CHAPTER 2

FIPS の設定

Federal Information Processing Standards（FIPS; 連邦情報処理標準規格）140-2、*暗号モジュール セキュリティ要件*は、暗号モジュールに対する米国政府の要求条件を定義しています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。

FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。

（注） Cisco MDS SAN-OS Release 3.1(1) および NX-OS Release 4.1(1b) 以降は FIPS に準拠して実装しており、現在のところ米国政府による認定途中にありますが、現時点では FIPS 準拠ではありません。

この章の内容は、次のとおりです。

設定時の注意事項

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 8 文字以上の長さで作成します。
- Telnet をディセーブルにします。ユーザのログインには Secure Shell（SSH; セキュア シェル）だけを使用します。
- RADIUS/TACACS+ によるリモート認証をディセーブルにします。スイッチに対してローカルのユーザだけが認証可能です。
- SNMP v1 および v2 をディセーブルにします。SNMP v3 に対して設定された、スイッチ上の既存ユーザ アカウントのいずれについても、認証用に Secure Hash Algorithm（SHA; セキュア ハッシュ アルゴリズム）およびプライバシー用に Advanced Encryption Standard（AES; 高度暗号化規格）/Triple Data Encryption Standard（3DES; トリプル データ暗号化規格）を設定する必要があります。
- Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）をディセーブルにします。

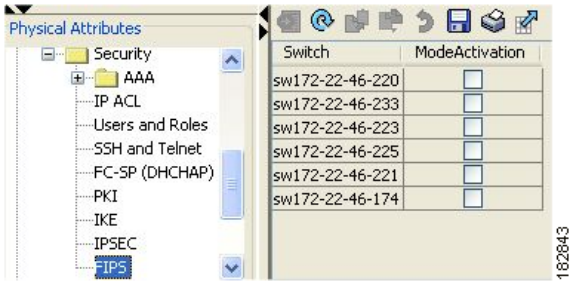
- 認証用 Message Digest 5（MD5; メッセージ ダイジェスト 5）または暗号用 DES のいずれかを含む、すべての Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ポリシーを削除します。認証用に SHA、暗号用に 3DES/AES を使用するようにポリシーを修正します。
- SSH サーバ の RSA1 キーペアすべてを削除します。

FIPS モードのイネーブル化

Fabric Manager を使用して FIPS モードをイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] を展開します。[Security] を展開し、[FIPS] を選択します。[Information] ペインに FIPS 有効設定の詳細が表示されます（図 2-1 を参照）。

図 2-1　Fabric Manager での FIPS 有効設定



ステップ 2　FIPS モードをイネーブルにするスイッチの [ModeActivation] チェックボックスをオンにします。

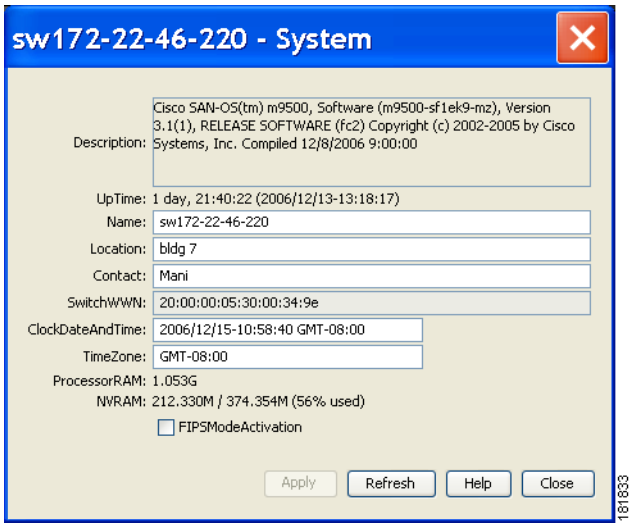
ステップ 3　[Apply Changes] アイコンをクリックして、変更内容をコミットして割り当てます。

ステップ 4　保存していない変更を廃棄するには、[Undo Changes] アイコンをクリックします。

Device Manager を使用して FIPS モードをイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical] > [System] を選択するか、右クリックして [Configure] を選択します。[System] ダイアログボックスが表示されます（図 2-2 を参照）。

図 2-2　[System] ダイアログボックス



ステップ 2　[FIPSModeActivation] チェックボックスをオンにして、選択したスイッチの FIPS モードをイネーブルにします。

ステップ 3　[Apply] ボタンをクリックして、変更内容を保存します。

ステップ 4　[Close] ボタンをクリックして、ダイアログボックスを閉じます。

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。

（注）　FIPS の電源投入時セルフテストは、FIPS モードがイネーブルであ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 モードをイネーブルにすると、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。

Known-Answer Test（KAT; 既知解テスト）を使用すると、暗号アルゴリズムは正しい出力があらかじめわかってい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：このテストでは公開キーと秘密キーの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。

これらのテストはいずれも、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。