

CSC 6. X: Почтовый пример конфигурации репутации

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Настройка](#)

[Проверка](#)

[Устранение неполадок](#)

[Неспособный получить электронные письма от некоторых доменов](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет пример конфигурации о том, как настроить почтовую репутацию на Безопасности содержания Cisco и Контроле (CSC) модуль служб безопасности (SSM).

Предварительные условия

Требования

У вас должна быть Безопасность Плюс лицензия для использования этой функции.

Используемые компоненты

Сведения в этом документе основываются на SSM Безопасности содержания и Контроля Cisco с Версией релиза ПО 6.3.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании](#)

Общие сведения

Почтовая Репутация является технологией, которая уменьшает почты спама. Путем активации этой опции SSM CSC проверяет, является ли инициатор почты помещенным в черный список адресом или нет. Это ведет список баз данных, который содержит все IP-адреса, которые получают сообщения спама. Если почта, как находят, имеет инициатора из этого списка, ту почту считают спамом и отбрасывают.

Уровни сервиса, предлагаемые этой Почтовой Технологией Репутации (ERS), являются в основном двумя типами. Эти сервисы базируются в основном на уровне подлинности IP - адресов источника.

- Стандарт ERS - Содержит известные источники спама
- Усовершенствованный ERS - Содержит известные источники и подозреваемые источники

Когда IP-адрес добавлен к Стандартной базе данных ERS, это называют источником спама и редко, чтобы вы наблюдали IP-адрес, удаленный из этого списка. Стандарт ERS содержит список IP-адресов, которые последовательно иницируют спам.

Усовершенствованный ERS содержит список IP-адресов, которые предназначаются, чтобы быть удаленными, если найдено для не создания спама дальше. Например, взломанный Почтовый сервер может быть перечислен в этой базе данных в то время, когда это поставилось под угрозу. Когда это восстановлено норме, это удалено из этой базы данных.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Используйте инструмент Command Lookup \(только для зарегистрированных пользователей\) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.](#)

1. Выберите **Mail (SMTP)> Anti-spam> Email Reputation**. Новое окно открывается.
2. От целевой вкладки нажмите **Enable** для активации этой Почтовой опции Репутации.
3. Выберите **Advanced** для уровня сервиса.
4. От поля Approved IP Addresses задайте диапазон IP-адресов, которые вы хотите освободить от сканирования.

TREND MICRO™ InterScan™ for Cisco CSC SSM

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.

Target **Action**

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.

[Email Reputation Services Portal](#)

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. От вкладки Action задайте тип действия на основе вашего правила корпоративной безопасности. Эти три действия доступны: Близкое соединение с сообщением об ошибках, Близкое соединение без сообщения об ошибках, Обойдите соединение

TREND MICRO™ InterScan™ for Cisco CSC SSM

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.

Target **Action**

Standard Reputation Database Action

Intelligent action - Permanent denial of connection for Standard Reputation Database matches
SMTP error code: (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: (range 400 - 599; default=450)

Close connection with no error message

Bypass (not recommended)

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Неспособный получить электронные письма от некоторых доменов

Проблема:

Проблемой является неспособность получить электронные письма от определенных доменов. Кажется, что модуль CSC блокирует электронные почты. При обходе модуля все хорошо работает. Это сообщение об ошибках получено: 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

Решение:

Для решения этого вопроса настройте почтовую функцию репутации должным образом.

Дополнительные сведения

- [Безопасность содержания Cisco ASA и контроль \(CSC\) поддержка модулей сервисов безопасности](#)
- [Cisco Systems – техническая поддержка и документация](#)