CHAPTER 11

Configuring Global Correlation

This chapter provides information for configuring global correlation. It contains the following sections:

- Understanding Global Correlation, page 11-1
- Participating in the SensorBase Network, page 11-2
- Understanding Reputation, page 11-2
- Understanding Network Participation, page 11-3
- Understanding Efficacy, page 11-4
- Reputation and Risk Rating, page 11-4
- Global Correlation and the Produce Alert Event Action, page 11-5
- Global Correlation Features and Goals, page 11-5
- Global Correlation Requirements, page 11-6
- Understanding Global Correlation Sensor Health Metrics, page 11-7
- Configuring Global Correlation Inspection and Reputation Filtering, page 11-8
- Configuring Network Participation, page 11-10
- Disabling Global Correlation, page 11-12
- Troubleshooting Global Correlation, page 11-12

Understanding Global Correlation

You can configure global correlation so that your sensors are aware of network devices with a reputation for malicious activity, and can take action against them. Participating IPS devices in a centralized Cisco threat database, the SensorBase, receive and absorb global correlation updates. The reputation data contained in the global correlation updates is factored in to the analysis of network traffic, which increases IPS efficacy, because traffic is denied or allowed based on the reputation of the source IP address. The participating IPS devices send data back to the Cisco SensorBase Network, which results in a feedback loop that keeps the updates current and global.

You can configure the sensor to participate in the global correlation updates and/or in sending telemetry data or you can turn both services off. You can view reputation scores in events and see the reputation score of the attacker.

Participating in the SensorBase Network

Cisco IPS contains a new security capability, Cisco Global Correlation, which uses the immense security intelligence that we have amassed over the years. At regular intervals, Cisco IPS receives threat updates from the Cisco SensorBase Network, which contain detailed information about known threats on the Internet, including serial attackers, Botnet harvesters, Malware outbreaks, and dark nets. The IPS uses this information to filter out the worst attackers before they have a chance to attack critical assets. It then incorporates the global threat data in to its system to detect and prevent malicious activity even earlier.

If you agree to participate in the SensorBase Network, Cisco will collect aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other confidential business or personal information. All data is aggregated and sent by secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco will be anonymous and treated as strictly confidential.

Table 11-1 shows how we use the data.

Table 11-1 Cisco Network Participation Data Use

Participation Level	Type of Data	Purpose
Partial	Protocol attributes (TCP maximum segment size and options string, for example)	Tracks potential threats and helps us to understand threat exposure
	Attack type (signature fired and risk rating, for example)	Used to understand current attacks and attack severity
	Connecting IP address and port	Identifies attack source
	Summary IPS performance (CPU utilization, memory usage, inline vs promiscuous, for example)	Tracks product efficacy
Full	Victim IP address and port	Detects threat behavioral patterns

When you enable Partial or Full Network Participation, the Network Participation Disclaimer appears. You must click **Agree** to participate. If you do not have a license installed, you receive a warning telling you that global correlation inspection and reputation filtering are disabled until the sensor is licensed. You can obtain a license at http://www.cisco.com/go/license.

For More Information

For information on how to obtain and install a sensor license, see Configuring Licensing, page 16-12.

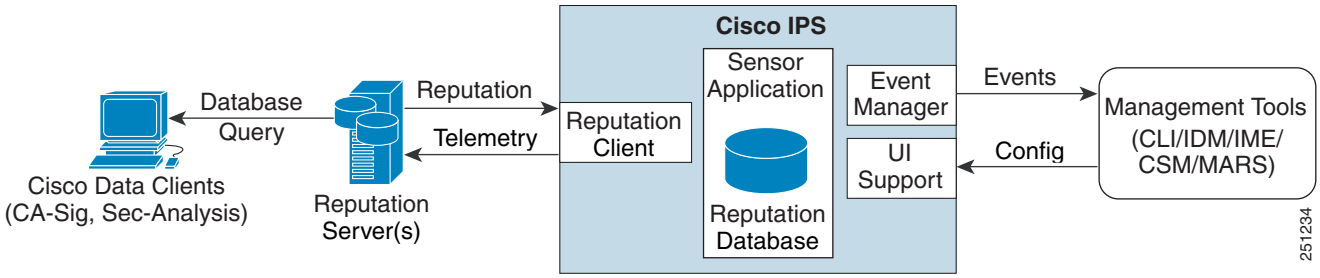
Understanding Reputation

Similar to human social interaction, reputation is an opinion toward a device on the Internet. It enables the installed base of IPS sensors in the field to collaborate using the existing network infrastructure. A network device with reputation is most likely either malicious or infected. You can view reputation information and statistics in the IDM.

