IRONPORT

SenderBase Reputation Score

OVERVIEW

The *SenderBase*® Reputation Score (SBRS) powers *IronPort Reputation Filters*™, the outer layer of defense available to IronPort® email security appliance customers to prevent email-based threats from entering their network. Tightly integrated with IronPort's email security appliance, *IronPort Reputation Filters* allow customers to apply policies—such as blocking known bad senders, throttling suspicious senders and allowing trusted senders to bypass traditional spam filters.

With *IronPort Reputation Filters*, every IP address connecting to an IronPort email security appliance is assigned an SBRS, based on the probability that a message from that IP address is unwanted. This architecture enables IronPort appliances to reject mail at the beginning of the SMTP conversation, dramatically improving performance and availability.

THE REAL DEAL

IRONPORT SENDERBASE

The SBRS relies on *SenderBase*, the world's largest email and Web traffic monitoring network and carefully researched public data sources to establish a sender's reputation.

SenderBase leverages data contributed by over 100,000 organizations receiving email and tracks a remarkable five billion messages per day. Today, *SenderBase* monitors over 25 percent of the world's Internet traffic, providing unprecedented real-time visibility into threats from around the world.

SENDERBASE REPUTATION SCORE INPUTS

Today, over 120 factors are used to determine a sender's reputation, providing the most complete and accurate understanding of email senders available. Specific examples of the factors used to assess a sender's reputation score include:

- An IP address' presence on reliable public blacklists or open proxy lists
- An IP address' presence in hijacked IP space
- The number of end-user complaints associated with an IP address
- The number of messages sent to invalid "spamtrap" accounts
- Global message volume and changes in message volume
- The date of first message seen from this IP address or domain
- The sender's category or industry (e.g. ISP, Fortune 1000 company, government organization, etc.)
- A sender's presence in third-party email certification programs such as Bonded Sender
- Whether message recipients are valid or invalid
- Frequency of URLs appearing in spam or viral messages

THE REAL DEAL
(CONTINUED)

These factors include “spammy” attributes (such as whether or not an IP address is on one of the leading blacklists or open proxy lists) as well as positive attributes (such as whether or not an IP address generates few complaints or is controlled by a Fortune 1,000 organization).

See Figure 1.

Each attribute used as an input is researched extensively. For instance, in the case of blacklists IronPort conducted a thorough evaluation before selecting the most accurate and reputable lists. Today, the blacklist “families” IronPort uses include:

- SpamHaus Blacklist (SBL)
- SpamCop
- The Composite Blocklist (CBL)
- NJABL
- SORBS
- OPM
- DSBL
- Dynablock

Most of the blacklist families actually have multiple lists associated with them—that is, traditional blacklists, open proxy lists, open relay lists and more, so the actual number of lists IronPort uses in *SenderBase* and as part of the *SenderBase* Reputation Score (SBRS) is much higher. A single blacklisting without corroboration of other factors may lead to a slightly negative SBRS, but will rarely result in blocking unless confirmed by other indicators of “spamminess” tracked by *SenderBase*.

HOW IS THE SENDERBASE REPUTATION SCORE CALCULATED?

Using this comprehensive set of factors, the *SenderBase* Reputation Score is generated in three steps:

1. Each factor is assigned a weight, based on the historical probabilities that messages from an IP address with that characteristic were spam.
2. Individual probabilities are aggregated using an advanced algorithm – which produces an overall probability that the message coming from a given IP address is spam.
3. The aggregate spam probability is mapped to a score between -10 and +10.
    - The lowest (most negative) scores are near-certain spam and the highest (most positive) scores represent sources of legitimate email.
    - Highly positive (less “spammy”) scores typically bypass content-based filters, while highly negative scores (more “spammy”) are rejected or throttled.

See Figure 2.

WHAT POLICIES ARE RECOMMENDED?

The following table shows the recommended policies for *IronPort Reputation Filters*, based on how conservative or aggressive a customer chooses to be:

See Figure 3.

Today, SBRS lets IronPort email security appliance customers block or throttle up to 80 percent of incoming spam, based on just the connecting IP address – dramatically improving the system's performance and reducing companies' vulnerability to denial of service attacks or hit and run spam attacks.

By comparison, most publicly available blacklists catch less than 20 percent of spam and have dramatically higher false positive rates. Customers using the SBRS also experience lower false positive rates by passing mail from trusted sources around spam filters.

FIGURE 1.

