目次

概要

この資料は E メール セキュリティ アプライアンス (ESA) の一般的 な 設定 エラーを記述したものです。

ESA の一般的 な 設定 エラーとは何か。

新しい評価を設定するか、または現在のコンフィギュレーションに検知 して いるかどうか、一般的 な 設定誤りのこのチェックリストを参照できます。

1. 帽子

- ホワイトリストに +5 か +7 のような肯定的な SBRS スコアを入れないで下さい。 9.0-10.0 の範囲は良いですが、スパムが通過することだけより低いスコアを含むことはそれの可能性を高くします。

- 実際にこれらを必要とし、理解したら UNKNOWNLIST、エンベロープ 送信側 DNS 確認およびホスト DNS 確認の接続をディセーブルにして下さい。

- 各メール フロー ポリシーの変更メッセージサイズおよび他のポリシー設定の代りに、行き、最後 の オプションを、「デフォルトポリシー パラメータ」はメール フロー Policies メニューに選択します。

- 最大接続をほとんどの送信側用の 3 に制限し、これに新しいメール フロー ポリシーのためのデフォルトをして下さい。

- -10.0 から -2.0 まで SenderBase スコアがブラックリストに含まれていることを確認して下さい。 ドキュメントおよびセットアップ ウィザードは過度に保守的です; この範囲で現在

false positive がありません。

2. ポリシー

- 何をだれがの後のそれらを得るかネーム ポリシー、ない。 する名付け、Q_basic_attachments のような省略形を、D_spoofers、検疫および D はドロップするを意味することを Q が意味する Strip_Multi-Media 使用して下さいことをの名にちなんでコンテンツ フィルターを。

- 実際に特別な設定を必要とするところもし「反スパム、Anit ウイルス、コンテンツ フィルターおよび発生フィルター用にデフォルト設定」を以外使用すればデフォルト以外のポリシー。 それが必要ではない場合各ポリシーのそれらの設定を作り直さないで下さい。

- Untick 「ドロップする添付ファイル」を感染させましたさもないとウイルスが除去された多くの本文 の ない 電子メールを渡します。

- 発信のアンチウィルス設定はない受信者送信側を知らせる必要があります

- 発生フィルターおよび反スパムは発信でディセーブルにする必要があります

3. 着信中継

「モニタ > 外観」があなた自身のサーバおよびドメインからの接続を表示する場合、着信中継セットアップにそれらを追加する必要があります。 非常によくある 間違いは、GUI を使用するとき、終了したのが表に追加する エントリをだけあるとき着信 リレー機能を有効に したと考えることです。 さらに、

- それらのための特別な帽子送信側 グループを、ホワイトリストの上で、報告目的のために追加して下さい。 比率制限するか、または DHAP を『No』 を選択 して下さい、しかし無差別に送信すればウイルス 検出は良いです。

- ブラックリスト ポリシー アクションを一致するためにメッセージ フィルターを追加して下さい。 次に、例を示します。

まれに E メールを再挿入しているところで (たとえば、相互サブスクライバ メールを受信 メール ポリシーによって再処理します) 、フィルタはまた reinjection インターフェイスを免除する必要があります。 通常これは必要ではないです。

4. DNS

多くの顧客は習慣から内部DNSサーバを問い合わせるために ESA を強制します。 ほとんどのインストールでは、必要とする DNS レコードの 100% はのインターネットに、ない内部 DNS あります。 それは内部 DNS のフォワーディング ロードを減らしているインターネット ルート サーバを問い合わせるより多くの理にかなっています。

5. メッセージおよびコンテンツ フィルター

もっとも一般的な エラーはそれらが必要とならないコンテンツ フィルターに一致する条件を置くことです。 ほとんどのフィルターはいくつかの操作をリストする必要があります条件は空白のままにする必要があります。 フィルタは常に本当常にで、動作します。 ユーザ/ポリシーが必要に応じて新しい着信か発信 メール ポリシーの作成によって受け取る、およびこれらの操作を制御しまこのフィルタをポリシーに適用します。 不正確で、正しい例はここにあります:

- それはほとんどの場合メッセージ フィルターで条件 rcpt に使用するエラーです。 正しいプロシージャは着信コンテンツ フィルタを書くこと受信者ベースの着信メール ポリシーの追加によって特定のユーザ向けに特定にします。

- それはほとんどの場合添付ファイルの存在のためのコンテンツ フィルタ テストを持つエラーでそして添付ファイルを廃棄します。 正しい方式は存在のためにテストしないでその添付ファイルを、常に廃棄することです。

- それはほとんどの場合 deliver() を使用するエラーです。 意味しますスキップしましたり残りのフィルターを、そして渡します渡して下さい。 フィルターの他をスキップしないでちょうど渡したいと思う場合明示的 な操作が必要となりません（意味される渡して下さい）。

7. リレー防止を開いて下さい

いくつかのサービスは Message Transfer Agent（MTA がことを）開いたリレー状態という結果に可能性としては終る可能性があるアドレスを受け入れればかどうか確認します。 機能開いたリレーとして MTA を残すことが悪いので、これらのサイトはブラックリストに SMTP メッセージ交換のこれらの危ないアドレスを拒否しなければ追加するかもしれません。

それらのための特別な帽子送信側 グループを、ホワイトリストの上で、報告目的のために追加して下さい。 比率制限するか、または DHAP を『No』 を選択 して下さい、しかしスパムおよびウイルス 検出を許可して下さい。

- 厳密なアドレスに解析を変更して下さい（デフォルトは緩くあります）。 これは倍を防いで必要@署名しますアドレスにです。

- リジェクト（ないストリップ）無効の文字列。 これは倍を防いでまた必要@署名しますアドレスにです。

- （受け入れないため）リテラルを拒否し、次の文字を入力して下さい: *%! \ \/か。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems