What are the best practices for using SenderBase?

Contents

Introduction

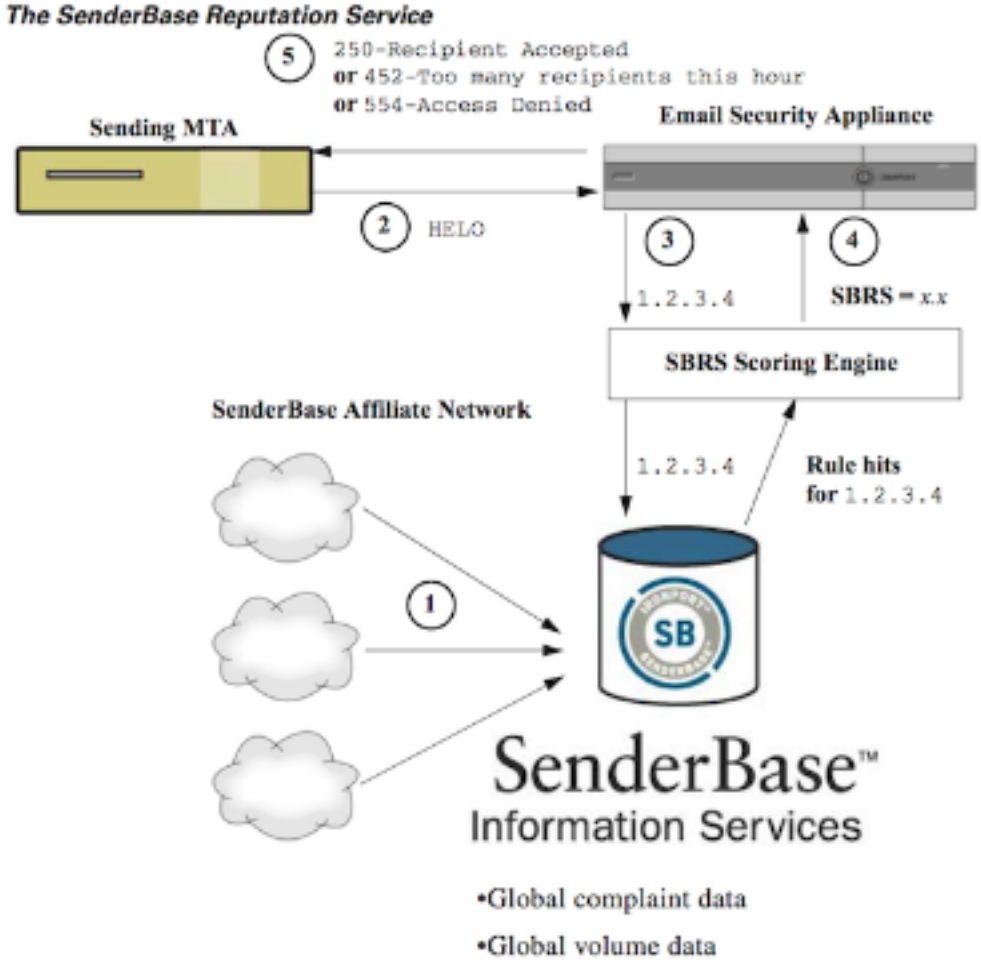
This document describes the best practices for using SenderBase.

What are the best practices for using SenderBase?

The SenderBase Reputation Service (SBRS) provides an accurate, flexible way for you to reject or throttle systems suspected to be transmitting spam based on the connecting IP address of the remote host. The SBRS returns a score based on the probability that a message from a given source is spam, ranging from -10 (certain to be spam) through 0 to +10 (certain not to be spam). Although SBRS can be used as a stand-alone anti-spam solution, it is most effective when combined with a content-based anti-spam scanner.

SenderBase scores can be used in the Host Access Table (HAT) on an SMTP listener to map incoming SMTP connections to different Sender Groups. Each Sender Group has associated with it a policy that affects how incoming email is handled. The most common things to do with SenderBase scores are to either reject mail entirely, or to throttle the suspected spam sender.

You can use SBRS scores in the HAT to reject or throttle email. You can also create message filters to specify "thresholds" for SBRS scores to further act upon messages processed by the system. The diagram below provides a rough outline of how SBRS scores can be used to block or throttle suspected senders:



1. SenderBase affiliates send real-time, global data.
2. Sending MTA opens connection with the appliance.
3. Appliance checks global data for the connecting IP address.
4. SenderBase Reputation Service calculates the probability this message is spam and assigns a SenderBase Reputations Score.
5. Appliance returns the response (either rejecting email or throttling sender) based on the SenderBase Reputation Score.

