目 录

1 FIPS

1.1 FIPS简介

FIPS（Federal Information Processing Standards，联邦信息处理标准）140-2 是 NIST（National Institute of Standards and Technology，美国国家标准与技术研究院）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，它们安全等级依次递增，可广泛适用于密码模块的各种应用环境。目前，设备支持 Level 2 级别的 FIPS 140-2。

若无特殊说明，本文中的 FIPS 即表示 FIPS 140-2。

1.2 配置限制和指导

- 执行 **fips mode enable** 命令之后，系统会提示用户选择启动方式，若用户未在 30 秒内作出选择，则系统默认用户采用了手动启动方式。
- 设备重启进入 FIPS 模式之前，系统会自动删除所有非 FIPS 模式下配置的密钥对和不符合 FIPS 标准（密钥位数小于 2048 位，签名 HSAH 算法为 MD5）的数字证书。因此，由非 FIPS 模式切换到 FIPS 模式后，用户将无法直接通过 SSH 方式登录设备。若需要进行 SSH 登录，必须先在 FIPS 模式下，通过 Console 口登录设备，并创建 SSH 服务器所需的密钥对，才能支持 SSH 用户登录。
- 登录 FIPS 模式下的设备时使用的用户密码必须符合 Password Control 密码管理策略，例如必须符合一定的密码长度策略、密码复杂度策略以及密码老化策略等。其中，密码的老化时间策略需要关注。当密码的使用时间超过老化时间后，系统会要求用户及时更换密码。一般设备的出厂系统时间比较早，等到进入 FIPS 模式之后再去调整正确的系统时间很可能会导致登录密码在下一次登录系统时过期。因此，如果选择自动重启方式进入 FIPS 模式，则建议在执行 **fips mode enable** 命令之前设置正确的系统时间；如果选择手动重启方式进入 FIPS 模式，则建议在配置本地用户名和密码之前设置正确的系统时间。
- 如果采用手动重启方式进入 FIPS 模式，在保存当前配置并设置为下次启动配置文件后，必须首先删除二进制类型的下次启动配置文件，然后再重启设备。如果不删除二进制类型的下次启动配置文件，则设备使用二进制配置文件启动时，FIPS 模式下不支持的命令（如果存在于配置文件中）也会被恢复，从而影响 FIPS 模式下系统的正常运行。
- 执行 **fips mode enable** 命令之后到系统重启之前的这个时间段，系统将进入一个准备进入 FIPS 模式之前的中间状态，若选择手动方式重启，则不建议在这个时间段执行除 **reboot**、**save** 以及相应的配置准备之外的其它命令，否则可能会不能达到预期的执行效果。
- 为保证自动重启方式进入的 FIPS 模式与非 FIPS 模式之间的配置成功进行回滚，设备进入 FIPS 模式后请首先保存配置，然后进行其它操作；为保证自动重启方式进入的非 FIPS 模式与 FIPS 模式之间的配置成功进行回滚，设备进入非 FIPS 模式后请首先保存配置，然后进行其它操作。
- 建议不要将 FIPS 模式状态不相同的设备进行 IRF。
- 如果在 IRF 环境下切换 FIPS 模式，需要重新启动整个 IRF 之后才能生效。

1.3 配置FIPS模式

1.3.1 进入FIPS模式

开启 FIPS 模式并重启设备之后，设备会运行于支持 FIPS 140-2 标准的工作模式下。在该工作模式下，系统将具有更为严格的安全性要求，并会对密码模块进行相应的自检处理，以确认其处于正常运行状态。

进入 FIPS 模式的设备同时也符合 CC（Common Criteria，公共准则）中的 NDPP（Network Device Protection Profile，网络设备保护特性）定义的功能要求。

系统提供了两种启动选择来进入 FIPS 模式：自动重启方式和手动重启方式。

1. 自动重启方式

该方式下，系统自动创建一个 FIPS 缺省配置文件（名称为 fips-startup.cfg），同时将其指定为下次启动配置文件，在要求用户完成配置下次登录设备所需的用户名和密码之后，自动使用 FIPS 缺省配置文件重启。具体步骤如下：

(1) 用户开启 FIPS 模式。

(2) 用户手工选择自动重启。如果在以下的输入过程中想退出配置流程，可以使用组合键<Ctrl+C>中断配置流程。配置流程中断后，已输入的开启 FIPS 模式的命令将不被执行。

