for summarization.

- Summary Key—Identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.

- Use Dynamic Global Summarization—Allows the sensor to dynamically enter global summarization mode:

    - Global Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

    Note   When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single summary alert to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

Global Summarization Window

The following field is found in the Global Summarization window of the Advanced Alert Behavior wizard:

- Global Summary Interval (seconds)—Identifies the time interval during which the sensor counts events for summarization.