SenderBase を使用する上でのベスト プラクティス

目次

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 を使用する上でのベスト 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き、-10 (スパムと特定) ~ 0 ~ +10 (スパムでないと特定) の範囲のスコアを返します。 SBRS は、スタンドアロンのスパム対策ソリューションとして使用できますが、コンテンツベースのスパム対策スキャナと組み合わせれば、最も効果的です。

SenderBase スコアを SMTP リスナー上のホスト アクセス テーブル (HAT) で使用することで、着信 SMTP 接続をさまざまな送信者グループにマップできます。 各送信者グループには、着信電子メールの処理方法に影響を与えるポリシーが関連付けられています。 SenderBase スコアを使用した最も一般的な処理は、メールを完全に拒否するか、または疑わしいスパム送信者をスロットリングすることです。

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]： [Conservative] アプローチでは、SenderBase レピュテーション スコアが -7.0 未満のメッセージをブロックし、-7.0 ~ -2.0 のメッセージをスロットリングし、-2.0 ~ +6.0 のメッセージにデフォルト ポリシーを適用し、+6.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。 このアプローチを使用すると、誤検出率をほぼ 0 に抑えながら、良好なシステム パフォーマンスを実現できます。
- **[Moderate]**： [Moderate] アプローチでは、SenderBase レピュテーション スコアが -4.0 未満のメッセージをブロックし、-4.0 ~ 0 のメッセージをスロットリングし、0 ~ +6.0 のメッセージにデフォルト ポリシーを適用し、+6.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。 このアプローチを使用すると、誤検出率を非常に低く抑えながら、良好なシステム パフォーマンスを実現できます（スパム対策の処理から除外されるメールが増えるため）。
- **[Aggressive]**： [Aggressive] アプローチでは、SenderBase レピュテーション スコアが -1.0 未満のメッセージをブロックし、-1.0 ~ 0 のメッセージをスロットリングし、0 ~ +4.0 のメッセージにデフォルト ポリシーを適用し、+4.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。 このアプローチを使用すると、誤検出がいくらか発生する場合があります。 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。

次のグラフと表で、上記の 3 つのポリシーを要約します。

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、シンプルな 2 段階方式に従うことです。 まず、ポリシーを決定し（たとえば、最初に上記の [Conservative] ポリシーを使用）、そのポリシーを送信者グループにマッピングします。 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。

デフォルトのポリシーに基づいて SenderBase のスロットリングを実装するには、[Mail Policies] > [Host Access Table (HAT) Overview] に移動して、4 つの送信者グループ（[Whitelist]、[Blacklist]、[Suspectlist]、および [Unknownlist]）を編集します。 まず、[Whitelist] 送信者グループをクリックします。 次に、[Senders] タブのドロップダウン メニューを使用して、[SenderBase Reputation Score (SBRS)] が選択されている状態で [Add Sender] をクリックします。 これにより、送信者のリストに SBRS 行が追加されます。 SBRS スコア範囲（この例の場合、6.0 ~ 10.0）を入力し、[Submit] ボタンをクリックします。

[Whitelist] 送信者グループのポリシーは [Trusted] です。デフォルトでは、このポリシーはスパム対策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することになります。 SBRS スコアが極めて高い送信者がスパムを送信している可能性は非常に低いことから、このステップだけでも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

Whitelist	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
Blacklist	-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。 既存の送信者グループに SBRS スコア ルールを追加するときには、そのグループの送信者のリストの一番下に追加します。 リスナーの HAT に送信者グループを定義する際は、順序が重要です。グループは上から下への順で評価されます。グループ内では、各ルールが上から下への順で個別の評価されます。 HAT で送信者と一致した最初のルールによって、ポリシーが選択されます。 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 の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