SenderBase 使用のベスト プラクティス

内容

概要

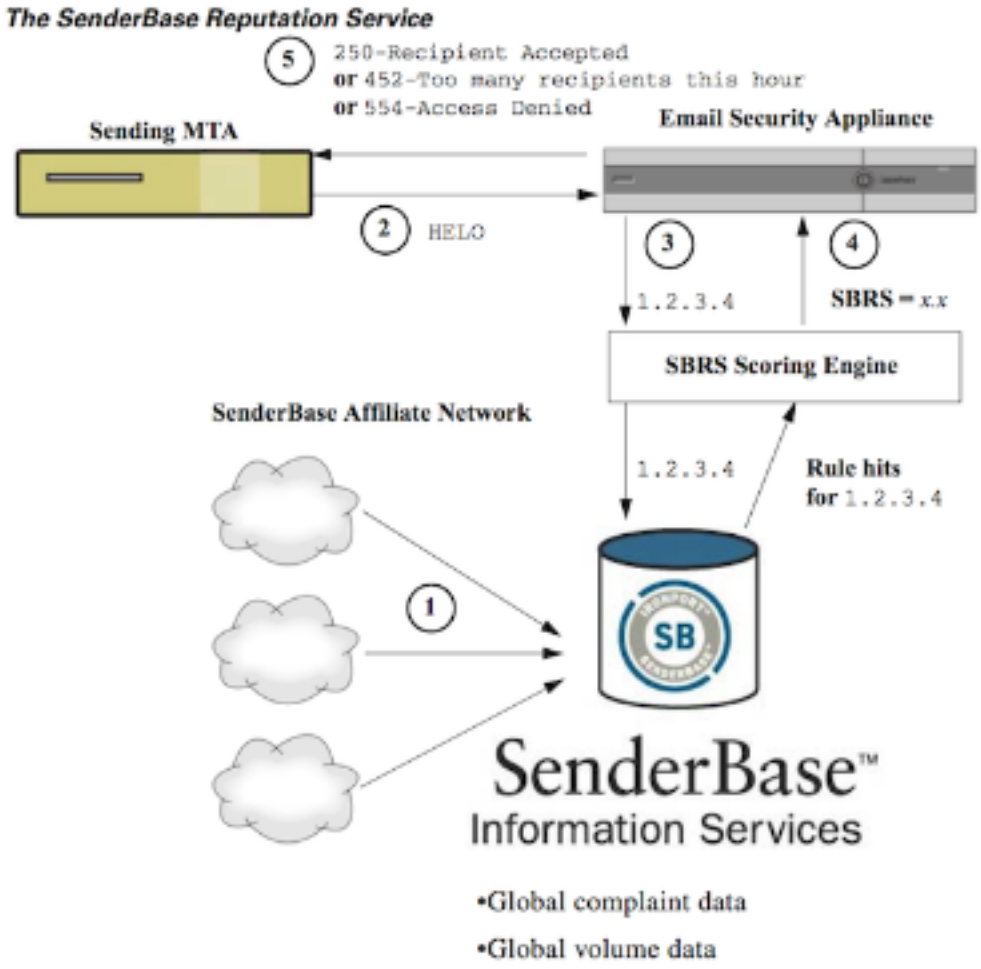
このドキュメントでは、SenderBase を使用する上でのベスト プラクティスについて説明します。

SenderBase 使用のベスト プラクティス

SenderBase レピュテーション サービス (SBRS) には、リモート ホストの接続 IP アドレスに基づいて、スパムを送信している疑いがあるシステムを拒否またはスロットリングするための正確で柔軟な方法が備わっています。SBRSは、特定の送信元からのメッセージがスパムである可能性に基づいてスコアを返します。スコアは–10 (スパムであることが確実) ~ 0 ~ +10 (スパムでないことが確実) です。

SenderBaseスコアは、SMTPリスナーのホストアクセステーブル(HAT)で異なる送信者グループに着信SMTP接続をマッピングするために使用できます。各送信者グループは、受信メールの処理方法に影響するポリシーを関連付けています。

HAT で SBRS スコアを使用することで、電子メールを拒否またはスロットリングできます。また、メッセージ フィルタを作成して SBRS スコアの「しきい値」を指定し、システムで処理されるメッセージに対してさらにアクションを実行することもできます。次の図に、SBRS スコアを使用して疑わしい送信者をブロックまたはスロットリングする方法を大まかに示します。



1. SenderBase アフィリエイトから、リアルタイムのグローバル データを送信します。
2. 送信側 MTA により、アプライアンスとの接続が開始されます。
3. アプライアンスにより、接続 IP アドレスのグローバル データがチェックされます。
4. SenderBase レピュテーション サービスにより、このメッセージがスパムである確率が計算され、SenderBase レピュテーション スコアが割り当てられます。
5. アプライアンスから、SenderBase レピュテーション スコアに基づく応答（電子メールの拒否または送信者のスロットリングのいずれか）が返されます。

