SPF配置和最佳实践

目录

简介

本文档介绍思科邮件安全设备(ESA)上发件人策略框架(SPF)的不同场景。

先决条件

思科建议您了解以下主题：

- 思科ESA
- 所有AsyncOS版本

什么是SPF?

发件人策略框架(SPF)是一个简单的邮件验证系统，旨在通过提供允许接收邮件交换器检查从域管理员授权的主机发送传入邮件的机制来检测邮件欺骗。域的授权发送主机列表以特殊格式的TXT记录形式发布在该域的域名系统(DNS)记录中。电子邮件垃圾邮件和网络钓鱼通常使用伪造的发件人地址，因此发布和检查SPF记录可以视为反垃圾邮件技术。

对ESA是否会有很大的性能影响？

从CPU潜在客户看，不会对性能产生巨大影响。但是，启用SPF验证会增加DNS查询和DNS流量的数量。对于每条消息，ESA可能必须启动1-3个SPF DNS查询，这将导致DNS缓存提前过期。因此，ESA也将生成更多其他进程的查询。

除以前的信息外，SPF记录还将是TXT记录，可能比普通DNS记录大，并可能导致一些额外的DNS流量。

如何启用SPF?

以下说明来自《高级用户指南》中有关设置SPF验证的说明：

要在默认邮件流策略上启用SPF/系统独立数据格式(SIDF)，请执行以下操作：

1. 单击**Mail Policies > Mail Flow Policy**。
2. 单击“**Default Policy Parameters**”。
3. 在默认策略参数中，查看“安全**功能**”部分。
4. 在SPF/SIDF验证部分，单击**是**。
5. 设置一致性级别（默认为SIDF兼容）。 此选项允许您确定要使用的SPF或SIDF验证标准。除SIDF一致性外，您还可以选择SIDF兼容性，它将SPF和SIDF结合在一起。符合性级别详细信息可在《最终用*户指南》中找到。*
6. 如果选择与SIDF兼容的符合级别，请配置如果存在Resent-Sender，验证是否将PRA身份的**Pass** 结果降级**为None:**或重发自：邮件中显示的信头。出于安全考虑，您可以选择此选项。
7. 如果选择SPF的符合性级别，请配置是否对HELO身份执行测试。您可以使用此选项通过禁用HELO检查来提高性能。这非常有用，因为spf-passed过滤器规则首先检查PRA或MAIL FROM身份。设备仅对SPF一致性级别执行HELO检查。

要对SPF验证结果采取操作，请添加内容过滤器：

1. 为每种SPF/SIDF验证类型创建spf-status内容过滤器。使用命名约定来指示验证类型。例如，对通过SPF/SIDF验证的消息使用**SPF-Passed**，或对于在验证期间由于暂时错误而未通过的消息使用**SPF-TempErr**。有关创建spf-status内容过滤器的信息，请参阅GUI中的spf-status内容过滤器规则。
2. 处理某些SPF/SIDF验证的邮件后，单击**Monitor > Content Filters**，查看触发每个SPF/SIDF验证的内容过滤器的邮件数。

“Helo测试”开和关是什么意思？如果Helo测试从特定域失败，会发生什么情况？

如果选择SPF的符合性级别，请配置是否对HELO身份执行测试。您可以使用此选项通过禁用HELO检查来提高性能。这非常有用，因为spf-passed过滤器规则首先检查PRA或MAIL FROM身份。设备仅对SPF一致性级别执行HELO检查。

有效SPF记录

要通过SPF HELO检查，请确保为每个发送MTA（与域分离）包含SPF记录。 如果不包括此记录，HELO检查可能会对HELO标识**生成**无判定。如果您注意到域的SPF发件人返回大量**None**判定，则这些发件人可能没有为每个发送MTA包含SPF记录。

如果未配置邮件/内容过滤器，邮件将被传送。同样，您可以对每个SPF/SIDF裁决使用邮件/内容过滤器执行某些操作。

只为一个外部域启用它的最佳方法是什么？

要为特定域启用SPF，可能需要定义启用SPF的邮件流策略的新发件人组；然后按前面所述创建过滤器。

您能否对可疑垃圾邮件启用SPF检查？

思科反垃圾邮件在计算垃圾邮件分数时考虑了许多因素。拥有可验证的SPF记录可能会降低垃圾邮件分数，但仍有可能将这些邮件捕获为可疑垃圾邮件。

最佳的解决方案是允许列出发件人IP地址或创建邮件过滤器以跳过具有多个条件（remote-ip、mail-from、X-skipspamcheck报头等）的垃圾邮件检查。 发送服务器可以添加报头，以识别来自其他类型的消息。

相关信息

- 思科邮件安全设备 — 最终用户指南
- 电子邮件身份验证最佳实践 — 部署SPF/DKIM/DMARC
- 技术支持和文档 - Cisco Systems