CES ESA の設定のベスト プラクティス

目次

概要

このドキュメントでは、シスコの Cloud Email Security (CES) を使用して Cisco Email Security Appliance (ESA) を設定する管理者のための推奨事項について概説します。

前提条件

要件

次の項目に関する知識が推奨されます。

- ESA 管理、CLI と GUI の両方のレベルでの管理

使用するコンポーネント

このドキュメントの情報は、CES のカスタマーおよび管理者のためのベスト プラクティスおよび推奨事項に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- AsyncOS for Email Security のバージョンを実行する ESA オンプレミス ハードウェアおよび仮想アプライアンス（非 CES）

CES ESA の設定のベスト プラクティス

> **警告**： このドキュメントで示されているベスト プラクティスに基づいて設定を変更する場合、それらの変更はよく確認および理解する必要があります。確認および理解した後で、実稼働環境で設定の変更を実施してください。 管理時に 100% 理解していない、または不安の残る設定の変更を実施する場合、事前に CES システム エンジニアまたはアカウント チームに相談してください。

セキュリティ サービス

IronPort Anti-Spam（IPAS）

- 常に 1.5 MB スキャンし、2 MB はスキャンしないようにします。

URL フィルタリング

- URL の分類およびレピュテーションを有効にします。
- Web インタラクション トラッキングを有効にします。

グレイメール検出

- 最大メッセージ サイズとして 1 MB を使用できるようにします。

アウトブレイク フィルタ

- 適応ルールを有効にし、最大スキャン サイズとして 1 MB を使用できるようにします。
- Web インタラクション トラッキングを有効にします。

高度なマルウェア防御

- 機能を有効にした後、追加のファイル タイプを使用可能にします。

メッセージ トラッキング

- 拒否された接続の口ギングを有効にします（必要な場合）。

システム管理

[ユーザ（Users）]

- パスワード ポリシーを設定します。
- 可能な場合、認証のために Lightweight Directory Access Protocol（LDAP）を活用します。

[ログ サブスクリプション（Log Subscriptions）]

- 設定履歴口グを有効にします。
- URL フィルタリング ログを有効にします。
- 追加ヘッダーの「From」を口グに記録します。

CLI レベルの変更

Web セキュリティ SDS URL フィルタリング

- **websecurityadvancedconfig**

```
Do you want to disable DNS lookups? [N]> y

Enter the maximum number of URLs that should be scanned:
[100]> 20

Enter the threshold value for outstanding requests:
[50]> 5

Enter the default time-to-live value (seconds):
[30]> 600

Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
```

URL ロギング

- ESA URL フィルタリングの有効化およびベスト プラクティス
- **outbreakconfig**

```
Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.
```

アンチ スプーフィング フィルタ

- Cisco Email Security による Forged Email Detection（FED）

ヘッダー スタンプ フィルタ

- 書き、有効に して下さい

```
Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.
```

ホスト アクセス テーブル

追加の送信者グループ

- ESA ユーザ ガイド： メッセージ処理のための送信者グループの作成 SKIP_SBRS – レピュテーションをスキップする送信元を上位に配置します。SPOOF_ALLOW – スプーフィング フィルタの一部PARTNER – TLS で適用される接続用

定義済みの SUSPECTLIST 送信者グループにおいて

- ESA ユーザ ガイド： 送信者検証： ホスト「なしの場合の SBRS スコア」を有効にします。

オプションで、「DNS の一時的な障害により、接続ホストの PTR レコードの検索が失敗」を有効にします。

アグレッシブ HAT の例

- BLACKLIST [-10 から -2] POLICY: BLOCKED
- SUSPECTLIST [-2 から -1] POLICY: HEAVYTHROTTLED
- GRAYLIST[-1 から 2 および NONE] POLICY: LIGHTTHROTTLED
- ACCEPTLIST [2 から 10] POLICY: ACCEPTED

注: 上記の HAT の例は、追加設定したメール フロー ポリシーを示しています。 MFP に関する詳細については、ESA で実行される AsyncOS for Email Security の該当バージョンのユーザ ガイドを参照してください。 たとえば、AsyncOS 10.0： ホスト アクセス テーブル（HAT）、送信者グループ、およびメール フロー ポリシーなどです。

メール フロー ポリシー（デフォルト ポリシー パラメータ）

セキュリティ設定

- Transport Layer Security（TLS）を優先に設定します。
- Sender Policy Framework（SPF）を有効にします。
- DomainKeys Identified Mail（DKIM）を有効にします。
- ドメイン ベースのメッセージ認証、レポート、および適合（DMARC）の検証および集計フィードバック レポートの送信を有効にします。

