Configuring Global Correlation

Note From 4.17, though Cisco Security Manager continues to support IPS features/functionality, it does not support any enhancements as IPS is now End of Life. For more information, see EOL notice.

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. Global correlation allows you to dynamically use information about malicious activity collected from networks around the globe to change the risk rating of events that have known bad devices as their source.

To configure global correlation, your sensor must be running IPS 7.0+ software. Global correlation is not available on Cisco IOS IPS devices.

This chapter contains the following topics:

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 into 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.

Tip The Botnet Traffic Filter feature of adaptive security appliances (ASA) is another dynamic feature you can deploy in your network to defend against malicious activity. Configuring global correlation on IPS devices, and Botnet Traffic Filtering on ASA firewalls, can be an effective combined security implementation. For more information about Botnet Traffic Filtering, see Managing Firewall Botnet Traffic Filter Rules.

There are three main features of global correlation:

- Global Correlation Inspection—The IPS uses the global correlation reputation knowledge of attackers to influence alert handling and to deny actions when attackers with a bad score are seen on the sensor. For more information about reputation, see Understanding Reputation , on page 2.
- Reputation Filtering—Applies automatic deny actions to packets from known malicious sites.
- Network Participation—The sensor sends alert and TCP fingerprint data to the SensorBase Network so that other users can share in the community knowledge. For more information, see Understanding Network Participation , on page 3.

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.

Tip You can use Report Manager to generate reports comparing the number of alerts generated by global correlation to those generated by traditional IPS inspection. For information on the Inspection/Global Correlation report, see Understanding General IPS Reports. For information on generating reports, see Opening and Generating Reports.

For information on how to configure global correlation, see the following topics:

- Global Correlation Requirements and Limitations , on page 4
- Configuring Global Correlation Inspection and Reputation , on page 5
- Configuring Network Participation , on page 7

Understanding Reputation

Similar to human social interaction, reputation is an opinion toward a device on the Internet. Reputation indicates the probability that a particular attacker IP address will initiate malicious behavior based on its known past activity. Reputation enables the installed base of IPS sensors to collaborate using the existing network infrastructure and identify network devices that are likely to be malicious or infected.

By collecting data about devices and assigning reputation scores to them, the global correlation database provides important data that the IPS sensor can use to adjust the risk rating of an attack. Risk rating is the probability that a network event is malicious. Each signature has an associated risk rating. If you enable global correlation, the IPS sensor computes a score based on the reputation of an attacker and adds this score to the risk rating of the event. The updated risk rating is then used by your event action override and filter policies to help determine what actions to take for the event.

Thus, you might have an event that is initially configured to simply produce an alert. But, if the attacker has a bad reputation, the IPS might increase the risk rating to a number high enough that it triggers an event action override rule that adds the Deny Packet Inline action. Thus, for some source devices, the event simply produces an alert, but for others, the event drops the packet in addition to producing the alert.

Tip The Produce Alert action is added to an event whenever global correlation raises the risk rating of the event, or when global correlation adds the Deny Packet Inline or Deny Attacker Inline actions.

Because the global correlation database changes rapidly, the sensor must periodically download global correlation updates from the global correlation servers.

Using reputation scores to adjust the risk rating of an event improves the efficacy of the sensor by improving the following metrics:

- 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.

Related Topics

- Understanding Global Correlation , on page 1
- Configuring Network Participation , on page 7
- Configuring Global Correlation Inspection and Reputation , on page 5
- Configuring Network Participation , on page 7

Understanding Network Participation

Network participation lets Cisco 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.

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.

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.

- **Full Participation**—The Network Participation server collects data, tracks statistics, and communicates with the SensorBase network. All data collected is sent.

If you select partial or full participation, you are prompted to accept a participation agreement. You must accept the agreement to participate or you cannot change the participation mode.

The following table explains the data collected and the purpose of collecting it.

Table 1: Network Participation Data Sharing and Usage

Participation Level	Type of Data	Purpose
Partial	Protocol attributes (TCP maximum segment size and options string, for example).	Tracks potential threats and helps Cisco to understand threat exposure.
	Attack type (signature fired, including signature ID and version, risk rating, and reputation, 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 pattern.

To configure network participation, the IPS device requires at least 100 MB of available memory, a network connection to the sensor, and a network connection to the Internet. For information on configuring network participation, see Configuring Network Participation , on page 7.

Global Correlation Requirements and Limitations

The following list explains the requirements that you must meet to configure and successfully use global correlation on IPS devices. It also explains some limitations.

- **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. For information on configuring licenses, see Updating IPS License Files.
- **Agree to Network Participation disclaimer**—If you decide to configure network participation, you must accept the disclaimer. For more information, see Understanding Network Participation , on page 3 and Configuring Network Participation , on page 7.
- **External connectivity for sensor and a DNS server or HTTP proxy**—Global correlation requires 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. For more information, see Identifying DNS Servers and Identifying an HTTP Proxy Server.

