TLS的全面的设置指南在ESA

目录

简介

本文描述如何创建一证书为了用在传输层安全(TLS)上，激活入站和出站TLS，并且排除故障在思科的基本TLS问题给安全工具(ESA)发电子邮件。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

在ESA的TLS实施为电子邮件点对点传输提供保密性通过加密。它允许管理员导入一证书和专用密钥从Certificate Authority (CA)服务或者使用自签名证书。

电子邮件安全的思科AsyncOS支持*STARTTLS*分机对简单邮件传输协议(SMTP) (*在TLS的安全SMTP*)。

> **提示**：关于TLS的更多信息，参考RFC 3207。

> **Note**:本文描述如何安装证书在集群级与使用在ESA的*集中管理*功能。证书可以应用在级的计算机;然而，如果计算机从集群然后被添加的上一步删除，计算机级别证书将丢失。

功能概述和需求

管理员也许希望创建在设备的一自签名证书的任何这些原因：

- 为了加密与使用TLS的其他MTA的SMTP会话(入站和出站会话)
- 为了通过HTTPS启用在设备的HTTPS服务对GUI的访问的
- 为使用作为轻量级目录访问协议的(LDAP)一个客户端证书，如果LDAP服务器要求客户端证书
- 为了允许设备和Rivest沙米尔Addleman (RSA)企业管理器之间的安全通信数据丢失保护(DLP)
- 为了允许设备和思科先进的恶意软件保护(AMP)威胁网格设备之间的安全通信

ESA来预先配置与能使用为了建立TLS连接的演示证书。

> **Caution**:当演示证书为一安全TLS连接的建立时是满足的，请注意不能提供一可核实的连接。

思科建议您获取X.509，或者保密性增强版从CA的电子邮件(PEM)证书。这也许也指*Apache*证书。从CA的证书在自签名证书是理想，因为自签名证书类似于以前被提及的演示证书，不能提供一可核实的连接。

> **Note**:PEM证书格式是进一步定义在RFC 1421通过RFC 1424。 PEM是能包括公共证书的容器格式(例如与Apache安装和CA证书文件*/etc/ssl/certs*)或仅一条整个证书链，包括公共密钥、专用密钥和根证明。名称*PEM*是从安全电子邮件的一个失败的方法，但是使用的容器格式仍然是活跃并且是X.509 ASN.1密钥的base-64转换。

带来您自己的证书

选项导入您自己的证书是可用的在ESA;然而，需求是证书在*PKCS-12*格式。此格式包括专用密钥。管理员经常没有是可用的在此格式的证书。为此，思科建议您生成在ESA的证书并且安排它适当地签字由CA。

更新当前证书

如果已经存在的证书超时，请跳过本文的*部署的自签名证书*部分并且重签存在的证书。

> **提示**：欲了解更详细的信息参考更新在电子邮件安全工具Cisco文档的一证书。

部署自签名证书

此部分描述如何生成自签名证书和证书签名请求(CSR)，提供自签名证书给CA为签字，上传签名证书到ESA，指定证书为了用在ESA服务上和备份设备配置和证书。

生成自签名证书和CSR

为了通过CLI创建自签名证书，请输入**certconfig**命令。

完成这些步骤为了创建从GUI的一自签名证书：

1. 导航对**网络>证书**从设备GUI的**>Add证书**。
2. 点击**创建自签名证书**下拉菜单。

   当您创建证书时，请保证公*用名称*匹配侦听的接口的主机名，或者匹配交付接口的主机名。

   *侦听的*接口是与监听程序连接配置在**网络>监听程序下的**接口。

   *交付*接口自动地选择，除非明确地配置从CLI用**deliveryconfig**命令。
3. 对于一个可核实的Inbound连接，请验证这三个项目配比：

   MX纪录(域名系统(DNS)主机名)

   公用名称

   接口主机名

   Note:系统主机名不关于是影响TLS连接可核实的。系统主机名显示在设备GUI的右上角，或者从CLI **sethostname**命令输出。

> **Caution**:在您导出CSR前，请切记**提交**和**确认**您的更改。 如果这些步骤没有完成，新证书不会做到设备配置，并且从CA的签名证书不能签字，也没有应用对，已经存在的证书。

提供自签名证书给CA

完成这些步骤为了提交自签名证书到签字的CA ：

1. 保存CSR到在PEM格式(**网络>证书>验证名称>*下载证书签名请求***)的一台本地计算机。

2. 发送生成的证书对签字的被认可的CA。

3. 请求X.509/PEM/Apache被格式化的证书，以及中间证书。

CA然后生成在PEM格式的一证书。

Note:对于CA供应商列表，参考认证机关维基百科条款。

上传签名证书对ESA

在CA返回由专用密钥签字的委托公共证书后，您必须上传签名证书到ESA。证书可能然后与公共或私有监听程序、一IP接口HTTPS服务、LDAP接口，或者所有出站TLS连接一起使用对目的地域。

完成这些步骤为了上传签名证书到ESA ：

1. 保证委托是接收的用途PEM格式的公共证书，或者可以转换到PEM的格式，在您上传它到设备前。 **提示**：您能使用OpenSSLtoolkit，免费软件程序，为了转换格式。
2. 上传签名证书：

