ESA に関する FAQ： SBRS 値「none」の意味と、これらのスコアを検出する方法を教えてください

目次

概要

このドキュメントでは、SenderBase レピュテーション スコア（SBRS）を理解し、それを検出する方法を説明します。

SBRS 値「none」の意味と、これらのスコアを検出する方法を教えてください

SBRS は IP アドレスに関連付けられる、50 種類の要因（メールのボリューム、ユーザの苦情件数、スパム トラップ件数など）に基づくスコアです。 SBRS は -10 ~ +10 の範囲の値で、その値は、送信側 IP アドレスから送信されるメールがスパムである可能性を反映します。 高い負のスコアは、スパムを送信する可能性が非常に高い送信者を示します。 高い正のスコアは、スパムを送信する可能性が低い送信者を示します。

ただし、一部の IP アドレスでは SenderBase スコアが「none」になります。 ESA が SBRS サーバに接続できない場合、接続側 IP アドレスは「none」のスコアを受け取ります。 SBRS データは非常にタイムリーであり、アプライアンスが SBRS スコアをキャッシュするのは約 30 分に限られます。 SBRS サーバへの接続に断続的な問題が発生した場合、前にスコアを付けられた IP アドレスが「none」スコアで示される可能性があります。

それ以外の場合、SenderBase スコアは SenderBase が IP アドレスに関して収集した客観的データに基づきます。 特定の IP アドレスに正確なレピュテーションを割り当てるのに十分な履歴データと情報がない場合もあります。 つまり、過去 30 日間にその IP アドレスから送信されたメールのボリュームが非常に少ないか、この期間内に送信されたメールがない場合です。 その場合、SenderBase は全世界の E メール トラフィックのサンプルを使用してボリュームを計算し、その IP アドレスのメール ボリュームが小さいと判断します。 特定のサーバ/ドメインのボリュームが小さければ、それは SenderBase が収集するサンプルには現れません。 統計的な意味をなすにはボリューム レベルが低すぎる場合もあります。 トラフィックのボリュームがどれだけ高くなった場合にスコアの累積を開始するかについてのしきい値はありませんが、現在のメール トラフィックは 1 日あたり約百億件のメッセージと推定されています。 特定の日の上位送信元ホストは、毎日 1,000 万件近くのメッセージを送信していることが考えられます。 この背景に照らし合わせると、1 日に数百件のメールしか送信しないサーバが登録される可能性はほとんどありません。 その IP アドレスに関する苦情がなければ、このアドレスが DNS ベースのいずれかのブラックリス

トに載ることはありません。

> **注:**「none」のスコアは、スコア「0」と同じではありません。 スコア 0.0 は、SenderBase がその送信者に関して収集したポジティブな情報の量とネガティブな情報の量が同じであり、その送信者には中間のレピュテーションが割り当てられたことを意味します。

Web GUI を使用してレピュテーション「none」の送信者を SENDERGROUP に追加するのは、以下のように簡単です。

[Mail Policies] > [HAT Overview] に移動し、[SENDERGROUP] を選択します。 [SUSPECTLIST] > [Edit Settings] に移動して、「none」スコアの送信者をグループに追加するためのチェックボックスをオンにすることが推奨されています。

> **注:** SBRS が「none」の送信者からの接続を拒否またはドロップすることは推奨されません。 極めて冗長性のある SBRS サーバ ファームへの接続を妨げる問題があるとすると、Cisco E メール セキュリティ アプライアンス (ESA) は着信メールのすべてをドロップすることになります。 通常は、メール フロー ポリシーとして ACCEPT または THROTTLE のいずれかを使用してください。

これらの送信者グループは、送信者単位で変更することができます。それには、送信者の IP アドレスをホスト アクセス テーブル (HAT) の送信者グループに追加します。 メッセージ フィルタで SenderBase レピュテーション スコア「none」と一致させる場合、以下のように入力することはできません。

```
"if (reputation == "(?i)none""
```

これは、レピュテーションは数値であり、文字列とは比較できないためです。 ただし、単純なネガティブ フィルタでは「none」が一致します。

```
sbrs_none:
if not (reputation <= 10)
{
insert-header('X-SBRS-none', '$reputation');
}
```

> **注:** SBRS スコアがリスナーで無効にされている場合も、実際にスコアが欠落している場合も、SBRS スコア比較の動作は同じです。 つまり、いずれの場合もデータが欠落します。