Firepower 4100/9300 上の論理デバイス

Firepower 4100/9300 は柔軟なセキュリティ プラットフォームが 1 つまたは複数の論理デバイスをインストールすることができます。

シャーシインターフェイスを設定し、論理デバイスを追加し、Secure Firewall シャーシマネージャ または FXOS の CLI を使用して Firepower 4100/9300 シャーシ上のデバイスにインターフェイスを割り当てる必要があります。これらのタスクは、Device Manager では実行できません。

この章では、基本的なインターフェイスの設定、および Chassis Manager を使用したスタンドアロンまたはハイ アベイラビリティ論理デバイスの追加方法について説明します。FXOS CLI を使用するには、FXOS CLI コンフィギュレーション ガイドを参照してください。高度な FXOS の手順とトラブルシューティングについては、FXOS コンフィギュレーション ガイドを参照してください。

インターフェイスについて

Firepower 4100/9300 シャーシ は、物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバ インターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または シャーシマネージャ によって、FXOS シャーシの管理に使用されます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLIから設定にする必要があります。このインターフェイスについての情報をFXOS CLIで表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

firepower(local-mgmt) # **show mgmt-port**

物理ケーブルまたはSFPモジュールが取り外されている場合や、**mgmt-port shut** コマンドが実行されている場合や、論理デバイスがオフラインになっている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

インターフェイス タイプ

物理インターフェイスおよびEtherChannel（ポートチャネル）インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは1つまたは複数の論理デバイス/コンテナインスタンス（脅威に対する防御 Management Center 専用）で共有できます。
- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。個別のシャーシ管理インターフェイスについては、シャーシ管理インターフェイス（1 ページ）を参照してください。

（注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Eventing： Management Center デバイスを使用した 脅威に対する防御 のセカンダリ管理インターフェイスとして使用します。

（注） 各アプリケーションインスタンスのインストール時に、仮想イーサネットインターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。Device Manager および Security Cloud Control はクラスタリングをサポートしていません。

FXOS インターフェイスとアプリケーション インターフェイス

Firepower 4100/9300 は、物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスの基本的なイーサネット設定を管理します。アプリケーション内で、より高いレベルの設定を行います。たとえば、FXOS では Etherchannel のみを作成できます。ただし、アプリケーション内の EtherChannel に IP アドレスを割り当てることができます。

続くセクションでは、インターフェイスの FXOS とアプリケーションの連携について説明します。

VLAN サブインターフェイス

すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるため、シャーシとアプリケーションの間で不一致が発生することがあります。

Firepower 9300 のハードウェアとソフトウェアの要件と前提条件

Firepower 9300 には、3 つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を確認します。

- セキュリティモジュール タイプ：Firepower 9300 には、さまざまなタイプのモジュールをインストールできます。たとえば、SM-48 をモジュール 1、SM-40 をモジュール 2 、SM-56 をモジュール 3 としてインストールできます。
- ネイティブインスタンスとコンテナインスタンス：セキュリティモジュールにコンテナインスタンスをインストールする場合、そのモジュールは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはモジュールのすべてのリソースを使用するため、モジュールにはネイティブインスタンスを 1 つのみインストールできます。一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用することができます。たとえば、モジュール 1 とモジュール 2 にネイティブインスタンスをインストールできますが、モジュール 3 にはコンテナインスタンスをインストールできます。
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。ただし、2 つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシには SM-40、SM-48、および SM-56 があります。SM-40 モジュール間、SM-48 モジュール間、および SM-56 モジュール間にハイアベイラビリティペアを作成できます。
- ASA および Threat Defense のアプリケーションタイプ：異なるアプリケーション タイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール 1 とモジュール 2 に ASA をインストールし、モジュール 3 に Threat Defense をインストールすることができます。
- ASA または Threat Defense のバージョン：個別のモジュールで異なるバージョンのアプリケーション インスタンス タイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール 1 に Threat Defense 6.3 を、モジュール 2 に Threat Defense 6.4 を、モジュール 3 に Threat Defense 6.5 をインストールできます。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

インターフェイスに関する注意事項と制限事項

デフォルトの MAC アドレス

デフォルトのMACアドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスでは、Burned-In MAC Address を使用します。
- EtherChannel: EtherChannelの場合は、そのチャネルグループに含まれるすべてのインターフェイスが同じMACアドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対して透過的になります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識し

ないからです。ポートチャネル インターフェイスは、プールにある一意の MAC アドレスを使用します。インターフェイス メンバーシップは MAC アドレスに影響しません。

