ESA DHAP 機能の有効化

内容

概要

このドキュメントでは、ディレクトリ獲得攻撃（DHA）を防止するために、Cisco E メール セキュリティ アプライアンス（ESA）のディレクトリ獲得攻撃防止（DHAP）機能を有効化する方法について説明します。

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

DHAは、スパマーが有効な電子メールアドレスを見つけるために使用する技術です。DHAがターゲットとするアドレスを生成するために使用される主な手法は2つあります。

- スパマーは、文字と数字のすべての可能な組み合わせのリストを作成し、ドメイン名を追加します。

- スパマーは標準的な辞書攻撃を使用し、一般的な名、姓、イニシャルを組み合わせたリストを作成します。

DHAPは、Lightweight Directory Access Protocol(LDAP)受け入れ検証が使用されるときに有効にできる、Ciscoコンテンツセキュリティアプライアンスでサポートされている機能です。DHAP機能は、特定の送信者からの無効な受信者アドレスの数を追跡します。

送信者が管理者が定義したしきい値を超えると、その送信者は信頼できないものとみなされ、その送信者からのメールはネットワーク設計要件(NDR)やエラーコードの生成なしでブロックされます。しきい値は、送信者のレピュテーションに基づいて設定できます。たとえば、信頼できない送信者や疑わしい送信者のDHAPしきい値は低く、信頼できる送信者や信頼できる送信者のDHAPしきい値は高くなります。

DHAPの有効化

DHAP機能を有効にするには、コンテンツセキュリティアプライアンスGUIから[Mail Policies] > [Host Access Table (HAT)] に移動し、[Mail Flow Policies] を選択します。[Policy Name] 列から、編集するポリシーを選択します。

HATには、リモートホストからの接続に応じて動作するために使用される4つの基本アクセスルールがあります。

- **ACCEPT**:接続は受け入れられ、電子メールの受け入れはリスナー設定によってさらに制限されます。これには、受信者アクセステーブル（パブリックリスナー用）が含まれます。
- **REJECT**:接続は最初は受け入れられますが、接続を試みるクライアントは4XXまたは5XXグリーティングを受信します。どの電子メールも許可されません。
- **TCPREFUSE**:接続はTCPレベルで拒否されます。
- **リレー**:接続が受け入れられます。受信者に対する受信は許可され、受信者アクセステーブルによって制限されません。ドメインキー署名は、中継メールフローポリシーでのみ使用できます。

選択したポリシーの[Mail Flow Limits] セクションで、[Max] を設定して[Directory Harvest Attack Prevention (DHAP)] 設定を見つけて設定します。1時間あたりの受信者が無効です。Max.1時間あたりの受信者コードと最大受信者数必要に応じて、1時間あたりの受信者のテキストが無効です。

追加のポリシーに対してDHAPを設定するには、このセクションを繰り返す必要があります。

GUIですべての変更を送信し、確定したことを確認します。

> **注**：[Maximum number of invalid recipients per hour from a remote host] 設定には、5から10までの最大数を使用することをお勧めします。

> **注**：詳細については、シスコサポートポータルの『**AsyncOSユーザガイド**』を参照してください。

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。