FIPS 管理

本章包含以下部分：

FIPS 管理概述

联邦信息处理标准 (FIPS) 140 是美国和加拿大联邦政府共同开发且公开发布的标准，其中规定了政府机构用于保护敏感但非保密性信息的密码模块的要求。思科安全邮件网关使用思科 SSL 密码工具条件来实现 FIPS 140-3 1 级合规。

思科 SSL 密码工具包是一个 GCT 批准的加密套件，其中包括作为 OpenSSL FIPS 支持增强版的思科 SSL 以及符合 FIPS 标准的思科通 FIPS 对象模块。The Cisco FIPS Object Module is a software library that Secure Email Gateway uses for FIPS-validated cryptographic algorithms for protocols such as SSH and TLS.

FIPS 模式下的配置更改

设备处于 FIPS 模式时，邮件安全设备使用 Cisco SSL 和符合 FIPS 标准的证书进行通信。有关详细信息，请参阅将设备切换到 FIPS 模式, on page 2。

为了符合 FIPS 级别 1 标准，邮件安全设备会对配置进行以下更改：

- **SMTP 接收和传送**。在邮件安全设备上的公共侦听程序与远程主机之间通过 TLS 进行的传入和传出 SMTP 会话使用 TLS 版本 1.1 或 1.2 及 FIPS 密码套件。在 FIPS 模式下可以使用 sslconfig 修改密码套件。TLS v1 在 FIPS 模式下支持的唯一版本的 TLS。

- **Web 界面**。与邮件安全设备的 Web 界面进行的 HTTPS 会话使用 TLS 版本 1.1 或 1.2和 FIPS 密码套件。这还包括与垃圾邮件隔离区和其他 IP 接口的 HTTPS 会话。在 FIPS 模式下可以使用 sslconfig 修改密码套件。
- **证书**。FIPS 模式会限制设备使用的证书类型。证书必须使用以下签名算法之一：SHA-224、SHA-256、SHA-384 和 SHA-512，以及长度为 1024、2048 或更长的 RSA 密钥。设备不会导入不使用其中一种算法的证书。如果设备使用任何不符合标准的证书，则无法切换到FIPS模式。它将显示错误消息。有关详细信息，请参阅管理证书和密钥, on page 5。
- **DKIM 签名和验证**。用于 DKIM 签名的 RSA 密钥的长度必须为 2048 位，用于验证的 RSA 密钥的长度必须为 1024、1536 或 2048 位。如果设备使用任何不符合标准的 RSA 密钥，则无法切换到 FIPS 模式。它将显示错误消息。当验证 DKIM 签名时，如果签名不使用符合 FIPS 标准的密钥，设备会返回永久故障。请参阅管理用于 DKIM 签名和验证的密钥, on page 5
- **LDAPS**。邮件安全设备与 LDAP 服务器之间的 TLS 事务（包括使用 LDAP 服务器进行外部身份验证）使用 TLS 第 1 版和 FIPS 加密套件。如果 LDAP 服务器使用 MD5 散列存储密码，则由于 MD5 不符合 FIPS 标准，因此 SMTP 身份验证查询会失败。
- **日志**。SSH2 是允许通过 SCP 推动日志的唯一协议。对于与 FIPS 管理相关的错误消息，请阅读信息级别的 FIPS 日志。
- **集中管理**。对于集群化设备，FIPS 模式只能在集群级别打开。
- **SSL 密码**。仅在 FIPS 模式下支持符合 FIPS 的 SSL 密码。

将设备切换到 FIPS 模式

使用 fipsconfig CLI 命令将设备切换到 FIPS 模式。

Note 只有管理员可以使用此命令。将设备从非 FIPS 模式切换到 FIPS 模式后，需要重新启动。

准备工作

确保设备没有不符合FIPS标准的任何对象（例如，密钥长度为512位的DKIM验证配置文件）。要启用 FIPS 模式，必须修改所有不符合 FIPS 标准的对象以符合 FIPS 要求。请参阅FIPS 模式下的配置更改, on page 1。有关检查设备是否包含不符合 FIPS 标准的对象的说明，请参阅检查 FIPS 模式合规性, on page 4。

程序

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.

Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
- ENCRYPTCONFIG - Configure encryption of sensitive data in the appliance.
[]> setup

To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.
```

```
Are you sure you want to enable FIPS mode and reboot now ? [N]> yes

Do you want to minimize FIPS restriction on SMTP in the email gateway ? [N]> no

Enter the number of seconds to wait before forcibly closing connections.
[30]>

System rebooting. Please wait while the queue is being closed...
Closing CLI connection.
Rebooting the system...
```

在 FIPS 模式下加密敏感数据

使用 `fipsconfig>encryptconfig` 子命令加密设备中的敏感数据（例如密码和密钥）。如果启用此选项，

- 将对设备中的以下重要安全参数进行加密和存储：
  - 证书私钥
  - RADIUS 密码
  - LDAP 绑定密码
  - 本地用户的密码散列
  - SNMP 密码
  - DK/DKIM 签名密钥
  - 外发 SMTP 身份验证密码
  - PostX 加密密钥
  - PostX 加密代理密码
  - FTP 推送日志订用的密码
  - IPMI LAN 密码
  - 更新程序服务器 URL

Note 包括管理员在内，所有用户都无法查看配置文件中的敏感信息。

- 设备中的交换空间将加密，以便在设备的物理安全受到损害时防止任何未经授权的访问或调查攻击。

程序

```
mail1.example.com> fipsconfig

FIPS mode is currently disabled.

Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
- ENCRYPTCONFIG - Configure encryption of sensitive data in the appliance.
[]> encryptconfig
```

```
Do you want to enable encryption of sensitive data in the appliance?  [Y]> yes

Encryption is in enable state.
mail1.example.com>
```

检查 FIPS 模式合规性

使用 fipsconfig 命令检查设备是否包含任何不符合 FIPS 标准的对象。

程序

```
mail.example.com> fipsconfig

FIPS mode is currently disabled.

Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
- ENCRYPTCONFIG - Configure encryption of sensitive data in the appliance
[]> fipscheck

Currently, there are non-FIPS-compliant objects configured.

List of non FIPS compliant DKIM Verification Profiles:
               Profile Name             Key Size
------------------------------------------------------------
 1.            DEFAULT                  512

To be FIPS compliant, you must modify the above listed objects to meet FIPS requirements.
For more information, see the
FIPS Management chapter in the Cisco AsyncOS Email User Guide.

FIPS mode is currently disabled.
```

在 FIPS 模式下最小化 SMTP 上的 FIPS 限制

使用 `fipsconfig` -> `MINMIZEDATA` 子命令可最小化 FIPS 模式下对 SMTP 的 FIPS 限制。

```
mail.example.com> fipsconfig

FIPS mode is currently enabled.

Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
- MINIMIZEDATA - Minimize FIPS restriction on SMTP
- ENCRYPTCONFIG - Configure encryption of sensitive data in the appliance.
[]> minimizedata

FIPS restriction is currently enforced for SMTP in the email gateway.

When you change FIPS restriction, the email gateway reboots immediately. No commit is
required.

Do you want to minimize FIPS restriction on SMTP in the email gateway ? [N]>y
```

管理证书和密钥

AsyncOS 允许使用证书和私钥对加密设备与外部计算机之间的通信。可以上传现有证书和密钥对、生成自签名证书或生成证书签名请求 (CSR)，从而提交到证书颁发机构以获得公共证书。证书颁发机构将返回由私钥签名的可信公共证书，然后，可以将该证书上传到设备。

当设备处于 FIPS 模式时，可以继续

设备的 FIPS 模式为设备使用的证书施加了许多限制，以便设备符合 FIPS 标准。证书必须使用以下签名算法之一：SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512。

设备不会导入不使用其中一种算法的证书。如果在侦听程序中使用了任何不符合标准的证书，则设备还无法切换到 FIPS 模式。它将显示错误消息。

当设备处于 FIPS 模式时，设备的非 FIPS 状态将显示在 CLI 和 GUI 中。当选择用于某项功能（例如监听程序或目标控制）的证书时，设备不会显示不符合标准的证书作为选项。

有关在设备上使用证书的详细信息，请参阅证书的使用。

可以将符合 FIPS 标准的证书与以下任何服务配合使用：

- **SMTP 接收和传送**。使用**网络 > 侦听程序**页面（或 listenerconfig -> edit -> certificate CLI 命令）为需要使用 TLS 加密的任何侦听程序分配证书。您可能希望在面向互联网的侦听程序（即公共侦听程序）上启用TLS，或者为包括内部系统在内所有侦听程序（即专用侦听程序）启用加密。
- **目标控制**。使用**邮件策略 > 目标控制**页面（或 destconfig CLI 命令）分配证书作为用于邮件传送的所有外发 TLS 连接的全局设置。
- **接口**。使用**网络 > IP 接口**页面（或 interfaceconfig CLI 命令）为某个接口（包括管理接口）中的 HTTPS 服务启用证书。
- **LDAP**。使用**系统管理 (System Administration) > LDAP** 页面为需要 TLS 连接的所有 LDAP 流量分配证书。设备还可以将 LDAP 用于对用户的外部身份验证。

管理用于 DKIM 签名和验证的密钥

有关 DomainKeys 和 DKIM 如何在邮件安全设备上运行的概述，请参阅邮件验证。

相关主题

- DKIM 签名, on page 5
- DKIM 验证, on page 6

DKIM 签名

当创建 DKIM 签名密钥时，需要指定密钥大小。FIPS 模式下的邮件安全设备的仅 支持 2048 位的密钥大小。密钥越长越安全；但是，较长的密钥可能会影响性能。

如果设备使用任何不符合标准的 RSA 密钥，则无法切换到 FIPS 模式。它将显示错误消息。

在使用**邮件策略 (Mail Policies) > 域配置文件 (Domain Profiles)** 页面创建或编辑域配置文件时，符合FIPS 标准的签名密钥可用于域配置文件，并且会显示在“签名密钥”(Signing Key) 列表中。将签名密钥与域配置文件相关联后，可以创建包含公钥的DNS文本记录。为此，可以通过域配置文件列表中“DNS 文本记录”列的“生成”链接（或通过 CLI 中的 domainkeysconfig -> profiles -> dnstxt）。

DKIM 验证

设备要求邮件使用符合FIPS标准的密钥来验证DKIM签名。如果签名不使用符合FIPS标准的密钥，则设备会返回永久故障。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。