セキュリティで保護された電子メールゲートウェイの送信者ドメイン例外リストの設定

内容

はじめに

このドキュメントでは、Cisco Secure Email Gateway(SEG)のSender Domain Reputation(SDR)設定オプションDomain Exception Listの「新しい変更」について説明します。

著者：Cisco TACエンジニア、Chris Arellano

前提条件

SEGの設定と設定に関する一般的な知識が必要です。

AsyncOS 15.0以降(Cisco Secure Email Gateway(SEG)用)

SDR機能の概要

要件

Sender Domain Reputation Service(SDS)を有効にし、Domain Onlyオプションでアドレスリストを作成します。

使用するコンポーネント

- このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。
  - Cisco Secure Email Gateway(SEG)AsyncOS 15.5.1以降。
- SEG送信者ドメインレピュテーション。
- Address List（アドレスリスト）。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Sender Domain Reputation(SDR)は、複数の送信者値を収集し、判定を導き出し、それらの判定に対してアクションを実行するオプションを提供するクラウドサービスです。SDRでは、ドメイン例外リストに適用されるアドレスリストを使用して、信頼できるドメインをバイパスするように設定できます。

SEG 15.0より前のAsynOSリリースのSDRドメイン例外リストには、次の2つのオプションがありました。

- Enabled = Match the Envelope From, domain to bypass SDR action」というエラーメッセージが表示されます。
- Disabled =すべてが存在する場合のみ一致：Envelope-from + Friendly From + Reply-To + SPF + DKIM + DMARC（デフォルト）。

SEG 15.0以降のオプションのドメイン例外リスト：

- Enabled = Match the Envelope From, domain to bypass SDR action」というエラーメッセージが表示されます。
- Disabled =ドメインが次のいずれかの値に存在する場合に一致します。
  - HELO
  - RDNS
  - エンベロープの送信者
  - 変更前
  - 返信先