SENDERBASE EMAIL AND WEB TRAFFIC MONITORING NETWORK

SenderBase Network: 100,000 contributing organizations, 5 billion queries equals unprecedented visibility

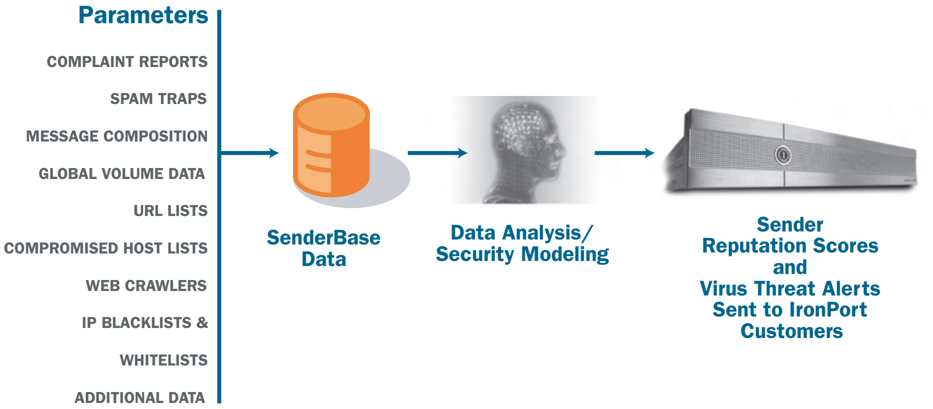
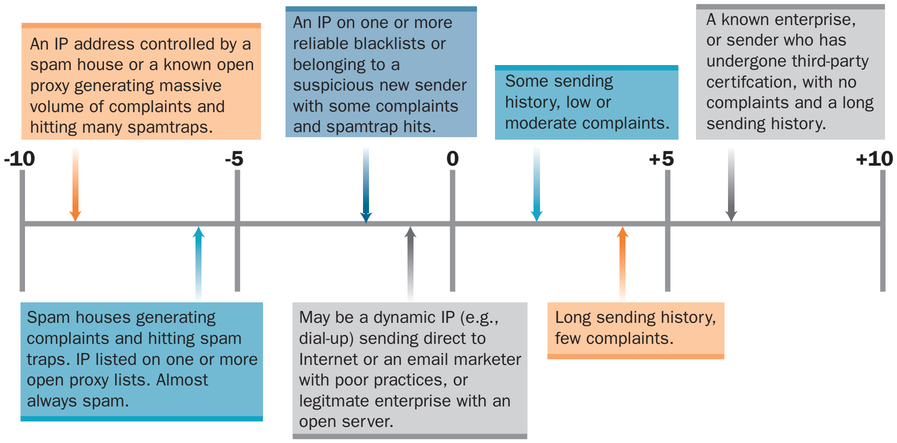


FIGURE 2.

WHAT DO REPUTATION SCORES MEAN?



An IP address controlled by a spam house or a known open proxy generating massive volume of complaints and hitting many spamtraps.

An IP on one or more reliable blacklists or belonging to a suspicious new sender with some complaints and spamtrap hits.

Some sending history, low or moderate complaints.

A known enterprise, or sender who has undergone third-party certifcation, with no complaints and a long sending history.

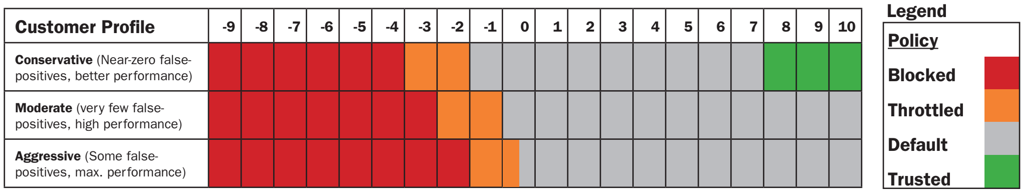
Spam houses generating complaints and hitting spam traps. IP listed on one or more open proxy lists. Almost always spam.

May be a dynamic IP (e.g., dial-up) sending direct to Internet or an email marketer with poor practices, or legitmate enterprise with an open server.

Long sending history, few complaints.

FIGURE 3.

SBRS POLICIES OVERVIEW



Customer Profile	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10
Conservative (Near-zero false-positives, better performance)	🟥	🟥	🟥	🟥	🟥	🟥	🟧	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩
Moderate (very few false-positives, high performance)	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟧	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Aggressive (Some false-positives, max. performance)	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟧	🟧⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜

Legend

Policy	
Blocked	🟥
Throttled	🟧
Default	⬜
Trusted	🟩

SUMMARY

The IronPort email security appliance intelligently throttles suspicious senders—the more hostile they appear, the slower they go. *IronPort Reputation Filters* provide the outer layer of defense for your email infrastructure. The IronPort email security appliance receives inbound mail and performs a threat assessment of the sender. This assessment returns a *SenderBase* Reputation Score that allows the IronPort email security appliance to apply mail flow policies as specified by the administrator. More suspicious senders are throttled or eventually blocked. Recognized senders, such as customers or corporate partners, are allowed access and can bypass filters per the administrator's needs.

IRONPORT®

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.

IRONPORT C600
04/06
DOC RELEASE