NAT の背後で SenderBase は正しく機能しますか

目次

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス（ESA）用のネットワーク アドレス変換（NAT）の背後で動作する SenderBase およびその機能について説明します。

NAT の背後で SenderBase は正しく機能しますか

SenderBase は、SenderBase レピュテーション サービス（SBRS）スコアを IP アドレスに割り当てる IP ベースのレピュテーション サービスです。 SenderBase スコアの範囲は -10 ～ +10 で、これは送信元 IP アドレスがスパムの送信を試みる可能性を表します。 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。

ESA 上の SMTP リスナーは、着信 TCP 接続の IP アドレスに基づく DNS クエリーを使用して SBRS スコア クエリーを実行します。 電子メール アプライアンスに表示される IP アドレスが送信者の「本当の」アドレスであれば、SBRS は期待どおりに機能します。

> **注:** ファイアウォールでソース IP アドレス用に NAT を使用する場合、最初の送信元 IP アドレスを含む新しいメッセージ ヘッダーは挿入されません。 最初の送信元 IP アドレスを含むメッセージ ヘッダーがないと、着信リレーが機能しません。 送信元 IP アドレスのヘッダー情報がない場合、ESA は最初の送信元 IP アドレスを判別できません。

NAT を使用するほとんどの企業は、内部アドレスをインターネットから隠すために（または NAT 機能や NAPT 機能なしで運用するのに十分な数の IP アドレスがないために）これを使用しています。 そのような状況では、外部送信者の IP アドレスが一切変更されないため、SenderBase は正しく機能します。

複雑なネットワーク トポロジを持ついくつかの企業では、自社のネットワーク内部に向けてネットワーク アドレス変換やプロキシ接続を行っています。 そのような状況では SenderBase クエリーが正しく機能せず、着信リスナーでこれを無効にする必要があります。（CLI から **listenerconfig > edit > setup** と入力します。）

アドレスが変換されているかどうか、また接続がプロキシされているかどうかについて疑問がある場合は、単に mail_logs ファイルを検査できます（**tail mail_logs** などの CLI コマンドを使用

）。 これにより、各リスナーへのそれぞれの着信接続が示され、ESA に表示される IP アドレスが一般的なインターネットからのものかどうか素早く確認できます。

> **注:** ESA メール ログで、パブリックまたはインバウンド リスナーへの接続のみを慎重に確認してください。

関連情報

- Cisco 電子メール セキュリティ アプライアンス ユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems