CSC 6.X: Ejemplo de Configuración de Reputación de Correo Electrónico

Contenido

Introducción

Este documento proporciona una configuración de ejemplo sobre cómo configurar la reputación del correo electrónico en el Cisco Content Security and Control (CSC) Security Services Module (SSM).

Prerequisites

Requirements

Necesita una licencia Security Plus para utilizar esta función.

Componentes Utilizados

La información de este documento se basa en Cisco Content Security and Control SSM con Software versión 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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

La reputación de correo electrónico es una tecnología que reduce los correos spam. Al habilitar esta función, CSC SSM verifica si el originador del correo es una dirección de la lista negra o no. Mantiene una lista de bases de datos que contiene todas las direcciones IP que originan los mensajes de spam. Si un correo tiene un originador de esta lista, ese correo se considera spam y se elimina.

Los niveles de servicio ofrecidos por esta tecnología de reputación de correo electrónico (ERS) son básicamente de dos tipos. Estos servicios se basan principalmente en el nivel de autenticidad de las direcciones IP de origen.

- Estándar ERS: contiene las fuentes conocidas de spam
- ERS Advanced: contiene las fuentes conocidas y las fuentes sospechosas

Cuando se agrega una dirección IP a la base de datos ERS Standard, se denomina origen de spam y es raro que observe una dirección IP eliminada de esta lista. El estándar ERS contiene la lista de direcciones IP que originan de forma consistente el spam.

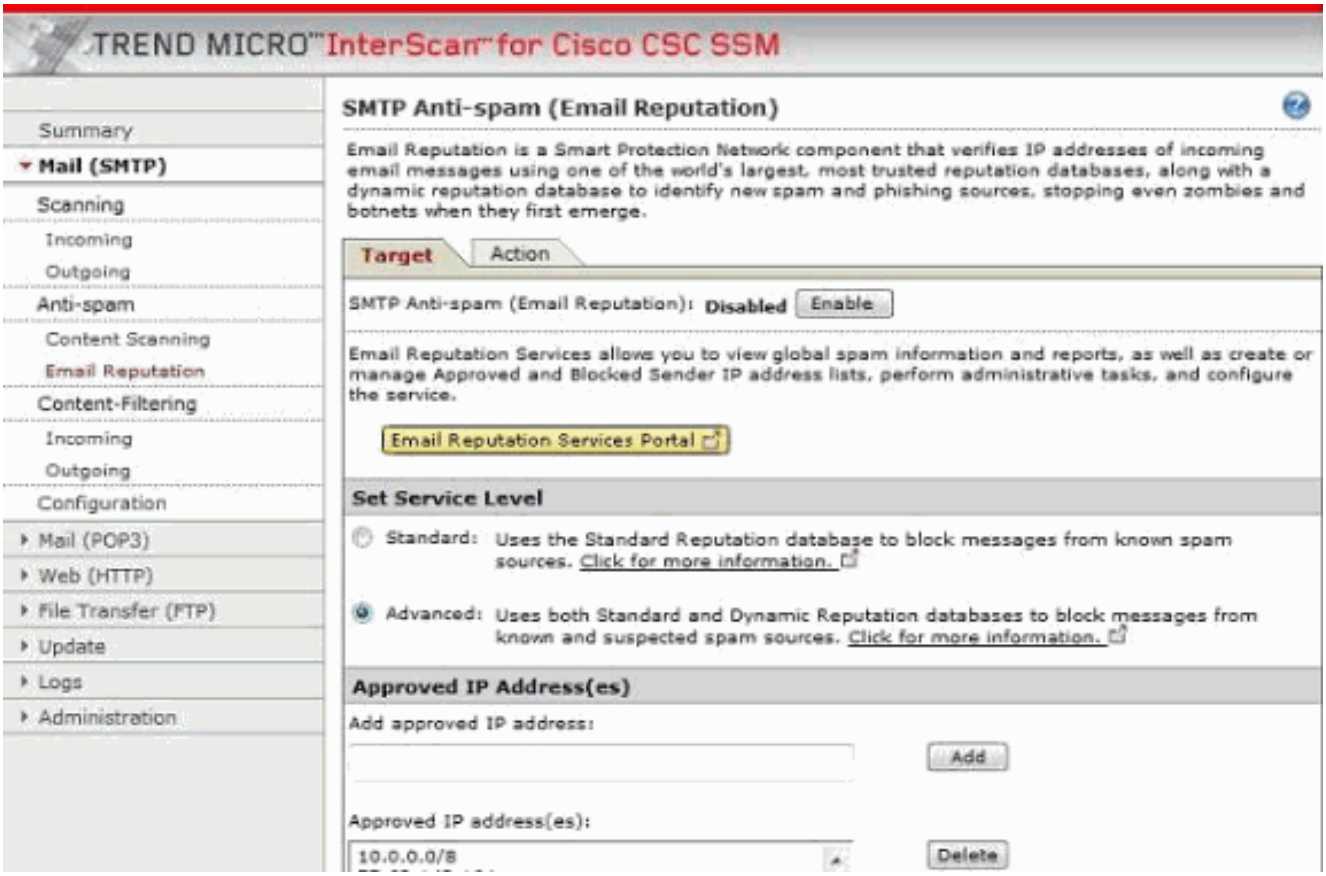
ERS Advanced contiene una lista de direcciones IP que deben eliminarse si se detecta que no producen más spam. Por ejemplo, un servidor de correo pirateado puede aparecer en esta base de datos en el momento en que se encuentre en peligro. Cuando se restablece a la normalidad, se elimina de esta base de datos.

