SPFの設定とベストプラクティス

内容

概要

このマニュアルでは、Cisco 電子メール セキュリティ アプライアンス（ESA）での Sender Policy Framework（SPF）を使用したさまざまなシナリオを示します。

前提条件

次の項目について理解しておくことをお勧めします。

- Cisco ESA
- AsyncOS のすべてのバージョン

SPF とは何ですか。

Sender Policy Framework（SPF）は、受信側のメール エクスチェンジャで、あるドメインからの着信メールがそのドメイン管理者が承認したホストから送信されたことをチェックできるメカニズムを提供することで、電子メールのスプーフィングを検出するように設計された単純な電子メール検証システムです。ドメインの承認済み送信元ホストのリストは特別な形式の TXT レコードの形でドメインのドメイン ネーム システム（DNS）レコードで公開されます。電子メールのスパムおよびフィッシングは偽造した送信者アドレスを使用することが多いため、SPF レコードの公開とチェックは、アンチスパム技術と見なすことができます。

ESA のパフォーマンスに対する多大な影響はありますか。

CPUの見込み客からは、パフォーマンスに大きな影響はありません。ただし、SPF検証を有効にすると、DNSクエリとDNSトラフィックの数が増加します。すべてのメッセージについて、ESAは1 ～ 3個のSPF DNSクエリを開始する必要があり、その結果、以前よりも早くDNSキャッシュが期限切れになります。したがって、ESA では他のプロセス用にも、より多くのクエリーを生成することになります。

上記の情報に加えて、SPFレコードは通常のDNSレコードよりも大きい可能性があり、いくつかの余分なDNSトラフィックを引き起こす可能性があるTXTレコードになります。

SPF はどのようにイネーブルにしますか。

次の手順の出典は、『Advance User Guide』の SPF 検証の設定に関する記述です。

デフォルトのメールフローポリシーでSPF/System Independent Data Format(SIDF)を有効にするには、次の手順を実行します。

1. [Mail Policies] > [Mail Flow Policies] をクリックします。
2. [Default Policy Parameters] をクリックします。
3. デフォルトのポリシー パラメータで、[Security Features] セクションを表示します。
4. [SPF/SIDF Verification] セクションで、[Yes] をクリックします。
5. 準拠のレベルを設定します (デフォルトは SIDF 互換) 。 このオプションを使用して、使用する SPF または SIDF 検証の規格を判別できます。SIDF 準拠に加えて、SPF と SIDF を組み合わせた SIDF 互換を選択できます。準拠レベルの詳細については、『エンドユーザーガイド』を参照してください。
6. 準拠レベルで SIDF 互換を選択した場合は、Resent-Sender: または Resent-From: ヘッダーがメッセージにある場合に、PRA ID の結果 **Pass を None に**ダウングレードするかどうかを設定します。このオプションはセキュリティを目的として選択できます。
7. SPF の準拠レベルを選択した場合は、HELO ID に対してテストを実行するかどうかを設定します。このオプションを使用して、HELO チェックをディセーブルにすることによって、パフォーマンスが向上することがあります。これは、spf-passed フィルタ ルールで、PRA または MAIL FROM ID が最初にチェックされるため、便利な場合があります。アプライアンスは SPF 準拠レベルに対してのみ HELO チェックを実行します。

SPF 検証結果を処理するには、コンテンツ フィルタを追加してください。

1. SPF/SIDF検証のタイプごとにspf-statusコンテンツフィルタを作成します。命名規則を使用して、検証のタイプを示します。たとえば、SPF/SIDF 検証に合格したメッセージには **SPF-Passed を使用し、検証中の一時的エラーのために合格しなかったメッセージには、SPF-TempErr を使用します。**spf-statusコンテンツフィルタの作成については、GUIのspf-statusコンテンツフィルタルールを参照してください。
2. SPF/SIDFで確認されたメッセージを処理した後、**[Monitor] > [Content Filters]をクリック**し、SPF/SIDFで確認されたコンテンツフィルタごとにトリガーされたメッセージの数を確認します。

「HELO テスト」のオン/オフにはどのような意味がありますか。特定のドメインでHelloテストが失敗した場合はどうなりますか。

SPF の準拠レベルを選択した場合は、HELO ID に対してテストを実行するかどうかを設定します。このオプションを使用して、HELO チェックをディセーブルにすることによって、パフォーマンスが向上することがあります。これは、spf-passed フィルタ ルールで、PRA または MAIL FROM ID が最初にチェックされるため、便利な場合があります。アプライアンスは SPF 準拠レベルに対してのみ HELO チェックを実行します。

有効な SPF レコード

SPF HELOチェックに合格するには、各送信MTAのSPFレコードを含めます（ドメインとは別）。 このレコードを含めないと、HELO チェックは HELO ID に **None 判定を下す可能性があります。**ドメインへのSPF送信者が大量のNone判定を返していることに気付いた場合、これらの送信者は各送信MTAのSPFレコードを含んでいない可能性があります。

このメッセージは、メッセージ フィルタまたはコンテンツ フィルタが設定されていない場合に出力されます。同じく、すべての SPF/SIDF 判定用にメッセージ フィルタまたはコンテンツ フィルタを使用して特定のアクションを実行できます。

単一の外部ドメインに対してのみイネーブルにするにはどのような方法が最適ですか。

特定のドメインのSPFを有効にするには、SPFを有効にしたメールフローポリシーを使用して新しい送信者グループを定義する必要があります。次に、前述のようにフィルタを作成します。

疑わしいスパムに対するSPFチェックを有効にできますか。

Cisco Anti-Spam ではスパム スコアの計算時に多数の要因を考慮します。検証可能なSPFレコードがあると、スパムスコアが低下する可能性がありますが、これらのメッセージが疑わしいスパムとして捕捉される可能性は依然として存在します。

最善の解決策は、送信者のIPアドレスを許可リストするか、複数の条件（remote-ip、mail-from、X-skipspamcheckヘッダーなど）でスパムチェックをスキップするメッセージフィルタを作成することです。 ヘッダーは送信サーバで追加して、あるタイプのメッセージを他のタイプのメッセージから識別できます。

関連情報

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- Eメール認証のベストプラクティス – SPF/DKIM/DMARCの導入
- テクニカル サポートとドキュメント – Cisco Systems