論理デバイス

- 論理デバイスについて，1 ページ
- スタンドアロン ASA 論理デバイスの作成，2 ページ
- 脅威に対する防御用のスタンドアロン論理デバイスの作成，4 ページ
- クラスタの展開，6 ページ
- セキュリティ モジュールのコンソールへの接続，13 ページ
- 論理デバイスの削除，14 ページ

論理デバイスについて

Firepower Chassis Manager の [論理デバイス（Logical Devices）] ページを使用して、論理デバイスを作成、編集、削除します。

論理デバイスを作成すると、Firepower アプライアンス Supervisor は、指定されたソフトウェアバージョンをダウンロードし、ブートストラップおよび管理インターフェイスの設定を指定されたモジュール、または、クラスタの場合は、Firepower シャーシにインストールされたすべてのモジュールにダウンロードして論理デバイスを展開します。

次の 2 つのタイプの論理デバイスのいずれかを作成できます。

（注） 作成できるのは、論理デバイスまたはその他のいずれか 1 つのタイプのみです。つまり、3 つのセキュリティ モジュールをインストールしている場合、セキュリティ モジュールにスタンドアロンの論理デバイスは作成できず、残りの2つの論理デバイスを使用してクラスタを作成することになります。

- スタンドアロン：Firepower シャーシにインストールされた各セキュリティ モジュールにスタンドアロンの論理デバイスを作成できます。

（注） スタンドアロンの論理デバイスを設定する場合は、同じソフトウェア タイプをシャーシ内のすべてのモジュールにインストールする必要があります。この時点では、異なるタイプのソフトウェアはサポートされていません。特定のデバイス タイプの異なるバージョンを実行することはできます。しかし、すべてのモジュールが同じタイプの論理デバイスとして設定されている必要があります。

- クラスタ：Firepower シャーシにインストールされたすべてのモジュールが単一の論理デバイスとしてまとめてグループ化されるクラスタを作成できます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

スタンドアロン ASA 論理デバイスの作成

クラスタを設定していない場合は、Firepower シャーシにインストールされた各セキュリティ モジュールにスタンドアロンの論理デバイスを作成できます。クラスタを設定している場合は、そのクラスタを削除してから、スタンドアロン デバイスを作成する必要があります。

（注） 同じソフトウェア タイプをシャーシ内のすべてのモジュールにインストールする必要があります。この時点では、異なるタイプのソフトウェアはサポートされていません。特定のデバイス タイプの異なるバージョンを実行することはできます。しかし、すべてのモジュールが同じタイプの論理デバイスとして設定されている必要があります。

はじめる前に

- 論理デバイスに使用するセキュリティ モジュールに設定済みの論理デバイスがすでにある場合は、最初にその既存の論理デバイスを削除する必要があります（論理デバイスの削除, （14 ページ）を参照）。
- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードし（Cisco.com からのイメージのダウンロードを参照）、次にそのイメージを Firepower アプライアンス にアップロードします（Firepower アプライアンス へのイメージのアップロードを参照）。
- 論理デバイスで使用する管理インターフェイスを設定します。

手順

ステップ 1 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。

[論理デバイス（Logical Devices）] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスをまったく設定していない場合は、その旨を通知するメッセージが表示されます。

ステップ 2 [デバイスの追加（Add Device）] をクリックし、[デバイスの追加（Add Device）] ダイアログボックスを表示します。

ステップ 3 [デバイス名（Device Name）] に論理デバイスの名前を入力します。

ステップ 4 [テンプレート（Template）] には、[Cisco 適応型セキュリティ アプライアンス（Cisco Adaptive Security Appliance）] を選択します。

ステップ 5 [イメージ バージョン（Image Version）] には、ASA ソフトウェアのバージョンを選択します。

ステップ 6 [デバイス モード（Device Mode）] で、[スタンドアロン（Standalone）] オプション ボタンをクリックします。

ステップ 7 [OK] をクリックします。
[プロビジョニング - デバイス名（Provisioning - device name）] ウィンドウが表示されます。

