目录

简介

默认情况下思科电子邮件安全工具(ESA)不防止寻址消息的入站交付？从？去同一个域的同一个域。这允许消息是？伪装？由使与客户的事务合法的外部公司。一些公司依靠第三方组织代表公司发送电子邮件例如卫生保健、旅行社等等。

欺骗保护使用发送方验证

配置邮件流量策略(MFP)

1. 从 GUI：**邮寄策略>邮件流量策略>Add策略…**
2. 创建一新的MFP使用是相关的类似SPOOF_ALLOW的名称
3. 在*发送方验证*部分，请更改*使用发送方验证例外表*配置从**使用默认**到**OFF**。
4. 在**邮件策略>邮件流量策略>默认策略参数**，设置*使用发送方验证例外表*配置至**开**。

配置帽子

1. 从 GUI： **邮寄策略>帽子概述>Add发送方组…**
2. 相应地设置名称为创建的MFP前，即SPOOF_ALLOW。
3. 设置命令，因此在WHITELIST和黑名单发送方上组。
4. 分配**SPOOF_ALLOW**策略到此发送方组设置。
5. 单击**提交并且添加发送方…**
6. 添加IP或域您要允许伪装内部域的所有外部当事人的。

配置例外表

1. 从 GUI：**邮寄策略>例外表>Add发送方验证例外…**
2.
3.

验证

这时，来自*your.domain的*邮件*到*your.domainwould拒绝，除非发送方在发送方组SPOOF_ALLOW中列出，因为不使用发送方验证例外表的将关联对MFP。

此的示例将通过完成监听程序的一手工的远程登录会话看到：

553 SMTP答复是从例外表的直接响应结果如配置在从上面步骤的ESA。

从邮件日志，您能看到192.168.0.9的IP地址不在正确发送方组的有效IP地址：

匹配与从以上的步骤的配置示例的一个允许IP地址被看到如下：

相关信息

- 与搜索日志的REGEX的ESA、SMA和WSA Grep
- ESA消息处理确定
- 技术支持和文档 - Cisco Systems