CSC 6.X: Email Reputation Configuration Example

Contents

Introduction

This document provides a sample configuration on how to configure the email reputation on the Cisco Content Security and Control (CSC) Security Services Module (SSM).

Prerequisites

Requirements

You need to have a Security Plus license to use this feature.

Components Used

The information in this document is based on the Cisco Content Security and Control SSM with Software release version 6.3.

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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Email Reputation is a technology that reduces the spam mails. By enabling this feature, CSC SSM verifies if the originator of the mail is a black-listed address or not. It maintains a list of databases that contains all the IP addresses that source the spam messages. If a mail is found to have an originator from this list, that mail is considered spam and is dropped.

The service levels offered by this Email Reputation Technology (ERS) are basically two types. These services are based mainly on the level of authenticity of the source IP addresses.

- ERS Standard - Contains the known sources of spam
- ERS Advanced - Contains the known sources and the suspected sources

When an IP address is added to ERS Standard database, it is termed a spam source and is rare that you observe an IP address removed from this list. ERS Standard contains the list of IP addresses that consistently originate spam.

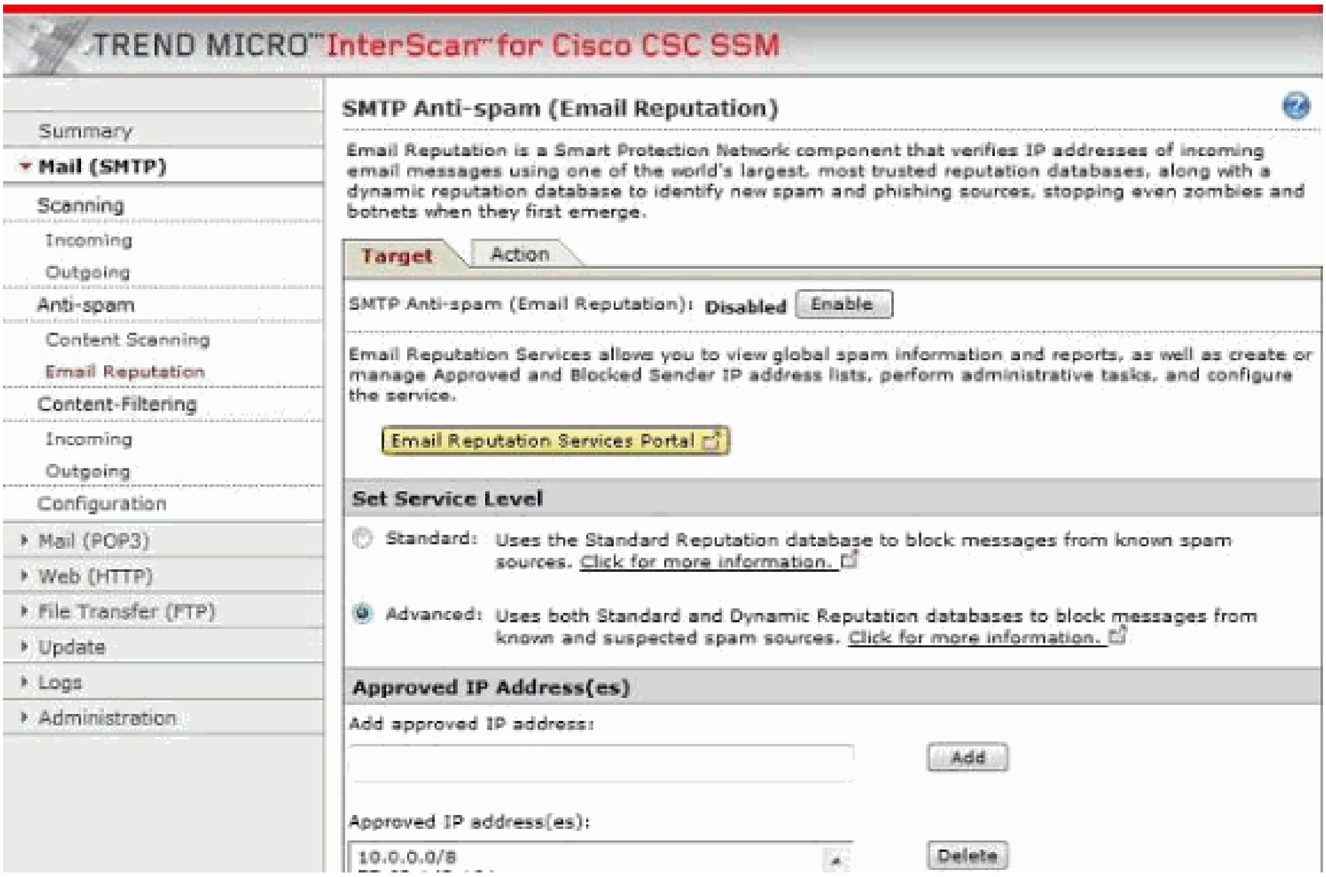
ERS Advanced contains a list of IP addresses which are meant to be removed if found to not produce the spam any further. For example, a hacked Mail server can be listed in this database at the time when it is compromised. When it is restored to normalcy, it is removed from this database.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

1. Choose **Mail (SMTP) > Anti-spam > Email Reputation**. A new window opens.
2. From the Target tab, click **Enable** in order to enable this Email Reputation feature.
3. Choose **Advanced** for the Service Level.
4. From the Approved IP Addresses field, specify the range of IP addresses that you want to exempt from
   scanning.