- **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 and IPS version that supports the global correlation features**—The sensor must run IPS 7.0+ software. You cannot configure global correlation on Cisco IOS IPS devices.
- **Sufficient available memory**—To configure network participation, the IPS device requires at least 100 MB of available memory.
- **Firewall access for port 80, 443 traffic**—Because global correlation updates occur through the sensor management interface, any firewall that lies between the sensor and the internet must allow traffic on ports 80 and 443. You can also use an HTTP proxy (see Identifying an HTTP Proxy Server).
- **Exposure to external traffic**—The global correlation database contains external IP addresses only, so if you position a sensor in an internal lab that has no interaction with outside networks, you might never receive global correlation information. The feature will have no effect.
- **Bypass mode might be triggered during global correlation updates**— As with signature updates, when the sensor applies a global correlation update, it might trigger bypass. Whether bypass is triggered depends on the traffic load of the sensor and the size of the signature or global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.
- **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.

Related Topics

- Understanding Global Correlation , on page 1
- Understanding Reputation , on page 2
- Understanding Network Participation , on page 3
- Configuring Global Correlation Inspection and Reputation , on page 5
- Configuring Network Participation , on page 7

Configuring Global Correlation Inspection and Reputation

Use the Inspection/Reputation policy to configure the sensor to use updates from the SensorBase Network to adjust the risk rating of events. The global correlation client on the sensor determines which updates are available and applicable to the sensor by communicating with the global correlation update server and a file server. The global correlation update server provides the server manifest document to the sensor, which identifies which updates are available and how to obtain them from a file server. The sensor downloads the update files from the file server using the information in the server manifest.

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

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.

Tip When you view IPS events in Event Viewer, there are several columns specific to global correlation that you can add to the event table; these columns are not shown by default, so you must add them to your view. To monitor global correlation in general, use the IPS device manager (IDM) and look at the Sensor Health gadget. Use either the full IDM or open a read-only copy from Security Manager by right-clicking the device in Device view and selecting **Device Manager**.

Before You Begin

- You must also configure a DNS server or HTTP proxy for global correlation to function. For details, see Identifying DNS Servers or Identifying an HTTP Proxy Server.
- There are several configuration requirements and limitations that you should be aware of before configuring global configuration. For details, see Global Correlation Requirements and Limitations , on page 4.

Related Topics

- Understanding Global Correlation , on page 1
- Understanding Reputation , on page 2
- Configuring Network Participation , on page 7

Step 1 Do one of the following to open the Inspection/Reputation policy:

- (Device view) Select **IPS > Global Correlation > Inspection/Reputation** from the Policy selector.
- (Policy view) Select **IPS > Global Correlation > Inspection/Reputation** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Configure the following settings:

- **Global Correlation Inspection**—Whether to enable global correlation inspection. When turned on, the sensor uses updates from the SensorBase Network to adjust the risk rating. Deselect this option to disable inspection.
- **Global Correlation Influence**—How aggressively the sensor uses global correlation information to initiate deny actions. Select one of the following:
  - **Permissive**—Has the least aggressive effect on deny actions.
  - **Standard**—(The default.) Has a moderately aggressive effect on deny actions.
  - **Aggressive**—Has a very aggressive effect on deny actions.

- **Reputation Filtering**—Select whether you want reputation filtering **on** or **off**. When turned on, the sensor denies access to malicious hosts that are listed in the global correlation database.
- **Test Global Correlation**—Whether to place global correlation in audit mode. In audit mode, reputation filtering does not deny access to known malicious hosts; only a report of what could have happened is generated.

Audit mode allows you to test the global correlation features without actually denying any hosts. If you decide the effects are desirable, you can deselect this option to activate reputation filtering.

Configuring Network Participation

Use the Network Participation policy to 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. For detailed information about network participation and the data that is collected, see Understanding Network Participation , on page 3.

Related Topics

- Understanding Global Correlation , on page 1
- Understanding Reputation , on page 2
- Global Correlation Requirements and Limitations , on page 4
- Configuring Global Correlation Inspection and Reputation , on page 5

Step 1 Do one of the following to open the Network Participation policy:

- (Device view) Select **IPS > Global Correlation > Network Participation** from the Policy selector.
- (Policy view) Select **IPS > Global Correlation > Network Participation** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Select the level of participation from the **Network Participation** list:

- **Off**—No data is contributed to the SensorBase network.
- **Partial**—Data is contributed to the SensorBase network but potentially sensitive information is withheld.

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.

- **Full**—All data is contributed to the SensorBase network.

Step 3 If you select Full or Partial, when you click Save, the Network Participation Disclaimer dialog box opens, prompting you to read and accept a disclaimer. Carefully read the disclaimer. Click **Agree** if you agree to it.

If you click **Disagree**, you cannot enable network participation. Change the setting to Off and save the policy.