SenderBase Network Participation

This chapter contains the following sections:

Overview of SenderBase Network Participation

SenderBase is an email reputation service designed to help email administrators research senders, identify legitimate sources of email, and block spammers.

Customers participating in the SenderBase Network allow Cisco to collect aggregated email traffic statistics about their organization, increasing the utility of the service for all who use it. Participation is voluntary. Cisco only collects summary data on message attributes and information about how different types of messages were handled by Cisco appliances. For example, Cisco does not collect the message body or the message subject. Personally identifiable information and information that identifies your organization is kept confidential.

Sharing Statistics with SenderBase

Procedure

Step 1 Go to **Security Services > SenderBase**.

Step 2 Click **Edit Global Settings**.

Step 3 Mark the box to enable sharing statistical data with the SenderBase Information Service.

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 **`senderbaseconfig`** command in the CLI

Step 4 (Optional) Enable a proxy server for sharing statistical data with the SenderBase Information Service.

If you define a proxy server to retrieve rules updates, you can also configure an authenticated username, passphrase, and specific port when connecting to the proxy server in the additional fields provided. To edit

these settings, see Configuring Server Settings for Downloading Upgrades and Updates. You can configure the same settings using the **updateconfig** command in the CLI.

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 in SenderBase Network Participation, 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.

Why should I participate?

Participating in the SenderBase Network helps us help you. Sharing data with us is important to helping stop email-based threats such as spam, viruses and directory harvest attacks from impacting your organization. Examples of when your participation is especially important include:

- Email attacks that are specifically targeted at your organization, in which case the data you contribute provides the primary source of information to protect you.
- Your organization is one of the first to be hit by a new global email attack, in which case the data you share with us will dramatically improve the speed with which we are able to react to a new threat.

What data do I share?

The data is summarized information on message attributes and information on how different types of messages were handled by Cisco 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 5 below).

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

Table 1: Statistics Shared Per Cisco Appliance

Item	Sample Data
MGA Identifier	MGA 10012
Timestamp	Data from 8 AM to 8:05 AM on July 1, 2005
Software Version Numbers	MGA Version 4.7.0
Rule Set Version Numbers	Anti-Spam Rule Set 102
Anti-virus Update Interval	Updates every 10 minutes
Quarantine Size	500 MB
Quarantine Message Count	50 messages currently in quarantine

Item	Sample Data
Virus Score Threshold	Send messages to quarantine at threat level 3 or higher
Sum of Virus Scores for messages entering quarantine	120
Count of messages entering quarantine	30 (yields average score of 4)
Maximum quarantine time	12 hours
Count of Outbreak quarantine messages broken down by why they entered and exited quarantine, correlated with Anti-Virus result	50 entering quarantine due to .exe rule 30 leaving quarantine due to manual release, and all 30 were virus positive
Count of Outbreak quarantine messages broken down by what action was taken upon leaving quarantine	10 messages had attachments stripped after leaving quarantine
Sum of time messages were held in quarantine	20 hours

Table 2: Statistics Shared Per Sender IP Address

Item	Sample Data
Message count at various stages within the appliance	Seen by Anti-Virus engine: 100 Seen by Anti-Spam engine: 80
Sum of Anti-Spam and Anti-Virus scores and verdicts	2,000 (sum of anti-spam scores for all messages seen)
Number of messages hitting different Anti-Spam and Anti-Virus rule combinations	100 messages hit rules A and B 50 messages hit rule A only
Number of Connections	20 SMTP Connections
Number of Total and Invalid Recipients	50 total recipients 10 invalid recipients
Hashed Filename(s): (a)	A file <one-way-hash>.pif was found inside an archive attachment called <one-way-hash>.zip.
Obfuscated Filename(s): (b)	A file aaaaaaa0.aaa.pif was found inside a file aaaaaaa.zip.
URL Hostname (c)	There was a link found inside a message to www.domain.com
Obfuscated URL Path (d)	There was a link found inside a message to hostname www.domain.com, and had path aaa000aa/aa00aaa.