(3) 用户手工配置登录 FIPS 模式的设备时所使用的用户名和密码。该用户将会成为 FIPS 模式中安全管理员（Crypto Officer），其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 15 位。

(4) 用户成功设置安全管理员用户名和登录密码之后，系统自动使用指定的启动配置文件重启。

(5) 系统进入 FIPS 模式。用户只能通过步骤（3）设置的用户名和密码登录运行于 FIPS 模式的设备。

2. 手动重启方式

该方式下，系统不自动创建进入 FIPS 模式的下次启动配置文件，需要用户手工完成进入 FIPS 模式所需的所有必要配置之后，手工重启设备。具体步骤如下：

(1) 用户完成以下配置准备，主要包括：

- 开启全局 Password Control 功能。
- 设置全局 Password Control 密码组合类型的个数为 4，每种类型至少 1 个字符。
- 设置全局 Password Control 的密码最小长度为 15。
- 添加设备管理类本地用户，设置密码、用户角色和服务类型。本地用户的密码需要符合以上 Password Control 配置的限制，用户角色必须是 network-admin，服务类型为 terminal。
- 删除不符合 FIPS 标准的本地用户服务类型（Telnet、HTTP 和 FTP）。

(2) 用户开启 FIPS 模式。

(3) 用户手工选择手动重启。

(4) 用户手工保存当前配置文件并设置为下次启动配置文件。

(5) 用户手工删除二进制类型的下次启动配置文件（文件名后缀为“.mdb”）。

(6) 重启设备。

(7) 系统进入 FIPS 模式。用户只能通过步骤（1）设置的本地用户名和密码登录处于 FIPS 模式的设备。

表1-1 开启 FIPS 模式

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

1.3.2 FIPS模式下的配置变化

系统进入 FIPS 模式，设备上的以下功能将发生变化：

- 仅支持 **scheme** 类型的用户登录认证方式。
- FTP/TFTP 服务器和客户端功能被禁用。
- Telnet 服务器和客户端功能被禁用。
- HTTP 服务器功能被禁用。
- SNMPv1 和 SNMPv2c 版本的 SNMP 功能被禁用，只允许使用 SNMPv3 版本。
- SSL 服务器功能只支持 TLS1.0、TLS1.1、TLS1.2 协议。
- SSH 服务器功能不兼容 SSHv1 客户端，不支持 DSA 类型的密钥对。
- 仅支持生成 2048 位的 RSA 密钥对和 2048 位的 DSA 密钥对。因此设备作为服务器时，若要求对客户端进行公钥认证，则客户端的密钥对也需要为 2048 位，否则服务器将会拒绝客户端的连接。
- 仅支持 256 位以上的 ECDSA 密钥对。因此设备作为服务器时，若要求对客户端进行公钥认证，则客户端的密钥对也需要为 256 位以上，否则服务器将会拒绝客户端的连接。
- SSH、SNMPv3、IPsec 和 SSL 不支持 DES、3DES、RC4、MD5 算法。
- 不能关闭全局 Password Control 功能，即 **undo password-control enable** 命令执行后不生效。
- 部分特性中的密码设置将具有更严格的安全性要求：
  - AAA 服务器的共享密钥、IKE 协商的预共享密钥、SNMPv3 用户的认证密钥都必须满足固定的要求：密码最小长度为 15，密码元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）。
  - 设备管理类本地用户的密码和用户角色切换密码受 Password Control 密码策略的管理，缺省要求为：密码最小长度为 15，密码元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）。

1.3.3 退出FIPS模式

关闭 FIPS 模式并重启设备之后，设备会返回到非 FIPS 的工作模式下。

系统提供了两种启动方式来退出 FIPS 模式：

- 自动重启方式：系统自动创建一个非 FIPS 缺省配置文件（名称为 non-fips-startup.cfg），同时将其指定为下次启动配置文件，之后自动使用非 FIPS 缺省配置文件重启。重启之后，当前登录用户不需要输入任何信息即可直接登录到非 FIPS 模式的系统。

- 手动重启方式：系统不自动创建进入非 FIPS 模式的下次启动配置文件，需要用户手工完成进入非 FIPS 模式所需的所有必要配置之后，手工重启设备。重启之后，当前登录用户需要根据配置的登录认证方式输入相应的用户信息登录到非 FIPS 模式的系统。

从 FIPS 模式切换到非 FIPS 模式时，登录设备的缺省认证方式如下，用户也可根据实际情况修改登录认证方式：

- 通过 VTY 用户线登录设备时的缺省认证方式为 **password**。
- 通过 Console 口登录设备时的缺省认证方式均为 **none**。

关闭 FIPS 模式之后、选择手动重启设备之前，需要注意的是：

- 对于当前远程登录的用户，若要登录非 FIPS 模式，则必须在不退出当前用户线的情况下，重新设置登录设备的认证方式为 **scheme**，并设置对应的登录用户和密码（也可使用当前的登录用户和密码）。
- 对于当前通过 Console 口登录的用户，若要登录非 FIPS 模式的系统：
  - 如果使用 **password** 登录认证方式，则还需要设置相应的认证方式为 **password**，并设置对应的登录密码。
  - 如果使用 **scheme** 登录认证方式，则需要设置相应的认证方式为 **scheme**，并设置对应的登录用户和密码（也可使用当前的登录用户和密码）。
  - 如果使用 **none** 登录认证方式，则需要设置相应的认证方式为 **none**。

表1-2 关闭 FIPS 模式

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

1.4 FIPS密码算法自检处理

FIPS 模式处于开启状态之后，为确保密码算法模块的功能正常运行，系统会进行一定的自检处理，具体包括启动自检、条件自检。启动自检失败后，设备自动重启。条件自检失败后，设备不重启，但系统会输出密码算法自检失败的提示信息。

设备运行过程当中，当用户或管理员需要确认当前 FIPS 模式下的系统中的密码算法模块是否正常工作时，可以通过执行命令来手工触发系统进行密码算法自检工作。手工自检失败后，整个设备会自动重启。

注意

如果自检失败，请联系用服工程师解决。

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。

启动自检包括：

- KAT（Known-answer Test，已知结果测试）：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。
- PWCT（Pairwise Conditional Test，密钥对有效性测试）
  - 签名和验证：生成 DSA/RSA/ECDSA 非对称密钥对时进行的自检，具体为，首先使用私钥对指定数据进行签名，然后使用公钥对该签名数据进行验证，如果解密成功，则表示自检通过，否则自检失败。
  - 加密和解密：生成 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。

启动自检具体内容如 表 1-3 所示。

表1-3 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： • SHA1、SHA224、SHA256、SHA384、SHA512（KAT） • HMAC-SHA1、HMAC-SHA224、HMAC-SHA256、HMAC-SHA384、HMAC-SHA512（KAT） • AES（KAT） • RSA 签名和验证（KAT） • RSA 签名和验证（PWCT） • RSA 加密和解密（PWCT） • DSA 签名和验证（PWCT） • ECDSA 签名和验证（PWCT） • DRBG（KAT） • ECDH (KAT) • GCM (KAT) • GMAC (KAT)

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：

- 签名和验证的 PWCT：生成 DSA/RSA 非对称密钥对时进行的自检，具体为，首先使用私钥对指定数据进行签名，然后使用公钥对该签名数据进行验证，如果验证成功，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（Power-up Self-tests）内容相同。该自检失败后，设备会自动重启。

表1-4 手工触发密码算法自检

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

1.5 FIPS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1-5 FIPS 的显示和维护

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

1.6 FIPS典型配置举例

1.6.1 自动重启设备进入FIPS模式

1. 组网需求

自动重启设备进入 FIPS 模式，并采用 Console 口登录 FIPS 模式的设备。

2. 配置步骤

若要保存当前配置，请在开启 FIPS 模式之前，执行 **save** 命令。

开启 FIPS 模式，并选择自动重启方式进入 FIPS 模式。设置用户名为 root，对应的密码为 12345zxcvb!@#$%ZXCVB。

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:y
The system will create a new startup configuration file for FIPS mode. After you set the login
username and password for FIPS mode, the device will reboot automatically.
Enter username(1-55 characters):root
Enter password(15-63 characters):
Confirm password:
Waiting for reboot... After reboot, the device will enter FIPS mode.
```

注意

在Reboot the device automatically?提示后，请不要使用Ctrl+c退出，否则设备将通过手动重启方式进入FIPS模式。有关手动重启方式的详细介绍和配置准备请参见 1.3.1 2. 手动重启方式。

3. 验证结果

重启设备后，输入用户名 root 和对应的密码。首次登录时，系统会提示重置密码。重置密码成功后，进入 FIPS 模式的系统。重置的密码必须是大写字母、小写字母、数字以及特殊字符的组合，最小长度为 15 位，且需要与旧密码不同（具体要求请见系统提示）。