SMTP Anti-spam (Email Reputation)

Email Reputation is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

SMTP Anti-spam (Email Reputation): **Disabled**

Email Reputation Services allows you to view global spam information and reports, as well as create or manage Approved and Blocked Sender IP address lists, perform administrative tasks, and configure the service.

Set Service Level

○ Standard: Uses the Standard Reputation database to block messages from known spam sources. Click for more information.

● Advanced: Uses both Standard and Dynamic Reputation databases to block messages from known and suspected spam sources. Click for more information.

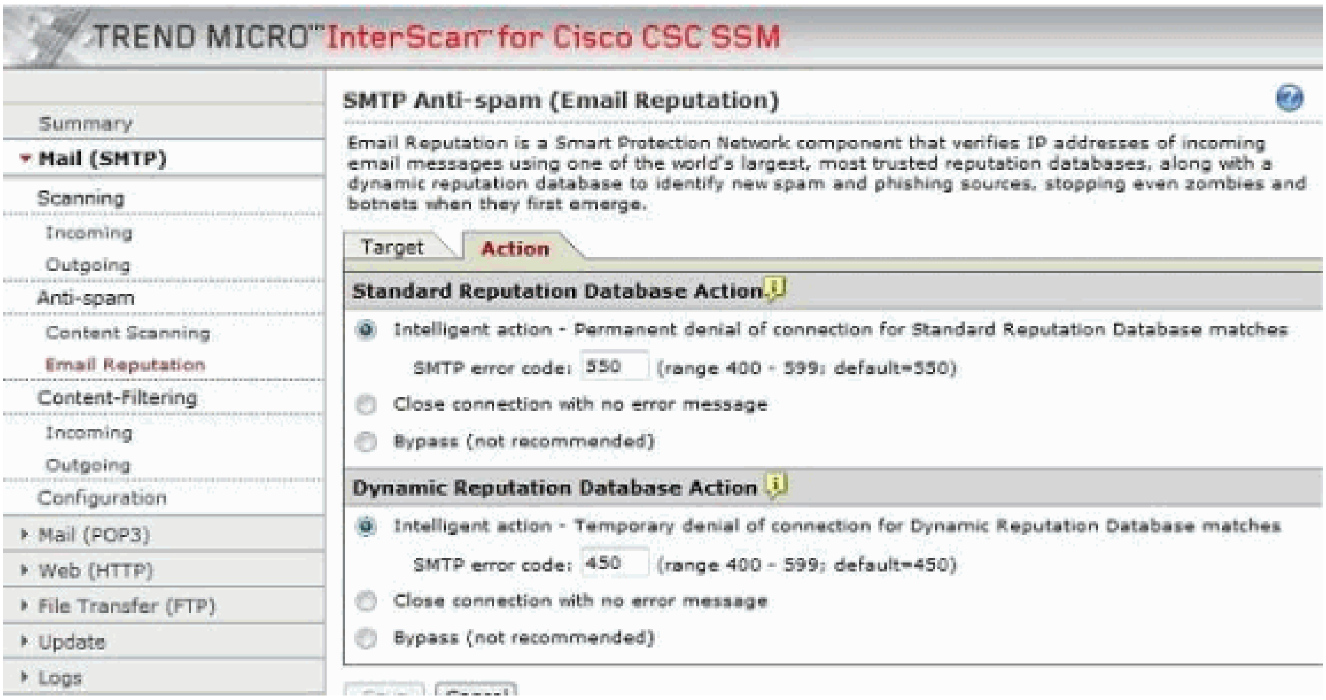
Approved IP Address(es)

Add approved IP address:

Approved IP address(es):

10.0.0.0/8

5. From the Action tab, specify the type of action based on your enterprise security policy. These three actions are available:Close connection with an error messageClose connection without error messageBypass the
connection



SMTP Anti-spam (Email Reputation)

Email Reputation is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

Standard Reputation Database Action

● Intelligent action - Permanent denial of connection for Standard Reputation Database matches

SMTP error code: 550 (range 400 - 599; default=550)

○ Close connection with no error message

○ Bypass (not recommended)

Dynamic Reputation Database Action

● Intelligent action - Temporary denial of connection for Dynamic Reputation Database matches

SMTP error code: 450 (range 400 - 599; default=450)

○ Close connection with no error message

○ Bypass (not recommended)

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Unable to receive emails from some domains

Problem:

The problem is the inability to receive the emails from specific domains. It appears that the CSC module is blocking the emails. When bypassing the module, everything works fine. This error message is received: `2012/02/06 14:33:00 GMT+00:00 NRS 174.37.94.181 RBL-Fail QIL-NA RejectWithErrorCode-550 NA 0 0 NA NA NA 0 NA`

Solution:

In order to resolve this issue, configure the email reputation feature properly.

Related Information

- **Cisco ASA Content Security and Control (CSC) Security Services Module Support**
- **Technical Support & Documentation - Cisco Systems**