Firepower Chassis Manager の設定

Firepower 2100 は、デバイスの基本的な動作を制御するために FXOS を実行します。GUI の Firepower Chassis Manager または FXOS CLI を使用してこれらの機能を設定できます。このマニュアルでは Firepower Chassis Manager について説明します。すべてのセキュリティ ポリシーおよびその他の動作は、ASA OS で設定される（CLI または ASDM を使用）ことに注意してください。

概要

[Overview] タブで、Firepower 2100 のステータスを簡単にモニタできます。[Overview] タブには次の要素が表示されます。

- [Device Information]：[Overview] タブの上部には Firepower 2100 に関する次の情報が表示されます。
  - [Chassis name]：シャーシに割り当てられた名前を表示します。デフォルトでは、名前は **firepower-***model* です（例：firepower-2140）。この名前が CLI プロンプトに表示されます。シャーシ名を変更するには、FXOS CLI **scope system / set name** コマンドを使用します。
  - [IP address]：シャーシに割り当てられた管理 IP アドレスを表示します。
  - [Model]：Firepower 2100 モデルを表示します。
  - [Version]：シャーシで実行されている ASA のバージョン番号を表示します。
  - [Operational State]：シャーシの動作可能ステータスを表示します。

- [Chassis uptime]：システムが最後に再起動されてからの経過時間を表示します。
- [Uptime Information] アイコン：アイコンにカーソルを合わせると、シャーシおよび ASA セキュリティ エンジンの稼働時間を表示します。

- [Visual Status Display]：[Device Information] セクションの下にはシャーシが視覚的に表示されて、搭載されているコンポーネントとそれらの全般ステータスを示します。[Visual Status Display] に表示されるポートにカーソルを合わせると、インターフェイス名、速度、タイプ、管理状態、動作状態などの追加情報が表示されます。
- Detailed Status Information：[Visual Status Display] の下に表示されるテーブルで、シャーシの詳細なステータス情報を含みます。ステータス情報は、[Faults]、[Interfaces]、[Devices]、[Inventory] の各セクションに分かれています。これらの各セクションの概要をテーブルの上に表示できます。さらに確認する情報の概要エリアをクリックするとそれぞれの詳細を表示できます。

  システムは、シャーシについての次の詳細ステータス情報を提供します。

  - [Faults]：システムで発生した障害をリスト表示します。 これらの障害は、[Critical]、[Major]、[Minor]、[Warning]、[Info] の重大度によってソートされます。一覧表示された障害ごとに重大度、障害の説明、原因、発生回数、最近発生した時刻を表示できます。また、障害が確認されているかどうかも確認できます。

    障害についての追加情報を表示したり、障害を確認するには、該当する障害をクリックします。

    （注） 障害の根本原因に対処すると、その障害は次のポーリング間隔中にリストから自動的にクリアされます。特定の障害に対処する場合、現在処理中であることが他のユーザにわかるように、その障害を確認済みにすることができます。

  - Interfaces：システムにインストールされているインターフェイスをリスト表示し、インターフェイス名、動作ステータス、管理ステータス、受信したバイト数、送信したバイト数を示します。

    いずれかのインターフェイスをクリックすると、過去 15 分間にそのインターフェイスが入出力したバイト数がグラフィック表示されます。

  - Devices：ASA を表示し、詳細（デバイス名、デバイス状態、アプリケーション、動作状態、管理状態、イメージ バージョン、および管理 IP アドレス）を示します。
  - Inventory：シャーシに搭載されているコンポーネントをリスト表示し、それらのコンポーネントの関連情報（[component] 名、コアの数、設置場所、動作ステータス、運用性、キャパシティ、電源、温度、シリアル番号、モデル番号、製品番号、ベンダー）を示します。

インターフェイス

FXOS で物理インタ フェースを管理できます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、ASA で論理的に有効にする必要があります。

Firepower 2100 は、デフォルトで有効になっているジャンボ フレームをサポートします。最大 MTU は 9184 です。

（注） フェールオーバーを有効にした後でFXOSのインターフェイスを変更する場合は（ネットワークモジュールを追加または削除する、あるいはEtherChannel設定を変更するなど）、スタンバイユニットの FXOS でインターフェイスを変更し、アクティブユニットで同じ変更を行います。

FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、ASA で論理的に有効にする必要があります。

手順

ステップ 1 [Interfaces] タブをクリックします。

ステップ 2 インターフェイスを有効または無効にするには、[Admin State] スライダをクリックします。チェックマークは有効であることを示し、X は無効であることを示します。