注: DMARC では、追加の調整を設定する必要があります。 DMARC に関する詳細については、ESA で実行される AsyncOS for Email Security の該当バージョンのユーザ ガイドを参照してください。 たとえば、AsyncOS 10.0： DMARC の検証などです。

受信メール ポリシー

スパム対策のしきい値

- しきい値は、デフォルトのしきい値のままにする必要があります。 スコアを変更すると、誤検出が増加する場合があります。

ウイルス対策

- メッセージのスキャン： ウイルススキャンのみ
- スキャン不能なメッセージ、ウイルス感染したメッセージ：「元のメッセージのアーカイブ化」を不可に設定します。

AMP

- スキャン不能の場合に付加される件名に「AMP」を追加し、「メッセージのアーカイブ化」を無効にします。

グレイメール

- 判定ごとに有効化されるスキャンを行い、件名を付加し、送信します。
- バルクメールに対して x ヘッダー（ヘッダー =「X-BulkMail」、値 =「True」）を追加します。

アウトブレイク フィルタ

- デフォルトの脅威レベルは 3 です。セキュリティ要件に応じて調整してください。 メッセージの脅威レベルがこのしきい値と等しいか、またはそれ以上の場合、そのメッセージはアウトブレイク隔離領域に送信されます。 ((1 = 最小の脅威、5 = 最大の脅威)
- メッセージの変更を有効にします。 未署名のメッセージの URL を書き換えます。
- 付加される件名を以下に変更します： [Possible $threat_category Fraud]

送信メール ポリシー

ウイルス対策

- メッセージのスキャン:
- ウイルススキャンのみ未チェックでは、X ヘッダーと AV スキャン結果をメッセージに含めます。
- すべてのメッセージについて： [Advanced] > [Other Notification] に移動し、[Others] を有効にし、管理者/SOC の連絡先電子メール アドレスを追加します。

ポリシー隔離領域

次の隔離領域を事前に作成します。

- 不適切なインバウンド
- 不適切なアウトバウンド
- URL の悪意のあるインバウンド
- URL の悪意のあるアウトバウンド
- スプーフィングの疑いあり
- マルウェア

その他の設定

ディクショナリ

- 不適切表現および性的表現のディクショナリを有効化/確認します。
- 適切な名前を使用して偽装電子メールのディクショナリを作成します。
- 制限キーワードまたはその他のキーワードのディクショナリを作成します。

送信先コントロール

- デフォルトの宛先に対して TLS を有効にします。
- Web メール ドメインに対して比較的低いしきい値を設定します。
- 宛先制御設定を使用して自分のアウトバウンド メールに対してレート制限を行います。

コンテンツ フィルタ

> **注:** コンテンツ フィルタに関する詳細については、ESA で実行される AsyncOS for Email Security の該当バージョンのユーザ ガイドを参照してください。 たとえば、AsyncOS 10.0： コンテンツ フィルタ

不適切コンテンツのフィルタ

- 不適切表現または性的表現ディクショナリに条件が一致した場合、コピーを不適切表現の隔離領域に送信します。

悪質な URL レピュテーション コンテンツのフィルタ

- 悪質な URL (-10 から -6) のコピーを隔離領域に送信します。

以下が選択された URL カテゴリ コンテンツ フィルタ

- アダルト、ポルノ、児童虐待、ギャンブル
- コピーを不適切隔離領域に送信します。

偽装メールの検出

- 「Executives_FED」という名前のディクショナリ
- FED() しきい値 90 でコピーを隔離領域に送信します。

マクロ対応ドキュメント コンテンツ フィルタ

- 1 つ以上の添付ファイルにマクロが含まれる場合。
- [Optional condition] -> [From Untrusted SBRS range]
- 隔離領域にコピーを送信します。

プロテクトされている添付ファイル

- 1 つ以上の添付ファイルがプロテクトされている場合
- [Optional condition] -> [From Untrusted SBRS range]
- 隔離領域にコピーを送信します。

関連情報

- BRKSEC-2131 - Cisco E メール セキュリティ： ベスト プラクティスおよび微調整 (2016 ラスベガス)
- BRKSEC-2131 - 非 E メール ユーザの E メール セキュリティ (2015 サンディエゴ)
- BRKSEC-3770 - (DMARC) - フィッシングを行わない： E メール認証技術の詳細 (2014 サンフランシスコ)
- CES エンド ユーザ ライセンス同意
- CES サービスの説明
- シスコ ユニバーサル クラウド チーム
- テクニカル サポートとドキュメント – Cisco Systems