Configurar

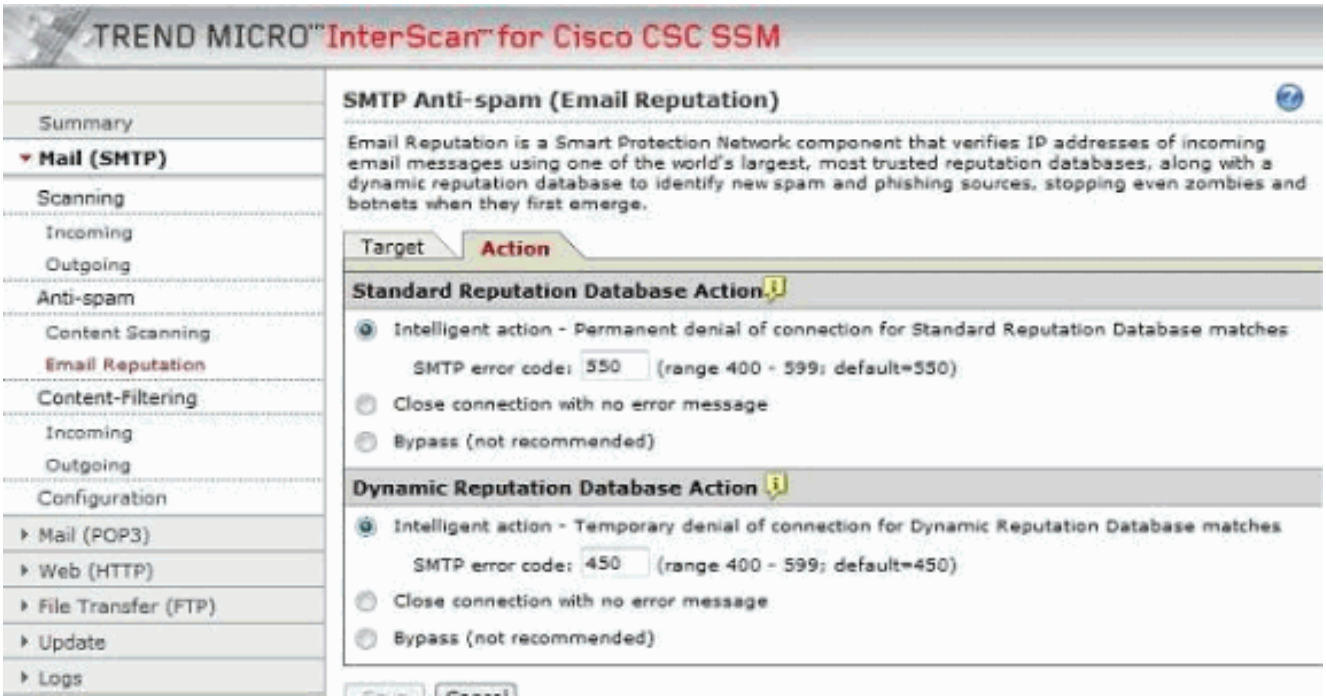
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

1. Elija **Mail (SMTP) > Anti-Spam > Email Reputation**. A new window opens.
2. En la pestaña Destino, haga clic en **Activar** para habilitar esta función de reputación de correo electrónico.
3. Elija **Advanced** para el nivel de servicio.
4. En el campo IP Addresses (Direcciones IP aprobadas), especifique el rango de direcciones IP que desea eximir del
   escaneo.



5. En la ficha Acción, especifique el tipo de acción en función de la política de seguridad de la empresa. Estas tres acciones están disponibles:Cerrar conexión con un mensaje de errorCerrar conexión sin mensaje de errorOmitir la conexión



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

No se pueden recibir mensajes de correo electrónico de algunos dominios

Problema:

El problema es la incapacidad de recibir los correos electrónicos de dominios específicos. Parece que el módulo CSC está bloqueando los correos electrónicos. Cuando se omite el módulo, todo funciona bien. Se recibe este mensaje de error: `2012/02/06 14:33:00 GMT+00:00 NRS 174.37.94.181 RBL-Fail QIL-NA RechazoWithErrorCode-550 NA 0 NA 0 NA NA NA NA 0 NA NA NA`

Solución:

Para resolver este problema, configure la función de reputación de correo electrónico correctamente.

Información Relacionada

- Compatibilidad con el módulo de servicios de seguridad Cisco ASA Content Security and Control (CSC)
- Soporte Técnico y Documentación - Cisco Systems