ESA DHAP Feature Enablement

Contents

Introduction

This document describes how to enable the Directory Harvest Attack Prevention (DHAP) feature on the Cisco Email Security Appliance (ESA) in order to prevent Directory Harvest Attacks (DHAs).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ESA
- AsyncOS

Components Used

The information in this document is based on all versions of AsyncOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

A DHA is a technique that is used by spammers in order to locate valid email addresses. There are two main techniques that are used in order to generate the addresses that DHA targets:

- The spammer creates a list of all possible combinations of letters and numbers, and then appends the domain name.

- The spammer uses a standard dictionary attack with the creation of a list that combines common first names, surnames, and initials.

The DHAP is a supported feature on the Cisco Content Security Appliances that can be enabled

when Lightweight Directory Access Protocol (LDAP) acceptance validation is used. The DHAP feature keeps track of the number of invalid recipient addresses from a given sender.

Once a sender crosses an administrator-defined threshold, the sender is deemed to be untrusted, and mail from that sender is blocked with no Network Design Requirement (NDR) or error code generation. You can configure the threshold based upon the reputation of the sender. For example, untrusted or suspicious senders can have a low DHAP threshold, and trusted or reputable senders can have a high DHAP threshold.

Enable DHAP

In order to enable the DHAP feature, navigate to **Mail Policies** > **Host Access Table (HAT)** from the Content Security Appliance GUI and select **Mail Flow Policies**. Choose the policy you wish to edit from the **Policy Name** column.

The HAT has four basic access rules that are used in order to act upon connections from remote hosts:

- **ACCEPT**: The connection is accepted, and email acceptance is restricted further by the listener settings. This includes the Recipient Access Table (for public listeners).
- **REJECT**: The connection is initially accepted, but the client that attempts to connect receives a 4XX or 5XX greeting. No email is accepted.
- **TCPREFUSE**: The connection is refused at the TCP level.
- **RELAY**: The connection is accepted. Receiving for any recipient is allowed and is not constrained by the Recipient Access Table. Domain Keys signing is available only on relay mail flow policies.

In the **Mail Flow Limits** section of the selected policy, find and set the **Directory Harvest Attack Prevention (DHAP) configuration by setting the Max. Invalid Recipients Per Hour. You can also choose to customize the Max. Invalid Recipients Per Hour Code and Max. Invalid Recipients Per Hour Text if you so desire.**

You must repeat this section in order to configure DHAP for additonal policies.

Ensure that you submit and commit all changes in the GUI.

> **Note**: Cisco recommends that you use a maximum number between five and ten for the **Maximum number of invalid recipients per hour from a remote host** setting.

> **Note**: For additional information, refer to the **AsyncOS User Guide** on the Cisco Support Portal.