目次

[概要](#)
[メール フロー ポリシーとは何か。](#)
[関連情報](#)

概要

メール フロー ポリシーが E メール セキュリティ アプライアンス (ESA) にある、およびメール フロー ポリシーに関連付けられる操作ものがこの資料に記述されています。

メール フロー ポリシーとは何か。

メール フロー ポリシーは SMTP メッセージ交換の間に送信側からのリスナーに電子メール メッセージのフローを制御するか、または制限することを可能にします。 メール フロー ポリシーのパラメータの次の型の定義によって SMTP メッセージ交換を制御します:

- 接続ごとのメッセージの最大数のような接続パラメータ。
- 1 時間あたりの受信者の最大数のようなパラメータを、制限する比率。
- SMTP メッセージ交換の間に伝えられる修正するカスタム SMTP コードおよび応答。
- イネーブル スパム 検出。
- イネーブル ウイルス 保護。
- TLS の SMTP 接続を暗号化するのに使用のような暗号化。
- DKIM の着信メールを確認するのに使用のような認証パラメータ。

メール フロー ポリシーはリモートホストからの接続の次のいずれかの操作を行います:

- 受け入れて下さい。 接続は許可され、電子メール承認は受信者のアクセス 表 (RATS) を含むリスナー設定によってそれからそれ以上の制限されています、行います (公共リスナーのために) 。
- リジェクト。 接続は最初に許可されますが、接続するように試みているクライアントは 4XX または 5XX SMTP ステータス スコードを得ます。 電子メールは受け入れられません。

  注 また SMTP メッセージ交換のはじめによりもむしろメッセージ受信者レベル (RCPT TO) でこの拒絶を、行うために AsyncOS を設定できます。 メッセージを拒否することはこのようにメッセージ拒絶を遅らせ、メッセージを跳ねま、拒否されたメッセージについての詳細な情報を保つように AsyncOS がします。 この設定は CLI **listenerconfig > setup コマンド**から行われます。

- TCPREFUSE. TCP レベルの接続は拒否されます。
- リレー。 接続は許可されます。 あらゆる受信者のための受信は RATS によって許可され、抑制されません。
- 続けて下さい。 ホスト アクセス 表 (帽子) のマッピングは、帽子の処理続きます無視され。 着信接続が続くことではないより遅いエントリと一致すればそのエントリは代りに使用されます。 継続ルールが GUI の帽子の編集を促進するのに使用されています。

留意して下さい、メール フロー ポリシーは電子メール パイプラインの始めにあります、従ってリモートホストが ESA の接続を確立するように試みると同時にこれらのパラメータは適用されます。

メール フロー ポリシーは反スパム、アンチウィルスの、ウイルス発生および郵送するために適用されるべきコンテンツ フィルター パラメーターを受け取られるか、または eメールアドレスの特定のドメイン、グループまたは仕様 eメールアドレスのために予定されて定義しなさい着信 および 発信メール ポリシーと異なります。

デフォルト メール フロー ポリシーは修正し、新しいメール フロー ポリシーは定義することができます。

公共リスナーで定義される 4 つのデフォルト メール フロー ポリシーがあります:

- 承諾
- BLOCKED
- 絞られる
- 信頼される

私用リスナーは次のメール フロー ポリシーを使用します:

- 承諾
- BLOCKED
- 中継で送られる

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