ESA DHAP 機能の有効化

Document ID: 117847

Updated: 2014 年 6 月 25 日

著者：Cisco TAC エンジニア、John Yu、Robert Sherwin

PDF のダウンロード
印刷
フィードバック

関連製品

- Cisco コンテンツ セキュリティ管理アプライアンス
- Cisco E メール セキュリティ アプライアンス
- Cisco Web セキュリティ アプライアンス

目次

概要

この資料にディレクトリ収穫不正侵入（DHAs）を防ぐことを Cisco E メール セキュリティ アプライアンス（ESA）のディレクトリ収穫攻撃防止（DHAP）機能が可能にする方法を記述されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ESA
- AsyncOS

使用するコンポーネント

このドキュメントの情報は、AsyncOS のすべてのバージョンに基づくものです。

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

DHA は有効な eメールアドレスを見つけるためにスパムの発信者によって使用する手法です。 アドレスを生成するためにその DHA ターゲット使用する 2 つの主要な手法があります:

- スパムの発信者は文字および数のすべての考えられる組み合わせのリストを作成し、次にドメイン名を追加 します。

- スパムの発信者はよくある名、姓および頭文字を結合するリストの作成と標準辞書攻撃を使用します。

DHAP は Lightweight Directory Access Protocol （LDAP）承認検証が使用されるとき有効に することができる Cisco コンテンツ セキュリティ アプライアンス モデルのサポートされる機能です。 DHAP 機能はある特定の送信側からの無効 な受信者のアドレスの数を把握します。

送信側が管理者定義されたしきい値を超えれば、送信側は信頼できない考えられその送信側からのメールはネットワーク設計 要件（NDR）またはエラーコード 生成無しでブロックされます。 送信側の評判に基づいてしきい値を設定できます。 たとえば、信頼できなくか疑わしい 送信側は下位 DHAP しきい値があり信頼されるか、または評判が良い送信側は高い DHAP しきい値がある場合があります。

イネーブル DHAP

DHAP 機能を有効に するために、**ポリシー** > コンテンツ セキュリティ アプライアンス モデル GUI からの**ホスト アクセス 表（帽子）を郵送し**、**メール フロー ポリシーを**選択するためにナビゲート して下さい。 **ポリシー名**カラムから編集したいポリシーを選択して下さい。

帽子にリモートホストからの接続に機能するために使用する 4 つの基本的なアクセス規則があります:

- ACCEPT: 接続は許可され、電子メール承認はリスナー設定によって更に制限 されます。 これには受信者のアクセス 表が含まれています（公共リスナーのために）。

- **REJECT**： 接続は最初に、接続する試みが 4XX か 5XX メッセージを受け取るクライアント許可されますが。 どの電子メールも許可されません。

- **TCPREFUSE**: TCP レベルの接続は拒否されます。

- **リレー**: 接続は許可されます。 あらゆる受信者のための受信は受信者のアクセス 表によって許可され、抑制されません。 ドメイン キー署名はリレー メール フロー ポリシーでだけ利用可能です。

指定ポリシーの**メール フロー制限**セクションでは、検索は最大値の設定によって**ディレクトリ収穫攻撃防止（DHAP）**設定を設定 し。 1 時間あたりの無効 な受信者。 また最大値をカスタマイズすることを選択できます。 時間コードおよび最大値ごとの無効 な受信者。 1 時間あたりの無効 な受信者はそう望む場合ショートメッセージを送ります。

additonal ポリシーのための DHAP を設定するためにこのセクションを繰り返して下さい。

GUI のすべての変更を入れ、保存するようにして下さい。

> **注:** Cisco は**リモートホスト**設定**からの 1 時間あたりの無効 な受信者の最大数**のために 5 と 10 間の最大数を使用することを推奨します。

> **注:** その他の情報に関しては、Ciscoサポート ポータルの **AsyncOS ユーザガイドを**参照して下さい。

Cisco サポート コミュニティ - 特集対話

Cisco サポート コミュニティでは、フォーラムに参加して情報交換することができます。

Updated: 2014 年 6 月 25 日
Document ID: 117847