メールフローポリシーおよび宛先制御に関連するパラメータについて

内容

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)の設定について、送信者をスロットル/レート制限し、配信する方法について説明します。この記事で説明する機能は、メールフローポリシーと宛先制御です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- メールフローポリシーと宛先制御の基本的な理解
- ESAの設定でこれらの機能を使用する知識

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの

ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

メールフローポリシーと宛先制御の利点

これらの機能とレート制限/スロットリングの両方で非常に重要な機能が1つあります。この側面により、管理者は、どのトラフィックをフリーフローし、どのトラフィックを制限で許可するかを制御できます。

メールフローポリシー

これらは、どの電子メールトラフィック変調が行われるかに基づいて、ESAの送信者グループに適用されるポリシーです。

メールフローポリシーは、電子メールが着信または発信であるかどうかに関係なく、常にESAに着信するトラフィックに適用されます。

メールフローポリシーは、そのポリシーに対して選択された接続動作に関してバックエンドで動作します。ESAで使用できるさまざまな接続動作は次のとおりです。

1. Accept
2. [Reject]
3. リレー
4. TCP拒否
5. [Continue]

Accept:接続が受け入れられ、電子メールの受け入れは、受信者アクセステーブル（パブリックリスナー用）などのリスナー設定によってさらに制限されます。 この接続動作では、電子メールは着信メールとして扱われます

Reject：接続しようとしているクライアントは、4XXまたは5XX SMTP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。これは主にブラックリストの送信者に使用されます

リレー:接続は許可されます。任意の受信者に対する受信が許可され、受信者アクセステーブルによって制限されません。これにより、電子メールがアウトバウンドとして処理されます

TCP拒否：TCP レベルで接続は拒否されます。

Continue:HATのマッピングは無視され、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のコンポーネント

最大接続ごとのメッセージ：リモートホストからの接続ごとに、このリスナーを介して送信できるメッセージの最大数。各ICIDは1つの接続を示します

最大メッセージごとの受信者：このメールフローポリシーを使用して処理された、このホストから受け入れられるメッセージごとの受信者の最大数

最大メッセージサイズ：メールフローポリシーにタグ付けされたこのリスナーによって受け入れられるメッセージの最大サイズ。メッセージの最大サイズの最小値は1キロバイトです。

最大単一IPからの同時接続：1つのIPアドレスからこのリスナーへの接続を許可された同時接続の最大数。

カスタム SMTP バナー コード:このリスナーとの接続が確立されたときに返される SMTP コード。

カスタムSMTPバナーテキスト：このリスナーとの接続が確立されたときに返される SMTP バナー テキスト。このフィールドでは、いくつかの変数を使用できます。

[SMTPバナーホスト名の上書き(Override SMTP Banner Hostname)]：デフォルトでは、リモートホストにSMTPバナーを表示するときに、リスナーのインターフェイスに関連付けられたホスト名がアプライアンスに含まれます（220-hostname ESMTPなど）。 このバナーを上書きするには、ここで別のホスト名を入力します。また、hostnameフィールドを空白のままにして、バナーにホスト名を表示*しない*ことを選択することもできます。

メールフローの制限

最大1時間あたりの受信者：このリスナーがリモートホストから受信する1時間あたりの最大受信者数。送信者のIPアドレスあたりの受信者数は、グローバルに追跡されます。各リスナーは独自のレート制限しきい値を追跡しますが、すべてのリスナーが1つのカウンタに対して検証するため、同じIPアドレス（送信者）が複数のリスナーに接続している場合は、レート制限を超える可能性が高くなります。このフィールドでは、いくつかの変数を使用できます。

最大1時間あたりの受信者コード：ホストがこのリスナーに定義されている1時間あたりの最大受信者数を超えたときに返されるSMTPコードです。

最大1時間あたりの受信者テキスト：ホストが、このリスナーに定義されている1時間あたりの最大受信者数を超えたときに返されるSMTPバナーテキスト。

エンベロープ送信者のレート制限

最大時間間隔ごとの受信者：指定した期間内に、このリスナーが一意のエンベロープ送信者から受信する受信者の最大数（メール送信者アドレスに基づく）。受信者の数はグローバルに追跡されます。各リスナーは、独自のレート制限しきい値を追跡します。ただし、すべてのリスナーが1つのカウンタに対して検証を行うため、同じmail-fromアドレスからのメッセージが複数のリスナーで受信される場合は、レート制限を超える可能性が高くなります。