（注） 管理 1/1 インターフェイスは、このテーブルで [MGMT] として表示されます。

ステップ 3 速度またはデュプレックスを編集するインターフェイスの [Edit] 鉛筆アイコンをクリックします。

（注） 管理 1/1 インターフェイスを有効または無効にすることのみが可能です。そのプロパティを編集することはできません。

ステップ 4 インターフェイスを有効にするには [Enable] チェックボックスをオンにします。

ステップ 5 [Admin Speed] ドロップダウン リストで、インターフェイスの速度を選択します。

ステップ 6 [Auto Negotiation] で [Yes] または [No] のオプション ボタンをクリックします。

ステップ 7 [Admin Duplex] ドロップダウン リストで、インターフェイスのデュプレックスを選択します。

ステップ 8 [OK] をクリックします。

EtherChannel の追加

EtherChannel（別名ポートチャネル）には、タイプと速度が同じ最大 16 個のメンバー インターフェイスを含めることができます。

（注） EtherChannel メンバー ポートは ASA に表示されますが、EtherChannel およびポート メンバーシップは FXOS でのみ設定できます。

フェールオーバーを有効にした後で EtherChannel 設定を変更する場合は、スタンバイユニットの FXOS でインターフェイスを変更し、アクティブユニットで同じ変更を行います。

始める前に

Firepower 2100 は、Link Aggregation Control Protocol（LACP）のアクティブモードまたはオンモードで EtherChannel をサポートします。デフォルトでは、LACP モードはアクティブに設定されています。CLI でモードをオンに変更できます。最適な互換性を得るために、接続スイッチ ポートをアクティブ モードに設定することを推奨します。

手順

ステップ 1 [Interfaces] タブをクリックします。

ステップ 2 インターフェイス テーブルの上の [Add Port Channel] をクリックします。

ステップ 3 [Port Channel ID] フィールドに、ポート チャネルの ID を入力します。有効な値は、1 ～ 47 です。

ステップ 4 ポート チャネルを有効にするには、[Enable] チェックボックスをオンにします。

[Type] ドロップダウン リストは無視します。使用可能なタイプは [Data] のみです。

ステップ 5 [Admin Speed] ドロップダウン リストで、すべてのメンバー インターフェイスの速度を選択します。

その速度（および選択したその他の設定）に対応していないインターフェイスを選択すると、可能な範囲で最速の速度が自動的に適用されます。

ステップ 6 すべてのメンバー インターフェイスについて、[Auto Negotiation] で [Yes] または [No] のオプション ボタンをクリックします。

ステップ 7 [Admin Duplex] ドロップダウン リストで、すべてのメンバー インターフェイスのデュプレックスを選択します。

ステップ 8 [Available Interface] リストで、追加するインターフェイスを選択し、[Add Interface] をクリックします。

同じタイプと速度の最大 16 のインターフェイスを追加できます。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

ヒント 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、Ctrl キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、Shift キーを押しながら最後のインターフェイスをクリックして選択します。

（注） EtherChannel にインターフェイスを割り当てた場合は、必要な調整を行うことができるように、ASA 設定で元のインターフェイスコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

たとえば、FXOS で Ethernet1/4 を Port-channel7 に割り当てた後も、Ethernet1/4 は ASA OS で使用可能なインターフェイスとして表示され、Ethernet1/4 の設定は保持されます。**show interface ethernet1/4** を入力すると、ASA ではインターフェイスが「スーパーバイザに関連付けられていません（not associated with the Supervisor）」と表示されます。余分な設定を削除するには、**no interface ethernet1/4** コマンドを使用します。

ステップ 9 [OK] をクリックします。

モニタリング インターフェイス

[Interfaces] タブで、シャーシにインストールされているインターフェイスのステータスを表示できます。下部のセクションには、Firepower シャーシにインストールされているインターフェイスの表が表示されます。上部のセクションには、Firepower シャーシにインストールされているインターフェイスが視覚的に表示されます。上部セクションでいずれかのインターフェイスにカーソルを合わせると、そのインターフェイスに関する追加情報が表示されます。

インターフェイスは現在のステータスを示すために色分けされています。

- 緑：動作状態は [Up] です。
- 濃い灰色：管理状態は [Disabled] です。
- 赤：動作状態は [Down] です。
- 淡い灰色：SFP がインストールされていません。

論理デバイス

[Logical Devices] ページには、ASA に関する情報とステータスが表示されます。スライダを使用して、トラブルシューティングのためにASAを無効または有効にすることもできます（チェックマークは有効であることを示し、X は無効であることを示します）。

ASA のヘッダーには [Status] が表示されます。

- [ok]：論理デバイスの設定は完了しています。
- [incomplete-configuration]：論理デバイス設定は未完了です。

論理デバイス領域にも ASA の詳細な [Status] が表示されます。

- [Online]：ASA は実行中および動作中です。
- [Offline]：ASA は停止中で、動作不能です。
- [Installing]：ASA のインストールが進行中です。
- [Not Installed]：ASA はインストールされていません。
- [Install Failed]：ASA のインストールに失敗しました。
- [Starting]：ASA は起動中です。
- [Start Failed]：ASA の起動に失敗しました。
- [Started]：ASA は正常に起動し、アプリケーションエージェントのハートビートを待機しています。
- [Stopping]：ASA は停止処理中です。
- [Stop Failed]：ASA をオフラインにできませんでした。
- [Not Responding]：ASA は応答していません。
- [Updating]：ASA ソフトウェアのアップグレードが進行中です。
- [Update Failed]：ASA ソフトウェアのアップグレードに失敗しました。
- [Update Succeeded]：ASA ソフトウェアのアップグレードに成功しました。