How you use SBRS scores will depend on how aggressive you want to be in pre-filtering email. The Email Security Appliance (ESA) offers three different strategies for implementing SenderBase:

- **Conservative**: A conservative approach is to block messages with a SenderBase Reputation Score lower than -7.0, throttle between -7.0 and -2.0, apply the default policy between -2.0 and +6.0, and apply the trusted policy for messages with a score greater than +6.0. Using this approach ensures a near zero false positive rate while achieving better system performance.
- **Moderate:** A moderate approach is to block messages with a SenderBase Reputation Score lower than -4.0, throttle between -4.0 and 0, apply the default policy between 0 and +6.0, and apply the trusted policy for messages with a score greater than +6.0. Using this approach ensures a very small false positive rate while achieving better system performance (because more mail is shunted away from Anti-Spam processing).
- **Aggressive:** An aggressive approach is to block messages with a SenderBase Reputation Score lower than -1.0, throttle between -1.0 and 0, apply the default policy between 0 and +4.0, and apply the trusted policy for messages with a score greater than +4.0. Using this approach, you might incur some false positives; however, this approach maximizes system performance by shunting the most mail away from Anti-Spam processing.

The table below summarizes these three policies:

Approach	Characteristics	Allowlist	Blocklist	Suspectlist	Unknownlis
		Sender Base Reputation Score range:			
Conservative	Near zero false positives, better performance	7 to 10	-10 to -4	-4 to -2	-2 to 7
Moderate (Default)	Very few false positives, high performance	Sender Base Reputation Scores are not used.	-10 to -3	-3 to -1	-1 to +10
Aggressive	Some false positives, maximum performance This option shunts the most mail away from Anti-Spam processing.	4 to 10	-10 to -2	-2 to -1	-1 to 4
All approaches		Mail Flow Policy: Trusted	Blocked	Throttled	Accepted

Implementing SenderBase Throttling or Blocking

The best way to use SenderBase scores means following a simple, 2-part methodology. First, you decide on your policy (for example, you could start with the "Conservative" policy above) and map that policy to Sender Groups. Then, you map those sender groups to the policy you want. The ESA has already created a matrix of Sender Groups and Mail Flow Policies that can serve as a template for your implementation of SBRS.

To implement SenderBase throttling based on the default policy, you will edit the four sender groups (Allowlist, Blocklist, Suspectlist, and Unknownlist) at Mail Policies > Host Access Table (HAT) Overview. Start by clicking on "Allowlist" sender group. Then, using the drop-down menu in the Senders tab, click on "Add Sender" with "SenderBase Reputation Score (SBRS)" selected. This will add an SBRS line to the list of senders. Fill in your SBRS score range (in this case 6.0 to 10.0) and click the **Submit** button.

The policy for the Allowlist sender group is "Trusted." By default, this policy will skip anti-spam processing, which will increase system performance. Because senders with very high SBRS scores are highly unlikely to be sending spam, this step alone will increase throughput. Edit the remaining three Sender Groups to add SBRS scores, according to the table below:

Sender Group	Score Range	Result
Allowlist	6 to 10	Known good senders will not be scanned
Unknownlist	-2 to +6	Senders with little information will be scanned normally
Suspectlist	-7 to -2	Senders with poor reputation will be heavily throttled to reduce the amount of s they can send
Blocklist	-10 to -7	Mail from known spammers will be rejected at SMTP time with a 5xx response

When you are done adding score ranges, do not forget to click "**Commit Changes**." When you are

adding SBRS scoring rules to existing sender groups, place them at the bottom of the list of senders in any group. Order matters when defining sender groups in a listener's HAT, as the groups are evaluated from top-to-bottom, and within each group, each rule is evaluated individually, from top-to-bottom. In a HAT, the first rule matching a sender will be used to select a policy. If an incoming connection from a sending domain has a definite SBRS score and matches the range in a rule in the listener's HAT, the mail flow policy will be applied, even if other rules further down in the list of sender groups might also match.

If your policy for putting senders into sender groups requires that all non-SBRS rules be evaluated before SBRS scores are considered, then you can simply add four new sender groups at the end of the list of existing sender groups specifically for SBRS policy matching along with their relevant policies.

Related Information

- **SenderBase Frequently Asked Questions**
- **Technical Support & Documentation - Cisco Systems**