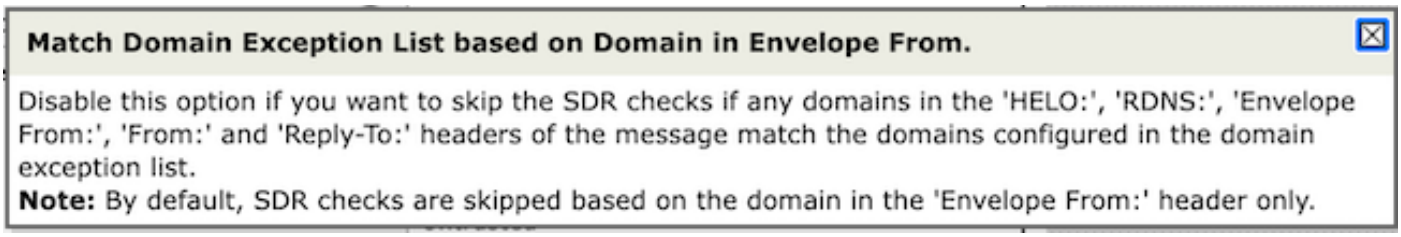
設定

この記事では、新しいドメイン例外リストの設定だけに焦点を当てます。SDRの完全なセットアップと設定は、ユーザガイドに記載されています。

WebUI内でSecurity Services > Domain Reputationの順に移動します。

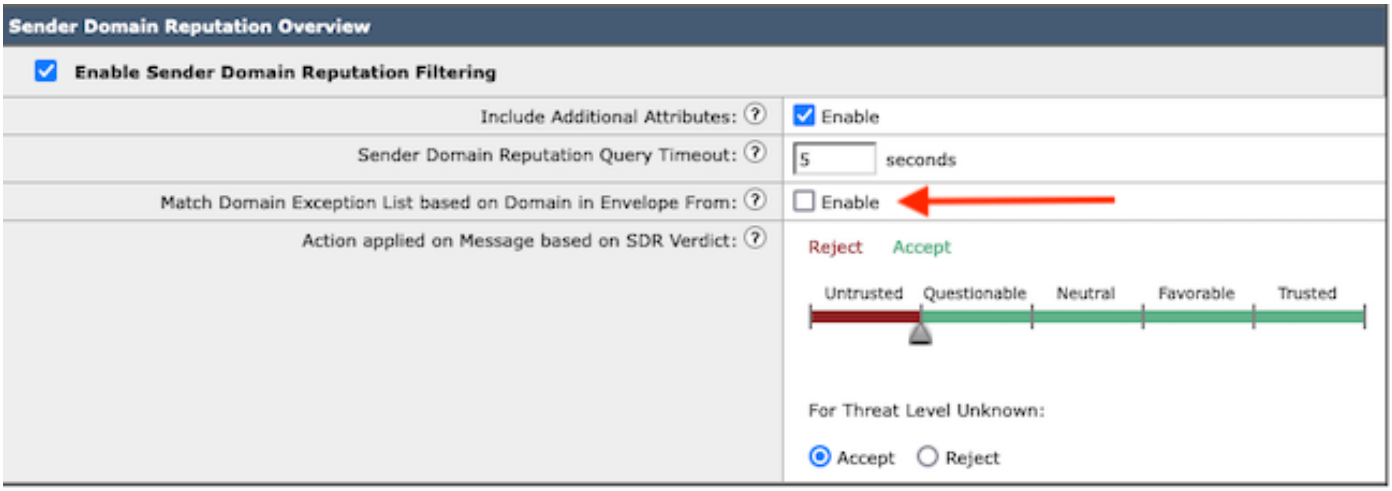
- Match Domain Exception List based on the Domain Name部分of the Envelope Fromオプションはデフォルトで有効になっています。
  - チェックボックスが有効になっている場合は、「Envelope From, header」の値のみが一致し、メッセージが無視されます。
  - チェックボックスが空白の場合、SDRドメイン例外リストはヘッダーフィールド'HELO:'、'RDNS:'、'Envelope From:'、'From:'、および'Reply-To:'のいずれかに一致し、もし有罪判決を受けた場合はメッセージをバイパスします。

関連する?情報アイコンを選択すると、設定の詳細が表示されます。



注：デフォルトでは、SDRチェックは「Envelope From:」ヘッダー内のドメインのみに基づいてスキップされます。

図に示すように、Edit Global Settingsを選択してチェックボックスオプションを削除します。



ドメイン例外リスト自体は、ドメイン名を含むアドレスリストです。

確認

新しいディセーブル機能を使用して正常に機能していることを確認するには、5つのヘッダー値のいずれかに一致するドメイン値を持つテストメッセージがSEGに送信される必要があります。

グローバル例外リスト内の例外を示し、メールフローポリシー内で一致したサンプルログは、初期段階でmail_logsに存在します。

```
Info: MID 14 SDR: MID 14 containing domain name'test1.example.com' matched the global domain exception
```

例外を示すサンプルログには、ドメインと例外リスト名の両方が含まれます。

```
Info: MID 16 containing domain name 'test3.example.com' matched the domain exception list 'SDR-TEST-3'
```

トラブルシュート

選択したメッセージ判定の精度について疑問が生じた場合は、その値を文書化し、メッセージトラッキングと比較します。

- グローバルドメインレピュテーションの設定> セキュリティの設定> ドメインレピュテーションを文書化します。
- グローバルドメインレピュテーション設定で設定された関連するアドレスリストを確認します。
- メッセージトラッキングに基づいて、一致するメールフローポリシーを確認します。
- ドメイン例外リストが設定されているメッセージフィルタまたはコンテンツフィルタの詳細を確認し、メモを取ります。

メッセージトラッキング、メールログ、および元の電子メールヘッダーを収集します。

- グローバル例外がメッセージで一致する場合、ドメインレピュテーションのログエントリは存在しません。これは、一致したドメインを示す行に過ぎません。
- グローバル例外リストがメッセージで一致しない場合は、ドメインレピュテーションのログエントリがあり、そこから値を比較します。
  - 情報：MID 16 SDR:SDRが要求されたドメイン：逆DNSホスト：存在しない、helo:mail1.example.com、env-from:test2.example.com、header-from:te destination.example.com、返信:test2.example.com
- 電子メールヘッダーには、設定と比較するために個々の電子メールに存在する5つの値のいずれかが含まれています。

すべてのデータが収集されたら、一致の有無をチェックして、適切な機能を判別します。

関連情報

- Eメールセキュリティ設定ガイド
- サポートガイドへのCisco Secure Email Gateway起動ページ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。