思科RES:如何使用TLS保护未加密的RES回复

目录

简介

本文档介绍如何使用传输层安全(TLS)来保护来自思科注册信封服务(CRES)的回复，该服务允许用户不需要与思科邮件安全设备(ESA)关联进行解密。

思科RES:如何使用TLS保护未加密的RES回复

默认情况下，对安全邮件的回复由Cisco RES加密并发送到邮件网关。然后，它们会传递到已加密的邮件服务器，供最终用户使用其Cisco RES凭证打开。

为避免用户需要向Cisco RES进行身份验证才能打开安全回复，Cisco RES以“未加密”形式向支持TLS的邮件网关发送。在大多数情况下，邮件网关是ESA，本文适用。

但是，如果ESA前面有另一个邮件网关，例如外部垃圾邮件过滤器，则无需在ESA上配置证书/TLS/邮件流。在本例中，您可以跳过本文档“解决方案”部分的步骤1至3。对于在此环境中工作的未加密回复，外部垃圾邮件过滤器（邮件网关）是需要支持TLS的设备。如果他们确实支持TLS，您可以让思科RES确认此情况，并设置“未加密”回复以保护电子邮件。

发送方策略框架

为避免发件人策略框架(SPF)验证失败，您必须将mx:res.cisco.com、mxnat1.res.cisco.com和mxnat3.res.cisco.com添加到SPF记录。 或者，您可以在SPF记**录中“包括”spfc._spf**.cisco.com。

示例：

```
 ~ dig txt spfc._spf.cisco.com +short
"v=spf1 mx:res.cisco.com mx:sco.cisco.com ~all"
```

将思科RES添加到SPF记录的位置和方式取决于在网络拓扑中实施域名系统(DNS)的方式。 有关详细信息，请务必与DNS管理员联系。

如果DNS未配置为包括Cisco RES，当安全合成和安全回复通过托管密钥服务器生成并传送时，传出IP地址将与收件人端列出的IP地址不匹配，从而导致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
mxnat1.res.cisco.com	208.90.57.32	A
mxnat2.res.cisco.com	208.90.57.33	A
mxnat3.res.cisco.com	184.94.241.96	A
mxnat4.res.cisco.com	184.94.241.97	A
mxnat5.res.cisco.com	184.94.241.98	A
mxnat6.res.cisco.com	184.94.241.99	A
mxnat7.res.cisco.com	208.90.57.34	A
mxnat8.res.cisco.com	208.90.57.35	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

注意：主机名和IP地址可能因服务/网络维护或服务/网络增长而改变。 并非所有主机名和IP地址都用于服务。 此处提供了它们以供参考。

解决方案

1. 在ESA上获取并安装签名证书和中间证书。 **注意**：从签名机构获取中间证书非常重要，因为设备上的演示证书会导致CRES验证过程失败。
2. 创建新邮件流策略： 从GUI中，选择**Mail Policies > Mail Flow Policies > Add Policy...**。输入名称，并保留除安全功能以外的所*有默认值：TLS*。将此设置为**Required**。
3. 创建新发件人组： 从GUI中，选择**Mail Policies > HAT Overview > Add Sender Group...**。输入名称并将订单编号设置为#1。您也可以输入可选注释。选择您在步骤2中创建的邮件流策略。将其他内容留空。单击“**提交并添加发件人”>>**。
4. 在“发件人”字段中，输入以下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. 提交并提交更改。
6. 在您确信ESA已准备好从Cisco RES服务器使用TLS后，请执行How do I test if my domain

support TLS with Cisco RES?中的步骤，以请求Cisco RES服务器开始使用TLS。

相关信息

- **思科RES:密钥服务器的IP地址和主机名**
- **思科邮件安全设备 — 最终用户指南**
- **技术支持和文档 - Cisco Systems**