Welche Best Practices gelten für die Verwendung von SenderBase?

Inhalt

Einführung

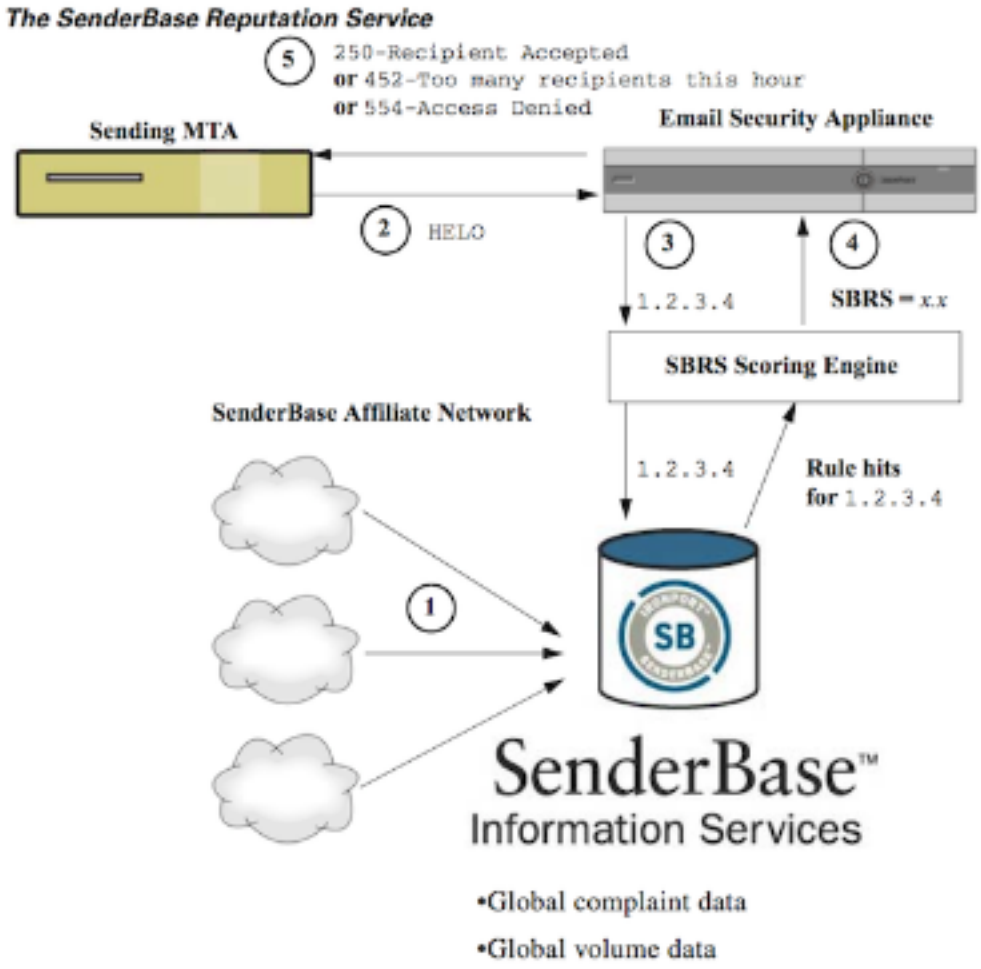
Dieses Dokument beschreibt die Best Practices für die Verwendung von SenderBase.

Welche Best Practices gelten für die Verwendung von SenderBase?

Der SenderBase Reputation Service (SBRS) bietet eine präzise und flexible Möglichkeit für Sie, Systeme abzulehnen oder zu drosseln, die vermutlich Spam übertragen, basierend auf der IP-Adresse des angeschlossenen Remote-Hosts. Das SBRS gibt einen Wert zurück, der auf der Wahrscheinlichkeit basiert, dass eine Nachricht aus einer bestimmten Quelle Spam ist. Dieser Wert reicht von -10 (sicher Spam) bis +10 (sicher nicht Spam). SBRS kann zwar als eigenständige Anti-Spam-Lösung eingesetzt werden, ist aber in Kombination mit einem inhaltsbasierten Anti-Spam-Scanner am effektivsten.

SenderBase-Bewertungen können in der Host Access Table (HAT) eines SMTP-Listeners verwendet werden, um eingehende SMTP-Verbindungen verschiedenen Absendergruppen zuzuordnen. Jede Absendergruppe hat dieser Richtlinie eine Richtlinie zugeordnet, die sich auf den Umgang mit eingehenden E-Mails auswirkt. Die gängigsten Dinge bei SenderBase-Bewertungen sind die vollständige Ablehnung von E-Mails oder die Drosselung des verdächtigen Spam-Absenders.