プラットフォーム設定

[Platform Settings] タブでは、時間や管理アクセスなどの FXOS の基本的な操作を設定できます。

NTP：時刻の設定

手動でクロックを設定することも、NTPサーバを使用する（推奨）こともできます。最大4台のNTPサーバを設定できます。

始める前に

- NTPは、デフォルトでは次のCisco NTPサーバで設定されます：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。
- NTPサーバのホスト名を使用する場合は、DNSサーバを設定する必要があります。DNS：DNS サーバの設定 （18 ページ）を参照してください。

手順

ステップ1 [Platform Settings] タブをクリックし、左側のナビゲーションで [NTP] をクリックします。

[Time Synchronization] タブがデフォルトで選択されています。

ステップ2 NTP サーバを使用するには：

a) [Use NTP Server] オプション ボタンをクリックします。

b) （任意）（ASA 9.10(1) 以降）NTPサーバで認証が必要な場合は、[NTP Server Authentication: Enable] チェックボックスをオンにします。

認証キー ID と値が必要な場合は、[Yes] をクリックします。

NTP サーバ認証では SHA1 のみがサポートされます。

c) [Add] をクリックして、IP アドレスまたはホスト名で最大 4 つの NTP サーバを識別します。

NTP サーバのホスト名を使用する場合は、この手順の後半で DNS サーバを設定します。

d) （ASA 9.10(1) 以降）NTP サーバの [Authentication Key] ID と [Authentication Value] を入力します。

NTP サーバからキー ID と値を取得します。たとえば、OpenSSL がインストールされた NTP サーバ バージョン 4.2.8 p8 以降で SHA1 キーを生成するには、**ntp-keygen -M** コマンドを入力して ntp. keys ファイルでキー ID と値を確認します。このキーは、クライアントとサーバの両方に対して、メッセージダイジェストの計算時に使用するキー値を通知するために使用します。

e) [Save] をクリックしてサーバを保存します。

ステップ3 手動で時刻を設定するには：

a) [Set Time Manually] オプション ボタンをクリックします。

b) [Date] ドロップダウン リストをクリックしてカレンダーを表示し、そのカレンダーで使用可能なコントロールを使用して日付を設定します。

c) 対応するドロップダウン リストを使用して、時刻を時間、分、および [AM/PM] で指定します。

ステップ 4 [Current Time] タブをクリックし、[Time Zone] ドロップダウン リストからシャーシに適したタイム ゾーンを選択します。

ステップ 5 [Save] をクリックします。

（注） システム時刻の変更に 10 分以上かかると、自動的にログアウトされ、Firepower Chassis Manager への再ログインが必要になります。

SSH：SSH の設定

次の手順では、Firepower シャーシへの SSH アクセスを有効または無効にする方法、およびシャーシを SSH クライアントとして有効にする方法について説明します。SSH サーバとクライアントはデフォルトで有効になっています。

手順

ステップ 1 [Platform Settings] > [SSH] > [SSH Server] > > を選択します。

ステップ 2 Firepower シャーシへの SSH アクセスを SSH サーバが提供できるようにするには、[Enable SSH] チェックボックスをオンにします。

ステップ 3 サーバの [Encryption Algorithm] について、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

ステップ 4 サーバの [Key Exchange Algorithm] として、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。

DH キー交換は、いずれの当事者も単独では決定できない共有秘密を提供します。キー交換を署名およびホスト キーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 5 サーバの [Mac Algorithm] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 6 サーバの [Host Key] について、RSA キー ペアのモジュラス サイズを入力します。

モジュラス値（ビット単位）は、1024 ～ 2048 の範囲内の 8 の倍数です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 2048 にすることをお勧めします。

ステップ 7 サーバの [Volume Rekey Limit] について、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 8 サーバの [キー再生成の時間制限（Time Rekey Limit）] では、FXOS がセッションを切断する前に SSH セッションがアイドル状態を続けられる長さを分単位で設定します。

ステップ 9 [Save]をクリックします。

ステップ 10 [SSH クライアント（SSH Client）] タブをクリックして、FXOS シャーシの SSH クライアントをカスタマイズします。

ステップ 11 [厳密なホストキー検査（Strict Host Keycheck）]について、[有効（enable）]、[無効（disable）]、または [プロンプト（prompt）] を選択して、SSH ホスト キー チェックを制御します。

- enable：FXOS が認識するホスト ファイルにそのホスト キーがまだ存在しない場合、接続は拒否されます。 FXOS CLI でシステムスコープまたはサービススコープの **enter ssh-host** コマンドを使用して、手動でホストを追加する必要があります。
- prompt：シャーシにまだ格納されていないホストキーを許可または拒否するように求められます。
- disable：（デフォルト）シャーシは過去に保存されたことがないホストキーを自動的に許可します。

ステップ 12 クライアントの [Encryption Algorithm] について、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

ステップ 13 クライアントの [キー交換アルゴリズム（Key Exchange Algorithm）] について、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。

DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 14 クライアントの [Mac アルゴリズム（Mac Algorithm）] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 15 クライアントの [Volume Rekey Limit] について、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 16 クライアントの [キー再生成の時間制限（Time Rekey Limit）] について、FXOS がセッションを切断する前に SSH セッションがアイドルであることができる時間を分単位で設定します。

ステップ 17 [Save] をクリックします。

SNMP：SNMP の設定

Firepower シャーシに Simple Network Management Protocol（SNMP）を設定するには、[SNMP] ページを使用します。

SNMP の概要

SNMP は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージフォーマットを提供します。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- SNMPマネージャ：SNMPを使用してネットワークデバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：Firepower のデータを維持し、必要に応じてそのデータを SNMP マネージャに報告するFirepowerシャーシ内のソフトウェアコンポーネント。Firepowerシャーシには、エージェントと一連の MIB が含まれています。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。

Firepower シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求をSNMPマネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Firepower シャーシは、トラップまたはインフォームとして SNMP 通知を生成します。SNMP マネージャはトラップ受信時に確認応答を送信せず、Firepower シャーシはトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。インフォーム要求を受信するSNMPマネージャは、SNMP応答プロトコルデータユニット（PDU）でメッセージの受信を確認応答します。Firepower シャーシが PDU を受信しない場合、インフォーム要求を再送できます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、およびSNMPv3はそれぞれ別のセキュリティモデルを表します。セキュリティ モデルと選択したセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。権限レベルは、メッセージが開示されないよう保護または認証の必要があるかどうかを決定します。サポートされるセキュリティ レベルは、セキュリティ モデルが設定されているかによって異なります。SNMPセキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし
- authPriv：認証あり、暗号化あり

SNMPv3では、セキュリティモデルとセキュリティ レベルの両方が提供されています。セキュリティモデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ

モデルとセキュリティ レベルの組み合わせにより、SNMPパケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

表 *1 : SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	水準器	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティストリング	なし	コミュニティストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティストリング	なし	コミュニティストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-SHA	なし	HMAC Secure Hash Algorithm（SHA）に基づいて認証します。
v3	authPriv	HMAC-SHA	DES	HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティ機能

SNMPv3は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3は、設定済みユーザによる管理動作のみを許可し、SNMPメッセージを暗号化します。SNMPv3ユーザベースセキュリティモデル（USM）はSNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

SNMP サポート

Firepower シャーシは SNMP の次のサポートを提供します。

MIB のサポート

Firepower シャーシは、MIB への読み取り専用アクセスをサポートします。

SNMPv3 ユーザの認証プロトコル

Firepower シャーシは、SNMPv3 ユーザの HMAC-SHA-96（SHA）認証プロトコルをサポートします。

SNMPv3 ユーザの AES プライバシー プロトコル

SHA ベースの認証に加えて、Firepower シャーシは AES-128 ビット Advanced Encryption Standard を使用したプライバシーも提供します。Firepower シャーシは、プライバシー パスワードを使用して 128 ビット AES キーを生成します。AES プライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合、最大 80 文字を指定できます。

SNMP の設定

SNMP を有効にし、トラップおよび SNMPv3 ユーザを追加します。

手順

ステップ 1 [Platform Settings] > [SNMP] > を選択します。

ステップ 2 [SNMP] 領域で、次のフィールドに入力します。

名前	説明
[Admin State] チェックボックス	SNMP を有効にするかまたは無効にするか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスを有効にします。
[Port] フィールド	Firepower シャーシが SNMP ホストと通信するためのポート。デフォルト ポートは変更できません。
[Community/Username] フィールド	Firepower シャーシが SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2 コミュニティの名前、あるいは SNMP v3 のユーザ名。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。デフォルトは **public** です。 [Community/Username] フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [Set: Yes] を読み取ることに注意してください。[Community/Username] フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [Set: No] を読み取ります。

名前	説明
[System Administrator Name] フィールド	SNMP の実装担当者の連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[Location]フィールド	SNMP エージェント（サーバ）が動作するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 3 [SNMP Traps] 領域で、[Add] をクリックします。

ステップ 4 [Add SNMP Trap] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Host Name] フィールド	Firepower シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。
[Community/Username] フィールド	Firepower シャーシがトラップを SNMP ホストに送信するときに含める SNMP v1 または v2 のコミュニティ名または SNMP v3 のユーザ名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。
[Port] フィールド	Firepower シャーシがトラップのために SNMP ホストと通信するポート。 1 ～ 65535 の整数を入力します。
[Version] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • **[V1]** • **[V2]** • **[V3]**
[Type] フィールド	バージョンとして [V2] または [V3] を選択した場合に、送信するトラップのタイプ。次のいずれかになります。 • **Traps** • **情報**

名前	説明
[v3 Privilege] フィールド	バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。 • [Auth]：認証あり、暗号化なし • [Noauth]：認証なし、暗号化なし • [Priv]：認証あり、暗号化あり