一般的なガイドラインと制限事項

ハイ アベイラビリティ

- アプリケーション設定内で高可用性を設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。
- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 同じモデルであること。
  - 高可用性論理デバイスに同じインターフェイスを割り当てること。
  - インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 詳細については、「ハイ アベイラビリティのシステム要件」を参照してください。

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスの有効化、Etherchannel の追加、VLAN サブインターフェイスの、インターフェイスプロパティの編集、を実行できます。

インターフェイスの有効化または無効化

各インターフェイスの [管理状態（Admin State）] を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスは無効になっています。

手順

ステップ 1 [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ページを開きます。

[インターフェイス]ページには、現在インストールされているインターフェイスの視覚的表現がページの上部に表示され、下の表にはインストールされているインターフェイスのリストが示されます。

ステップ 2 インターフェイスを有効にするには、 [disabled **無効なスライダ**（  ）] をクリックして、[enabled **有効なスライダ**（  ）] に変更します。

[はい]をクリックして、変更を確認します。視覚的表現の対応するインターフェイスがグレイから緑に変化します。

ステップ 3 インターフェイスを無効にするには、 [有効なスライダ（enabled **有効なスライダ**（  ））] をクリックして、[無効なスライダ（disabled **無効なスライダ**（  ））] に変更します。

[はい]をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。

物理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、アプリケーションで論理的に有効にする必要があります。

（注）
- QSFPH40G-CUxMの場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。
- ポートのSFPを別のSFPモジュールに交換しても、インターフェイスの速度、デュプレックス、および自動ネゴシエーションは自動的に更新されません。インターフェイスを再構成する必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

EtherChannel（ポート チャネル）の追加

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大16個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプはRJ-45またはSFPのいずれかです。異なるタイプ（銅と光ファイバ）のSFPを混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1GBインターフェイスと10GBインターフェイスなど）を混在させることはできません。リンク集約制御プロトコル（LACP）では、2つのネットワー

クデバイス間でリンク集約制御プロトコルデータユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データインターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

（注） モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

各メンバーインターフェイスが LACP 更新を送受信するように、Firepower 4100/9300 シャーシは Etherchannel をアクティブ LACP モードでしかサポートしません。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [一時停止（Suspended）] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータ インターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止（Suspended）] または [ダウン（Down）] 状態に戻ります。

論理デバイスの設定

スタンドアロン論理デバイスまたはハイ アベイラビリティのペアを Firepower 4100/9300 シャーシ に追加します。

Device Manager のスタンドアロン Threat Defense を追加します。

Device Manager はネイティブインスタンスで使用できます。コンテナインスタンスはサポートされていません。スタンドアロン論理デバイスは、単独で、または高可用性ペアで動作します。

始める前に

- 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、そのイメージを Firepower 4100/9300 シャーシ。
- 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。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません。
- また、少なくとも 1 つのデータ タイプのインターフェイスを設定する必要があります。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス
  - DNS サーバの IP アドレス
  - Threat Defense ホスト名とドメイン名

手順

セキュリティポリシーの設定を始めるには、Device Manager のコンフィギュレーション ガイドを参照してください。

ハイ アベイラビリティ ペアの追加

Threat Defense ハイ アベイラビリティ（フェールオーバーとも呼ばれます）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイアベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

ハイ アベイラビリティのシステム要件を参照してください。

手順

ステップ 1 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 2 フェールオーバーリンクとステートリンクに 1 つまたは 2 つのデータインターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間で高可用性トラフィックを交換します。フェールオーバーリンクとステートリンクの組み合わせには、10 GB のデータインターフェイスを使用することを推奨します。使用可能なインターフェイスがある場合は、別のフェールオーバーリンクとステートリンクを使用できます。ステートリンクには、最も多くの帯域幅が必要です。フェールオーバーリンクまたはステートリンクに管理タイプのインターフェイスを使用することはできません。シャーシ間でスイッチを使用することをお勧めします。この場合、フェールオーバーインターフェイスと同じネットワークセグメント上に他のデバイスを配置できません。

ステップ 3 論理デバイスで高可用性を有効にします。 高可用性（フェールオーバー）を参照してください。

ステップ 4 高可用性を有効にした後にインターフェイスを変更する必要がある場合は、最初にスタンバイユニットで変更を実行してから、アクティブユニットで変更を実行します。

Threat Defense 論理デバイスのインターフェイスの変更

脅威に対する防御 論理デバイスでは、インターフェイスの割り当てや割り当て解除を行うことができます。その後、Device Manager でインターフェイス設定を同期できます。

