H3C NIST FIPS 140
コンフィギュレーションガイド

New H3C Technologies Co., Ltd.
https://www.h3c.com/

ドキュメントバージョン：6W100-20200907

環境保護

この製品は、環境保護要件に準拠するように設計されています。この製品の保管、使用、および廃棄は、適用される国内法および規制を満たしている必要があります。

序文

このガイドでは、H3C NIST FIPS 140について説明します。この序文に

は、ドキュメントに関する次のトピックが含まれています:

- 対象読者。
- 表記法。
- ドキュメントへのフィードバック。

対象読者

このドキュメントの対象読者は次のとおりです:

- ネットワーク計画者。
- フィールドテクニカルサポートおよびサービスエンジニア。
- Cloudnetを使用するネットワーク管理者。

表記法

次の情報は、ドキュメントで使用されている表記法について説明しています。

コマンド規則

表記法	説明
太字	**太字** のテキストは、示されている文字の通りに入力するコマンドとキーワードを表します。
イタリック	*イタリック のテキストは、示されている文字の通りに入力するコマンドとキーワードを表します。*
[ ]	角括弧は、オプションの構文の選択肢（キーワードまたは引数）を囲みます。
{ x | y | ... }	中括弧は、垂直バーで区切られた必要な構文の選択肢のセットを囲み、そこから1つを選択します。
[x | y | ...]	角括弧は、縦棒で区切られたオプションの構文の選択肢のセットを囲み、そこから1つまたは何も選択しません。
{ x | y | ... } *	アスタリスクでマークされた中括弧は、垂直バーで区切られた必要な構文の選択肢のセットを囲み、そこから少なくとも1つを選択します。
[x | y | ...] *	アスタリスクでマークされた角括弧は、垂直バーで区切られたオプションの構文の選択肢を囲み、そこから1つの選択肢、複数の選択肢、または何も選択しません。
&<1-n>	アンパサンド（&）記号の前の引数またはキーワードと引数の組み合わせは、1～n回入力できます。
#	シャープ（#）記号で始まる行はコメントです。

GUIの規則

表記法	説明
太字	ウインドウ名、ボタン名、フィールド名、およびメニュー項目は太字で表示されます。例えば、**New User** ウインドウを開いて**OK** をクリックします。
>	マルチレベルメニューは山括弧で区切られています。例えば、**File** > **Create** > **Folder**.

記号

表記法	説明
警告！	理解または従わないと怪我につながる可能性のある重要な情報に注意を喚起する警告。
注意：	重要な情報に注意を喚起する警告。理解または従わないと、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性があります。
重要：	重要な情報に注意を喚起する警告。
注意：	追加情報または補足情報を含む警告。
ヒント：	役立つ情報を提供する警告。

ネットワークトポロジーアイコン

表記法	説明
	ルーター、スイッチ、ファイアウォールなどの一般的なネットワークデバイスを表します。
	ルーターやレイヤー3スイッチなどのルーティング対応デバイスを表します。
	レイヤー2またはレイヤー3スイッチなどの汎用スイッチ、またはレイヤー2転送およびその他のレイヤー2機能をサポートするルーターを表します。
	統合有線WLANスイッチ上のアクセスコントローラ、統合有線WLANモジュール、またはアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネーターを表します。
	メッシュアクセスポイントを表します。
	全方向性信号を表します。
	指向性信号を表します。
	ファイアウォール、UTM、マルチサービスセキュリティゲートウェイ、負荷分散デバイスなどのセキュリティ製品を表します。
	ファイアウォール、負荷分散、NetStream、SSL VPN、IPS、ACGモジュールなどのセキュリティモジュールを表します。

このドキュメントで提供される例

このドキュメントの例では、ハードウェアモデル、構成、またはソフトウェアバージョンがデバイスとは異なるデバイスを使用している場合があります。例で示されるポート番号、サンプル出力、スクリーンショット、およびその他の情報は、デバイスにあるものとは異なる場合があります。

