目 录

1 FIPS配置命令

1.1 FIPS配置命令

1.1.1 fips mode enable

【命令】

fips mode enable

undo fips mode enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

fips mode enable 命令用来开启 FIPS 模式。**undo fips mode enable** 命令用来关闭 FIPS 模式。

缺省情况下，FIPS 模式处于关闭状态。

设备支持的 FIPS 模式是符合 FIPS 140-2 标准的模式。

FIPS 模式必须在重启设备之后才会生效。在重启设备之前，还必须完成如下操作：

- 设置用户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 RSA 密钥对和长度小于 1024 比特的 DSA 密钥对。

重启设备以后，设备进入 FIPS 模式，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 服务器功能只支持 TLS1.0 协议。
- SSH 服务器功能不兼容 SSHv1 客户端。
- 仅支持生成 1024～2048 位的 RSA/DSA 密钥对。
- SSH、SNMP v3、IPsec 和 SSL 不支持 DES、RC4、MD5 算法。

相关配置可参考命令 **display fips status**。

【举例】

开启 FIPS 模式。

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

1.1.2 fips self-test

【命令】

fips self-test

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

无

【描述】

fips self-test 命令用来手工触发密码算法自检。

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，可以执行本命令触发密码算法自检。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。

【举例】

手工触发密码算法自检。

```
<Sysname> fips self-test
Self-tests are running. Please wait...
Self-tests succeeded.
```

1.1.3 display fips status

【命令】

display fips status

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

无

【描述】

display fips status 用来显示当前的 FIPS 模式状态。

相关配置可参考命令 **fips mode enable**。

【举例】

显示当前的 FIPS 模式状态。

```
<Sysname> system-view
<Sysname> display fips status
FIPS mode is enabled
```