新しいインターフェイスの追加や未使用のインターフェイスの削除が、脅威に対する防御 の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバなど、脅威に対する防御 の設定における多くの場所で直接参照されている可能性があります。セキュリティゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつ Device Manager での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

古いインターフェイスを削除する前に、あるインターフェイスから別のインターフェイスに設定を移行できます。

始める前に

- 物理インターフェイスの設定 （6 ページ） および EtherChannel（ポート チャネル）の追加 （6 ページ） に従って、インターフェイスを設定し、EtherChannel を追加します。

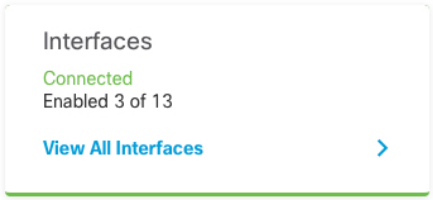
- すでに割り当てられているインターフェイスをEtherChannelに追加する場合(たとえば、すべてのインターフェイスがデフォルトでクラスタに割り当てられる場合)、最初にそのインターフェイスを論理デバイスから割り当て解除してから、EtherChannelに追加する必要があります。新しいEtherChannelの場合、EtherChannelをデバイスに割り当てることができます。
- ハイアベイラビリティのため、Device Manager で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。最初にスタンバイユニットでインターフェイスを変更してから、アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイス モニタリングに影響を及ぼさないことに注意してください。
- マルチインスタンスモードでは、サブインターフェイスを同じ VLAN タグを持つ別のサブインターフェイスと変更するには、最初にインターフェイスのすべての設定（nameif config を含む）を削除してから、シャーシマネージャからインターフェイスの割り当てを解除する必要があります。割り当てが解除されたら、新しいインターフェイスを追加し、Management Center からインターフェイスの同期を使用します。

手順

ステップ 1 Device Manager でインターフェイスを同期して移行します。

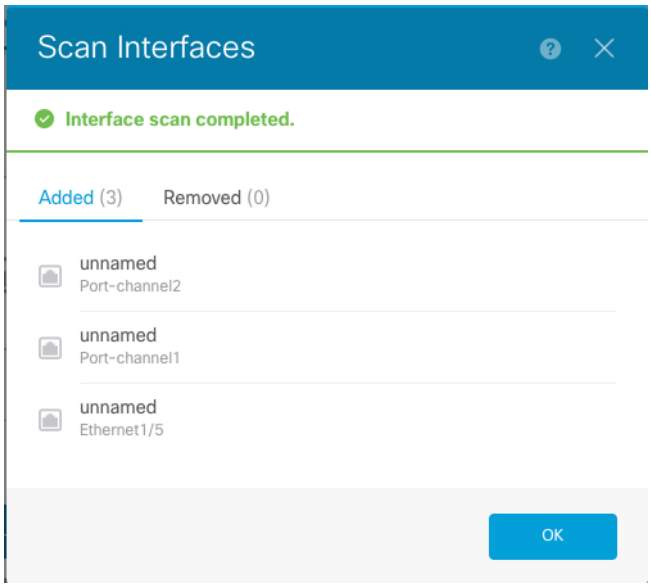
a) Device Manager にログインします。

b) [デバイス（Device）] をクリックしてから、**[インターフェイス（Interfaces）]** サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。



c) [インターフェイス（Interfaces）] アイコンをクリックします。

d) インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。



e) 新しいインターフェイスに名前、IPアドレスなどを設定します。

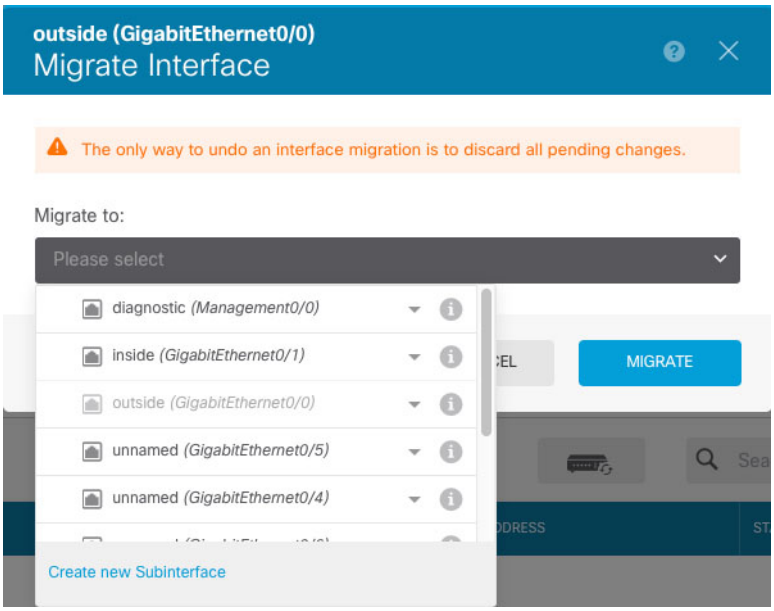
削除するインターフェイスの既存のIPアドレスと名前を使用する場合は、新しいインターフェイスでこれらの設定を使用できるように、古いインターフェイスをダミーの名前とIPアドレスで再設定する必要があります。