ドキュメントへのフィードバック

製品マニュアルに関するご意見は、info@h3c.comまで電子メールでお寄せください。

ご感想をお寄せいただければ幸いです。

内容

FIPSの設定

この機能のサポートは、デバイスモデルによって異なります。詳細については、「*H3Cアクセスコントローラコンフィギュレーションガイド*」を参照してください。

概要

Federal Information Processing Standards(FIPS)は、米国のNational Institute of Standard and Technology(NIST)によって開発されました。FIPSは、暗号モジュールの要件を規定しています。FIPS140 - 2では、「Level 1」から「Level 4」までの4つのセキュリティレベル(低から高)が定義されています。デバイスはLevel 2をサポートします。
特に明記しない限り、本書では「FIPS」という用語はFIPS140 - 2を指します。

FIPSセルフテスト

注意:
デバイスが繰り返し再起動する場合は、ソフトウェアの障害またはハードウェアの損傷が原因である可能性があります。H3Cサポートに連絡して、ソフトウェアをアップグレードするか、破損したハードウェアを修理してください。

デバイスがFIPSモードで動作している場合は、電源投入時のセルフテストや、条件付きセルフテストなどの、セルフテストメカニズム使用して、暗号モジュールが正しく動作することを確認します。

電源投入時セルフテスト

「既知の応答テスト」とも呼ばれる電源投入時セルフテストでは、FIPS許可暗号化アルゴリズムの可用性が検証されます。暗号化アルゴリズムは、正しい出力が既知のデータに対して実行されます。計算された出力は既知の応答と比較されます。それらが同一でない場合、既知の応答テストは失敗します。
電源投入時セルフテストでは、表1に示す暗号アルゴリズムが検証されます。

表1 電源投入時セルフテストリスト

タイプ	操作
暗号アルゴリズムセルフテスト	以下のアルゴリズムをテストします。 •DSA(署名と認証) •RSA(署名と認証) •RSA(暗号化および復号化) •AES •3DES (SHA)1 •256 •512 •HMAC-SHA1 •乱数生成アルゴリズム
暗号化エンジンのセルフテスト	暗号化エンジンが使用する次のアルゴリズムをテストします。 •DSA(署名と認証) •RSA(署名と認証) •RSA(暗号化および復号化) •AES •3DES (SHA)1 •HMAC-SHA1 •乱数生成アルゴリズム

条件付きセルフテスト

条件付きセルフテストは、非対称暗号化モジュールまたは乱数生成モジュールが起動されたときに実行されます。条件付きセルフテストには、次のタイプがあります。

- **Pair-wise consistency test** - このテストは、DSA/RSA非対称キーペアが生成されたときに実行されます。公開キーを使用してプレーン・テキストを暗号化し、秘密キーを使用して暗号化テキストを復号化します。復号化に成功すると、テストは成功します。それ以外の場合、テストは失敗します。
- **Continuous random number generator test**-このテストは、乱数が生成されたときに実行されます。連続する2つの乱数が異なる場合、テストは成功します。異なる場合、テストは失敗します。このテストは、DSA/RSA非対称キーペアが生成されたときにも実行できます。

トリガーセルフテスト

暗号化モジュールが正常に動作しているかどうかを確認するには、暗号化アルゴリズムのセルフテストをトリガーします。トリガーされるセルフテストは、電源投入時のセルフテストと同じです。セルフテストに失敗すると、デバイスは自動的に再起動します。
セルフテストをトリガーする手順は、次のとおりです。

手順	**コマンド**
1.system view.と入力します。	system-view
2.セルフテストを起動します。	fips selftest

コンフィグレーションの考慮事項

FIPSモードを開始するには、次の手順を実行します。

1. FIPSモードを有効にします。
2. パスワード制御機能を有効にします。
3. FIPSモードでデバイスにログインするためのユーザー名とパスワードを設定します。パスワードは10文字以上で、大文字と小文字、数字、および特殊文字を含む必要があります。
4. MD5ベースのデジタル証明書をすべて削除します。
5. モジュラス長が1024ビット未満のDSAキーペアとすべてのRSAキーペアを削除します。
6. 構成を保存します。