The IPS sensor collaborates with the global correlation servers (also known as reputation servers) to improve the efficacy of the sensor.

Figure 11-1 shows the role of the sensor and the global correlation servers.

Figure 11-1 IPS Management and Global Correlation Server Interaction



The global correlation servers provide information to the sensor about certain IP addresses that may identify malicious or infected hosts. The sensor uses this information to determine which actions, if any, to perform when potentially harmful traffic is received from a host with known reputation. Because the global correlation database changes rapidly, the sensor must periodically download global correlation updates from the global correlation servers.

Caution As with signature updates, when the sensor applies a global correlation update, it may trigger bypass. Whether or not bypass is triggered depends on the traffic load of the sensor and the size of the signature/global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

For More Information

For more information about viewing global correlation statistics, see Displaying Statistics, page 17-30.

Understanding Network Participation

Network participation lets us collect nearly real-time data from sensors around the world. Sensors installed at customer sites can send data to the SensorBase Network. These data feed in to the global correlation database to increase reputation fidelity. Communication between sensors and the SensorBase Network involves an HTTPS request and response over TCP/IP.

Network participation gathers the following data:

- Signature ID
- Attacker IP address
- Attacker port
- Maximum segment size
- Victim IP address
- Victim port
- Signature version

- TCP options string
- Reputation score
- Risk rating
- Data gathered from the sensor health metrics

The statistics for network participation show the hits and misses for alerts, the reputation actions, and the counters of packets that have been denied.

There are three modes for network participation:

- Off—The network participation server does not collect data, track statistics, or try to contact the Cisco SensorBase Network.
- Partial Participation—The network participation server collects data, tracks statistics, and communicates with the SensorBase Network. Data considered to be potentially sensitive is filtered out and never sent.
- Full Participation—The network participation server collects data, tracks statistics, and communicates with the SensorBase Network. All data collected is sent.

Network participation requires a network connection to the Internet.

Caution As with signature updates, when the sensor applies a global correlation update, it may trigger bypass. Whether or not bypass is triggered depends on the traffic load of the sensor and the size of the signature/global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

For More Information

- For more information on network participation, see Configuring Network Participation, page 11-10.
- For more information on bypass mode, see Configuring Bypass Mode, page 5-27.

Understanding Efficacy

Obtaining data from participating IPS clients and using that in conjunction with the existing corpus of threat knowledge improves the efficacy of the IPS. We measure efficacy based on the following:

- False positives as a percentage of actionable events
- False negatives as a percentage of threats that do not result in actionable events
- Actionable events as a percentage of all events

For More Information

For more information about reputation and risk rating, see Reputation and Risk Rating, page 11-4.

Reputation and Risk Rating

Risk rating is the concept of the probability that a network event is malicious. You assign a numerical quantification of the risk associated with a particular event on the network. By default, an alert with an extreme risk rating shuts down traffic. Reputation indicates the probability that a particular attacker IP address will initiate malicious behavior based on its known past activity. A certain score is computed for

this reputation by the Alarm Channel and added to risk rating, thus improving the efficacy of the IPS. When the attacker has a bad reputation score, an incremental risk is added to the risk rating to make it more aggressive.

The Alarm Channel handles signature events from the data path. The alert processing units have multiple aggregation techniques, action overrides, action filters, attacker reputation, and per-action custom handling methods. We use the large reputation data from the reputation participation client to score attackers in the Alarm Channel and then use this score to influence the risk rating and actions of the alert.

For More Information

- For a detailed description of risk rating, see Calculating the Risk Rating, page 9-2.
- For a detailed description of threat rating, see Understanding Threat Rating, page 9-4.
- For a detailed description of event action filters, see Understanding Event Action Filters, page 9-5.
- For a detailed description of Alarm Channel, see Understanding SensorApp, page A-24.
- For a detailed description of event action aggregation, see Event Action Aggregation, page 9-5.