Sie können SBRS-Bewertungen im HAT verwenden, um E-Mails abzulehnen oder zu drosseln. Sie können auch Nachrichtenfilter erstellen, um "Schwellenwerte" für SBRS-Bewertungen anzugeben, um weiter auf vom System verarbeitete Nachrichten zu reagieren. Das folgende Diagramm bietet eine grobe Übersicht darüber, wie SBRS-Bewertungen verwendet werden können, um verdächtige Absender zu blockieren oder zu drosseln:



1. SenderBase-Partner senden globale Echtzeitdaten.
2. Beim Senden von MTA wird die Verbindung mit der Appliance geöffnet.
3. Appliance prüft globale Daten auf die Verbindungs-IP-Adresse.
4. SenderBase Reputation Service berechnet die Wahrscheinlichkeit, dass es sich bei dieser Nachricht um Spam handelt, und weist eine SenderBase Reputations Score zu.
5. Appliance gibt die Antwort (entweder die Ablehnung von E-Mails oder die Drosselung des Senders) basierend auf der SenderBase-Reputationsbewertung zurück.

Wie Sie die SBRS-Bewertungen verwenden, hängt davon ab, wie aggressiv Sie bei der Vorabfilterung von E-Mails sein möchten. Die E-Mail Security Appliance (ESA) bietet drei verschiedene Strategien zur Implementierung von SenderBase:

- **Konservativ**: Ein konservativer Ansatz besteht darin, Nachrichten mit einem SenderBase-Reputationswert unter -7.0 zu blockieren, eine Drosselung zwischen -7.0 und -2.0 vorzunehmen, die Standardrichtlinie zwischen -2.0 und +6.0 anzuwenden und die vertrauenswürdige Richtlinie für Nachrichten mit einer Punktzahl größer als +6.0 anzuwenden. Durch diesen Ansatz wird eine Fehlalarmquote von nahezu null gewährleistet und gleichzeitig eine bessere Systemleistung erzielt.
- **Mittel:** Ein moderater Ansatz besteht darin, Nachrichten mit einem SenderBase-Reputationswert unter -4,0 zu blockieren, eine Drosselung zwischen -4,0 und 0 vorzunehmen, die Standardrichtlinie zwischen 0 und +6,0 anzuwenden und die vertrauenswürdige Richtlinie für Nachrichten mit einer Punktzahl größer als +6,0 anzuwenden. Mit diesem Ansatz wird eine sehr geringe Fehlalarmquote sichergestellt und gleichzeitig eine bessere Systemleistung erzielt (da mehr E-Mails von der Anti-Spam-Verarbeitung abgezogen werden).
- **Aggressiv:** Ein aggressiver Ansatz besteht darin, Nachrichten mit einem SenderBase-

Reputationswert unter -1,0 zu blockieren, eine Drosselung zwischen -1,0 und 0 vorzunehmen, die Standardrichtlinie zwischen 0 und +4,0 anzuwenden und die vertrauenswürdige Richtlinie für Nachrichten mit einer Punktzahl größer als +4,0 anzuwenden. Bei diesem Ansatz könnten einige Fehlalarme auftreten. Dieser Ansatz maximiert jedoch die Systemleistung, indem die meisten E-Mails von der Anti-Spam-Verarbeitung entfernt werden.

In der folgenden Tabelle sind die drei Richtlinien zusammengefasst:

Ansatz	Merkmale	Zulässige Liste	Sperrliste	Verdächtige	Unbekannte
		Sender Base Reputation Score-Bereich:			
Konservative	Nahezu null Fehlalarme, bessere Leistung	7 bis 10	-10 bis -4	-4 bis -2	-2 bis 7
Moderat (Standard)	Sehr wenige Fehlalarme, hohe Leistung	Sender Base Reputation Scores werden nicht verwendet.	-10 bis -3	-3 bis -1	-1 bis +10
aggressiv	Einige Fehlalarme, maximale Leistung Mit dieser Option wird die meiste E-Mail von der Anti-Spam-Verarbeitung entfernt.	4 bis 10	-10 bis -2	-2 bis -1	-1 bis 4
Alle Ansätze		Mail Flow Policy: Vertrauenswürdig	Gesperrt	gedrosselt	Akzeptiert

