Configuring FIPS

The Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, details the U.S. government requirements for cryptographic modules. FIPS 140-2 specifies that a cryptographic module should be a set of hardware, software, firmware, or some combination that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.

FIPS specifies certain crypto algorithms as secure, and it also identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

Note From Cisco MDS NX-OS Release 8.3(1) and later, FIPS is compliant on Cisco MDS devices. On Cisco MDS NX-OS Release 7.x and earlier, FIPS feature is supported, but it is not FIPS compliant (certification process is with the U.S. government). For current FIPS compliance, refer to the Table 1 Current FIPS Compliance Reviews section in the Cisco FIPS 140 document.

This chapter includes the following sections:

設定のガイドライン

FIPS モードをイネーブルにする前に次の注意事項を守ってください。

- パスワードは最小限 8 文字の長さで作成してください。
- Telnet をディセーブルにします。ユーザーのログインは SSH だけで行ってください。
- RADIUS/TACACS+ によるリモート認証をディセーブルにしてください。スイッチに対してローカルのユーザーだけが認証可能です。
- SNMP v1 および v2 をディセーブルにしてください。SNMP v3 に対して設定された、スイッチ上の既存ユーザー アカウントのいずれについても、認証およびプライバシー用 AES/3DES は SHA で設定されていなければなりません。

- VRRP をディセーブルにしてください。
- スイッチ上で FIPS と IPsec を同時に構成しないでください。FIPS が有効になっている場合、IKE を構成すると、FCIP リンクは起動しません。
- SSH サーバーの RSA1 キー ペアすべてを削除してください。
- FIPS が有効になっていて、Cisco MDS NX-OS リリース 6.x、7.x、または 8.1（x）から Cisco MDS NX-OS リリース 8.2（1）以降のリリースにアップグレードする場合、8.2（x）リリースにアップグレードされたリリースで FIPS を無効化することはできません。

FIPS モードのイネーブル化

FIPS モードを有効にするには、次の手順に従ってください。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	**fips mode enable** **Example:** `switch(config)# fips mode enable`	FIPS モードをイネーブルにします。
ステップ 3	**no fips mode enable** **Example:** `switch(config)# no fips mode enable`	（オプション）FIPS モードをディセーブルにします。

FIPS ステータスの表示

FIPS のステータスを表示するには **show fips status** コマンドを入力します。

FIPS のセルフテスト

暗号モジュールは、適正に動作していることを確認するために、電源投入時のセルフテストと条件付きセルフテストを実行しなければなりません。

Note FIPS の電源投入時セルフテストは、fips mode enable コマンドを入力して FIPS モードがイネーブルにされていると自動的に実行されます。スイッチが FIPS モードに入るのは、すべてのセルフテストが正しく完了したときだけです。セルフテストのいずれかが失敗すると、スイッチは再起動します。

電源投入時セルフテストは、FIPSモードのイネーブル後、即時に実行されます。既知の解を使用する暗号アルゴリズムテストは、Cisco MDS 9000 ファミリ製品に実装されている FIPS 140-2 認定暗号アルゴリズムのそれぞれに対して、すべての暗号機能で実行されなければなりません。

既知解テスト（KAT）を利用すると、暗号アルゴリズムは正しい出力があらかじめわかってるデータに対して実行され、その計算出力は前回生成された出力と比較されます。計算出力が既知解と等しくない場合は、既知解テストに失敗したことになります。

何かに対応してセキュリティ機能または操作が始動された場合は、条件付きセルフテストが実行されなければなりません。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

条件付きセルフテストでは次を含むテストが行われます。

- ペア整合性テスト：このテストは公開キー/秘密キー ペアが生成されたときに実行されます。
- 乱数連続生成テスト：このテストは乱数が生成されたときに実行されます。

以上の両方はスイッチが FIPS モードに入っていると自動的に実行されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。