

SEGに対する脅威スキャナのポリシーごとのスキャンの設定

内容

[はじめに](#)

[前提条件](#)

[使用するコンポーネント](#)

[概要](#)

[設定](#)

[Webインターフェイスの設定](#)

[コマンドラインインターフェイスの設定](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Secure Email Gateway(SEG)のポリシー統合ごとの脅威スキャナ(TS)のサービスと設定について説明します。

前提条件

SEGの一般的な設定と設定に関する知識が必要です。

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。
- グレイメールサービス。
- スпам対策サービス。
- 受信メール ポリシー。

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

Graymailサービスの新たに起動されたサブコンポーネントであるThreat Scanner(TS)は、スパム対策CASEと統合されており、スパム対策の検出をより効果的に行うことができます。

グレイメールサービスがアクティブになると、各受信メールポリシーのスパム対策設定で脅威スキャナを有効にするオプションがアクティブになります。TSを有効にすると、HTMLの密入国の検出に重点を置いて、スパム対策全体の検出機能が向上します。

- HTML解析と悪意のあるスクリプト検出
- URL解析とリダイレクト検出

スパム対策CASEエンジンは2つのサービスを制御し、更新とスパムの有罪判決を管理します。

TSには、各受信メールポリシーのスパム対策設定内に表示される有効/無効の設定があります。

TSは判定に影響を与えるため、最終的なスパム対策CASE判定の重要性が高まります。

設定

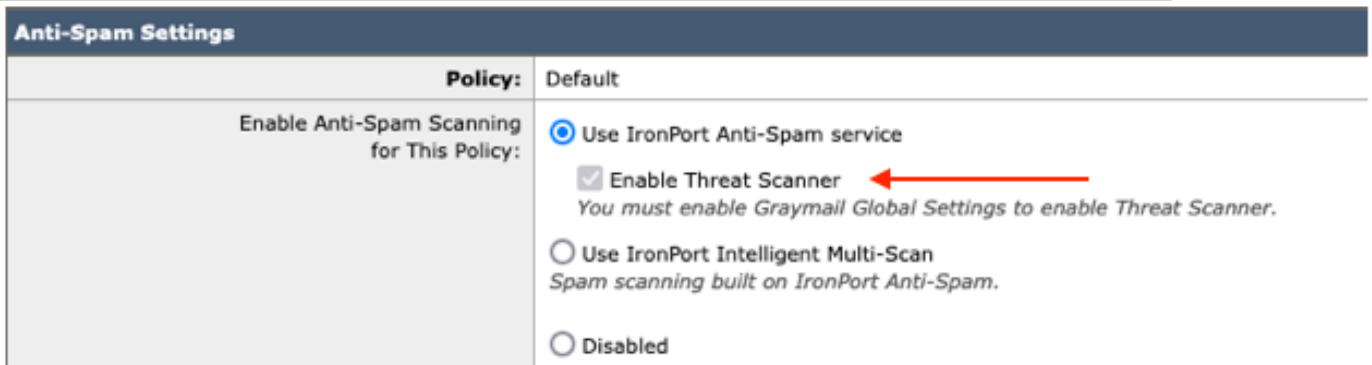
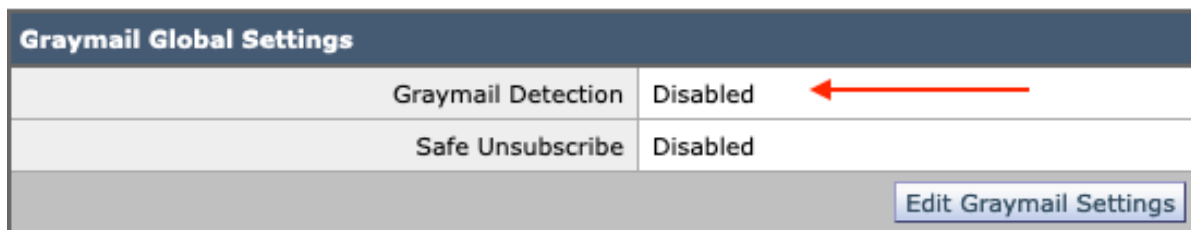
設定は、グレイメール検出の有効化と受信メールポリシー内でのTSの有効化の2つのアクションで構成されます。

- TSをアクティブにするには、Graymailグローバルサービスを有効にする必要があります。
- Graymailがグローバルに有効になると、インバウンドメールポリシーの「スパム対策」オプションから「脅威スキャナを有効にする」オプションが使用可能になります。

Webインターフェイスの設定

WebUIでGraymailを有効にするには、次の手順に従います。

- セキュリティサービスに移動します
 - IMSおよびGraymail
 - グレイメールのグローバル設定
 - グレイメール設定の編集
 - グレイメール検出を有効にするオプションを選択します。
- 変更を送信して確定し、アクションを完了します。



