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

内容

概要

次に示す手順と推奨事項は、ESA を通過するスパムの量を減らすための「ベスト プラクティス」です。お客様ごとに違いがあり、ここに示す推奨事項にはスパムとして分類される正当な電子メール（誤検出）の数を増やすおそれがある点に注意してください。

基本的な設定

1. アンチスパムがオンになっていることを確認します。

   すべてのMXレコード（優先順位の低いレコードを含む）がESA経由でメールを中継していることを確認します。アプライアンスに有効なアンチスパム機能キーがあることを確認します。すべての適切な受信メールポリシーでスパム対策が有効になっていることを確認します。

2. スパム対策ルールの更新を受信していることを確認します。[セキュリティサービス] > [スパム対策]**の下の更新に対**する最新のタイムスタンプが過去2時間以内のものであることを確認します。

3. メッセージがアンチスパムによってスキャンされていることを確認します。

   次のヘッダーのスパムメッセージのサンプルを確認します。X-Ironport-Anti-Spam-Result:そのヘッダーがない場合：

   スパムがスパムスキャンをバイパスする許可リストのエントリまたはフィルタがないことを確認します（下記参照）。メッセージが最大メッセージスキャンサイズ（デフォルトは262144バイト）を超えているため、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ます。 この設定を減らしても、パフォーマンスは大幅に向上せず、SPAMの損失が発生する可能性があります。評価中は、IPAS設定がテスト対象の他の製品と同じであることを確認することも重要です。各HATエントリを確認し、すべての着信メールフローポリシーについて「spam_check=on」であることを確認します。デフォルトが「spam_check= on」で、明示的にオフにするメールフローポリシーがない限り、これは正しく設定されます。TRUSTED/allowLIST設定に特に注意してください。スパムを転送している許可リストに誤って送信者を追加するケースが多くあります。たとえば、スパムと正当な電子メールの両方をallowLIST送信者グループに転送するISPまたはパートナーのドメインを追加します。

メッセージフィルタを調べて、「skip-spamcheck」のフィルタがないことを確認します。メッセージが存在する場合は、メッセージが必要な処理を行っていることを確認します（30人以上の受信者とのメッセージで1つのrcpt-toを照合することは可能です）。

最近のSPAMの例（時刻、日付、rcptなど）を見つけ、mail_logsを参照して何が起こったかを確認します。アンチスパムが否定判定を返したことを確認します。

4. 迷惑メールの肯定的なメッセージに対して必要なアクションを実行していることを確認します。アンチスパム判定の処理方法については、インバウンドメールポリシーを確認してください。SPAM positiveメッセージとsuspectメッセージがデフォルトポリシーでドロップまたは隔離され、他のすべてのポリシーがデフォルト動作を使用するか、意図的にデフォルトを上書きすることを確認します。

5. 誤検出がスパムの見逃しよりも少ない場合は、よりアグレッシブなスパムしきい値を適用します。

   「特定」のしきい値でfalse-positiveが問題にならない場合は、Positive Spam Thresholdを80（デフォルトは90）に減らします。

   「疑わしい」しきい値でfalse-positiveが問題にならない場合は、「疑わしいスパムしきい値」を40（デフォルトは50）に減らします。

   スパムの苦情の大部分が受信者のサブセットから来ている場合は、スパムしきい値が低いこれらのユーザに対して個別のメールポリシーを作成して、これらの受信者に対してより積極的にフィルタリングできます。

   これらの値に対する変更は軽く行わないでください。また、再利用の影響を確認するためにハードデータを使用せずに行う必要があります。

   また、誤検出を避けるために必ずしも他の方向の値を調整しないでください。誤検出と誤検出がTACに提出されていることを確認してください。

6. SBRS設定とHATポリシーの最適化：

   ほとんどの組織は、SBRS -10 ~ -3.0をブロックリストに、SBRS -3.0 ~ -1.0をSUSPECTLISTに追加することに満足しています。より積極的なお客様は、SBRS -10を–2.0にブロックリストし、-2.0を–0.6にSUSPECTLISTに追加できます。

   場合によっては、送信者がまだSenderBaseレピュテーションスコア(SBRS)を持っていない事実が、この送信者がスパマーである可能性があることを示しています。SBRS「none」を、たとえばSUSPECT送信者グループに対して「Throttled」ポリシーを取得する送信者グループに直接追加できます。