ステップ 5 [OK] をクリックして、[Add SNMP Trap] ダイアログボックスを閉じます。

ステップ 6 [SNMP Users] 領域で、[Add] をクリックします。

ステップ 7 [Add SNMP User] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	SNMP ユーザに割り当てられるユーザ名。 32 文字までの文字または数字を入力します。名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アット マーク）、-（ハイフン）も指定できます。
[Auth Type] フィールド	許可タイプ：**SHA**。
[Use AES-128] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。
[Password] フィールド	このユーザのパスワード。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Privacy Password] フィールド	このユーザのプライバシー パスワード。
[Confirm Privacy Password] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 8 [OK] をクリックして [Add SNMP User] ダイアログボックスを閉じます。

ステップ 9 [Save] をクリックします。

HTTPS：ポートの変更

HTTPS サービスは、デフォルトでポート 443 で有効化になります。HTTPS をディセーブルにすることはできませんが、HTTPS 接続に使用するポートは変更できます。

始める前に

ASA データ インターフェイスで HTTPS アクセスを有効にする場合は、HTTPS ポートを 443 から変更しないでください。デフォルトのポートのみがサポートされます。

手順

ステップ 1 [Platform Settings] > [HTTPS] > を選択します。

ステップ 2 HTTPS 接続に使用するポートを [Port] フィールドに入力します。1 ～ 65535 の範囲内の整数を指定します。このサービスは、デフォルトではポート 443 で有効になっています。

ステップ 3 [Save] をクリックします。

Firepower シャーシが指定した HTTPS ポートで設定されます。

HTTPS ポートを変更した後に、現在のすべての HTTPS セッションが閉じられます。ユーザは、次のように新しいポートを使用して再度 Firepower Chassis Manager にログインする必要があります。

https://<*chassis_mgmt_ip_address*>:<*chassis_mgmt_port*>

<*chassis_mgmt_ip_address*> は、初期設定時に入力した Firepower シャーシの IP アドレスまたはホスト名で、<*chassis_mgmt_port*> は設定が完了した HTTPS ポートです。

DHCP：管理クライアント用に DHCP サーバを設定する

管理 1/1 インターフェイスに接続しているクライアントに対して DHCP サーバを有効にすることができます。デフォルトでは、サーバはアドレス範囲 192.168.45.10 ～ 192.168.45.12 で有効になっています。管理 IP アドレスを変更する場合、DHCP を無効にする必要があります。その後、新しいネットワークの DHCP を再度有効にすることができます。

手順

ステップ 1 [Platform Settings] > [DHCP] > を選択します。

ステップ 2 [Enable DHCP service] チェックボックスをオンにします。

ステップ 3 [Start IP] と [End IP] にアドレスを入力します。

ステップ 4 [Save] をクリックします。

syslog：syslog メッセージングの設定

ログは、ルーチンのトラブルシューティングおよびインシデント処理の両方で役立ちます。syslog メッセージは、Firepower 2100 コンソール、SSH セッション、またはローカルファイルに送信できます。

これらの syslog メッセージは FXOS シャーシにのみ適用されます。ASA syslog メッセージの場合、ASA 設定でロギングを設定する必要があります。

（注） リモート宛先はサポートされていません。

手順

ステップ 1 [Platform Settings] > [Syslog] > を選択します。

ステップ 2 ローカル宛先を設定します。

a) [Local Destinations] タブをクリックします。

b) 次のフィールドに入力します。

名前	説明
コンソール	
[Admin State]	コンソールに syslog メッセージを表示するには、[Enable] チェックボックスをオンにします。
[Level]	コンソールに表示するメッセージの最低レベルをクリックします。Firepower シャーシにはそのレベル以上のメッセージが表示されます。 • **[Emergencies]** • **[Alerts]** • **[Critical]**
プラットフォーム	
[Admin State]	プラットフォーム syslog は常に有効です。

名前	説明
[Level]	表示するメッセージの最低レベルを選択します。Firepower シャーシにはそのレベル以上のメッセージが表示されます。デフォルトは [Informational] です。 • **[Emergencies]** • **[Alerts]** • **[Critical]** • **[Errors]** • **[Warnings]** • **[Notifications]** • **[Information]** • **[Debugging]**
[File]	
[Admin State]	syslog メッセージをファイルに保存するには、[Enable] チェックボックスをオンにします。
[Level]	保存するメッセージの最低レベルを選択します。システムはそのレベル以上のメッセージを保存します。 • **[Emergencies]** • **[Alerts]** • **[Critical]** • **[Errors]** • **[Warnings]** • **[Notifications]** • **[Information]** • **[Debugging]**
[Name]	16 文字までのファイル名を設定します。
[Size]	最新のメッセージで最も古いメッセージが上書きされる前の最大ファイルサイズ（バイト単位）を指定します。有効な範囲は 4096 ～ 4194304 バイトです。

c) [Save] をクリックします。

ステップ 3 ローカル送信元を設定します。

a) [Local Sources] タブをクリックします。

b) 次のフィールドに入力します。

名前	説明
Faults Admin State	システム障害ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべてのシステム障害をログに記録します。
Audits Admin State	監査ロギングを有効化するかどうか。[Enable]チェックボックスをオンにすると、Firepower シャーシはすべての監査ログ イベントをログに記録します。
Events Admin State	システムイベントロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべてのシステム イベントをログに記録します。

c) [Save] をクリックします。

DNS：DNS サーバの設定

システムでホスト名の IP アドレスへの解決が必要な場合は、DNS サーバを指定する必要があります。最大 4 台の DNS サーバを設定できます。複数の DNS サーバを設定する場合、システムによるサーバの検索順はランダムになります。