ステップ 8 [データ ポート（Data Ports）] 領域を展開し、デバイスに割り当てる各ポートをクリックします。

ステップ 9 画面の中央のデバイス アイコンをクリックします。
[ASA 設定（ASA Configuration）] ダイアログボックスが表示されます。

ステップ 10 論理デバイスで使用する管理インターフェイスを [管理インターフェイス（Management Interface）] ドロップダウン リストから選択します。

ステップ 11 [IPv4] 領域または [IPv6] 領域、あるいはその両方に、管理 IP アドレス情報を設定します。
この情報は、セキュリティ モジュール設定に管理インターフェイスを設定するために使用されます。この管理 IP アドレスは、ASDM への接続にも使用する IP アドレスです。

a) [管理 IP（Management IP）] フィールドには、ローカル IP アドレスを設定します。
b) [ネットワーク マスク（Network Mask）] または [プレフィックス長（Prefix Length）] に入力します。
c) [ネットワーク ゲートウェイ（Network Gateway）] にネットワーク ゲートウェイ アドレスを入力します。

ステップ 12 [パスワード（Password）] フィールドには、「管理者」ユーザのパスワードを入力します。

ステップ 13 [セキュリティ モジュールの選択（Select Security Module）] で、この論理デバイスに使用するセキュリティ モジュールをクリックして選択します。

ステップ 14 [OK] をクリックして [ASA の設定（ASA Configuration）] ダイアログボックスを閉じます。

ステップ 15 [保存（Save）] をクリックします。
Firepower eXtensible Operating System は、指定されたソフトウェアのバージョンをダウンロードし、ブートストラップ設定と管理インターフェイス設定を指定したセキュリティ モジュールにプッシュすることで、論理デバイスを展開します。

脅威に対する防御用のスタンドアロン論理デバイスの作成

クラスタを設定していない場合は、Firepower シャーシにインストールされた各セキュリティ モジュールにスタンドアロンの論理デバイスを作成できます。クラスタを設定している場合は、そのクラスタを削除してから、スタンドアロン デバイスを作成する必要があります。

（注） 同じソフトウェア タイプをシャーシ内のすべてのモジュールにインストールする必要があります。この時点では、異なるタイプのソフトウェアはサポートされていません。特定のデバイス タイプの異なるバージョンを実行することはできます。しかし、すべてのモジュールが同じタイプの論理デバイスとして設定されている必要があります。

はじめる前に

- 論理デバイスに使用するセキュリティ モジュールに設定済みの論理デバイスがすでにある場合は、最初にその既存の論理デバイスを削除する必要があります（論理デバイスの削除, （14 ページ）を参照）。
- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードし（Cisco.com からのイメージのダウンロードを参照）、次にそのイメージを Firepower アプライアンス にアップロードします（Firepower アプライアンス へのイメージのアップロードを参照）。
- 論理デバイスで使用する管理インターフェイスを設定します。また、データ タイプのインターフェイスを 1 つ以上設定する必要があります。

手順

ステップ 1 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。
[論理デバイス（Logical Devices）]ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスをまったく設定していない場合は、その旨を通知するメッセージが表示されます。

ステップ 2 [デバイスの追加（Add Device）] をクリックし、[デバイスの追加（Add Device）] ダイアログボックスを表示します。

ステップ 3 [デバイス名（Device Name）] に論理デバイスの名前を入力します。
この名前は、管理設定を行い、インターフェイスを割り当てるために Firepower 9300 が使用します。セキュリティ モジュールの設定で使用するデバイス名ではありません。

ステップ 4 [テンプレート（Template）] には、[Cisco Firepower 脅威に対する防御（Cisco Firepower Threat Defense）] を選択します。

