

SenderBase Network Participation

OVERVIEW

HOW TO INCREASE PROTECTION FOR YOUR MESSAGING INFRASTRUCTURE BY JOINING THE SENDERBASE NETWORK

The *IronPort SenderBase® Network* is the world's largest email and Web traffic monitoring system and is the powerhouse behind IronPort's preventive security services that block spam and other email threats, defend against new viral outbreaks, and identify legitimate sources of email.

As an optional feature in the IronPort® email security appliance, *SenderBase Network Participation (SBNP)* enables you to share summary statistics about your incoming email traffic with IronPort — so that we can help protect you and others.

FAQ

FREQUENTLY ASKED QUESTIONS

IronPort 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*, IronPort will collect aggregated statistics about your organization's email traffic; however, we do not collect or use any personally identifiable information. Any information IronPort 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?

If you agree to participate in the *SenderBase Network*, IronPort will collect aggregated statistics about email sent to your organization. The data is summarized information on message attributes and information on how different types of messages were handled by IronPort appliances. We do not collect the full message body. Again, any identifying user or organizational information provided to IronPort will be kept strictly confidential.



**FREQUENTLY
ASKED
QUESTIONS**
(CONTINUED)**What does IronPort do to make sure that the data I share is secure?**

If you agree to participate in the *SenderBase Network*:

- Data sent from your IronPort appliances will be sent to the *IronPort SenderBase Network* servers using the secure protocol HTTPS.
- All customer data will be handled with care at IronPort. This data will be stored in a secure location and access to the data will be limited to employees and contractors at IronPort 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 IronPort Systems when reports or statistics are generated based on the data.

Will sharing data impact the performance of my IronPort appliances?

Most customers will not see a noticeable change in the performance of their IronPort appliance when they start sharing data with the *SenderBase Network*.

Statistics on incoming mail are collected using IronPort's *Context Adaptive Scanning Engine*[™] (CASE). Leveraging IronPort's "one scan, multi-threat" architecture, the CASE scans a message once and reuses results collected during the scan in multiple applications. This means that customers using either *IronPort Anti-Spam*[™] or *IronPort Virus Outbreak Filters*[™] will not see any change in performance when they begin sharing data with the *SenderBase Network*.

Customers who receive high volumes of email and who are not using either *IronPort Anti-Spam* or *IronPort Virus Outbreak Filters* may experience some decrease in overall system throughput and are recommended to consult with their IronPort representative when enabling data sharing.

After data is collected during the mail delivery process, the data is then aggregated on the appliance and sent to *SenderBase* servers in batches, typically every five minutes. We anticipate that the total size of data transferred via HTTPS will be less than 1 percent of the bandwidth of a typical company's email traffic.

Are there other ways I can share data?

There is a command that allows customers to share additional data, and do even more to help IronPort provide top quality security services. This higher level of data sharing will also provide attachment filenames in clear, unhashed text. If you are interested in learning more about this feature, please talk to your Systems Engineer or contact IronPort Customer Care.



TABLE 1. EXAMPLE STATISTICS SHARED PER IRONPORT APPLIANCE

Tables 1 and 2 explain the type of data you can provide in a “human-friendly” format and summarizes how the data will be used by IronPort.

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 4.5.0
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
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. EXAMPLE STATISTICS SHARED PER IP ADDRESS

Item	Sample Data
Message count at various stages within the MGA	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): ¹	A file <one-way-hash>.pif was found inside an archive attachment called <one-way-hash>.zip.
Obfuscated Filename(s): ²	A file aaaaaaa0.aaa.pif was found inside a file aaaaaaa.zip.
URL Hostname ³	There was a link found inside a message to www.domain.com
Obfuscated URL Path ⁴	There was a link found inside a message to hostname www.domain .com, and had path aaa000aa/aa00aaa.
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

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

² 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.

³ 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. (See: Will the data I share be secure?).

⁴ URL information following the hostname is obfuscated to ensure that any personal information of the user is not revealed.



SUMMARY

RESPONDING QUICKLY TO NEW THREATS

Contributing data to *SenderBase* is an important step you can take to ensure your network and your users have the highest level of security available. Providing IronPort an additional level of visibility into your email traffic patterns allows us to respond that much more quickly and precisely to new and emerging threats.

It's easy—once you've signed up in your IronPort email security appliance GUI, there is nothing more you need to do! It's safe, and your sensitive data is protected. Specific information such as the message body or other information that can be considered confidential is not collected and remains private. This one small step can make a real difference in helping protect your infrastructure and users.

Note: For C300 and C10 appliances, if you choose to participate in the SenderBase Network, a "body scan" is performed on each message in order to provide attachment information as described in the above tables. Once again, we do not collect the message body or the message subject. This happens regardless of whether a filter or other action applied to the message would have triggered a body scan. See "Body Scanning Rule" in the Policy Enforcement chapter of the Advanced User Guide for more information about body scanning.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

To begin sharing data with the *SenderBase Network*, or if you have additional questions, please contact your IronPort Sales Representative or IronPort Customer Care at <http://www.ironport.com/support/>



IronPort Systems, Inc.

950 Elm Avenue, San Bruno, CA 94066

TEL 650.989.6500 FAX 650.989.6543

EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is the leading email and Web security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high-performance, easy-to-use, and technically innovative products for those faced with the monumental task of managing and protecting their mission-critical networks from Internet threats.