SBRS スコアをどのように使用するかは、どれだけ積極的に電子メールを事前フィルタリングするかによって異なります。E メール セキュリティ アプライアンス（ESA）では、SenderBase の実装戦略として次の 3 つを使用できます。

- **[Conservative]**：控えめなアプローチとして、SenderBaseレピュテーションスコアが–7.0より低く、スロットルが–7.0 ~ -2.0のメッセージをブロックし、デフォルトのポリシーを–2.0 ~ +6.0のスコアに適用します。
- **[Moderate]**：中程度のアプローチは、SenderBaseレピュテーションスコアが–4.0より低く、スロットルが–4.0 ~ 0のメッセージをブロックし、デフォルトのポリシーを0 ~ +6.0のスコアのメッセージに適用します。このアプローチを使用すると、システム性能が向上します。
- **[Aggressive]**：アグレッシブなアプローチは、SenderBaseレピュテーションスコアが–1.0より低いメッセージをブロックし、-1.0 ~ 0の範囲でデフォルトのポリシーを適用し、+4.0より大きいスコアのメッセージに信頼ポリシーを適用することです。ただし、ほとんどのメールがスパム対策の処理から除外されることから、システム パフォーマンスが最大化されます。

次の表は、これら3つのポリシーをまとめたものです。

アプローチ	特性	Allowlist	ブロックリスト	Suspectlist	Unknownlist
		送信者基準レピュテーションスコアの範囲：			
保守派	誤検出がほとんどなく、パフォーマンスが向上	7 ~ 10	-10 ~ -4	-4 ~ -2	-2 ~ 7
中（デフォルト）	false positiveはほとんどなく、高パフォーマンス	Sender Base Reputation Scoresは使用されません。	-10 ~ -3	-3 ~ -1	-1 ~ +10
アグレッシブ	誤検出、最大パフォーマンス このオプションは、スパム対策の処理から最も遠いメールを排除します。	4 ~ 10	-10 ~ -2	-2 ~ -1	-1 ~ 4
すべてのアプローチ		メール フロー ポリシー: TRUSTED	Blocked	THROTTLED	受諾済み

SenderBase のスロットリングまたはブロッキングの実装

SenderBaseスコアを使用する最善の方法は、単純な2部構成の方法に従うことです。まず、ポリシーを決定し（例えば、上の「控えめ」ポリシーから開始できます）、そのポリシーを送信者グループにマップします。次に、これらの送信者グループを目的のポリシーにマッピングします。SBRS 実装のテンプレートとして使用できる送信者グループとメール フロー ポリシーのマトリクスは、ESA によってすでに作成されています。

既定のポリシーに基づいてSenderBaseスロットリングを実装するには、[メールポリシー] > [ホストアクセステーブル(HAT)]の4つの送信者グループ(Allowlist、Blocklist、Suspectlist、Unknownlist)を編集します。 sender" with "SenderBase Reputation Score (SBRS)"が選択されています。これにより、SBRS行が送信者のリストに追加されます。SBRSスコア範囲（この場合は6.0 ~ 10.0）を入力し、[送信]ボタンをクリックします。

Allowlist送信者グループのポリシーは"信頼されています。既定では、このポリシーはアンチスパム処理をスキップするため、システムパフォーマンスが向上します。SBRSスコアが非常に高い送信者はスパムを送信することはほとんどないため、この手順だけでスループットが向上します。残りの 3 つの送信者グループを編集し、次の表に従って SBRS スコアを追加します。

送信者グループ	スコア範囲	結果
Allowlist	6 ~ 10	正当であることが既知の送信者はスキャンされません。
Unknownlist	-2 ~ +6	通常、ほとんど情報がない送信者はスキャンされます
Suspectlist	-7 ~ -2	レピュテーションが低い送信者は、それらが送信する可能性のあるスパムの
ブロックリスト	-10 ~ -7	既知のスパム送信者からのメールは、SMTP 時に 5xx 応答で拒否されます。

スコア範囲の追加が完了したら、必ず [Commit Changes] をクリックしてください。 SBRSスコアリング・ルールを既存の送信者グループに追加する場合は、グループ内の送信者グループを定義する際に重要な順序を指定します。リスナーのHATでは、グループが上から下に評価され、各グループ内で評価されます。送信側ドメインからの着信接続で、確定された SBRS スコアが設定されており、リスナーの HAT 内の特定のルールの範囲と一致する場合、送信者グループのリスト内でそのルールより下にある他のルールにも一致するとしても、その特定のルールのメール フロー ポリシーが適用されます。

送信者を送信者グループに追加するためのポリシーで、すべての非 SBRS ルールを評価してから SBRS スコアを考慮することを要件としている場合、既存の送信者グループのリストの最後に新しい 4 つの送信者グループを追加するだけで、関連するポリシーと併せて SBRS ポリシーと照合することができます。

関連情報

- SenderBase に関してよく寄せられる質問（FAQ）
- テクニカル サポートとドキュメント – Cisco Systems