Global Correlation and the Produce Alert Event Action

A Produce Alert event action is added for an event under the following conditions:

- Global correlation has increased the risk rating of an event.
- Global correlation has added either the Deny Packet Inline or Deny Attacker Inline event action.

Adding the Produce Alert event action ensures that all events being denied by global correlation result in alerts that you can view through your monitoring tool. This prevents global correlation from denying events that you do not know about.

Note This feature only applies to global correlation inspection where the traffic is allowed if no specific signature is matched. It does not apply to reputation filtering where the packet is denied before signature analysis, and no alerts are generated when packets are denied by reputation filtering.

For More Information

For detailed information about event actions, see Event Actions, page 9-8.

Global Correlation Features and Goals

There are three main features of global correlation:

- Global Correlation Inspection—We use the global correlation reputation knowledge of attackers to influence alert handling and deny actions when attackers with a bad score are seen on the sensor.
- Reputation Filtering—Applies automatic deny actions to packets from known malicious sites.
- Network Reputation—Sensor sends alert and TCP fingerprint data to the SensorBase Network.

Global correlation has the following goals:

- Dealing intelligently with alerts thus improving efficacy.
- Improving protection against known malicious sites.

- Sharing telemetry data with the SensorBase Network to improve visibility of alerts and sensor actions on a global scale.
- Simplifying configuration settings.
- Automatic handling of the uploads and downloads of the information.

Global Correlation Requirements

Global correlation has the following requirements:

- Valid license—You must have a valid sensor license for global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.
- Agree to Network Participation disclaimer
- External connectivity for sensor and a DNS server—The global correlation features of IPS 7.0 require the sensor to connect to the Cisco SensorBase Network. Domain name resolution is also required for these features to function. You can either configure the sensor to connect through an HTTP proxy server that has a DNS client running on it, or you can assign an Internet routeable address to the management interface of the sensor and configure the sensor to use a DNS server. In IPS 7.0 the HTTP proxy and DNS servers are used only by the global correlation features.

  If you are connecting through an HTTP proxy, make sure you have the following configuration:

  - The proxy must allow HTTP requests from the IPS systems to http://updates.ironport.com/ibrs/ on port 80.
  - The proxy must allow HTTPS requests from the IPS systems to update-manifests.ironport.com on port 443.
  - The firewall must allow access from the proxy to the internet (any destination address) on ports 80 and 443.

  If you are NOT connecting through the HTTP proxy:

  - The firewall must allow access from each IPS to the Internet (any destination address) on ports 80 and 443.

  Note The IPS does not support the use of authenticated proxies.

Caution Sensors deployed in an environment with a slow command and control connection will be slow to download global correlation updates.

- No IPv6 address support—Global correlation inspection and the reputation filtering deny features do not support IPv6 addresses. For global correlation inspection, the sensor does not receive or process reputation data for IPv6 addresses. The risk rating for IPv6 addresses is not modified for global correlation inspection. Similarly, network participation does not include event data for attacks from IPv6 addresses. And finally, IPv6 addresses do not appear in the deny list.
- Sensor in inline mode—The sensor must operate in inline mode so that the global correlation features can increase efficacy by being able to use the inline deny actions.
- Sensor that supports the global correlation features

- IPS version that supports the global correlation features

Note IPS 6.1 and 6.2 do not support the global correlation features.

For More Information

- For information on how to obtain and install a sensor license, see Configuring Licensing, page 16-12.
- For information about the network participation disclaimer, see Participating in the SensorBase Network, page 11-2.
- For information about configuring an HTTP proxy or DNS server to support global correlation, see Configuring Network Settings, page 4-1.

Understanding Global Correlation Sensor Health Metrics

For global correlation, the following metrics are added to sensor health monitoring:

- Green indicates that the last update was successful.
- Yellow indicates that there has not been a successful update within the past day (86,400 seconds).
- Red indicates that there has not been a successful update within the last three days (259,200 seconds).

For network participation, the following metrics are added to sensor health monitoring:

- Green indicates that the last connection was successful.
- Yellow indicates that less than 6 connections failed in a row.
- Red indicates that more than 6 connections failed in a row.

You can view the metrics in the Sensor Health gadget and the Global Correlation Health gadget.

