查看DMARC报告并解决DMP验证问题

目录

简介

本文档介绍如何验证DMP处理的DMARC报告，以了解SPF和DKIM判定并维护安全的电子邮件生态系统。

SPF如何工作？

答：发件者策略框架(SPF)允许域所有者指定哪些发件人可以代表您的域发送邮件。

DKIM如何工作？

A.已识别的域密钥邮件(DKIM)使用密钥对。授权发件人向消息添加数字签名的私钥和接收者验证数字签名的真实性的公钥，确保消息在传输过程中未被修改。

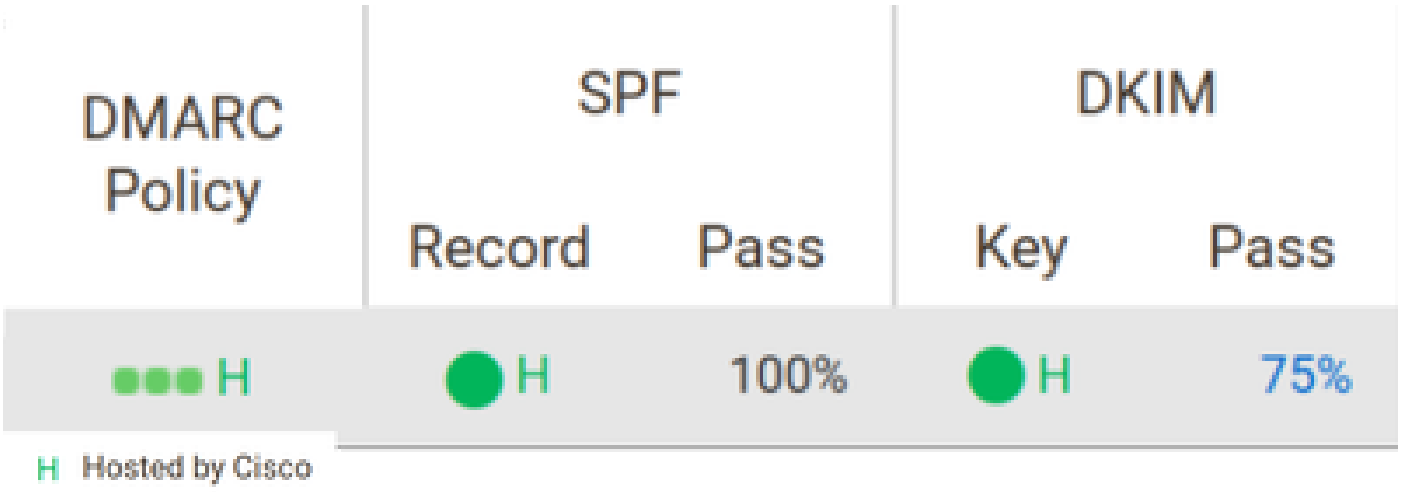
DMARC如何工作？

A.基于域的消息身份验证、报告和一致性(DMARC)确保所有可用身份与From报头保持一致。域所有者为接收者指定处理失败邮件的方式以及发送反馈报告的位置策略，以便轻松识别错误或网络钓鱼活动。

问：如何使用DMP设置电子邮件身份验证？

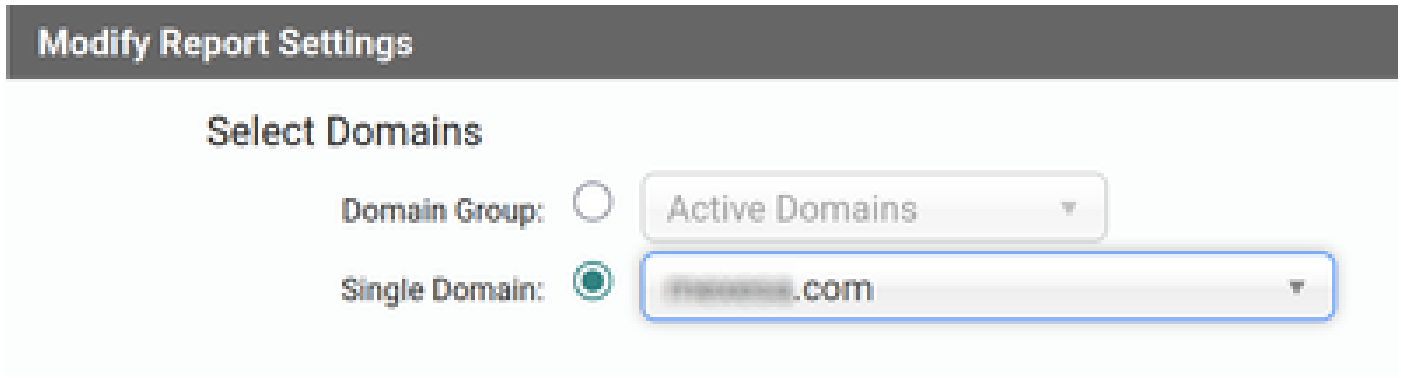
答：思科域保护(DMP)可以管理和托管您的SPF、DKIM和DMARC记录。它要求您在域中发布DNS TXT记录，以将管理委托给DMP。DMP托管您的记录后，您可以通过DMP管理门户管理批准的发件人、DKIM签名密钥和DMARC策略。

