Cisco E メール セキュリティ アプライアンス（ESA）の Anti-Spam の効果性チェックリスト

目次

次の手順および推奨事項は ESA によって得るスパムの量を減らすための「最良の方法」です。各顧客が異なっていること、そしていくつかのこれらの推奨事項がスパム（false positive）として分類される正規のメールの数を増加するかもしれないことに注目して下さい。

基本的な設定

1. 反スパムがつくことを確かめて下さい:

   MX レコード（を含む低優先順位） MX レコードがすべて ESA によってメールを中継で送っていることを確認して下さい。有効な反スパム フィーチャーキーを持つために機器を確かめて下さい。反スパムをすべての適切な着信メール ポリシーのためにイネーブルになっています確認して下さい。

2. 反スパム ルール更新を受信していることを確認して下さい。 セキュリティ サービス > 反スパムの下の更新のための**最新**タイムスタンプが最後の 2 時間内からであることを確認するためにチェックして下さい。

3. メッセージが反スパムによってスキャンされていることを確かめて下さい:

   次のヘッダがあるように抜けていたスパム メッセージのサンプルを確認して下さい: X IronPort 反スパム結果:そのヘッダが抜けていれば:

   スパム スキャン（下記参照）をバイパスしますスパムはホワイトリスト エントリかフィルターによりないことをチェックして下さい。最大メッセージ スキャン サイズを超過するのでメッセージがスキャンをバイパスしていないことを確認して下さい（デフォルトは 262144 バイトです）。 この設定を減らすことはパフォーマンスを大幅に改善しないし、抜けていた SPAM という結果に終る場合があります。 評価の間に、IPAS 設定がテストされる他の製品同じであることを確かめることもまた重要です。通過し、ことをすべての受信メール フロー ポリシーのための「spam_check=on」は各帽子エントリを確認します。 デフォルトに「spam_check= の」があり、メール フロー ポリシーのどれも明示的にそれを消さない限り、これは正しく設定されます。 TRUSTED/WHITELIST 設定に特別な注意を注意して下さい。 多くの場合顧客を不注意に追加しますスパムを転送する転送して、ホワイトリスト送信側グループにメールを正当化するパートナーまたは ISP のドメインの追加によってスパ

ムを-たとえば、ホワイトリストに送信側を時間を計ります。

「スキップしspamcheck なさい」フィルターがないことを確かめるためにメッセージ フィルターを通して素早いチェックをして下さい。 ある場合、それらがしていることを確かめて下さいによってべきであるものを (一致することができます rcpt に単一と一致するそれに留意することは 30+ 受信者が付いているメッセージで)。

最近の SPAM 例 (時間、日付、rcpt、等) を見つけ、何が起こったか見るために mail_logs を参照して下さい。 反スパムが否定的な評決を戻したことを確認して下さい。

4. スパム陽性メッセージの望ましい アクションを奪取 して いることを確かめて下さい。 反スパム評決がどのようにがあるように処理されるか受信メール ポリシーを確認して下さい。 こと SPAM がデフォルトポリシーで肯定的で、疑わしいメッセージ、廃棄されるか、または検疫されることを確かめればデフォルトを無効にしなさいことを他のポリシーがすべてデフォルトの動作を使用したりまたは慎重に。

5. false positive が抜けていたスパムより問題のより少しである場合より積極的なスパムしきい値を加えて下さい:

   80 に肯定的なスパムしきい値を減らして下さい (デフォルトは 90) false positive が「一定の」しきい値に問題ではない場合です。

   疑いました 40 にスパムしきい値を減らして下さい (デフォルトは 50) false positive が「疑わしい」しきい値に問題ではない場合です。

   スパム不平のほとんどが受信者のサブセットから来る場合、より低いスパムしきい値でちょうどこれらの受信者のためにより積極的にフィルタリングするためにこれらのユーザ向けの別途のメール ポリシーを作成できます。

   これらの値への変更はハード データなしで制定する必要があります repurcussive 効果があるもの確認するために軽く 奪取 するべきではありません。

   また、必ずしも False positive しか避けないために他の方向の値を調節して下さい。False positive および偽陰性が TAC に入ることを確かめて下さい。

6. SBRS 設定および帽子ポリシーを最適化して下さい:

   ほとんどの組織はブラックリストへの快適な追加 SBRS -10 に -3.0 および SUSPECTLIST への SBRS -3.0 に 1.0 です。 より積極的な顧客は SBRS -10 に -2.0 をブラックリストに載せ、SUSPECTLIST に -2.0 から -0.6 を追加できます。

   場合によっては、送信側にまだ SenderBase 評判スコアがあっていないというファクトはこの送信側がスパムの発信者であるかもしれないという証拠です。 「絞られた」ポリシーを得る送信側グループに疑わしい送信側グループに SBRS を「どれも」直接、たとえば追加できません。