   导航对**网络>证书**。

   点击发送对签字的CA证书的名称。

   输入路径到在本地设备或网络音量的文件。

   Note: 当您上传新证书时，覆盖当前证书。中间证书与的自签名证书涉及可能也上传。

   Caution:在您上传签名证书后，请切记**提交**和**确认**更改。

指定证书为了用在ESA服务上

即然证书创建，签字，并且上传对ESA，可以用于需要证书使用情况的服务。

入站TLS

完成这些步骤为了使用证书入站TLS服务：

1. 导航给**网络>监听程序**。

2. 点击监听程序名称。

3. 选择从*证书*下拉菜单的验证名称。

4. 单击 **submit**。

5. 重复步骤1至4当必要时为所有另外的监听程序。

6. **确认**更改。

出站TLS

完成这些步骤为了使用证书出站TLS服务：

1. 导航**邮寄策略>目的地控制**。
2. 单击**编辑全局设置...**在*全局设置*部分。
3. 选择从*证书*下拉菜单的验证名称。
4. 单击 **submit**。
5. **确认**更改。

HTTPS

完成这些步骤为了使用证书HTTPS服务：

1. 导航对**网络> IP接口**。
2. 点击接口名称。
3. 选择从*HTTPS证书*下拉菜单的验证名称。
4. 单击 **submit**。
5. 重复步骤1至4当必要时为所有额外接口。
6. **确认**更改。

LDAP

完成这些步骤为了使用证书LDAP ：

1. 导航对**系统管理> LDAP**。
2. 单击**编辑设置...**在*LDAP全局设置*部分。
3. 选择从*证书*下拉菜单的验证名称。
4. 单击 **submit**。
5. **确认**更改。

URL 过滤

完成这些步骤为了使用证书URL过滤：

1. 输入**websecurityconfig**命令到CLI。
2. 通过命令提示继续。保证您选择**Y**，当您到达此提示符：

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. 选择关联与证书的编号。
4. 输入**commit命令**为了确认配置更改。

备份设备配置和证书

保证设备配置此时保存。设备配置包含通过以前描述的进程应用的完成证书工作。

完成这些步骤为了保存设备配置文件：

1. 导航到**系统管理>配置文件>下载文件到查看或保存的本地计算机。**
2. 导出证书：

   导航对**网络>证书。**

   点击**出口许可证。**

   选择证书导出。

   输入证书的文件名。

   输入证书文件的一个密码。

   点击**出口。**

   保存文件对本地或网络计算机。

   另外的证书可以此时导出，或者请点击**取消**为了返回到**网络>证书**位置。

   Note:此进程保存在PKCS-12格式的证书，创建并且保存有密码保护的文件。

激活入站TLS

为了激活所有Inbound的会话的TLS，请连接对Web GUI，选择**邮件策略>**已配置的入站监听程序的**邮件流量策略**，然后完成这些步骤：

1. 选择策略必须修改的监听程序。
2. 点击策略的名称的链路为了编辑它。

3. 在*安全功能请*区分，选择之一这些*加密和认证选项*为了设置为该监听程序和邮件流量策略要求的级别TLS ：

   当此选项选择时，没有使用TLS。

   首选的–当此选项选择时， TLS能从远程MTA协商到ESA。然而，如果远程MTA不协商(在一*220*答复的接收之前)， SMTP处理*无危险*继续(没加密)。尝试没有被做为了验证证书是否起源于委托认证机关。如果错误出现，在220答复接收后，则SMTP处理不下跌回到明文。

   需要的–当此选项选择时， TLS可以从远程MTA协商到ESA。 尝试没有被做为了验证域的证书。如果协商发生故障，电子邮件没有通过连接被发送。如果协商成功，则邮件通过加密的会话传送。
4. 单击 **submit**。

5. 点击**进行更改**按钮。如果需要您能此时添加一个可选注释。

6. 点击**进行更改**为了保存更改。

监听程序的邮件流量策略当前更新与您选择的TLS设置。

完成这些步骤为了激活从挑选套域到达的Inbound的会话的TLS ：

1. 连接对Web GUI并且选择**邮件策略>帽子概述**。

2. 添加发送方到适合的发送方组。

3. 编辑关联与发送方组您在上一步修改邮件流量策略的TLS设置。

4. 单击 **submit**。

5. 点击**进行更改**按钮。如果需要您能此时添加一个可选注释。

6. 点击**进行更改**为了保存更改。

发送方组的邮件流量策略当前更新与您选择的TLS设置。

> **提示**：参考以下条款欲知关于ESA如何的详情处理TLS验证：[什么是证书验证的算法在ESA？]

激活出站TLS

为了激活呼出会话的TLS，请连接对Web GUI，选择**邮件策略>目的地控制**，然后完成这些步骤：

1. 点击**添加目标....**

2. 添加目的地域(例如*domain.com*)。

3. 在*TLS支持部分*，请点击下拉菜单并且选择这些选项之一为了启用将配置TLS的种类：

无–当此选项选择时， TLS没有为从接口的出站连接协商到域的MTA。

首选的–当此选项选择时， TLS从ESA接口协商到域的MTA。然而，如果TLS协商发生故障(在220答复的接收之前)， SMTP处理*无危险*继续(没加密)。尝试没有被做为了验证证书是否起源于委托CA。如果错误出现，在220答复接收后，则SMTP处理不下跌回到明文。

需要的–当此选项选择时， TLS从ESA接口协商到域的MTA。尝试没有被做为了验证域的证书。如果协商发生故障，电子邮件没有通过连接被发送。如果协商成功，则邮件通过加密的会话传送。

首选的验证–当此选项选择时， TLS从ESA到域的MTA和设备尝试验证域证书协商。在这种情况下，这三种结果是可能的：

TLS协商，并且证书验证。邮件通过加密的会话传送。

TLS协商，但是证书没有验证。邮件通过加密的会话传送。

TLS联系没有被建立，并且证书没有验证。电子邮件消息在纯文本传送。**要求验证**–当此选项选择时， TLS从ESA协商到域的MTA，并且域证书的验证要求。在这种情况下，这三种结果是可能的：

TLS连接协商，并且证书验证。电子邮件消息通过加密的会话传送。

TLS连接协商，但是证书没有由委托CA验证。邮件没有传送。

TLS连接没有协商，但是邮件没有传送。

4. 其中任一进一步做是需要的目的地域的*目的地控制的*变动。

5. 单击 **submit**。

6. 点击**进行更改**按钮。如果需要您能此时添加一个可选注释。

7. 点击**进行更改**为了保存更改。

故障排除

此部分描述如何排除故障在ESA的基本TLS问题。

半成品证书

特别是当当前证书更新而不是新证书创建时，您应该寻找重复的半成品证书。中间证书也许已经更改或者也许已经不正确地被串连了，并且证书也许已经上传多个半成品证书。这能引入证书链和验证问题。

需要的TLS连接失败的Enable (event)通知

您能配置ESA为了发送警报，如果TLS协商发生故障，当消息传送对要求TLS连接的域时。警报消息包含目的地域的名称失败的TLS协商的。ESA传送警报消息对设置收到*系统*警报类型的警告严重级别警报的所有收件人。

Note: 这是全局设置，因此不可能设置根据一个每域基本类型。

完成这些步骤为了启用TLS连接警报：

1. 导航**邮寄策略>目的地控制。**
2. 单击**编辑全局设置。**
3. **当一需要的TLS连接发生故障**复选框时，请检查**发送警报。**

   提示：您能也配置与**destconfig的**此设置**>设置的**CLI命令。

ESA也记录TLS为域要求的实例，但是不可能用于设备邮件日志。当这些情况中的任一个符合时，这发生：

- 远程MTA不支持ESMTP (例如，没有了解*EHLO命令*从ESA)。
- 远程MTA支持ESMTP，但是*STARTTLS*命令不在其*EHLO*答复通告扩展的列表。
- 当ESA发送了*STARTTLS*命令，远程MTA通告*STARTTLS*分机，但是响应与错误。

找出邮件日志的成功的TLS通信会话

TLS连接在邮件日志被记录，与与消息涉及，例如过滤器操作，抗病毒和反垃圾邮件判决的其他重大的操作和交付尝试一起。如果有一成功的TLS连接，将有在邮件日志的一个TLS*成功*条目。同样，一失败的TLS连接导致一个TLS*失败的*条目。如果消息没有在日志文件的一个相关的TLS条目，该消息未在TLS连接传送。

提示：为了了解邮件日志，参考ESA消息处理确定Cisco文档。

这是一成功的TLS连接的示例从远程主机(接收)的：

```
Wed Jul 20 19:47:40 2005 Info: New smtp ICID 282204970 interface mail.example.com
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 ACCEPT SG None match SBRS None
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 TLS success
Wed Jul 20 19:47:40 2005 Info: Start MID 200257070 ICID 282204970
```

这是一失败的TLS连接的示例从远程主机(接收)的：

```
Tue Jun 28 19:08:49 2005 Info: New SMTP ICID 282204971 interface Management
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 ACCEPT SG None match SBRS None
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS failed
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 lost
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS was required but remote host did
```

```
not initiate it
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 close
```

这是一成功的TLS连接的示例对远程主机(交付)的：

```
Tue Jun 28 19:28:31 2005 Info: New SMTP DCID 834 interface 10.10.10.100 address
192.168.1.25 port 25
Tue Jun 28 19:28:31 2005 Info: DCID 834 TLS success protocol TLSv1 cipher
DHE-RSA-AES256-SHA
Tue Jun 28 19:28:31 2005 Info: Delivery start DCID 834 MID 1074 to RID [0]
```

这是一失败的TLS连接的示例对远程主机(交付)的：

```
Fri Jul 22 22:00:05 2005 Info: DCID 2386070 IP 10.3.4.5 TLS failed: STARTTLS
unexpected response
```

相关信息

- 思科电子邮件安全工具-最终用户指南
- 思科内容安全管理设备-最终用户指南
- 技术支持和文档 - Cisco Systems