

配置Inbound连接加密的TLS在ESA监听程序

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[通过GUI启用在一项帽子邮件流量策略的TLS监听程序的](#)

[通过CLI启用在一项帽子邮件流量策略的TLS监听程序的](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述如何启用传输层安全(TLS)在电子邮件安全工具的(ESA)监听程序。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据与所有AsyncOS版本的ESA。

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

您必须启用您需要Inbound连接的加密的所有监听程序的TLS。您也许要启用TLS在面对互联网的监听程序(公共监听程序),但是不内部系统的(私有监听程序)监听程序的。或者,您也许要启用所有监听程序的加密。默认情况下,私有和公共监听程序不允许TLS连接。您必须使在监听程序的主机访

问表(帽子)的TLS为了启用入站(接收)或出站(发送的)电子邮件的TLS。另外，私有和公共监听程序的邮件流量策略设置有TLS启用“默认情况下。

配置

您能指定TLS的三不同的设置在监听程序：

设置 含义

无 TLS没有为流入连接允许。对监听程序的连接不要求已加密简单邮件传输协议(SMTP)会话。这是您

首选的 TLS为对监听程序的流入连接允许从消息传输代理(MTA)。

需要的 TLS为对监听程序的流入连接允许从MTA，并且直到STARTTLS命令接收，除没有选项(NOOP)，E或者离开。如果TLS ‘需要的’含义发送方不想要已加密与TLS将由ESA拒绝的该电子邮件，在发送前

在帽子邮件流量策略的Enable (event) TLS监听程序的通过GUI

完成这些步骤：

1. 从Policies页的邮件流量，请选择策略您要修改然后单击策略名称的链路编辑的监听程序。(您也能编辑默认策略参数。)Policies页编辑的邮件流量显示。
2. 在“加密和验证”部分，为“使用TLS：”字段，选择您为监听程序希望的级别TLS。
3. 单击 **submit**。
4. 单击**进行更改**，如果需要，添加一个可选注释和然后单击**进行更改**为了保存更改。

Note:当您创建监听程序时，您能为对各自的公共监听程序的TLS连接分配一特定证书。

在帽子邮件流量策略的Enable (event) TLS监听程序的通过CLI

1. 请使用**listenerconfig > Edit**命令为了选择您要配置的监听程序。
2. 请使用**hostaccess > default**命令为了编辑监听程序的默认帽子设置。
3. 当提示时，请输入这些选择之一为了更改设置的TLS您：

```
Do you want to allow encrypted TLS connections?
```

- ```
1. No
2. Preferred
3. Required
[1]>3
```

```
You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there is a valid certificate configured.
```

注意此示例要求您使用**certconfig**命令为了保证有能使用与监听程序的有效证书。如果未创建任何证书，监听程序使用在设备被事先装配的演示证书。为了便于测试您能启用与演示证书的TLS，但是不安全和没有推荐为一般用途。请使用**listenerconfig > Edit > certificate**命令为了分配证书到监听程序。一旦配置TLS，设置在监听程序的摘要反射CLI的：

```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
```

TLS: Required

4. 输入**commit**命令为了启用更改。

## 验证

使用本部分可确认配置能否正常运行。

- 请使用文本邮件日志文件并且请参阅本文：[确定ESA是否使用TLS交付或接收](#)
- 使用消息跟踪：GUI：监视器>消息跟踪
- 使用报告：GUI：监视器> TLS连接
- 请使用第三方网站例如checktls.com

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

您能指定ESA是否发送警报，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传送警报消息到所有收件人设置收到系统警报类型的警告严重级别警报。您能通过GUI的系统管理>警报页管理提醒的收件人(或通过**alertconfig** in命令CLI)。

## 相关信息

- [电子邮件的最终用户指南AsyncOS](#)
- [技术支持和文档 - Cisco Systems](#)