送信者レート制限エラーコード：エンベロープが、このリスナーに定義された時間間隔で受信者の最大数を超えたときに返されるSMTPコード。

送信者速度制限のエラーテキスト：エンベロープ送信者が、このリスナーに定義された時間間隔で受信者の最大数を超えたときに返されるSMTPバナーテキスト。

例外： 特定のエンベロープ送信者を定義されたレート制限から除外する場合は、エンベロープ送信者を含むアドレス一覧を選択します。

アドレスリストは、メールポリシーからアドレスリストに定義されます（完全な電子メールアドレス、ドメイン、IPアドレスを除外に使用できます）

フロー制御にSenderBaseを使用：このリスナーのSenderBaseレピュテーションサービスへの「ルックアップ」を有効にします。

IPアドレスの類似性によるグループ：リスナーのホストアクセステーブル(HAT)のエントリを大きなCIDRブロックで管理しながら、着信メールをIPアドレスごとに追跡およびレート制限するために使用されます。レート制限の目的で類似のIPアドレスをグループ化し、その範囲内の各IPアドレスの個々のカウンタを維持する重要なビットの範囲(0 ~ 32)を定義します。

注：[SenderBaseの使用]を無効にする必要があります。

Directory Harvest Attack Prevention(DHAP)

最大1時間あたりの無効な受信者：このリスナーがリモートホストから受信する1時間あたりの無効な受信者の最大数。こののしきい値は、RAT拒否およびSMTP前方参照サーバー拒否の合計数と、SMTPカンバセーションでドロップまたは作業キューでバウンスされた無効なLDAP受信者へのメッセージの合計数を表します（関連付けられたリスナーのLDAP受信設定で設定）。

SMTPカンバセーション内でDHAPしきい値に達した場合の接続のドロップ：

無効な受信者のしきい値に達すると、アプライアンスはホストへの接続をドロップします。

最大無効な受信者/時間コード：接続をドロップするときに使用するコードを指定します。デフォルトコードは550です。

最大1時間あたりの無効な受信者テキスト：ドロップされた接続に使用するテキストを指定します。デフォルトのテキストは「無効な受信者が多すぎます。

セキュリティ機能

スパム/AMP/ウイルス/送信者ドメインレピュテーション検証/アウトブレイクフィルタ/高度なフィッシング保護/グレイメール/コンテンツ&メッセージフィルタ：セキュリティエンジン/スキャンおよびフィルタに関連するスキャンは、ここから有効または無効にできます

暗号化と認証：このリスナーのSMTPカンバセーションで、設定をOff、Prefer、またはRequire Transport Layer Security(TLS)に変更できます。

[クライアント証明書の確認(Verify Client Certificate)]オプションは、クライアント証明書が有効な場合に、電子メールセキュリティアプライアンスがユーザのメールアプリケーションへのTLS接続を確立するように指示します。

TLS優先の場合は、ユーザが証明書を持っていない場合はアプライアンスで非TLS接続が許可されますが、ユーザに無効な証明書がある場合は接続が拒否されます。

[TLS Required]設定で、このオプションを選択すると、アプライアンスが接続を許可するために、ユーザが有効な証明書を持っている必要があります。

SMTP認証：リスナーに接続しているリモートホストからのSMTP認証を許可、禁止、または要求

する

TLSとSMTPの両方の認証が有効になっている場合（デフォルト）:SMTP認証を提供するためにTLSが必要

ドメインキー/DKIM署名：このリスナーでドメインキーまたはDKIM署名を有効にする

DKIM検証：DKIM検証を有効にします。

S/MIME復号化/検証：S/MIME復号化または検証を有効にします。

処理後の署名：S/MIME検証後にデジタル署名を保持するか、メッセージから削除するかを選択します。

S/MIME公開キーの収集：S/MIME公開キーの収集を有効にします。

検証失敗時の証明書の取得：受信署名メッセージの検証が失敗した場合に公開キーを取得するかどうかを選択します。

更新された証明書の保存：更新された公開キーを取得するかどうかを選択します

SPF/SIDFの検証： このリスナーでSPF/SIDF署名を有効にします。

準拠レベル：SPF/SIDF準拠レベルを設定します。SPF、SIDF、またはSIDF互換から選択できます

「Resent-Sender:」または「Resent-From:」を使用した場合のPRA検証結果をダウングレードします。SIDF互換の準拠レベルを選択する場合、Resent-Senderが存在する場合は、PRA ID検証のPass resultをNoneにダウングレードするかどうかを設定します。ダウングレードするメッセージ内のヘッダー

HELOテスト：HELO IDに対してテストを実行するかどうかを設定します（SPFおよびSIDF互換の準拠レベルに使用します）

DMARCの検証：このリスナーでDMARC検証を有効にする

DMARC検証プロファイルの使用：このリスナーで使用するDMARC検証プロファイルを選択します。同じことが[Mail Policies] —> [DMARC] —> [Add Profile]から作成されます

