使用TLS加密配置CRES安全加密服务消息回复

目录

简介

Cisco RES：如何使用TLS保护未加密的RES应答

- 发送方策略框架
- 主机名和IP地址

解决方案

相关信息

简介

本文档介绍为CRES入站安全回复（而不是安全信封附件）配置TLS加密的操作。

Cisco RES：如何使用TLS保护未加密的RES应答

默认情况下，对安全邮件的回复由Cisco RES加密并发送到您的邮件网关。然后，它们会传递到您的邮件服务器，这些邮件服务器经过加密，可供最终用户使用其Cisco RES凭证打开。

为了在打开Cisco RES安全邮件回复时无需进行用户身份验证，Cisco RES会以“未加密”形式向支持传输层安全(TLS)的邮件网关提供身份验证。 在大多数情况下，邮件网关是思科邮件安全设备(ESA)，本文适用。

但是，如果另一个邮件网关位于ESA前面（例如外部垃圾邮件过滤器），则不需要在ESA上配置证书/TLS/邮件流。在这种情况下，您可以跳过本文档的“解决方案”部分中的步骤1 - 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。如果它们支持TLS，您可以让思科RES确认这一点，并让您设置“未加密”回复安全邮件。

发送方策略框架

为避免发件人策略框架(SPF)验证失败，请将这些值添加到SPF记录。

思科注册信封服务(CRES)SPF记录值与此表“主机名和IP地址”的IP/主机名匹配。

使用Cisco提供的SPF机制的输出：

<#root>

```
~ dig txt
```

res.cisco.com

```
 +short
"v=spf1
```

mx:res.cisco.com

exists:%{i}.spf.res.cisco.com

-all"

将此机制添加到现有SPF记录：

<#root>

include:res.cisco.com

包含新res.cisco.com机制的FAKE/test SPF记录示例：

<#root>

"v=spf1 mx:sampleorg1.com ip4:1.2.3.4

include:res.cisco.com

-all"

将Cisco RES添加到SPF记录的位置和方式取决于如何在网络拓扑中实施域名系统(DNS)。请务必联系您的DNS管理员以获取更多信息。

如果DNS未配置为包括Cisco RES，当通过托管密钥服务器生成和传送安全合成和安全应答时，传出IP地址与收件人末尾列出的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

主机名	IP Address	记录类型
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地址可能会因服务/网络维护或服务/网络增长而发生变化。并非所有主机名和IP地址都用于服务。此处提供以供参考。

解决方案

- 在ESA上获取并安装签名证书和中间证书。

  注意：您必须从签名机构获取中间证书，因为设备上的演示证书会导致CRES验证过程失败。

- 创建新的邮件流策略：
  a. 从GUI中选择Mail Policies > Mail Flow Policies > Add Policy。

  - 输入一个名称，并保留除“Security Features: TLS”以外的所有默认值。将此项设置为**Required**。

  - 创建新的发件人组：

a. 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。您还可以输入可选注释。选择您在第2步中创建的邮件流策略。将其他所有内容留空。
- 单击Submit 和Add Senders。

- 在Sender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)
```

-

提交并确认更改。

- 在您确信思科RES服务器已准备好协商TLS加密后，请执行CRES管理员门户中的步骤如何测试我的域是否支持使用思科RES的TLS?

相关信息

- Cisco RES：关键服务器的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

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）。