グレイメールを有効にすると、各受信メールポリシーで脅威スキャナ選択ボックスが使用可能になります。

WebUIで脅威スキャナを有効にするには、次の手順を実行します。

- メールポリシーに移動
 - 受信メール ポリシー
 - 目的のメールポリシーを選択します
 - Anti-Spamを選択します。
 - 設定ページの上部に、脅威スキャナを有効にするチェックボックスオプションが表示されます。
- 変更を送信して確定し、設定を完了します

Graymail Global Settings	
Graymail Detection	Enabled ←
Safe Unsubscribe	Disabled
Automatic Updates (?)	Enabled

[Edit Graymail Settings](#)

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input checked="" type="radio"/> Use IronPort Anti-Spam service <input checked="" type="checkbox"/> Enable Threat Scanner ← <input type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

スパム対策の脅威スキャナオプション

コマンドラインインターフェイスの設定

CLIコマンドを使用してグレイメールサービスを有効にします。

- `imsandgraymailconfig`
 - グレイメール
 - `setup`
 - グレイメール検出を使用しますか？[Y]>
 - グレイメールエンジンの自動更新を有効にしますか？[Y]>
 - 残りのプロンプトを完了して、メインマシンのプロンプトに戻ります。
- コミット+コメントの追加> 「Return」キーを押して操作を完了します。

CLIからのポリシー内の脅威スキャナの有効化または無効化

• CLI>ポリシー設定

受信メールポリシーまたは送信メールポリシーを構成するか、ヘッダーの優先順位を一致させますか？

1. 受信メール ポリシー
2. 送信メール ポリシー
3. ヘッダーの優先順位の照合

[1]> 1

受信メールポリシーの設定

1. 北1
2. BLOCKED_LIST
3. ALLOWED_LIST
4. ALLOW_SPOOF
5. デフォルト

編集するエントリの名前または番号を入力します。

[]> 1

実行する操作を選択します。

- NAME – ポリシーの名前を変更する
- NEW – 新しいポリシーメンバー行を追加します
- DELETE – ポリシーメンバー行を削除します
- PRINT – ポリシーメンバー行を印刷する
- スпам対策 – スпам対策ポリシーの変更
- ウイルス対策 – ウイルス対策ポリシーの変更
- OUTBREAK – アウトブレイクフィルタポリシーの変更
- 高度なマルウェア – 高度なマルウェア防御ポリシーの変更
- GRAYMAIL – グレイメールポリシーの変更
- THREATDEFENSECONNECTOR - Threat Defenseコネクタの変更
- FILTERS – フィルタの変更

[]>スパム対策

実行する操作を選択します。

- DISABLE – スпам対策ポリシーを無効にする (ポリシー関連のアクションをすべて無効にする)
- 有効 – スпам対策ポリシーを有効にする

[]>有効

スパム対策設定の開始

このポリシーでインテリジェントマルチスキャンを使用しますか？[N]>

このポリシーでIronPortスパム対策を使用しますか？[Y]>

スパムとして識別されるメッセージもあります。次のメッセージがあります
スパムの疑いとして識別されます。IronPort Anti-Spam Suspected Spamを設定できます
しきい値を下回っています。

設定オプションは、次のように明確に示されるメッセージに適用されます
スパム：

脅威スキャナ判定の特別な処理を有効にしますか？[N]> y

メニュー選択を続行してメールポリシーの選択を完了し、「returnキー」を押して各選択のデフ
ォルトのアクションを受け入れます。

コマンドを使用して保存を完了します。

- コミット+コメントの追加> 「Return」キーを押して操作を完了します。

確認

ログの読み方と解釈方法

Mail Logging of Threat Scannerでは暫定的な判定のみが表示され、CASEでは最終的な判定が表
示されます。

メールログには、Threat Scanner Verdictsに対するクリーンな判定と有罪判決に関する2つの異な
る判定が示されています

- Threat Scanner Interimの判定がクリーンな場合、ログはこれらのサンプルと同様に表示さ
れます。
 - 情報：仮グレーメール判定- LEGIT (0) <メッセージの消去>
 - Info: interim graymail verdict - MCE (11) <その他のメールキャンペーン>
- Threat Scanner Interimの判定で有罪と判定されたログは、次のサンプルと同様に表示され
ます。
 - 情報：暫定ThreatScanner判定 – フィッシング(101)
 - 情報：暫定ThreatScanner判定 – ウイルス(2)

メールログのサンプル：脅威スキャナClean Verdictは異なる表現を使用しています： graymail
verdict。

<#root>

Wed Jan 31 08:19:32 2024 Info: MID 3189755


interim graymail verdict - LEGIT (0) <Clean message>

Wed Jan 31 08:19:33 2024 Info: MID 3189755 interim verdict using engine: CASE negative