ステップ 5 [イメージ バージョン（Image Version）] には、脅威に対する防御のソフトウェアのバージョンを選択します。

ステップ 6 [デバイス モード（Device Mode）] で、[スタンドアロン（Standalone）] オプション ボタンをクリックします。

ステップ 7 [OK] をクリックします。
[プロビジョニング - デバイス名（Provisioning - device name）] ウィンドウが表示されます。

ステップ 8 [データ ポート（Data Ports）] 領域を展開し、デバイスに割り当てる各ポートをクリックします。

ステップ 9 画面の中央のデバイス アイコンをクリックします。
[設定（Configuration）] ダイアログボックスが表示されます。

ステップ 10 [一般情報（General Information）] タブで、次の項目を入力します。

a) [セキュリティ モジュールの選択（Security Module Selection）] で、この論理デバイスに使用するセキュリティ モジュールをクリックして選択します。

b) 論理デバイスで使用する管理インターフェイスを [管理インターフェイス（Management Interface）] ドロップダウン リストから選択します。

c) [デフォルトおよび Firepower（Default and Firepower）] で、管理インターフェイスを設定します。
デフォルトの管理トラフィック チャネルは、すべての内部トラフィック（アプライアンスおよびシステムの管理専用のデバイス間トラフィックなど）を伝送し、Firepower トラフィック チャネルは、すべてのイベント トラフィック（Web イベントなど）を伝送します。

1. [アドレス タイプ（Address Type）] ドロップダウン リストから、アドレスのタイプを選択します。
2. [管理 IP（Management IP）] フィールドには、ローカル IP アドレスを設定します。
3. [ネットワーク マスク（Network Mask）] または [プレフィックス長（Prefix Length）] に入力します。
4. [ネットワーク ゲートウェイ（Network Gateway）] にネットワーク ゲートウェイ アドレスを入力します。

ステップ 11 [設定（Settings）] タブで、次の項目を入力します。

a) [登録キー（Registration Key）] フィールドで、登録時に Firepower Management Center と デバイス間で共有するキーを入力します。

b) デバイスのパスワードを入力します。

c) [Firepower Management Center の IP（Firepower Management Center IP）] フィールドに、管理側の Firepower Management Center の IP アドレスを入力します。

d) ファイアウォール モードを選択します。

e) ファイアウォールイベントを送信するインターフェイスを選択します。指定しない場合は、管理インターフェイスが使用されます。

ステップ 12 [利用規約（Agreement）] タブで、エンド ユーザ ライセンス（EULA）を読んで、同意します。

ステップ 13 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 14 [保存（Save）] をクリックします。
Firepower eXtensible Operating System は、指定されたソフトウェアのバージョンをダウンロードし、ブートストラップ設定と管理インターフェイス設定を指定したセキュリティ モジュールにプッシュすることで、論理デバイスを展開します。

クラスタの展開

クラスタリングを利用すると、シャーシ内のすべてのセキュリティ モジュールをまとめて 1 つの論理デバイスとしてグループ化できます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） Firepower 9300 は複数のシャーシにまたがる（シャーシ間）クラスタをサポートしません。シャーシ内クラスタリングのみをサポートします。

クラスタリングについて

クラスタは、複数のセキュリティモジュールで構成され、1つの単一ユニットとして機能します。Firepower 9300 にクラスタを展開すると、次を実行します。

- クラスタ制御リンクを作成し、セキュリティモジュール間での通信を行います。このリンクは、クラスタ通信に Firepower 9300 のバックプレーンを利用します。
- すべてのセキュリティ モジュール上のアプリケーション内にクラスタ ブートストラップ設定を作成します。

  クラスタを展開すると、Firepower 9300 スーパバイザが最小限のブートストラップ設定を各セキュリティモジュールにプッシュします。この設定には、クラスタ名、クラスタ制御リンクのインターフェイス、およびその他のクラスタ設定が含まれています。クラスタリング環境をカスタマイズする場合は、ユーザはセキュリティ モジュール内でブートストラップ設定の一部を設定できます。
- データ インターフェイスをスパンド *EtherChannel* としてクラスタに割り当てます。