```
Press ENTER to get started.
login: root
Password:
First login or password reset. For security reason, you need to change your password. Please enter your password.
old password:
new password:
confirm:
Updating user information. Please wait ... ...
…（略）
<Sysname>
```

显示当前 FIPS 模式状态。

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

查看缺省的配置文件内容。

```
<Sysname> more fips-startup.cfg
#
 password-control enable
#
local-user root class manage
 service-type terminal
 authorization-attribute user-role network-admin
#
 fips mode enable
#
return

<Sysname>
```

1.6.2 手动重启设备进入FIPS模式

1. 组网需求

手动重启设备进入 FIPS 模式，并采用 Console 口登录 FIPS 模式的设备。

2. 配置步骤

开启全局 Password Control 功能。

```
<Sysname> system-view
[Sysname] password-control enable
```
设置全局 Password Control 密码组合类型的个数为 4，每种类型至少一个字符。
```
[Sysname] password-control composition type-number 4 type-length 1
```
设置全局 Password Control 的密码最小长度为 15。
```
[Sysname] password-control length 15
```
添加设备管理类本地用户：用户名为 test、密码为 12345zxcvb!@#$%ZXCVB、用户角色为 network-admin，服务类型为 Terminal。
```
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password simple 12345zxcvb!@#$%ZXCVB
[Sysname-luser-manage-test] authorization-attribute user-role network-admin
[Sysname-luser-manage-test] service-type terminal
[Sysname-luser-manage-test] quit
```
开启 FIPS 模式，并选择手动重启方式进入 FIPS 模式。
```
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:n
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.
```
将当前配置保存到存储介质的根目录，并将该文件设置为下次启动配置文件。
```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[Sysname] quit
```
删除二进制类型的下次启动配置文件。
```
<Sysname> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.
```
重启设备。
```
<Sysname> reboot
```
3. 验证结果

重启设备后，输入用户名 test 和对应的密码首次登录时，系统会提示重置密码。重置密码成功后，进入 FIPS 模式的系统。重置的密码必须是大写字母、小写字母、数字以及特殊字符的组合，最小长度为 15 位，且需要与旧密码不同（具体要求请见系统提示）。
```
Press ENTER to get started.
login: test
Password:
First login or password reset. For security reason, you need to change your pass
word. Please enter your password.
```

```
old password:
new password:
confirm:
Updating user information. Please wait ... ...
…（略）
<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.
```

1.6.3 自动重启设备退出FIPS模式

1. 组网需求

当前用户已使用 Console 口登录到 FIPS 模式，要求自动重启设备退出 FIPS 模式。

2. 配置步骤

关闭 FIPS 模式。

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode and then reboot automatically. Continue? [Y/N]:y
Waiting for reboot... After reboot, the device will enter non-FIPS mode.
```

3. 验证结果

重启设备后，用户可直接进入系统。

```
<Sysname>
```

显示当前 FIPS 模式状态。

```
<Sysname> display fips status
FIPS mode is disabled.
```

1.6.4 手动重启设备退出FIPS模式

1. 组网需求

当前用户已使用 SSH 远程登录到 FIPS 模式，用户名为 test、密码为 12345zxcvb!@#$%ZXCVB，要求手动重启设备退出 FIPS 模式。

2. 配置步骤

关闭 FIPS 模式。

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode, and then reboot automatically. Continue? [Y/N]:n
Change the configuration to meet non-FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter non-FIPS mode.
```

设置登录 VTY 用户线的登录认证方式为 **scheme**。

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
```

将当前配置保存到存储介质的根目录，并将该文件设置为下次启动配置文件。

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[Sysname] quit
```

删除二进制类型的下次启动配置文件。

```
<Sysname> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.
```

重启设备。

```
<Sysname> reboot
```

3. 验证结果

重启设备后，输入用户名 test 和对应的密码 12345zxcvb!@#$%ZXCVB，进入非 FIPS 模式的系统。

```
Press ENTER to get started.
login: test
Password:
Last successfully login time:…
（略）
<Sysname>
```

显示当前 FIPS 模式状态，可见设备工作在非 FIPS 模式下。

```
<Sysname> display fips status
FIPS mode is disabled.
```