Wed Jan 31 08:19:33 2024 Info: MID 3189755 using engine: CASE spam negative

メッセージトラッキングには脅威スキャナログエントリは表示されず、CASE: Final Verdictのみ
が表示されます。

次に示す脅威スキャナ(TS)のサンプルは、4つの判定シナリオを示しています。

 注: 「フィッシング」および「ウイルス」のTSカテゴリは、CASE Verdictの重要度を高める唯一の検出です。

メールログのサンプル : フィッシングTSの有罪判決とアンチスパムの有罪判決の両方が存在します

<#root>

Thu Jan 25 09:05:23 2024 Info: MID 3057397

interim

ThreatScanner verdict - PHISHING (101)

<Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>

Thu Jan 25 09:05:23 2024 Info: MID 3057397 interim verdict using engine: CASE spam positive

Thu Jan 25 09:05:23 2024 Info: MID 3057397

using engine: CASE spam positive

Thu Jan 25 09:05:23 2024 Info: Message aborted MID 3057397 Dropped by CASE

追跡サンプル : フィッシングTSの有罪判決は存在せず、CASEの有罪判決が存在します。

25 Jan 2024 07:05:23 (GMT -08:00) Message 3057397 matched per-recipient policy DEFAULT for inbound mail policies.

25 Jan 2024 07:05:23 (GMT -08:00) Message 3057397 scanned by Anti-Spam engine: CASE. Interim verdict: Positive

25 Jan 2024 07:05:23 (GMT -08:00) Message 3057397 scanned by Anti-Spam engine: CASE. Final verdict: Positive

フィッシングTSに有罪判決、アンチスパムに有罪判決

メールログのサンプル : PHISHING TS ConvictionとAntiSpam Negativeの両方が存在します。

<#root>

Thu Jan 25 09:05:47 2024 Info: MID 3057413

interim ThreatScanner verdict - PHISHING (101)

<Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>

Thu Jan 25 09:05:47 2024 Info: MID 3057413 interim verdict using engine: CASE spam negative

Thu Jan 25 09:05:47 2024 Info: MID 3057413

using engine: CASE spam negative

追跡サンプル : フィッシングTSは有罪判決を受け、アンチスパムネガが存在します。

```
25 Jan 2024 07:05:47 (GMT -08:00) Message 3057413 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:47 (GMT -08:00) Message 3057413 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
25 Jan 2024 07:05:47 (GMT -08:00) Message 3057413 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
25 Jan 2024 07:05:47 (GMT -08:00) Message 3057413 scanned by Anti-Spam engine: CASE. Final verdict: Negative
```

メールログのサンプル : メールログのVIRUS TS ConvictionおよびAntiSpam Convictionサンプル
。

<#root>

Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim

ThreatScanner verdict - VIRUS (2)

<Virus detected by ThreatScanner engine>

Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim verdict using engine: CASE spam positive

Thu Jan 25 13:37:16 2024 Info: MID 3066060

using engine: CASE spam positive

Thu Jan 25 13:37:16 2024 Info: Message aborted MID 3066060 Dropped by CASE

追跡サンプル : ウイルスTSの有罪判決がなく、アンチスパムの有罪判決が出ています。

```
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 scanned by Anti-Spam engine: CASE. Final verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 aborted: Dropped by CASE
```

メールログのサンプル : VIRUS TS ConvictionとAntiSpam Negativeの両方が存在します。

<#root>

Jan 23 21:38:57 2024 Info: MID 3013692

interim ThreatScanner verdict - VIRUS (2)

<Virus detected by ThreatScanner engine>

Jan 23 21:38:58 2024 Info: MID 3013692 interim verdict using engine: CASE spam negative

Jan 23 21:38:58 2024 Info: MID 3013692

using engine: CASE spam negative

トラッキングサンプル : VIRUS TS Conviction absentおよびAntiSpam Negativeが存在。

```
23 Jan 2024 19:38:57 (GMT -08:00) Message 3013692 matched per-recipient policy DEFAULT for inbound mail policies.
23 Jan 2024 19:38:58 (GMT -08:00) Message 3013692 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
23 Jan 2024 19:38:58 (GMT -08:00) Message 3013692 scanned by Anti-Spam engine: CASE. Final verdict: Negative
```

Graymailログには、誤検出のチャレンジが行われた場合のTALOS分析に使用する脅威スキャナ判定およびサポートコンテンツが含まれています。

脅威スキャナの未処理の結果が存在するため、グレイメールのロギングが迅速にロールオーバーされました。この動作に対処するために、Graymailログに対してSEGの変更が行われています。

- AsyncOS 15.5では、Graymailログファイルのデフォルトログサブスクリプションが20に設定され、ログの保持が向上します。
 - ログなし：アップグレード時に設定が20より大きい場合、ファイル設定は変更されません。
- 受信Graymail Interim convictedメッセージは、フルスキャンのraw結果を情報レベルで表示します。
- 他のすべてのメッセージのグレイメールスキャン結果は、デバッグレベルで表示されます。

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。