茨雷斯岛FAQ ：如何使用TLS获取未加密茨雷斯岛回复？

目录

简介

本文描述如何使用传输层安全(TLS)获取从思科注册的信封服务(茨雷斯岛)的回复，允许用户不需要解密他们，与思科电子邮件安全工具(ESA)有关系。

如何使用TLS获取未加密茨雷斯岛回复？

默认情况下，对一安全电子邮件的回复由茨雷斯岛加密并且被发送到您的邮件网关。他们然后通过到为了最终用户加密的您的邮件服务器能打开与他们的茨雷斯岛凭证。

为了避免需要对于用户验证与茨雷斯岛打开安全回复，茨雷斯岛传送以“未加密”形式到支持TLS的邮件网关。 在大多数情况下邮件网关是ESA，并且此条款应用。

然而，如果有在ESA前面坐例如一个外部垃圾邮件过滤器的另一邮件网关，那里是对certificate/TLS/mail的没有需要在您的ESA的流程配置。在这种情况下，您能跳到在本文的Solution部分的步骤1到3。为了使未加密回复工作在此环境，外部垃圾邮件过滤器(邮件网关)是需要支持TLS的设备。如果他们支持TLS，您能有茨雷斯岛确认这和获得您设置为“未加密”回复为了巩固电子邮件。

发送方策略框架

为了避免发送方政策架构(SPF)验证失败，您必须添加mx ：res.cisco.com、mxnat1.res.cisco.com和mxnat3.res.csico.com对您的SPF记录。

您在哪里和怎样补充说您的SPF记录的茨雷斯岛依赖于怎样域名系统(DNS)在您的网络拓扑方面实现。与您的DNS管理员联系欲知更多信息。

如果DNS没有配置包括茨雷斯岛，当安全请撰写并且获取回复生成，并且传送通过主机密钥服务器，流出的IP地址不会匹配列出的IP地址在收件人结束，造成SPF验证失败。

主机名和IP地址

主机名	IP Address	记录类型
res.cisco.com	184.94.241.74	A

esa1.cres.iphmx.com	68.232.140.79	MX
esa2.cres.iphmx.com	68.232.140.57	MX
esa3.cres.iphmx.com	68.232.135.234	MX
esa4.cres.iphmx.com	68.232.135.235	MX
mxnat1.res.cisco.com	208.90.57.32	A
mxnat3.res.cisco.com	184.94.241.96	A

主机名和IP地址是随时根据服务/network维护和服务/network增长的变化。

解决方案

1. 获取并且安装一签名证书和中间证书在ESA。 **Note**: 是重要您从您的签署机关获取中间证书作为在设备来造成茨雷斯岛验证进程发生故障的证书示例。
2. 创建一项新的邮件流量策略： 从GUI，请选择**邮件策略>邮件流量策略>Add策略…**.输入名称并且留下所有在默认除了*安全功能：TLS.*设置此对**需要的**。
3. 创建一新的发送方组： 从GUI，请选择**邮件策略>帽子概述>Add发送方组…**.输入名称和集合订单编号对#1。 您能也输入一个可选注释。选择您在步骤2.事假创建一切别的东西空白的邮件流量策略。单击**提交并且添加发送方>>**。
4. 在发送方领域，请输入这些IP范围和主机名：
   ```
   .res.cisco.com
   .cres.iphmx.com
   208.90.57.0/26 (current CRES IP network range)
   204.15.81.0/26 (old CRES IP network range)
   ```
5. 提交并且确认更改。
6. 在您确信后ESA为从茨雷斯岛服务器的TLS准备，遵从在如何的步骤我测试，如果我的域支持与茨雷斯岛的TLS ？ 为了请求茨雷斯岛服务器开始使用TLS。

相关信息

- ESA FAQ ：什么是茨雷斯岛密钥服务器的IP和主机名？
- 思科电子邮件安全工具-最终用户指南
- 技术支持和文档 - Cisco Systems