Note Global correlation health status defaults to red and changes to green after a successful global correlation update. Successful global correlation updates require a DNS server or an HTTP proxy server. Because DNS and HTTP proxy server configuration features are new to IPS 7.0, they are unconfigured after an upgrade to 7.0. As a result, global correlation health and overall sensor health status are red until you configure a DNS or HTTP proxy server on the sensor. If the sensor is deployed in an environment where a DNS or HTTP proxy server is not available, you can address the red global correlation health and overall sensor health status by disabling global correlation and configuring sensor health status not to include global correlation health status.

For More Information

- For more information about the sensor health metrics, see Configuring Sensor Health, page 16-16.
- For information about configuring a DNS or HTTP proxy server to support global correlation, see Configuring Network Settings, page 4-1.
- For the procedure to disable global correlation, see Configuring Global Correlation Inspection and Reputation Filtering, page 11-8.

Configuring Global Correlation Inspection and Reputation Filtering

This section describes how to set up global correlation inspection and reputation, and contains the following topics:

- Inspection/Reputation Pane, page 11-8
- Inspection/Reputation Pane Field Definitions, page 11-9
- Configuring Global Correlation Inspection and Reputation Filtering, page 11-10

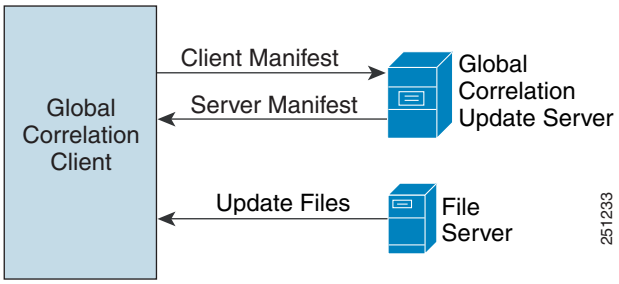
Inspection/Reputation Pane

Note You must be administrator or operator to configure inspection/reputation settings.

In the Inspection/Reputation pane you can configure the sensor to use updates from the SensorBase Network to adjust the risk rating. The client determines which updates are available and applicable to the sensor by communicating with the global correlation update server and a file server, which is a two-phase process. In the first phase the sensor sends a client manifest to the global correlation update sever via an HTTPS POST request. The server then returns the server manifest document in the HTTPS response. In the next phase the sensor identifies the updates that are available and how to obtain them from a file server. The sensor downloads the encrypted update files via HTTP from the file server using the information in the server manifest. The integrity of these update files has been verified by comparing its MD5 hash with the hash value specified in the server manifest.

Figure 11-2 demonstrates how the global correlation update client obtains the files.

Figure 11-2 Global Correlation Update Client



Caution You must have a valid sensor license for global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.

Once you configure global correlation, updates are automatic and happen at regular intervals, approximately every five minutes by default, but this interval may be modified by the global correlation server. The sensor gets a full update and then applies an incremental update periodically.

You configure an HTTP proxy or a DNS server in the Network pane. If you turn on global correlation, you can choose how aggressively you want the deny actions to be enforced against malicious hosts. You can then enable reputation filtering to deny access to known malicious hosts. If you only want a report of what could have happened, you can enable **Test Global Correlation**. This puts the sensor in Audit mode, and actions the sensor would have performed are generated in the events.

To view the status of global correlation in the Sensor Health gadget, click **Details**. The status of global correlation reads Normal, Needs Attention, or Critical.

Caution As with signature updates, when the sensor applies a global correlation update, it may trigger bypass. Whether or not bypass is triggered depends on the traffic load of the sensor and the size of the signature/global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

For More Information

- For the procedure for configuring the HTTP proxy or DNS server, see Configuring Network Settings, page 4-1.
- For more information on bypass mode, see Configuring Bypass Mode, page 5-27.

Inspection/Reputation Pane Field Definitions

The following fields are found in the Inspection/Reputation pane:

- Global Correlation Inspection—Lets you turn global correlation off and on. When turned on, the sensor uses updates from the SensorBase Network to adjust the risk rating. The default is On, however, you must have a DNS server or proxy server configured for global correlation inspection to take effect.

  There are three modes that let you determine how aggressively the sensor uses global correlation information to initiate deny actions:

  - Permissive—Has the least aggressive effect on deny actions.
  - Standard—Has a moderately aggressive effect on deny actions. This is the default.
  - Aggressive—Has a very aggressive effect on deny actions.
- Reputation Filtering—Lets you turn reputation filtering on and off. When turned on, the sensor denies access to malicious hosts that are listed in the global correlation database. The default is On.
- Test Global Correlation—Enables reporting of deny actions that are affected by global correlation. Allows you to test the global correlation features without actually denying any hosts.