   [Throttled]ポリシーの最大受信者数を1時間あたり5に変更します。

   1時間ごとに異なる受信者の制限を適用する複数の「スロットル」ポリシーを作成することを検討してください。たとえば、1時間あたりSBRSが–2 ~ -1 ~ 5人、1時間あたりSBRSが

–1 ~ 0 ~ 20人の送信者のレート制限などです。

7. 「Throttled」メールフローポリシーの送信者検証を有効にします。

   お客様は、DNSが存在しない、または正しく設定されていない送信者をSUSPECTLIST送信者グループに追加できます。

   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。

   DNSが正しく設定されていない送信者からの誤検出のリスクがあるため、理由メッセージが拒否されたことを示すカスタム4xx応答を返す別のメールフローポリシーを設定する必要があります。

   送信者検証の詳細については、オンラインヘルプまたはAsyncOSユーザガイドを参照してください

8. LDAP受け入れとディレクトリ獲得攻撃保護を有効にします。

   多くのスパマーが大量の無効なアドレスに電子メールを送信するため、無効な受信者に送信する送信者をブロックすると、スパムを減らすこともできます。

   LDAP acceptがすでにオンの場合は、各着信リスナーに対してDirectory Harvest Protection(DHAP)も設定されており、IPごとの最大無効試行回数が5 ~ 10であることを確認してください。

9. コンテンツ辞書を有効にする：

   ESAには2つのコンテンツディクショナリが付属しています。profanity.txtおよびsetic_content.txtこれらの辞書を使用すると誤検出が発生する可能性がありますが、不適切な単語にメールストリームをフィルタリングすると、「間違った人」が「間違った電子メール」を受け取るリスクが減る可能性があることが判明しています。 これらのフィルタは、特定のメールポリシーのユーザグループに対して有効にすることによって、「キーホイール」にのみ適用できます。

10. 誤って分類されたメッセージをCisco TACに報告します。

11. 大量の誤検出を防止するには、SBRSをアウトバウンドスキャン用に無効にする必要があります。これは、SBRSが着信IPのレピュテーションを調べ、内部ネットワークでは、これらのIPの大部分が動的であるためです。次のセクションの手順に従います。

SBNPの有効化

1. 受信メールと送信メールが別々のリスナーにあることを確認します。

2. 以下の送信電子メールのSenderBaseルックアップを無効にします。これをGUIから行うには、[Network] > [Listeners]に移動し、任意のアウトバウンドリスナーを選択し、[Advanced]を選択して、[Use SenderBase IP profiling]の横にあるボックスをオフにします。

   SenderBase Network Participation(SBNP)は、レピュテーションフィルタ、アンチスパム、およびウイルスアウトブレイクフィルタの有効性を大幅に高めることができます。また、SBNPは、アンチスパムを使用するときに有効にした場合に顕著なパフォーマンスへの影響はなく、非常にセキュアです。

   注：組織が受信するスパムの量は、時間とともに変化します。過去よりも多くのスパムを受信しているため、ESAを通過するスパムの数が増える可能性があります。[Incoming Mail Overview（受信メールの概要）]ページを見て、[Stopped by reputation filtering（レピュテーションフィルタリングで停止）]および[Spam messages detected（スパムメッセージが検出されました）]行を追加することで、この動作を時間の経過とともに追跡できます。

SBRSの根拠

誤検出に関する大きな懸念は、重要な電子メールが失われることです。このコンテキストでは、SPAM陽性電子メールを隔離または廃棄する方法に問題があります。正当な電子メールが検疫フォルダまたはスパムフォルダに送信された場合は、プロアクティブな検索を行い、ハムがスパムとして誤って分類されたことを「通知」する必要があります。

これに対し、ブロックリストとレート制限された電子メールは、送信者に即時に通知されるようにブロックされます。この送信者がスパム送信者でない場合は、他の方法で連絡を取ることができます。実際、全体的なポリシーとして、デフォルトでブロックし、要求に応じて信頼できるパートナーを受け入れる方が、一部の企業にとってより良いポジションです。

適切に設定されたスロットリングは、パートナーに影響が及ぶ場合にはまれですが、ウイルスに感染したドメインからの保護を提供します。スロットリングもスパマーに影響を与えません。私たちは、大量のIPを購入し、適切なSBRSスコアを得るために十分な「良い」電子メールを生成し、スパミングを開始するスパマー技術を認識しています。より大きな疑わしいリスト範囲が、これらを捕捉する必要があります。これらのリストのダメージを制限し、最終的にドメインへのスパムの送信を停止させる可能性があります。