f) 古いインターフェイスを新しいインターフェイスに置き換えるには、古いインターフェイスの [置換（Replace）] アイコンをクリックします。

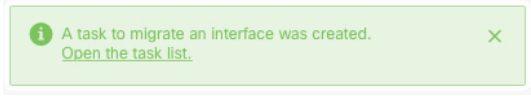
[置換（Replace）] アイコン

このプロセスによって、インターフェイスを参照しているすべての設定で、古いインターフェイスが新しいインターフェイスに置き換えられます。

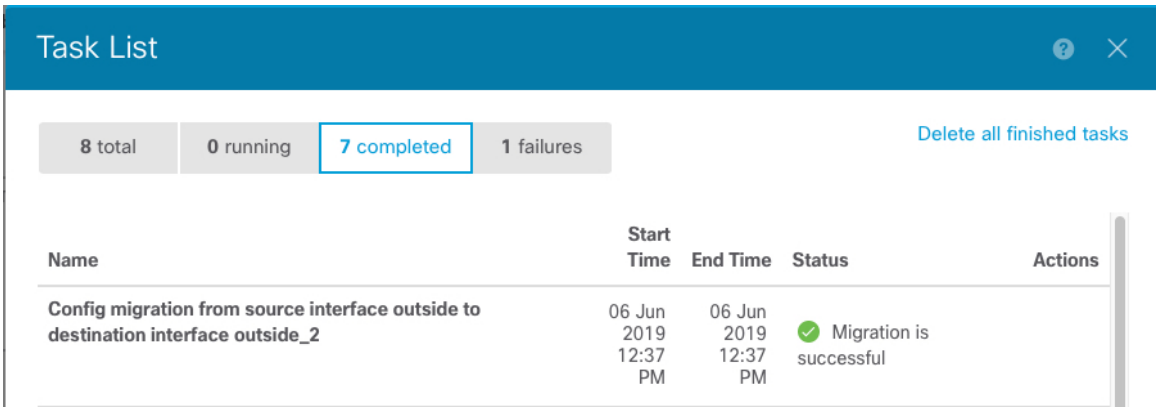
g) [交換用インターフェイス（Replacement Interface）]：ドロップダウン リストから新しいインターフェイスを選択します。



h) [インターフェイス（Interfaces）] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。

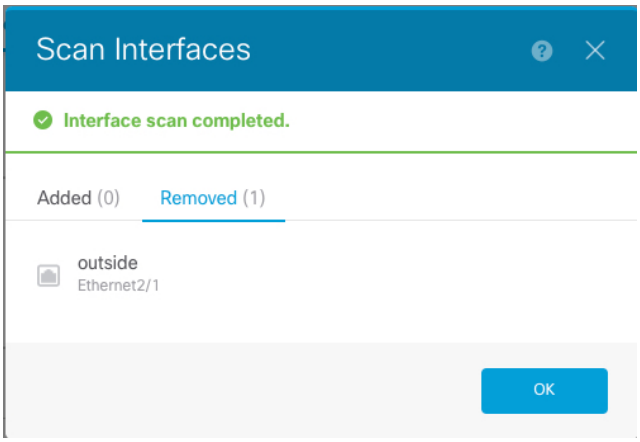


i) [タスクリスト（Task List）] を調べて、移行が成功したことを確認します。



ステップ 2 Device Manager でインターフェイスを再度同期します。

図 *1 : Device Manager* によるインターフェイスのスキャン



アプリケーションのコンソールへの接続

アプリケーションのコンソールに接続するには、次の手順を使用します。

手順

ステップ 1 コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
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>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect ftd *name*

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- Threat Defense ：「**exit**」と入力します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

Firepower 4100/9300 論理デバイスの履歴

機能	バージョン	詳細
Firepower 4100/9300 での Device Manager のサポート	6.5.0	Firepower 4100/9300 の 脅威に対する防御 論理デバイスで Device Manager を使用できるようになりました。Device Manager はマルチインスタンス機能をサポートしていません。ネイティブインスタンスのみがサポートされています。 （注） FXOS 2.7.1 が必要です。

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。