SenderBase-Einschränkung oder Blockierung implementieren

Die beste Möglichkeit, SenderBase-Bewertungen zu verwenden, ist eine einfache, zweiteilige Methodik. Zuerst entscheiden Sie über Ihre Richtlinie (Sie können z. B. mit der oben stehenden "Conservative"-Richtlinie beginnen) und ordnen diese Richtlinie Absendergruppen zu. Anschließend ordnen Sie diese Absendergruppen der gewünschten Richtlinie zu. Die ESA hat bereits eine Matrix von Absendergruppen und Mail Flow-Richtlinien erstellt, die als Vorlage für Ihre Implementierung von SBRS dienen kann.

Um die SenderBase-Drosselung basierend auf der Standardrichtlinie zu implementieren, bearbeiten Sie die vier Absendergruppen (Zulässige Liste, Sperrliste, Suspectlist und Unbekannte Liste) unter Mail Policies > Host Access Table (HAT) Overview. Klicken Sie zunächst auf "Allowlist". Klicken Sie dann im Dropdown-Menü auf der Registerkarte "Absender" auf "Absender hinzufügen", wobei "SenderBase Reputation Score (SBRS)" ausgewählt ist. Damit wird der Absenderliste eine SBRS-Zeile hinzugefügt. Füllen Sie den SBRS-Punktebereich (in diesem Fall 6.0 bis 10.0) aus, und klicken Sie auf die Schaltfläche **Senden**.

Die Richtlinie für die Allowlist-Absendergruppe lautet "Trusted" (Vertrauenswürdig). Diese Richtlinie überspringt standardmäßig die Verarbeitung von Spam-Nachrichten, wodurch die Systemleistung erhöht wird. Da Absender mit sehr hohen SBRS-Bewertungen höchstwahrscheinlich keine Spam-E-Mails versenden, erhöht allein dieser Schritt den Durchsatz. Bearbeiten Sie die verbleibenden drei Absendergruppen, um SBRS-Bewertungen hinzuzufügen,

wie in der nachfolgenden Tabelle dargestellt:

Absendergruppe	Leistungsbereich	Ergebnis
Zulässige Liste	6 bis 10	Zweifelsfrei funktionierende Absender werden nicht gescannt.
Unbekannte Liste	-2 bis +6	Absender mit wenigen Informationen werden normal gescannt
Verdächtige	-7 bis -2	Absender mit schlechter Reputation werden stark gedrosselt, um die Menge an Spam zu reduzieren, die sie senden können
Sperrliste	-10 bis -7	E-Mails bekannter Spammer werden zur SMTP-Zeit mit einer 5xx-Ant abgelehnt.

Wenn Sie alle Bereiche hinzugefügt haben, vergessen Sie nicht, auf "**Änderungen bestätigen**" zu klicken. Wenn Sie vorhandenen Absendergruppen SBRS-Bewertungsregeln hinzufügen, platzieren Sie diese am unteren Ende der Absenderliste in einer beliebigen Gruppe. Bei der Definition von Absendergruppen in der HAT eines Listeners spielt die Reihenfolge eine Rolle, da die Gruppen von oben nach unten ausgewertet werden. Innerhalb jeder Gruppe wird jede Regel einzeln von oben nach unten ausgewertet. In einer HAT wird die erste Regel, die einem Absender entspricht, zur Auswahl einer Richtlinie verwendet. Wenn eine eingehende Verbindung aus einer sendenden Domäne eine bestimmte SBRS-Bewertung hat und mit dem Bereich einer Regel in der HAT des Listeners übereinstimmt, wird die Mail-Flow-Richtlinie angewendet, selbst wenn andere Regeln, die weiter unten in der Liste der Absendergruppen aufgeführt sind, ebenfalls übereinstimmen können.

Wenn Ihre Richtlinie zum Einfügen von Absendern in Absendergruppen vorsieht, dass alle Nicht-SBRS-Regeln ausgewertet werden, bevor SBRS-Bewertungen in Betracht gezogen werden, können Sie einfach vier neue Absendergruppen am Ende der Liste der bestehenden Absendergruppen hinzufügen, die speziell für die Übereinstimmung von SBRS-Richtlinien mit den entsprechenden Richtlinien ausgelegt sind.

Zugehörige Informationen

- Häufig gestellte Fragen zu SenderBase
- Technischer Support und Dokumentation - Cisco Systems