  Firepower 9300 スーパバイザは、スパンド EtherChannel 上のトラフィックの負荷をすべてのセキュリティ モジュールに分散させます。

（注） 管理インターフェイスを除き、インターフェイスは個別にサポートされません。

- すべてのセキュリティ モジュールが共有する管理インターフェイスを別に割り当てます。

クラスタリングおよびセキュリティ モジュール レベルでの動作の詳細については、お使いのセキュリティモジュールアプリケーションのクラスタリングの章を参照してください。以下のセクションで、クラスタリングの概念および実装について詳しく説明します。

マスターおよびスレーブ ユニットのロール

クラスタ内のメンバの 1 つがマスター ユニットです。マスター ユニットは自動的に決定されます。他のすべてのメンバはスレーブ ユニットです。

マスターユニットでのみ、すべての設定を行う必要があります。その設定がスレーブユニットに複製されます。

クラスタ制御リンク

クラスタ制御リンクはポートチャネル48を使用して自動的に作成されます。メンバインターフェイスはありません。このクラスタ タイプの EtherChannel はシャーシ内クラスタリングのためのクラスタ通信に Firepower 9300 のバックプレーンを利用します。後でクラスタ間クラスタリングをサポートするときに、この EtherChannel に外部接続用のメンバ インターフェイスを追加できます。ポートチャネル 48 インターフェイスを使用しない場合は、代わりにクラスタ タイプの EtherChannel を事前に定義しておき、それをクラスタ制御リンクとして使用します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てることができます。このインターフェイスはスパンドEtherChannelとは対照的に、特殊な独立型のインターフェイスです。管理インターフェイスでは、各ユニットに直接接続することができます。

メインクラスタIPアドレスは、そのクラスタのための固定アドレスであり、常に現在のマスターユニットに属します。管理者はアドレス範囲も設定します。これで、各ユニット（現在のマスターも含まれます）がその範囲内のローカルアドレスを使用できるようになります。このメインクラスタIPアドレスによって、管理アクセスのアドレスが一本化されます。マスターユニットが変更されると、メイン クラスタ IP アドレスは新しいマスター ユニットに移動するので、クラスタの管理をシームレスに続行できます。ローカルIPアドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。

たとえば、クラスタを管理するにはメインクラスタIPアドレスに接続します。このアドレスは常に、現在のマスター ユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスターユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

クラスタリングに関するガイドライン

- EtherChannel を VSS または vPC に接続して冗長性を得ることを推奨します。
- スタンドアロン モードでは、一部のシャーシ セキュリティ モジュールはクラスタ化できません。また、他のセキュリティ モジュールも実行できません。したがって、すべてのセキュリティ モジュールをクラスタに含める必要があります。

クラスタリングのデフォルト

クラスタ制御リンクは、ほかのクラスタ タイプのインターフェイスが定義されていない場合は、ポートチャネル 48 を使用します。

ASA クラスタリングの設定

クラスタは、Firepower 9300 スーパバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。

手順

ステップ 1 クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。ポートチャネルの作成またはインターフェイス プロパティの編集を参照してください。
また、データ インターフェイスはクラスタを展開した後でも、そのクラスタに追加できます。

ステップ 2 管理タイプのインターフェイスまたは EtherChannel を追加します。ポートチャネルの作成またはインターフェイス プロパティの編集を参照してください。

ステップ 3 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。
[論理デバイス（Logical Devices）] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスをまったく設定していない場合は、その旨を通知するメッセージが表示されます。

ステップ 4 [デバイスの追加（Add Device）] をクリックし、[デバイスの追加（Add Device）] ダイアログボックスを表示します。
既存のクラスタが存在する場合は、そのクラスタを削除し、新しいクラスタを追加するように求められます。セキュリティ モジュール上のすべてのクラスタ関連の設定が新しい情報で置換されます。