始める前に

- DNS は、デフォルトでは次の OpenDNS サーバで構成されています：208.67.222.222、208.67.220.220。

手順

ステップ 1 [Platform Settings] > [DNS] > を選択します。

ステップ 2 [Enable DNS Server] チェックボックスをオンにします。

ステップ 3 追加する DNS サーバ（最大 4 台）ごとに、それぞれの IP アドレスを [DNS Server） フィールドに入力し、[Add] をクリックします。

ステップ 4 [Save] をクリックします。

ステップ 5 [Domain Name Configuration] タブをクリックし、Firepower シャーシが非修飾名にサフィックスとして追加する [Domain name] を入力し、[Add] をクリックします。

たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、Firepower シャーシ によって名前が修飾されて「jupiter.example.com」となります。

FIPSおよびコモンクライテリア：FIPSおよびコモンクライテリアモードの有効化

Firepower 2100 で FIPS またはコモン クライテリア（CC）モードを有効にするには、次の手順を実行します。

また、**fips enable** コマンドを使用して ASA で個別に FIPS モードを有効にする必要もあります。ASA には、コモン クライテリア モードに関する個別の設定はありません。CC または UCAPL のコンプライアンスに関する追加の制限があれば、シスコのセキュリティ ポリシーのマニュアルに従って設定する必要があります。

最初に ASA で FIPS モードを設定し、デバイスのリロードを待ってから、FXOS で FIPS モードを設定することをお勧めします。

手順

ステップ 1 [Platform Settings] > [FIPS and Common Criteria] > を選択します。

ステップ 2 [Enable] チェックボックスをオンにすることにより、[FIPS] を有効にします。

ステップ 3 [Enable] チェックボックスをオンにすることにより、[Common Criteria] を有効にします。

コモン クライテリアを有効にすると、[FIPS Enable] チェックボックスはデフォルトでオンになります。

ステップ 4 [Save] をクリックします。

ステップ 5 プロンプトに従ってシステムをリブートします。

アクセス リスト：管理アクセスの設定

デフォルトでは、Firepower 2100 は、管理 1/1 192.168.45.0/24 ネットワークで、Firepower Chassis Manager への HTTPS アクセス、および SSH アクセスを許可します。他のネットワークからのアクセスを許可、または SNMP を許可する場合は、アクセス リストを追加または変更する必要があります。

IP アドレス（v4 または v6）のブロックごとに、サービスごとに最大 25 個の異なるサブネットを設定できます。

手順

ステップ 1 [Platform Settings] > [Access List] > を選択します。

ステップ 2 [IPv4 Access List] 領域で：

a) [Add] をクリックします。

b) 次の値を入力します。

- [IP Address]：IP アドレスを設定します。すべてのネットワークを許可するには、**0.0.0.0** と入力します。
- [Prefix Length]：サブネット マスクを設定します。 すべてのネットワークを許可するには、**0** と入力します。
- [Protocol]：[HTTPS]、[SNMP]、または [SSH] を選択します。

c) [OK] をクリックします。
d) サービスごとにネットワークを追加するには、これらのステップを繰り返します。

ステップ 3 [IPv6 Access List] 領域で：

a) [Add] をクリックします。
b) 次の値を入力します。

- [IP Address]:IP アドレスを設定します。 すべてのネットワークを許可するには、:: と入力します。
- [Prefix Length]：プレフィックス長を設定します。 すべてのネットワークを許可するには、**0** と入力します。
- [Protocol]：[HTTPS]、[SNMP]、または [SSH] を選択します。

c) [OK] をクリックします。
d) サービスごとにネットワークを追加するには、これらのステップを繰り返します。

ステップ 4 [Save] をクリックします。

システム アップデート

この作業はスタンドアロン ASA に適用されます。フェールオーバー ペアをアップグレードする場合は、『Cisco ASA Upgrade Guide』を参照してください。アップグレードプロセスには通常 20 ～ 30 分かかります。

ASA、ASDM、および FXOS のイメージは 1 つのパッケージにバンドルされています。パッケージのアップデートは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできません。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。

ASDM の場合は例外です。ASA オペレーティング システム内からアップグレードできるため、必ずしもバンドルされた ASDM イメージを使用する必要はありません。手動でアップロードする ASDM イメージは FXOS イメージ リストに表示されません。ASA から ASDM イメージを管理する必要があります。

（注） バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが前の ASDM バンドル イメージを置き換えます。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドル アップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、またはASAバンドルをアップグレードする直前に、バンドルされたASDMイメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