For More Information

- For information on how to obtain and install a sensor license, see Configuring Licensing, page 16-12.
- For more information about the sensor health metrics, see Configuring Sensor Health, page 16-16

Configuring Global Correlation Inspection and Reputation Filtering

To configure global correlation inspection and reputation filtering, follow these steps:

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

Step 2 Choose **Configuration > Policies > Global Correlation > Inspection/Reputation**.

Step 3 To turn on global correlation inspection and reputation filtering, click the **On** radio button. Global correlation inspection and reputation filtering are turned off by default.

Step 4 From the drop-down list, choose how you want the sensor to use global correlation information to initiate deny actions:

- Permissive—Has the least aggressive effect on deny actions.
- Standard—Has a moderately aggressive effect on deny actions.
- Aggressive—Has a very aggressive effect on deny actions.

Step 5 To turn on reputation filtering, click the **On** radio button. Reputation filtering is turned off by default.

Step 6 To test global correlation, but not let global correlation influence whether traffic is denied, click the **Test Global Correlation** check box. This gives you reports as if global correlation inspection and reputation filtering were on.

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

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

Configuring Network Participation

This section describes how to configure network participation, and contains the following topics:

- Network Participation Pane, page 11-10
- Network Participation Pane Field Definitions, page 11-11
- Configuring Network Participation, page 11-10

Network Participation Pane

Note You must be administrator or operator to configure network participation.

In the Network Participation pane, you can configure the sensor to send data to the SensorBase Network. You can configure the sensor to fully participate and send all data to the SensorBase Network. Or you can configure the sensor to collect the data but to omit potentially sensitive data, such as the destination IP address of trigger packets.

Note Configuring the sensor for partial network participation limits a third party from extracting reconnaissance information about your internal network from the global correlation database.

Network Participation Pane Field Definitions

The following fields are found in the Network Participation pane:

- Off—No data is contributed to the SensorBase Network.
- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network.

Configuring Network Participation

To configure network participation, follow these steps:

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

Step 2 Choose **Configuration > Policies > Global Correlation > Network Participation**.

Step 3 To turn on network participation, click the **Partial** or **Full** radio button:

- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network.

Caution You must accept the disclaimer to participate in network participation.

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

Step 4 Click **Apply** to apply your changes and save the revised configuration.

Disabling Global Correlation

If your sensor is deployed in an environment where a DNS server or HTTP proxy server is not available, you may want to disable global correlation so that global correlation health does not appear as red in the overall sensor health, thus indicating a problem. You can also configure sensor health not to include global correlation.

To disable global correlation inspection, reputation filtering, and network participation, follow these steps:

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

Step 2 Choose **Configuration > Policies > Global Correlation > Inspection/Reputation**.

Step 3 To disable global correlation inspection and reputation filtering, click the **Off** radio button.

Step 4 To disable reputation filtering, click the **Off** radio button.

Step 5 Choose **Configuration > Policies > Global Correlation > Network Participation**

Step 6 To disable network participation, click the **Off** radio button.

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

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

For More Information

For the procedure for excluding global correlation from overall sensor health, see Configuring Sensor Health, page 16-16.

Troubleshooting Global Correlation

Make sure you observe the following when configuring global correlation:

- Because global correlation updates occur through the sensor management interface, firewalls must allow port 443/80 traffic.
- You must have a DNS or HTTP proxy server configured to allow global correlation features to function.
- If you have an HTTP proxy server configured, the proxy must allow port 443/80 traffic from IPS systems.
- You must have a valid IPS license to allow global correlation features to function.
- Global correlation features only contains external IP addresses, so if you position a sensor in an internal lab, you may never receive global correlation information.
- You must have a sensor that supports global correlation.
- Make sure your IPS version supports the global correlation features.

Note IPS 6.1 and 6.2 do not support the global correlation features.

For More Information

- For the procedure for configuring a DNS or HTTP proxy server, see Configuring Network Settings, page 4-1.
- For the procedure for obtaining an IPS license, see Configuring Licensing, page 16-12.
- For detailed information about HTTP proxy server configuration, see Global Correlation Requirements, page 11-6.