Improving Phishing Detection Efficacy using Service Logs

This chapter contains the following sections:

- Overview, on page 1
- Enabling Service Logs on Appliance , on page 1
- Disabling Service Logs on Appliance , on page 2
- Frequently Asked Questions, on page 2

Overview

The Service Logs are used to collect personal data based on the Cisco Email Security Appliance Data Sheet guidelines.

The Service Logs are sent to the Cisco Talos Cloud service to improve Phishing detection.

Note From AsyncOS 13.5 onwards, Service Logs replaces senderbase as the telemetry data that is sent to Cisco Talos Cloud service.

The email gateway collects limited personal data from customer emails and offers extensive useful threat detection capabilities that can be coupled with dedicated analysis systems to collect, trend, and correlate observed threat activity. Cisco uses the personal data to improve your email gateway capabilities to analyze the threat landscape, provide threat classification solutions on malicious emails, and to protect your email gateway from new threats such as spam, virus, and directory harvest attacks.

Enabling Service Logs on Appliance

Procedure

Step 1 Go to **Security Services** > **Service Logs**.

Step 2 Click **Edit Global Settings**.

Step 3 Check the **Enable sharing limited data with the Service Logs Information Service (Recommended)** check box.

Checking this box enables the feature globally for the appliance . When enabled, the Context Adaptive Scanning Engine (CASE) is used to collect and report the data (regardless of whether or not Cisco anti-spam scanning is enabled). You can configure the same settings using the `servicelogsconfig` command in the CLI

Step 4 Click **Submit** and commit your changes.

Disabling Service Logs on Appliance

Procedure

Step 1 Go to **Security Services > Service Logs**.

Step 2 Click **Disable** and commit your changes.

Frequently Asked Questions

Cisco recognizes that privacy is important to you, so we design and operate our services with the protection of your privacy in mind. If you enroll to Cisco Talos Cloud service, Cisco will collect aggregated statistics about your organization's email traffic; however, we do not collect or use any personally identifiably information. Any information Cisco collects that would identify your users or your organization will be treated as confidential.

What data do I share?

The data is summarized information on message attributes and information on how different types of messages were handled by appliances . We do not collect the full body of the message. Again, information provided to Cisco that would identify your users or your organization will be treated as confidential. (See What does Cisco do to make sure that the data I share is secure?, on page 3 below).

The following tables explain a sample log entry in a "human-friendly" format.

Table 1: Statistics Shared per Email Message Information

Item	Sample Data
GUID for the inbound SMTP connection	0FyIkNX8ThST1 /IdfyNshg==
GUID for the email message	1Hss77LIS6u7y5 GDn0QFEQ==
Email Security Appliance message ID	5191655
Number of recipients and their validity	1

Item	Sample Data
Scanner verdicts from non-Cisco Talos engines (for example, Anti-Virus or Advanced Malware Protection)	4
Message disposition	MSG_DISP_DROPPED
Message disposition reason	MSG_DISP_FILTER
Is the message for outbound delivery?	true
Message size	35100
Incoming mail relay	true
Mail flow direction	IP_DIR_OUT
AMP verdict information	file_sha2_256: "\217\263\037\004\374`N \3264\265\016\314\227\005E\337\373q \177A\245 \017\004\204\340\231\260!^
Sampling of dropped messages	true

Table 2: Statistics Shared per Periodic Configuration Information

Item	Sample Data
Outbreak Filters feature enabled	true
Sender Domain Reputation (SDR) disabled flag	true
Context Adaptive Scanning Engine (CASE) version	3.8.5-036
Talos engine	1.95.0.220
Generic list of enabled features	Sophos_enabled

What does Cisco do to make sure that the data I share is secure?

If you agree to enroll to Cisco Talos Cloud service:

- Data sent from your appliances will be sent to the Cisco Talos Cloud service using the secure gRPC/HTTP2 protocol.
- All customer data will be handled with care at Cisco. This data will be stored in a secure location and access to the data will be limited to employees and contractors at Cisco who require access in order to improve the company's email security products and services or provide customer support.
- No information identifying email recipients or the customer's company will be shared outside of Cisco Systems when reports or statistics are generated based on the data.

Will sharing data impact the performance of my Cisco appliances ?

Cisco believes that there will be a minimal performance impact for most customers. We record data that already exists as part of the mail delivery process. Customer data is then aggregated on the appliance and sent to Cisco Talos Cloud service. We anticipate that the total size of data transferred via HTTPS will be less than 1% of the bandwidth of a typical company's email traffic.

When enabled, the Context Adaptive Scanning Engine (CASE) is used to collect and report the data (regardless of whether or not Cisco anti-spam scanning is enabled).

If you have additional questions, please contact Cisco Customer Support. See Cisco Support Community.

Are there other ways I can share data?

For customers wanting to do even more to help Cisco provide top quality security services, there is a command that allows you to share additional data. This higher level of data sharing will also provide attachment filenames in clear, unhashed text, as well as hostnames of URLs in messages. If you are interested in learning more about this feature, please talk to your Systems Engineer or contact Cisco Customer Support.