DMARCフィードバックレポート：DMARC集約フィードバックレポートの送信を有効にします。

バウンス検証

タグなしバウンスを有効にすることを検討してください。バウンス検証タギングが有効になっている場合にのみ適用されます。デフォルトでは、アプライアンスはタグなしバウンスを無効と見なし、バウンス検証の設定に応じて、バウンスを拒否するか、カスタムヘッダーを追加します。タグなしバウンスを有効にすることを選択した場合、アプライアンスはバウンスメッセージを受け入れます。

送信者の確認

エンベロープ送信者のDNS検証：

送信者は、さまざまな理由で未検証にすることができます。未検証の送信者は、次のカテゴリに分類されます。

- 接続ホストのPTRレコードがDNSに存在しません。
- 一時的なDNS障害により、接続ホストのPTRレコードのルックアップが失敗します。
- 接続ホストの逆DNSルックアップ(PTR)が前方DNSルックアップ(A)と一致しません。

送信者検証機能を有効または無効にできます。

送信者確認例外テーブルの使用：送信者検証ドメイン例外テーブルを使用して、除外を許可できます。例外テーブルは1つしかありませんが、メールフローポリシーごとに有効にできます。

例外テーブルは、[Mail Policies] —> [Sender Verification Exception Table] —> [Add Sender Verification Exception]から作成できます

送信先コントロール

これは、電子メールの配信を制御する機能です。ESA経由で処理を終了し、さらに配信するためにESAを終了しようとするすべての電子メールは、宛先制御機能で制御できます。

デフォルトの**宛先管**理プロファイルは、すべての搬送に適用されます。ドメイン固有の配信制御が必要な場合は、カスタマイズされた宛先制御プロファイルを作成する必要があります。

宛先制御プロファイルのコンポーネント

Limits

同時接続：アプライアンスが配信を完了するために開こうとするリモートホストへの同時接続数(DCID)。

接続ごとの最大メッセージ数：アプライアンスが新しい接続を開始する前に、ESAが接続(DCID)経由で宛先ドメインに送信するメッセージの数。

受信者：特定の時間内にアプライアンスが特定のリモートホストに送信する受信者数。

制限の適用：この側面は、宛先ごとに、およびMGAホスト名ごとに指定した制限を適用する方法を決定するのに役立ちます。

TLSサポート

これは、リモートホストへのTLS接続を[なし(None)]、[優先(Preferred)]、[必須(Required)]に設定するかどうかを決定するのに役立ちます

DANEサポート：DANEを「Opportunistic」として設定し、リモートホストがDANEをサポートしない場合は、SMTP通信の暗号化にOpportunistic TLSが推奨されます。

DANEを[Mandatory]として設定し、リモートホストがDANEをサポートしない場合、宛先ホストへの接続は確立されません。

DANEを[Mandatory]または[Opportunistic]に設定し、リモートホストがDANEをサポートしている場合は、SMTP通信の暗号化に適しています。

注：DANEは、SMTPルートが設定されているドメインには適用されません。

バウンス検証

これは、バウンス検証を介してエンベロープ送信者アドレスタギング(prvs-xxxxxx-xxxx)を実行するかどうかを決定するのに役立ちます。

バウンス検証は、[Mail Policies] —> [Bounce Verification] —> [Add New Key]から設定できます

バウンスプロファイル

バウンスプロファイルは、特定のリモートホストのアプライアンスで使用できます。このコマンドは、電子メールのハードバウンスの前に、配信の問題がある場合にESAの配信キューに電子メールを保持する時間を決定します

バウンスプロファイルは、[Network] —> [Bounce Profiles]で設定します

グローバル設定

証明書:これは、ネクストホップへの電子メール配信を開始するときにSSL/TLS接続を確立するときに使用する証明書を定義する点です。この側面では、必ず認証局(CA)署名付き証明書を使用することをお勧めします。

必要なTLS接続が失敗した場合にアラートを送信：TLS接続が必要なドメインへのメッセージの配信時にTLSネゴシエーションが失敗した場合にアプライアンスがアラートを送信するかどうかを指定できます。アラートメッセージには、失敗したTLSネゴシエーションの宛先ドメインの名前が含まれています。アプライアンスは、システムアラートタイプの警告の重大度レベルのアラートを受信するように設定されたすべての受信者に**アラートメ**ッセージを送信する**ように設定**します。

[System Administration] —> [Alerts]でアラート受信者を管理できます