ステップ 5 [デバイス名（Device Name）] に論理デバイスの名前を入力します。この名前はクラスタリングの設定を行ってインターフェイスを割り当てるために Firepower 9300 が使用します。これは、セキュリティ モジュールの設定で使用するクラスタ名ではありません。

ステップ 6 [テンプレート（Template）] には、[Cisco 適応型セキュリティ アプライアンス（Cisco Adaptive Security Appliance）] を選択します。

ステップ 7 [イメージ バージョン（Image Version）] には、ASA ソフトウェアのバージョンを選択します。

ステップ 8 [デバイス モード（Device Mode）] では、[クラスタ（Cluster）] オプション ボタンをクリックします。

ステップ 9 [OK] をクリックします。
スタンドアロン デバイスを設定している場合は、新しいクラスタと置換するように求められます。[プロビジョニング - デバイス名（Provisioning - device name）] ウィンドウが表示されます。

ステップ 10 デフォルトでは、定義済みのすべてのインターフェイスがクラスタに割り当てられます。[データ ポート（Data Ports）] 領域を展開し、割り当てをクラスタから解除する各インターフェイスをクリックします。

ステップ 11 画面の中央のデバイス アイコンをクリックします。
[ASA 設定（ASA Configuration）] ダイアログボックスが表示されます。

ステップ 12 [管理インターフェイス（Management Interface）] をクリックし、以前に作成した管理インターフェイスを選択します。

ステップ 13 [クラスタ情報（Cluster Information）] 領域で、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。
共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

ステップ 14 [サービス タイプ名（ServiceType Name）][クラスタ グループ名（Cluster Group Name）] を設定します。これは、セキュリティモジュール設定内のクラスタ グループです。
名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

ステップ 15 [IPv4] 領域または [IPv6] 領域、あるいはその両方に、管理 IP アドレス情報を設定します。
この情報は、セキュリティ モジュール設定に管理インターフェイスを設定するために使用されます。

a) [管理 IP プール（Management IP Pool）] フィールドで、ローカル IP アドレスのプールを設定します。このアドレスの 1 つが開始アドレスと終了アドレスをハイフンで区切って入力することにより、インターフェイスの各クラスタ ユニットに割り当てられます。
最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスターユニットに属する仮想 IP アドレス（メイン クラスタ IP アドレスとも呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメイン クラスタ IP アドレス用に確保してください。

b) [ネットワーク マスク（Network Mask）] または [プレフィックス長（Prefix Length）] に入力します。

c) [ネットワーク ゲートウェイ（Network Gateway）] に入力します。
d) [仮想 IP アドレス（Virtual IP address）] に入力します。
この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

ステップ 16 [パスワード（Password）] フィールドには、「管理者」ユーザのパスワードを入力します。

ステップ 17 [OK] をクリックして [ASA の設定（ASA Configuration）] ダイアログボックスを閉じます。

ステップ 18 [保存（Save）] をクリックします。
Firepower 9300 は、指定されたソフトウェアのバージョンをダウンロードし、クラスタのブートストラップ設定と管理インターフェイス設定を各セキュリティ モジュールにプッシュすることで、クラスタを展開します。

ステップ 19 セキュリティ モジュールに接続し、クラスタリング設定をカスタマイズします。

脅威に対する防御用のクラスタリングの設定

クラスタは、Firepower 9300 スーパバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。

手順

ステップ 1 クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。ポートチャネルの作成またはインターフェイス プロパティの編集を参照してください。
また、データ インターフェイスはクラスタを展開した後でも、そのクラスタに追加できます。

ステップ 2 管理タイプのインターフェイスまたは EtherChannel を追加します。ポートチャネルの作成またはインターフェイス プロパティの編集を参照してください。

ステップ 3 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。
[論理デバイス（Logical Devices）]ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスをまったく設定していない場合は、その旨を通知するメッセージが表示されます。