点击DMP控制面板中的配置已完成栏以验证您的域状态。



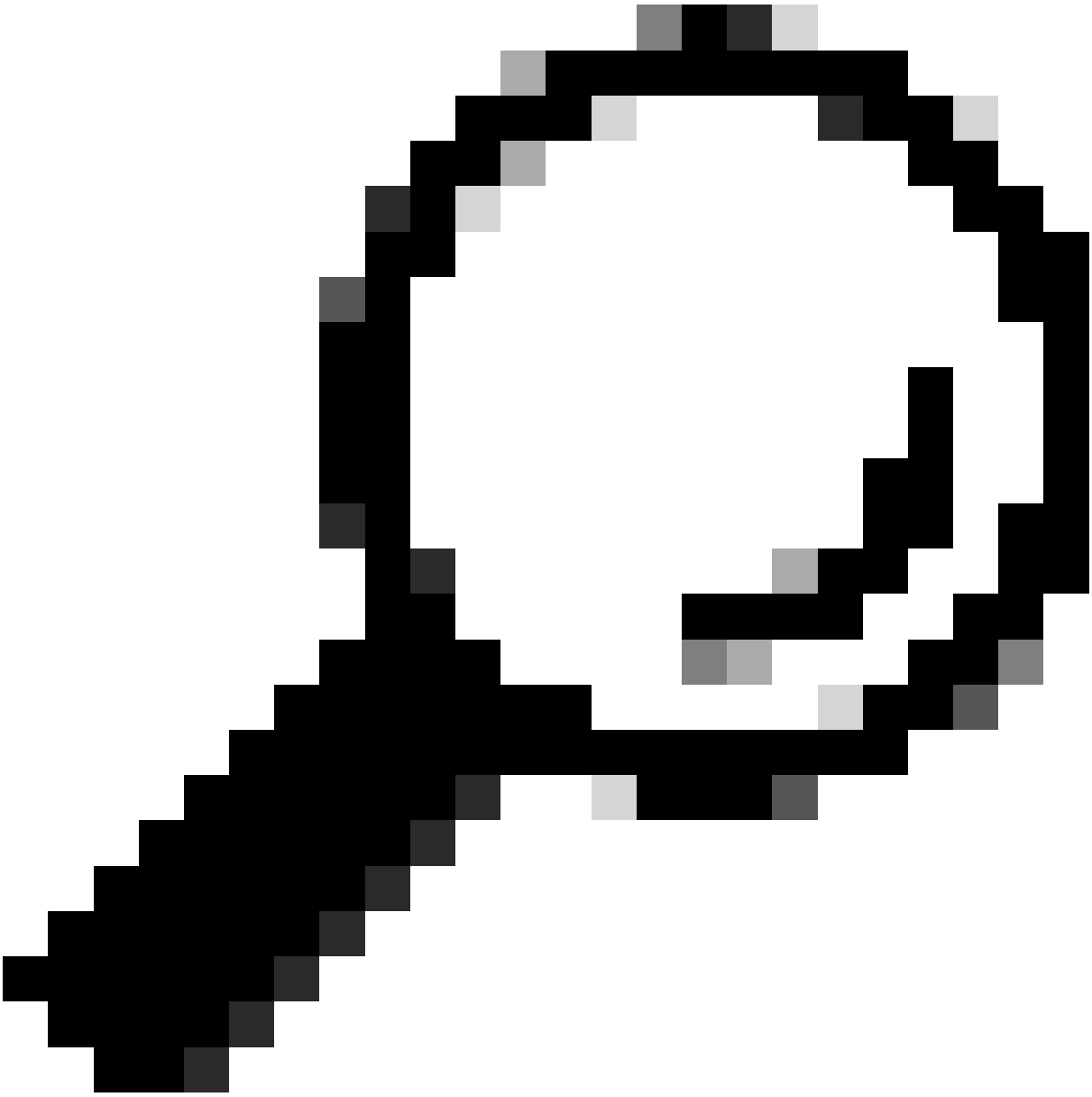
Q. DMP托管我的SPF记录、DKIM记录和DMARC策略。如何检测错误或恶意活动？

答：您可以通过DMP管理员门户诊断错误和恶意活动。导航到分析>电子邮件流量。单击修改设置按钮。选择Single Domain，然后从下拉菜单中选择域。



在Things I Can Fix部分下，选择What are my SPF problems? 或What are my DKIM problems? 报告。

将鼠标悬停在图表部分上可查看相应问题的说明，或单击某个部分可细化详细信息。



提示：在修改报告设置中选择更长的数据范围，以便准确了解您的电子邮件生态系统状态。您可以在域中找到您不知道或尚未对邮件进行签名的有效发件人。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。