始める前に

アップロードするイメージがローカル コンピュータで使用可能であることを確認してください。

手順

ステップ 1 [System] > [Updates] > を選択します。

[Available Updates] ページに、シャーシで使用可能なパッケージのリストが表示されます。

ステップ 2 [Upload Image] をクリックします。

ステップ 3 [Browse] をクリックし、アップロードするイメージまで移動して選択します。

ステップ 4 [Upload] をクリックします。

選択したイメージがシャーシにアップロードされます。イメージの整合性は、新しいイメージがシャーシに追加されると自動的に確認されます。手動で確認する場合は、[Verify]（チェックマーク アイコン）をクリックします。

ステップ 5 アップグレードする ASA パッケージを選択し、[Upgrade] をクリックします。

ステップ 6 インストールの続行を確定するには [Yes] を、インストールをキャンセルするには [No] をクリックします。

アップグレード中に、Firepower Chassis Manager からログアウトされます。

ユーザ管理

ユーザ アカウントは、Firepower 2100 シャーシにアクセスするために使用されます。これらのアカウントは、Firepower Chassis Manager および SSH アクセスで使用されます。ASA には別のユーザ アカウントと認証があります。

ユーザ アカウントについて

管理者アカウント

管理者アカウントはデフォルト ユーザ アカウントであり、変更や削除はできません。このアカウントは、システム管理者またはスーパーユーザアカウントであり、すべての権限が与えられています。デフォルトのパスワードは **Admin123** です。

管理者アカウントは常にアクティブで、有効期限がありません。管理者アカウントを非アクティブに設定することはできません。

ローカル認証されたユーザ アカウント

最大48のローカルユーザ アカウントを設定できます。各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

ローカル認証されたユーザアカウントは、管理者権限を持つユーザであれば誰でも有効または無効にすることができます。

ユーザ アカウントに関するガイドライン

ユーザ名

ユーザ名は、Firepower Chassis Manager および FXOS CLI のログイン ID として使用されます。ログインIDの割り当てにあたっては、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）
  - .（ドット）
- ログイン ID は一意である必要があります。
- ログイン ID は、英文字で開始する必要があります。数字やアンダースコアなどの特殊文字から始めることはできません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

パスワード

ローカル認証されたユーザアカウントごとに、パスワードが必要です。管理者権限を持つユーザは、ユーザパスワードのパスワード強度チェックを実行するようにシステムを設定できます。パスワード強度チェックをイネーブルにすると、各ユーザが強力なパスワードを使用する必要があります。

各ユーザが強力なパスワードを設定することを推奨します。ローカル認証ユーザのパスワード強度チェックを有効にすると、FXOS は次の要件を満たしていないパスワードを拒否します。

- 少なくとも 8 文字を含み、最大 127 文字であること

（注） コモンクライテリア要件に準拠するために、オプションでシステムの最小文字数 15 文字の長さのパスワードを設定できます。

- アルファベットの大文字を少なくとも 1 文字含む。
- アルファベットの小文字を少なくとも 1 文字含む。
- 英数字以外の文字（特殊文字）を少なくとも 1 文字含む。
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- passwordABC や password321 などの 3 つの連続した数字や文字をどのような順序であっても含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。たとえば、辞書に記載されている標準的な単語に基づくパスワードを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- 空白にすることはできません。

ユーザの追加

Firepower Chassis Manager および FXOS CLI アクセスのローカル ユーザを追加します。

手順

ステップ 1 [System] > [User Management] > を選択します。

ステップ 2 [Local Users] タブをクリックします。

ステップ 3 [Add User] をクリックして [Add User] ダイアログボックスを開きます。

ステップ 4 ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。

- [User Name]：ユーザ名を設定します。この名前は、固有であり、ユーザ アカウント名のガイドラインと制限を満たしている必要があります（ユーザアカウントに関するガイドラ

イン （22 ページ）を参照）。ユーザを保存した後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

- [First Name]：ユーザの名を設定します。このフィールドには、32 文字までの値を入力できます。
- [Last Name]：ユーザの姓。このフィールドには、32 文字までの値を入力できます。
- [Email]：ユーザの電子メールアドレスを設定します。
- [Phone Number] ：ユーザの電話番号を設定します。
- [Password] および [Confirm Password]：このアカウントに関連付けられているパスワードを設定します。パスワード強度チェックを有効にした場合は、ユーザパスワードを強固なものにする必要があります。FXOS は強度チェック要件を満たしていないパスワードを拒否します（ユーザ設定値の設定 （25 ページ）およびユーザ アカウントに関するガイドライン （22 ページ）を参照）。
- [Account status]：ステータスを**アクティブ**または**非アクティブ**に設定します。
- [User Role]：ユーザ アカウントに割り当てる権限を表すロールを設定します。すべてのユーザはデフォルトでは [Read-Only] ロールが割り当てられます。このロールは選択解除できません。管理者ロールを割り当てるには、ウィンドウ内の [Admin] をクリックして強調表示します。管理者ロールでは、設定への読み取りと書き込みのアクセスが許可されます。ユーザ ロールおよび権限の変更は次回のユーザ ログイン時に有効になります。ユーザアカウントへの新しいロールの割り当てや既存のロールの削除を行うときにユーザがログインしている場合、アクティブなセッションは以前のロールや権限を引き続き使用します。
- [Account expires]：このアカウントの有効期限を設定します。アカウントは、[Expiry Date] フィールドで指定された日付の後には使用できません。ユーザアカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。デフォルトでは、ユーザアカウントの有効期限はありません。
- [Expiry Date]：アカウントが期限切れになる日付。日付の形式は yyyy-mm-dd です。このフィールドの終端にあるカレンダーアイコンをクリックするとカレンダーが表示され、それを使用して期限日を選択できます。