FIPSモードをイネーブルにする

FIPSモードをイネーブルにする場合は、次の注意事項に従ってください。

- FIPSモードとパスワード制御機能の両方をイネーブルにする必要がある場合は、最初にFIPSモードをイネーブルにします。
- FIPSモードとパスワード制御機能の両方を無効にする必要がある場合は、最初にパスワード制御を無効にします。
- FIPSモードをイネーブルにした後、デバイスをリブートする前に、FIPS140 - 2非準拠ローカルユーザサービスタイプのTelnet、HTTP、またはFTPを削除します。

FIPSモードをイネーブルにするには、次の手順を実行

手順	**コマンド**	**備考**
1. システムビューに入る	System-view	N/A
2. FIPS モードをenableにする	fips mode enable	デフォルトではfips modeはdisableです。

FIPSモードでの設定変更

FIPSモードをイネーブルにしてデバイスをリブートすると、次のシステム変更が発生します。

- FTP/TFTPサーバーが無効になっています。
- Telnetサーバーが無効です。
- HTTPサーバーが無効になっています。
- SNMPv1およびSNMPv2cは無効です。SNMPv3のみが使用可能です。
- SSLサーバーはTLS1.0のみをサポートします。
- SSHサーバーは、SSHv1クライアントをサポートしません。
- 生成されたRSAキーペアのモジュラス長は2048ビットである必要があり、DSAキーペアのモジュラス長は1024～2048ビットである必要があります。
- SSH、SNMPv3、IPSec、およびSSLは、DES、RC4、またはMD5をサポートしていません。

FIPSの表示と保守

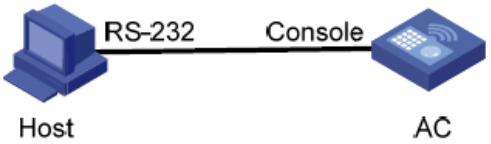
タスク	コマンド	備考
FIPSモードの状態を表示	**display fips status**	どのビューからも実行可能

FIPSの設定例

ネットワークの要件

図1に示すように、ホストはコンソールポートを介してACに接続します。FIPSモードで動作するようにACを設定し、ホストがACにログインできるようにホストのローカルユーザーを作成します。

図1 ネットワークダイアグラム



設定手順

注意:
FIPSモードをイネーブルにしたら、デバイスをリブートする前にローカルユーザー
とそのパスワードを作成する必要があります。そうしないと、デバイスにログインできません。デバイスにログインするには、コンフィギュレーションファイルを使用せずにデバイスをリブートして(コンフィギュレーションファイルを無視または削除して)、デバイスが非FIPSモードで動作するようにしてから、正しい設定を行います。

#FIPSモードを有効にします。

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue?[Y/N]:y
Modify the configuration to be fully compliant with FIPS mode, save the configuration to
the next-startup configuration file, and then reboot to enter FIPS mode.
```

#パスワード制御機能を有効にします。

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

#testという名前のローカルユーザーを作成し、サービスタイプをterminal、権限レベルを3、パスワードを

#AAbbcc1234%に設定します。パスワードはデフォルトで10文字以上の文字列で、大文字と小文字、数字および
#特殊文字の両方を含む必要があります。(ローカルユーザーのパスワードを構成するには対話型の方法を使用し
#ます。ローカル・ユーザー・ビューでパスワードを入力し、プロンプトに従ってパスワードを入力します。)

```
[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#
```

設定を保存します。

```
[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....
Configuration is saved to device successfully.
```

#デバイスを再起動します。

```
<Sysname> reboot
```

コンフィギュレーションの検証

デバイスの再起動後、ユーザー名testとパスワードAAbcc1234%を入力します。最初のログインが成功したことを示すプロンプトが表示され、新しいパスワードの入力が要求されます。以前のパスワードと4文字以上異なる新しいパスワードを入力し、パスワードを確認します。次に、<Sysname>プロンプトが表示されます。

```
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>
```

#現在のFIPSモードを表示します。

```
<Sysname> display fips status
```

FIPS mode is enabled