目 录

1 FIPS配置

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 900	FIPS配置	不支持
MSR 930		不支持
MSR 20-1X		不支持
MSR 20		支持
MSR 30		支持，仅MSR 3016不支持
MSR 50		支持
MSR 2600		支持

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 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。

注意

如果出现反复自检失败重启的状况，有可能是设备内部的软件或者设备本身硬件损坏，需要更新软件或对设备硬件进行维修，请联系用服工程师解决。

1.2.1 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，具体内容如下表所示：

表1-1 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 • SHA256 • SHA512 • 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
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

1.2.2 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。

1.2.3 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。

1.3 配置FIPS

配置 FIPS 的基本配置思路如下：

(1) 使能 FIPS 功能；

(2) 使能 Password-control 功能；

(3) 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 10 位；

(4) 配置用户授权级别为 3 级，用户服务类型为 Terminal 服务或者 Web 服务；

(5) 删除所有包含 MD5 算法的数字证书；

(6) 删除所有 RSA 密钥对和长度小于 1024 比特的 DSA 密钥对；

(7) 保存配置。

1.3.2 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1-2 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。

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 DSA 密钥对。
- 仅支持生成 2048 位的 RSA 密钥对
- SSH、SNMPv3、IPsec 和 SSL 不支持 DES、RC4、MD5 算法。

1.3.3 配置手工触发算法自检

表1-3 配置手工执行算法自检

操作	命令	说明
进入系统视图	**system-view**	-
手工触发算法自检	**fips self-test**	必选

1.4 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**

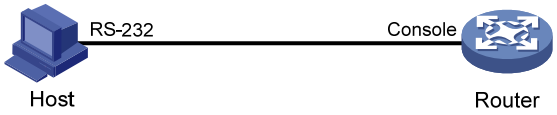
1.5 FIPS典型配置举例

1. 组网需求

- Host 通过 Console 口与路由器 Router 相连。
- 通过配置 Router，使终端 Host 成功登录路由器，并进入设备的 FIPS 模式。

2. 组网图

图1-1 进入设备 FIPS 模式登录组网图



3. 配置步骤

配置 FIPS 模式。

```
<Sysname> system-view
[Sysname] fips mode enable
```

开启密码管理功能。

```
[Sysname] password-control enable
```

在设备上添加一个本地用户 test，服务类型为终端用户类型，用户级别为 3 级，并设置其认证密码为 AAbbcc1234%（密码要包含大小写字母，数字和特殊符号组成，并且默认最短为 10 位）。

```
[Sysname] local-user test
[Sysname-luser-test] service-type terminal
[Sysname-luser-test] authorization-attribute level 3
[Sysname-luser-test] password
Password:***********
Confirm :***********
Updating user(s) information, please wait...........
[Sysname-luser-test] quit
```

注意

设置本地用户的密码时，请采用交互式方式进行设置，即本地用户视图下输入“passowrd”回车后，在提示信息下输入相应密码。

保存配置。

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
cfa0:/startup.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait....
 The current configuration is saved to the active main board successfully.
 Configuration is saved to device successfully.
[Sysname] quit
```

重启设备。

```
<Sysname> reboot
```

4. 验证结果

重启设备后，输入用户名（test）密码（AAbbcc1234%），提示首次登录成功，请用户输入新密码（新密码和老密码必须至少四个字符不同）并确认后，成功登录设备。

```
User interface con0 is available.

Please press ENTER.

Login authentication

Username:test
Password:
Info: First logged in. For security reasons you will need to change your password.
 Please enter your new password.
Password:**********
Confirm :**********
Updating user(s) information, please wait...........
<Sysname>
```

显示当前 FIPS 模式状态，可见设备工作在 FIPS 模式下。

```
<Sysname> display fips status
 FIPS mode is enabled
```

注意

- 如果配置 FIPS 模式之前未配置本地用户名或密码，只能通过忽略配置文件重启或删除配置文件后重新启动设备，设备恢复到非 FIPS 模式启动。
- 模式切换前要先修改时间，否则导致密码过期。关闭 FIPS 模式时必须先关闭 password-control 功能，然后再关闭 FIPS 模式，保存配置重启。有关 password-control 的具体情况，请参见“安全配置指导”中的“Password Control”