ステップ 4 [デバイスの追加（Add Device）] をクリックし、[デバイスの追加（Add Device）] ダイアログボックスを表示します。
既存のクラスタが存在する場合は、そのクラスタを削除し、新しいクラスタを追加するように求められます。セキュリティ モジュール上のすべてのクラスタ関連の設定が新しい情報で置換されます。

ステップ 5 [デバイス名（Device Name）] に論理デバイスの名前を入力します。この名前はクラスタリングまたは管理の設定を行ってインターフェイスを割り当てるために Firepower 9300 が使用します。これは、セキュリティ モジュールの設定で使用するクラスタ名ではありません。

ステップ 6 [テンプレート（Template）] には、[Cisco Firepower 脅威に対する防御（Cisco Firepower Threat Defense）] を選択します。

ステップ 7 [イメージ バージョン（Image Version）] には、脅威に対する防御のソフトウェアのバージョンを選択します。

ステップ 8 [デバイス モード（Device Mode）] では、[クラスタ（Cluster）] オプション ボタンをクリックします。

ステップ 9 [OK] をクリックします。
スタンドアロン デバイスを設定している場合は、新しいクラスタと置換するように求められます。[プロビジョニング - デバイス名（Provisioning - device name）] ウィンドウが表示されます。

ステップ 10 デフォルトでは、定義済みのすべてのインターフェイスがクラスタに割り当てられます。データ インターフェイスの割り当てを解除するには、[データ ポート（Data Ports）] 領域を展開し、クラスタから割り当てを解除する各インターフェイスをクリックします。

ステップ 11 画面の中央のデバイス アイコンをクリックします。
[Cisco Firepower 脅威に対する防御の設定（Cisco Firepower Threat Defense Configuration）] ダイアログボックスが表示されます。

ステップ 12 [クラスタ情報（Cluster Information）] タブで、次の項目を入力します。

a) [クラスタ キー（Cluster Key）] フィールドで、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。
共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

b) セキュリテ モジュール設定のクラスタ グループ名である [クラスタ グループ名（Cluster Group Name）] を設定します。
名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

c) 論理デバイスで使用する管理インターフェイスを [管理インターフェイス（Management Interface）] ドロップダウン リストから選択します。

d) [デフォルト（Default）] で、デフォルトの管理インターフェイスを設定します。
デフォルトの管理トラフィック チャネルは、すべての内部トラフィック（アプライアンスやシステムの管理専用のデバイス間トラフィックなど）を伝送します。

1. [アドレス タイプ（Address Type）] ドロップダウン リストから、アドレスのタイプを選択します。

2. [管理 IP プール（Management IP Pool）] フィールドで、ローカル IP アドレスのプールを設定します。このアドレスの 1 つが開始アドレスと終了アドレスをハイフンで区切って入力することにより、インターフェイスの各クラスタ ユニットに割り当てられます。

   最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスター ユニットに属

する仮想 IP アドレス（メイン クラスタ IP アドレスとも呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメイン クラスタ IP アドレス用に確保してください。

3. [仮想 IP アドレス（Virtual IP address）] に入力します。

   この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

4. [ネットワーク マスク（Network Mask）] または [プレフィックス長（Prefix Length）] に入力します。

5. [ネットワーク ゲートウェイ（Network Gateway）] にネットワーク ゲートウェイ アドレスを入力します。

ステップ 13 [設定（Settings）] タブで、次の項目を入力します。

a) [登録キー（Registration Key）] フィールドで、登録時に Firepower Management Center と デバイス間で共有するキーを入力します。
b) デバイスのパスワードを入力します。
c) [Firepower Management Center の IP（Firepower Management Center IP）] フィールドに、管理側の Firepower Management Center の IP アドレスを入力します。
d) ファイアウォール モードを選択します。
e) ファイアウォールイベントを送信するインターフェイスを選択します。指定しない場合は、管理インターフェイスが使用されます。