ステップ 5 [Add] をクリックします。

ステップ 6 ユーザを非アクティブ化するには、次の手順を実行します。

a) 非アクティブ化するユーザについて、[Edit] アイコン（✎） をクリックします。

管理者ユーザアカウントは、常にアクティブに設定され、非アクティブ化できません。

b) [Account Status] フィールドで、[Inactive] オプションボタンをクリックします。

c) [Save] をクリックします。

ユーザ設定値の設定

すべてのユーザのグローバル設定値を設定できます。

手順

ステップ 1 [System] > [User Management] > を選択します。

ステップ 2 [Settings] タブをクリックします。

ステップ 3 次のフィールドに入力します。

- [Default Authentication]：リモートログイン時にユーザを認証するデフォルトの方法。次のいずれかになります。
  - [Local]：ユーザ アカウントは、Firepower シャーシでローカルに定義する必要があります。
  - [None]：ユーザアカウントが Firepower シャーシに対してローカルである場合は、ユーザがリモート ログインするときにパスワードは必要ありません。
- [Password Strength Check]：オンにすると、すべてのローカルユーザパスワードは強固なパスワードのガイドラインに準拠する必要があります（ユーザアカウントに関するガイドライン （22 ページ）を参照）。デフォルトでは、強力なパスワードチェックが有効になっています。
- [History Count]：以前に使用したパスワードが再使用可能になるまでにユーザが作成する必要がある、一意のパスワードの数。履歴カウントは、最も新しいパスワードを先頭に時系列とは逆の順番で表示され、履歴カウントのしきい値に到達すると、最も古いパスワードのみが使用可能になります。この値は、0 ～ 15 から自由に設定できます。[History Count] フィールドを 0 に設定すると、履歴カウントが無効になり、ユーザは以前に使用していたパスワードを再利用できます。
- [Change Interval]：[Change Count] フィールドで指定したパスワード変更回数が適用される最大時間数。この値は、1 ～ 745 時間から自由に設定できます。たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。この機能を有効にするにはチェックボックスをオンにします。
- [Change Count]：ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数。この値は、0 ～ 10 の範囲で自由に設定できます。
- [No Change Interval]：ローカル認証されたユーザが、新しく作成したパスワードを変更する前に待機する最小時間数。この値は、1 ～ 745 時間の範囲で自由に設定できます。この機能を有効にするにはチェックボックスをオンにします。
- [Passphrase Expiration Days]：有効期限を 1 ～ 9999 日の間で設定します。デフォルトでは、有効期限は無効になっています。

- [Passphrase Expiration Days]：ログインごとに有効期限の何日前にパスワードの有効期限をユーザに警告するかを 0 ～ 9999 の間で設定します。デフォルトは、14 日です。
- [Expiration Grace Period]：有効期限の何日後までにユーザがパスワードを変更する必要があるかを 0 ～ 9999 の間で設定します。デフォルトは 3 日です。
- [Password Reuse Interval]：パスワードの再利用が可能になるまでの日数を 1 ～ 365 の間で設定します。デフォルトは 15 日です。[History Count] と [Password Reuse Interval] の両方を有効にする場合は、両方の要件を満たしている必要があります。たとえば、履歴カウントを 3 に設定し、再利用間隔を 10 日に設定すると、パスワードを変更できるのは 10 日間経過した後で、パスワードを 3 回変更した場合に限られます。

ステップ 4 [Save] をクリックします。

Firepower Chassis Manager の設定の履歴

機能	バージョン	詳細
ユーザパスワードの改善	9.13(1)	次のようなパスワードセキュリティの改善が追加されました。 • ユーザパスワードには最大 127 文字を使用できます。古い制限は 80 文字でした。 • デフォルトでは、強力なパスワードチェックが有効になっています。 • 管理者パスワードの設定を求めるプロンプトが表示されます。 • パスワードの有効期限切れ。 • パスワード再利用の制限。 新しい/変更された画面： • [System] > [User Management] > [Local Users] > > • [System] > [User Management] > [Settings] > >

機能	バージョン	詳細
Firepower 2100 の NTP 認証のサポート	9.10(1)	FXOS で SHA1 NTP サーバ認証を設定できるようになりました。 新規/変更された [Firepower Chassis Manager] 画面： [Platform Settings] > [NTP] > [NTP Server Authentication: Enable] > > チェックボックス、[Authentication Key] フィールド、[Authentication Value] フィールド