

CSC 6.X : 电子邮件名誉配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[验证](#)

[故障排除](#)

[无法收到从一些域的电子邮件](#)

[相关信息](#)

[简介](#)

本文提供一配置示例关于怎样配置在思科内容安全和控制(CSC)安全服务模块(SSM)的电子邮件名誉。

[先决条件](#)

[要求](#)

您需要有一安全加上许可证使用此功能。

[使用的组件](#)

本文档中的信息根据与软件版本6.3的Cisco内容安全和控制SSM。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档规则的详细信息,请参阅 [Cisco 技术提示规则](#)。

[背景信息](#)

电子邮件名誉是减少垃圾邮件邮件的技术。通过启用此功能, CSC SSM验证, 如果邮件的创建人是一个列入黑名单的地址。它维护包含所有IP地址来源垃圾邮件消息数据库的列表。如果发现邮件

有从此列表的一创建人，该邮件认为垃圾邮件和丢弃。

此电子邮件名誉技术提供的服务级别(ERS)是基本上两个类型。这些服务主要根据级别IP原地址的真实性。

- ERS英文虎报-包含垃圾邮件已知来源
- ERS提前-包含已知来源和怀疑的来源

当IP地址被添加到ERS标准数据库时，它被叫做垃圾邮件来源并且是少见的您观察从此列表删除的一个IP地址。ERS英文虎报包含一致产生垃圾邮件IP地址的列表。

提前的ERS包含被认为删除，如果找到其中任一进一步不生产垃圾邮件IP地址的列表。例如，当减弱的时候，被删改的邮件服务器在此数据库可以列出。当它恢复对常态时，从此数据库删除。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

1. 选择**邮件(SMTP) >反垃圾邮件>电子邮件名誉**。此时将打开一个新窗口。
2. 从目标选项卡，请点击**Enable (event)**为了启用此电子邮件名誉功能。
3. 选择**先进**服务级别的。
4. 从已批准IP地址字段，请指定您要从扫描豁免的IP地址范围。

The screenshot shows the configuration interface for Trend Micro's InterScan for Cisco CSC SSM. The main heading is "SMTP Anti-spam (Email Reputation)". Below the heading, there is a description: "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." There are two tabs: "Target" and "Action". Under the "Target" tab, the status is "SMTP Anti-spam (Email Reputation): Disabled" with an "Enable" button. Below this, there is a section for "Set Service Level" with two radio buttons: "Standard" and "Advanced". The "Advanced" option is selected. The "Advanced" option description is: "Advanced: Uses both Standard and Dynamic Reputation databases to block messages from known and suspected spam sources. Click for more information." Below the service level section is the "Approved IP Address(es)" section, which has a text input field for "Add approved IP address:" and an "Add" button. Below that, there is a field for "Approved IP address(es):" containing "10.0.0.0/8" and a "Delete" button.

5. 从Action Tab，请指定根据您的企业安全策略的操作种类。这三操作是可用的：与错误消息的密切关系密切关系不出错误消息绕过连接

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.

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)

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

无法收到从一些域的电子邮件

问题：

问题是收到从特定域的电子邮件的无法。看来CSC模块阻塞电子邮件。当绕过模块时，一切良好工作。会收到以下错误消息：2012/02/06 14:33:00 GMT+00:00 NRS 174.37.94.181 RBL FAIL QIL-NA RejectWithErrorCode-550 NA 0 ONA NA NA 0 NA

解决方案：

为了解决此问题，请适当配置电子邮件名誉功能。

相关信息

- [思科ASA内容安全和控制\(CSC\)安全服务模块技术支持](#)
- [技术支持和文档 - Cisco Systems](#)