目 录

1 FIPS配置

1.1 简介

FIPS（Federal Information Processing Standards，联邦信息处理标准）140-2 是 NIST（National Institute of Standard and Technology，美国标准与技术研究所）颁布的针对密码算法安全的一个标准，它规定了一个安全系统中的密码模块应该满足的安全性要求。FIPS 140-2 定义了四个安全级别：Level 1、Level 2、Level 3 和 Level 4，它们安全级别依次递增，可广泛适应于密码模块的各种应用环境。目前，设备支持 Level 2。

若无特殊说明，文中的 FIPS 即表示 FIPS 140-2。

1.2 配置FIPS

通过使能 FIPS 模式，使得设备运行于支持 FIPS 140-2 标准的工作模式下。

1.2.1 配置准备

使能 FIPS 模式之前，还需要完成以下配置任务：

- 设置登录设备的用户名和密码，密码必须是大写字母、小写字母、数字以及特殊字符的组合，且最小长度为 6 位；
- 删除所有包含 MD5 算法的数字证书；
- 删除所有 RSA 密钥对和长度小于 1024 比特的 DSA 密钥对。

1.2.2 使能FIPS模式

使能 FIPS 模式并重启设备之后，设备将进入 FIPS 模式。

表1-1 使能 FIPS 模式

操作	命令	说明
进入系统视图	**system-view**	-
使能 FIPS 模式	**fips mode enable**	必选 缺省情况下，FIPS 模式处于关闭状态

注意

若要同时使能 FIPS 模式和 Password Control 功能，则必须先使能 FIPS 模式，再开启 Password Control 功能；若要同时关闭 FIPS 模式和 Password Control 功能，则必须先关闭 Password Control 功能，再关闭 FIPS 模式。

1.3 FIPS模式下的配置变化

使能 FIPS 模式并重启设备后，设备上的以下功能将发生变化：

- FTP/TFTP 服务器功能被禁用。
- Telnet 服务器功能被禁用。
- HTTP 服务器功能被禁用。
- SNMP v1 和 SNMP v2c 版本的 SNMP 功能被禁用，只允许使用 SNMP v3 版本。
- SSL 服务器只支持 TLS1.0 协议。
- SSH 服务器不兼容 SSHv1 客户端。
- 仅支持生成 1024～2048 位的 RSA/DSA 密钥对。
- SSH、SNMPv3、IPsec 和 SSL 不支持 DES、RC4、MD5 算法。

1.4 FIPS的自检处理

使能 FIPS 模式并重启设备后，系统会进行启动自检和条件自检来确保密码模块的功能正常运行。算法自检或条件自检失败后，设备均会自动重启。

1.4.1 启动自检（Power-up Self-tests）

启动自检是在设备启动过程中对 FIPS 允许使用的密码算法进行的自检。启动自检也称为已知结果的自检，即使用密码算法对已知的密钥和明文进行运算，如果运算结果与已知结果相同，则表示该算法的启动自检通过，否则表示自检失败。

启动自检又分为三种类型，具体内容如 表 1-2所示：

表1-2 启动自检列表

启动自检类型	自检操作
软件加密算法自检	对以下软件加密算法进行自检： • DSA（签名和验证） • RSA（签名和验证） • RSA（加密和解密） • AES • 3DES • SHA1 • HMAC-SHA1 • 随机数生成算法
加密引擎自检	在支持加密引擎的设备上，对以下加密引擎使用的算法进行自检： • DSA（签名和验证） • RSA（签名和验证） • RSA（加密和解密） • AES • 3DES • SHA1 • HMAC-SHA1 • 随机数生成算法

启动自检类型	自检操作
加密卡自检	在支持加密卡的设备上，对以下加密卡使用的算法进行自检： • AES • 3DES • SHA1 • HMAC-SHA1

1.4.2 条件自检（Conditional Self-tests）

条件自检是在非对称密码模块和随机数生成模块被使用时进行的自检，具体包括以下两种测试：

- 密钥对有效性测试：生成 DSA/RSA 非对称密钥对时进行的自检，具体为，首先使用公钥加密任意一段明文，然后使用对应的私钥对生成的密文进行解密，如果解密成功，则表示自检通过，否则自检失败。
- 随机数连续性测试：生成随机数的过程中进行的自检，如果前后两次生成的随机数不同，则表示自检通过，否则自检失败。该自检过程也会在生成 DSA/RSA 非对称密钥对时进行。

1.4.3 手工触发算法自检

当管理员需要确认当前系统中的密码算法模块是否正常工作时，可以手动触发密码算法自检。手工触发的密码算法自检内容与设备启动时自动进行的启动自检内容相同。

该自检失败后，设备会自动重启。

表1-3 手工执行算法自检

操作	命令	说明
手工触发算法自检	**fips self-test**	必选

1.5 FIPS的显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 FIPS 模式的状态，通过查看显示信息验证配置的效果。

表1-4 FIPS 的显示和维护

操作	命令
显示 FIPS 模式的状态	**display fips status**