ステップ 14 [インターフェイス情報（Interface Information）] タブで、クラスタ内のセキュリティ モジュールのそれぞれに管理インターフェイスを設定します。これは、すべてのイベント トラフィック（たとえば、Web イベント）を伝送する Firepower イベント トラフィック チャネルのインターフェイスです。[アドレス タイプ（Address Type）] ドロップダウン リストから、アドレスのタイプを選択し、各セキュリティ モジュールについて次の項目を入力ます。

a) [管理 IP（Management IP）] フィールドには、ローカル IP アドレスを設定します。
b) [ネットワーク マスク（Network Mask）] または [プレフィックス長（Prefix Length）] に入力します。
c) [ネットワーク ゲートウェイ（Network Gateway）] にネットワーク ゲートウェイ アドレスを入力します。

ステップ 15 [利用規約（Agreement）] タブで、エンド ユーザ ライセンス（EULA）を読んで、同意します。

ステップ 16 [OK] をクリックして [Cisco Firepower 脅威に対する防御の設定（Cisco Firepower Threat Defense Configuration）] ダイアログボックスを閉じます。

ステップ 17 [保存（Save）] をクリックします。
Firepower 9300 は、指定されたソフトウェアのバージョンをダウンロードし、クラスタのブートストラップ設定と管理インターフェイス設定を各セキュリティ モジュールにプッシュすることで、クラスタを展開します。

ステップ 18 セキュリティ モジュールに接続し、クラスタリング設定をカスタマイズします。

クラスタリングの履歴

機能名	プラットフォームリリース	機能情報
Cisco ASA のシャーシ内クラスタリング	1.1(1)	Firepower 9300 シャーシ内のすべての ASA セキュリティ モジュールをクラスタ化できます。 [論理デバイス（Logical Devices）] > [設定（Configuration）] 画面を導入しました。
Cisco Firepower Threat Defense のシャーシ内クラスタリング	1.1(2)	Firepower 9300 シャーシ内のすべての Threat Defense セキュリティ モジュールをクラスタ化できます。

セキュリティ モジュールのコンソールへの接続

セキュリティ モジュールのコンソールに接続するには、次の手順を使用します。

（注） コンソールへの接続に問題が発生した場合は、別の SSH クライアントを試すか、SSH クライアントを新しいバージョンにアップグレードすることを推奨します。

手順

ステップ 1 セキュリティ モジュールのコンソールに接続するには、次の手順を実行します。

a) FXOS CLI から、セキュリティ モジュールに接続します。
Firepower-chassis # **connectmodule***slot_number***console**

セキュリティ モジュールに初めてアクセスした場合は、FXOS モジュールの CLI にアクセスします。

b) モジュールの OS に接続するには、お使いのデバイスに該当するコマンドを入力します。
Firepower-module1>**connect asa**

Firepower-module1>**connect ftd**

これ以降、FXOS CLI のスーパバイザ レベルからセキュリティ モジュールへ接続すると、モジュール OS に直接アクセスします。

ステップ 2 （任意） モジュール OS を終了して FXOS モジュールの CLI に戻るには、Ctrl-A-D を入力します。トラブルシューティングのために FXOS モジュールの CLI にアクセスする場合があります。

ステップ 3 FXOS CLI のスーパバイザ レベルに戻ります。

a) セキュリティ モジュール コンソールを終了するには、~ を入力します。
Telnet アプリケーションに戻ります。

b) Telnet アプリケーションを終了するには、次のように入力します。
telnet>**quit**

例

次に、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

論理デバイスの削除

手順

ステップ 1 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。
[論理デバイス（Logical Devices）]ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスをまったく設定していない場合は、その旨を通知するメッセージが表示されます。

ステップ 2 削除する論理デバイスの [削除（Delete）] をクリックします。

ステップ 3 [はい（Yes）] をクリックして、この論理デバイスを削除することを確認します。

ステップ 4 [はい（Yes）] をクリックして、このアプリケーション設定を削除することを確認します。