ESA に関する FAQ： メール フロー ポリシーについて

目次

概要

このドキュメントでは、E メール セキュリティ アプライアンス (ESA) のメール フロー ポリシーと、メール フロー ポリシーに関連付けられているアクションについて説明します。

メール フロー ポリシーについて

メール フロー ポリシーでは SMTP カンバセーション中の送信者からリスナーへの電子メール メッセージのフローを制御または制限することができます。 メール フロー ポリシーに次のパラメータ タイプを定義することで SMTP カンバセーションを制御します。

- 接続ごとの最大メッセージ数などの接続パラメータ。
- 1 時間あたりの受信者の最大数など、レート制限パラメータ。
- SMTP カンバセーション中に通信するカスタム SMTP コードと応答を変更します。
- スパム検出の有効化。
- ウイルス保護の有効化。
- TLS を使った SMTP 接続の暗号化などの暗号化。
- DKIM を使った着信メールの確認などの認証パラメータ。

メール フロー ポリシーが、リモート ホストからの接続に対し、次のいずれかのアクションを実行します。

- 承認 (ACCEPT)。 接続が許可された後、電子メールの許可がさらに受信者アクセス テーブル (RAT) (パブリック リスナーの場合) などのリスナーの設定によって制限されます。
- 拒否 (REJECT)。 接続は、最初は許可されますが、接続しようとするクライアントは、4XX または 5XX SMTP のステータス コードを取得します。 どの電子メールも許可されません。

  注: また、SMTP カンバセーションの開始時ではなく、メッセージ受信者レベル (RCPT TO) でこの拒否を実行するように、AsyncOS を設定できます。 この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。 この設定は、CLI の **listenerconfig > setup** コマンドから設定されます。

- TCPREFUSE TCP レベルで接続は拒否されます。
- リレー（RELAY）。 接続は許可されます。 すべての受信者の受信は許可され、RAT で制限されません。
- 継続（CONTINUE）。 ホスト アクセス テーブル（HAT）内のマッピングが無視され、HAT の処理が継続されます。 着信接続が、CONTINUE でない後続のエントリに一致する場合、代わりにそのエントリが使用されます。 CONTINUE ルールは、GUI での HAT の編集を容易にするために使用されます。

メール フロー ポリシーは電子メール パイプラインの先頭に位置しているため、これらのパラメータは、リモート ホストが ESA との接続を確立しようとするときに適用されることに注意してください。

メール フロー ポリシーは、着信/送信メール ポリシーとは異なります。着信/送信メール ポリシーでは、特定のドメイン、電子メール アドレス グループ、または特定の電子メール アドレスが送信元または宛先であるメールに適用するスパム対策、ウイルス対策、ウイルス発生、およびコンテンツ フィルタのパラメータを定義します。

デフォルトのメール フロー ポリシーを変更したり、新しいメール フロー ポリシーを定義したりできます。

パブリック リスナーで定義されている 4 つのデフォルト メール フロー ポリシーを次に示します。

- ACCEPTED
- BLOCKED
- THROTTLED
- TRUSTED

プライベート リスナーは、次のメール フロー ポリシーを使用します。

- ACCEPTED
- BLOCKED
- RELAYED

関連情報

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