ESA での一般的な設定エラー

目次

はじめに
ESA での一般的な設定エラーにはどのようなものがありますか。
1. HAT
2. ポリシー
3. 着信リレー
4. DNS
5. メッセージ フィルタとコンテンツ フィルタ
7. オープン リレーの防止
関連情報

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) での一般的な設定エラーについて説明します。

ESA での一般的な設定エラーにはどのようなものがありますか。

新しい評価版をセットアップする場合でも、既存の設定を確認する場合でも、次に示すチェックリストで一般的な設定ミスを確認できます。

1. HAT

- 正の値の SBRS スコア (+5 または +7 など) を WHITELIST に追加しないでください。 9.0 ~ 10.0 は OK ですが、これよりも低いスコアを追加すると、スパムが通過する可能性が高くなります。

- UNKNOWNLIST、Envelope Sender DNS Verification および Connecting Host DNS Verification は、これらの機能が実際に必要であり、これらの機能について理解している場合を除き、無効にしてください。

- 各メール フロー ポリシーでメッセージ サイズやその他のポリシー設定を変更する代わりに、[Mail Flow Policy] メニューに移動し、最後のオプション [Default Policy Parameters] を選択します。

- ほとんどの送信者の場合、最大接続数を 3 に制限し、この値を新しいメール フロー ポリシーのデフォルトにします。

- SenderBase スコア -10.0 ~ -2.0 が BLACKLIST に含まれていることを確認します。 資料とセットアップ ウィザードの説明は非常に控えめです。 現時点では、この範囲での誤検出はありません。

2. ポリシー

- ポリシーの名前は、ポリシーの処理内容ではなく、ポリシーの対象に基づいて指定します。コンテンツ フィルタの名前は、フィルタの処理内容に基づいて指定します。また、省略形を使用します（例：Q_basic_attachments、D_spoofers、Strip_Multi-Media など。この場合 Q は検疫（quarantine）、D はドロップ（drop）を意味します）。

- 特殊な設定が実際に必要ではない限り、デフォルト以外のポリシーでは、[Anti-Spam]、[Anit-Virus]、[Content Filters]、および [Outbreak Filters] で [Use Default Settings] を選択してください。 これらの設定が必要ではない場合は、各ポリシーでこれらの設定を再作成しないでください。

- [Drop infected attachments] をオフにしてください。オフにしないと、ウィルスが除去された空白の電子メールが多数送信されることになります。

- アウトバウンドの [Anti-Virus] の設定は、受信者ではなく送信者を通知するようにします。

- アウトバウンドでは [Outbreak Filters] と [Anti-Spam] を無効にしてください。

3. 着信リレー

[Monitor] > [Overview] に、各自のサーバとドメインからの接続が表示される場合は、これらの接続を [Incoming Relays] の設定に追加する必要があります。 非常によくある誤りとして、GUI を使用している場合に、テーブルにエントリを追加しただけで、[Incoming Relay] 機能を有効にしたと思い込むことがあります。 さらに、

- 報告の目的で、WHITELIST の上に、それらの機能の特殊な HAT 送信者グループを追加します。 レート制限なしまたは DHAP を選択してください。ただし、スパムおよびウィルス検出は適切です。

- BLACKLIST ポリシー アクションに一致するメッセージ フィルタを追加します。 次に、例を示します。

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

電子メールを再注入するという稀な状況（例：インバウンド メール ポリシーによるサブスクライバ間メールの再処理）では、フィルタで再注入インターフェイスを除外する必要があります。 通常は必要ありません。

4. DNS

多くの顧客は、通常の動作から逸脱し、ESA に内部 DNS サーバの照会を強制的に行わせます。 ほとんどのインストール環境では、必要となる DNS レコードはすべて、内部 DNS ではなくインターネット上に存在します。 このためインターネット ルート サーバを照会し、内部 DNS での転送に伴う負荷を減らす方が適切です。

5. メッセージ フィルタとコンテンツ フィルタ

最もよくあるエラーとして、コンテンツ フィルタに、不要な一致条件を設定することがあります。 ほとんどのフィルタでは何らかのアクションを指定する必要がありますが、条件が空白になっているというものです。 このようなフィルタは常に *true* となり、常に実行されます。 これらのアクションを受け取るユーザ/ポリシーを制御するため、必要に応じて新しい着信メール ポリシーまたは送信メール ポリシーを作成し、このフィルタをポリシーに適用します。 正しい例と誤った例を次に示します。

- ほとんどの場合、メッセージ フィルタで rcpt-to 条件を使用することは正しくありません。 正しい手順は、着信コンテンツ フィルタを作成し、このフィルタを特定のユーザ向けにするため受信者ベースの着信メール ポリシーを追加するという手順です。

- ほとんどの場合、コンテンツ フィルタを使用して添付ファイルの有無を確認し、添付ファイルを削除するという操作は正しくありません。 正しい手順は、添付ファイルの有無を確認せずに、添付ファイルを常に削除することです。

- ほとんどの場合、deliver() を使用することは正しくありません。 deliver では、残りのフィルタすべてがスキップされた後に配信が行われます。 残りのフィルタをスキップせずに配信を行う場合は、明示的なアクションは不要です（暗黙の配信）。

7. オープン リレーの防止

一部のサービスは、オープン リレー状態を発生させる可能性があるアドレスをメッセージ転送エージェント（MTA）が受け入れるかどうかを確認します。 MTA でオープン リレーが機能するままにしておくことは適切ではないため、ユーザが SMTP 変換でこのような危険なアドレスを拒否しない限り、これらのサイトではユーザがブラックリストに追加されます。

報告の目的で、WHITELIST の上に、それらの機能の特殊な HAT 送信者グループを追加します。 レート制限なしまたは DHAP を選択しますが、スパムおよびウィルス検出は有効にします。

- [Strict Address Parsing] に変更します（デフォルトは [Loose]）。 これは、アドレスの 2 つの @ 記号を防ぐために必要です。

- 無効な文字を拒否します（ストリップしません）。 これもまた、アドレスの 2 つの @ 記号を防ぐために必要です。

- リテラルを拒否し（受け入れない）、次の文字を入力します。 *%! \\/?

関連情報

- テクニカル サポートとドキュメント – Cisco Systems