   「絞られた」ポリシーのための 5 に 1 時間あたりの受信者の最大数を変更して下さい。

作成する Consider 複数時間制限ごとの別の受信者を実施するためにポリシーを「絞りました」-たとえば時間毎に -2 人および -1 人から 5 人の受信者と時間毎に -1 人および 0 人から 20 人の受信者間の SBRS の送信側間の SBRS の送信側を制限することを評価して下さい。

7. Mailflow 「絞られた」ポリシーの送信側確認を有効に して下さい:

   顧客は SUSPECTLIST 送信側グループに非存在か不適当に設定された DNS の送信側を追加することを希望することができます。

   ホスト PTR レコードを接続することは DNS にありません。ホスト PTR を接続することはルックアップを失敗します一時 DNS 失敗が原因で記録します。

   ホスト リバース DNS ルックアップ（PTR）を接続することは前方 DNS lookup （a）を一致する。

   原因メッセージは拒否されることを示すカスタム 4xx 応答を返す不適切に設定された DNS の送信側からの false positive リスクがあります、従って顧客は Mailflow 別途のポリシーを設定したいと思う場合もあります。

   送信側確認に関するあるように AsyncOS オンライン ヘルプかユーザガイドを確認して下さい

8. イネーブル LDAP は不正侵入保護受け入れ、ディレクトリ収穫:

   多くのスパムの発信者はそうまた無効な受信者にスパムを減少できる送信 する送信側をブロックする高頻度の無効アドレスにメールを、送信 します。

   ディレクトリはまた IP ごとに 5 と 10 間の最大不正な試みで各々の受信リスナー用に収穫保護（DHAP）設定されることを LDAP が既にあっていれば、確かめれば受け入れれば。

9. イネーブル コンテンツ辞書:

   ESA は 2 冊のコンテンツ辞書が付いています: profanity.txt および sexual_content.txt。 これらの辞書を使用しながらが false positive を生成するかもしれない何人かの顧客は不適当なワードのためのメール ストリームをフィルタリングすることが「間違ったメール」を得ている「間違った人」のリスクを軽減するかもしれないことが分りました。 これらのフィルターは「ピカピカのホイール」に仕様メール ポリシーのユーザのグループのためにそれらをイネーブルにすることによって加えられるだけかもしれません。

10. Cisco TAC に誤って分類されたメッセージを報告して下さい。

11. 多数の false positive を防ぐために、SBRS は送信スキャンのために無効であるはずです。これは着信 IPS の、および内部ネットワークの評判の SBRS 外観が、これらの IPS のほとんどダイナミックであるという理由によります。 次の セクションのステップに従って下さい。

SBNP を有効に して下さい

1. 受信および送信メールを別々のリスナーにありなさいことを確かめて下さい。

2. 下記にごとの送信メールのための SenderBase ルックアップを無効に して下さい。 これを GUI からし、ネットワーク > リスナーに行き、送信リスナーを選択し、ボックスをチェックを外すため「プロファイルする」使用 SenderBase IP の隣で"Advanced"を 選択する。

   SenderBase ネットワーク参加 (SBNP) は評判フィルター、反スパムおよびウイルス発生フィルターの効果を大幅に高めることができます。 反スパムを使用するときイネーブルになったないし、非常にセキュア SBNP にまた顕著なパフォーマンス影響がです。

組織が受け取るスパムの音量が一定時間にわたり変更することに注目して下さい。 より多くのスパムが以前よりより多くのスパムを受け取っているというファクトによる ESA によって単に得ていることは可能性のあるです。 によって着信メール概要ページを検知 し、「立寄られた評判フィルタリング」および「スパム メッセージによって検出される」一般 品目を追加することこの動作を一定時間にわたりトラッキングできます。

SBRS 理論的根拠

False positive との大きい問題は重要なメールが失われて得る可能性があることです。 このコンテキストでは、SPAM 肯定的なメールを検疫するか、または廃棄することの推奨事項は問題となります。 正規のメールが検疫かスパム フォルダに送信 される場合、予防的な検索が入るように要求し、ハムがスパムとして誤って分類されたこと「注意して下さい」。

それに対して送信側がすぐに知らせられるように、ブラックリストおよびレートリミットされたメールはブロックされます。 この送信側がスパムの発信者ではない場合、彼らは多分あなたが付いている連絡先を作る別の方法を見つけ出します。 実際、デフォルトでブロックし、次に信頼されたパートナーを要求あり次第受け入れることはオーバーオール ポリシーとしていくつかのビジネスのためのよりよい位置です。

スロットリングは、場合きちんと設定された、影響が組めばがまれにべきでなかったり、提供しますウイルスに感染させて得るドメインからの保護を。 スロットリングはまたスパムの発信者に不快です。 多数の IP を購入するスパムの発信者手法に気づいていましたり適当な SBRS スコアを得、次に無差別に送信し始めるように十分な good メールを生成します。 より大きく疑わしいリスト範囲は制限しますするにより結局それらはドメインにスパムを送信 することを止めますかもしれません被害をこれらをつかまえる必要があり。