Item	Sample Data
Number of Messages by Spam and Virus Scanning Results	10 Spam Positive 10 Spam Negative 5 Spam Suspect 4 Virus Positive 16 Virus Negative 5 Virus Unscannable
Number of messages by different Anti-Spam and Anti-Virus verdicts	500 spam, 300 ham
Count of Messages in Size Ranges	125 in 30K-35K range
Count of different extension types	300 “.exe” attachments
Correlation of attachment types, true file type, and container type	100 attachments that have a “.doc” extension but are actually “.exe” 50 attachments are “.exe” extensions within a zip
Correlation of extension and true file type with attachment size	30 attachments were “.exe” within the 50-55K range
Number of attached files uploaded to the file reputation service (AMP cloud)	1110 files were uploaded to the file reputation service
Verdicts on files uploaded to the file reputation service (AMP cloud)	10 files were found to be malicious 100 files were found to be clean 1000 files were unknown to the reputation service
Reputation score of files uploaded to the file reputation service (AMP cloud)	50 files had a reputation score of 37 50 files had a reputation score of 57 1 file had a reputation score of 61 9 files had a reputation score of 99
Names of files uploaded to the file reputation service (AMP cloud)	example.pdf testfile.doc
Names of malware threats detected by the file reputation service (AMP cloud)	Trojan-Test

Table 3: Statistics Shared Per Message

Message Identifier	Internal Message Identifier - 10010
Recipients Count	Number of recipients in the message - 15

Rejected Recipients Count	Number of recipients found invalid and rejected - 5
Antivirus Verdict	The verdict received from the Anti-Virus engine.
AMP Verdict	If the verdict from the Advanced Malware Protection engine was malware positive.
High-Volume Mail	If the message matched the Header Repeats message filter rule.
Internal Ironport Anti-Spam data	The Ironport Anti-Spam score and message identifier, if the message was scanned by the Ironport Anti-Spam engine.

(a) Filenames will be encoded in a 1-way hash (MD5).

(b) Filenames will be sent in an obfuscated form, with all lowercase ASCII letters ([a-z]) replaced with “a,” all uppercase ASCII letters ([A-Z]) replaced with “A,” any multi-byte UTF-8 characters replaced with “x” (to provide privacy for other character sets), all ASCII digits ([0-9]) replaced with “0,” and all other single byte characters (whitespace, punctuation, etc.) maintained. For example, the file Britney1.txt.pif would appear as Aaaaaaa0.aaa.pif.

(c) URL hostnames point to a web server providing content, much as an IP address does. No confidential information, such as usernames and passwords, are included.

(d) URL information following the hostname is obfuscated to ensure that any personal information of the user is not revealed.

From AsyncOS 8.5 for Email and later, if IronPort Anti-Spam or Intelligent Multi-Scan feature keys are active and SenderBase Network Participation is enabled, AsyncOS performs the following actions to improve the efficacy of the product:

- Collects information about repetition of certain headers in messages, encrypts the collected information, and adds the encrypted information to the respective messages as headers.

  You can submit these processed messages to Cisco for analysis. Each message is reviewed by a team of human analysts and used to enhance the efficacy of the product. For instructions to submit messages to Cisco for analysis, see Reporting Incorrectly Classified Messages to Cisco.

- Sends a random sample of messages to CASE for Antispam scanning, irrespective of their sender's SBRS. CASE scans these messages and uses the results to improve the efficacy of the product. AsyncOS performs this action only when it is idle. As a result, this feedback mechanism does not have any significant impact on the processing of messages.

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

If you agree to participate in the SenderBase Network:

- Data sent from your Cisco appliances will be sent to the Cisco SenderBase Network servers using the secure protocol HTTPS.
- 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 SenderBase servers in batches, typically every 5 minutes. 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).

Note If you choose to participate in the SenderBase Network, a “body scan” is performed on each message. This happens regardless of whether a filter or other action applied to the message would have triggered a body scan. See “Body Scanning Rule” for more information about body scanning.

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.