



## 仮想スイッチのセットアップ

以下のトピックでは、Firepower システムで仮想スイッチをセットアップする方法について説明します。

- [仮想スイッチ \(1 ページ\)](#)
- [スイッチドインターフェイスの設定 \(2 ページ\)](#)
- [仮想スイッチの設定 \(7 ページ\)](#)

### 仮想スイッチ

レイヤ2 展開の 7000 または 8000 シリーズ デバイスは、2 つ以上のネットワーク間でパケットスイッチングを提供するように設定できます。レイヤ2 展開では、仮想スイッチをスタンドアロンブロードキャスト ドメインとして機能させ、ネットワークを論理セグメントに分割するように設定できます。仮想スイッチでは、ホストからの Media Access Control (MAC) アドレスを使用して、パケットの送信先を判断します。

仮想スイッチを設定すると、スイッチはまず、スイッチ上の使用可能なすべてのポートからパケットをブロードキャストします。その後は、タグ付きのリターントラフィックを使用して、各ポートに接続されたネットワーク上にどのホストが存在するのかを学習していきます。

仮想スイッチがトラフィックを処理するには、仮想スイッチに複数のスイッチドインターフェイスがなければなりません。仮想スイッチごとに、トラフィックは、スイッチ型インターフェイスとして設定されたいくつかのポートに限定されます。たとえば、4 つのスイッチ型インターフェイスのある仮想スイッチを設定した場合、ブロードキャスト用に 1 つのポートを介して送られるパケットは、そのスイッチ上の残る 3 つのポートからのみ送出可能です。

物理スイッチ型インターフェイスを設定するときには、仮想スイッチにそれを割り当てる必要があります。また、必要に応じて、物理ポート上に追加の論理スイッチドインターフェイスを定義することもできます。複数の物理インターフェイスを Link Aggregation Group (LAG) と呼ばれる単一の論理スイッチドインターフェイスにグループ化できます。この単一の集約論理リンクによって、帯域幅と冗長性の向上と、2 つのエンドポイント間でのロードバランシングが実現されます。



**注意** レイヤ2展開に何らかの理由で障害が発生した場合、デバイスはトラフィックを転送しなくなります。

## スイッチドインターフェイスの設定

物理設定または論理設定を備えるよう、スイッチ型インターフェイスをセットアップできます。タグなし VLAN トラフィックを処理するよう物理スイッチ型インターフェイスを設定できます。また、VLAN タグが指定されたトラフィックを処理するよう論理スイッチ型インターフェイスを作成することもできます。

レイヤ2展開では、外部の物理インターフェイス上でトラフィックを受信した場合、それを待機しているスイッチ型インターフェイスがなければ、システムはそのトラフィックをドロップします。VLAN タグのないパケットを受信した場合、そのポート用の物理スイッチ型インターフェイスが未設定であれば、システムはパケットをドロップします。VLAN タグ付きパケットを受信した場合、論理スイッチ型インターフェイスが未設定であれば、システムは同様にパケットをドロップします。

スイッチ型インターフェイスで VLAN タグ付きで受信されたトラフィックをシステムが処理するときには、ルールの評価や転送の決定を行う前に、入力における最も外側の VLAN タグを取り除きます。VLAN タグ付き論理スイッチ型インターフェイスを介してデバイスから出るパケットは、出力において関連する VLAN タグ付きでカプセル化されます。

親の物理インターフェイスをインラインまたはパッシブに変更すると、システムは関連するすべての論理インターフェイスを削除することに注意してください。

## スイッチ型インターフェイスの設定メモ

管理対象デバイス上の1つ以上の物理ポートはスイッチ型インターフェイスとして設定できます。トラフィックを処理できるようにするには、その前に、物理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。リンク モード設定および MDI/MDIX 設定は、銅線インターフェイスにのみ設定できます。



(注) 8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。


物理スイッチ型インターフェイスごとに、複数の論理スイッチ型インターフェイスを追加できます。物理インターフェイスで受信される VLAN タグ付きトラフィックを処理するには、各論理インターフェイスをその特定のタグに関連付ける必要があります。トラフィックを処理するには、論理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。

スイッチ型インターフェイスを設定する場合、設定可能な MTU の範囲は、Firepower システムのデバイスのモデルとインターフェイスのタイプによって異なる可能性があります。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。



**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「[Snort® の再起動によるトラフィックの動作](#)」を参照してください。

既存の論理スイッチ型インターフェイスを編集するには、インターフェイスの横にある編集アイコン ([]) をクリックします。

論理スイッチ型インターフェイスを削除すると、それが存在する物理インターフェイスから、および関連付けられている仮想スイッチとセキュリティゾーンからそれが削除されます。


#### 関連トピック


[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲](#)  
[Snort® の再起動シナリオ](#)

## 物理スイッチドインターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** スイッチドインターフェイスを設定するデバイスの横にある編集アイコン () をクリックします。  
 マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** スイッチドインターフェイスとして設定するインターフェイスの横にある編集アイコン () をクリックします。

**ステップ 4** [スイッチド (Switched)] タブをクリックします。

**ステップ 5** セキュリティゾーンをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [セキュリティゾーン (Security Zone)] ドロップダウン リストから既存のセキュリティゾーンを選択します。

- [新規 (New) ] を選択して新しいセキュリティ ゾーンを追加します。 [セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成](#) を参照してください。

**ステップ 6** 仮想スイッチをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [仮想スイッチ (Virtual Switch) ] ドロップダウン リストから既存の仮想スイッチを選択します。
- [新規 (New) ] を選択して新しい仮想スイッチを追加します。 [仮想スイッチの追加 \(8 ページ\)](#) を参照してください。

**ステップ 7** スwitchドインターフェイスにトラフィックを処理させるには、[有効 (Enabled) ] チェックボックスをオンにします。

(注) このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

**ステップ 8** [モード (Mode) ] ドロップダウンリストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション (Auto Negotiation) ] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

**ステップ 9** [MDI/MDIX] ドロップダウンリストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス)、MDIX (メディア依存型インターフェイス クロスオーバー)、または自動 MDIX のいずれかを指定するオプションを選択します。

デフォルトでは、[MDI/MDIX] は [自動 MDIX (Auto-MDIX) ] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。

**ステップ 10** [MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイスタイプによって異なる場合があります。

**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「[Snort® の再起動によるトラフィックの動作](#)」を参照してください。

**ステップ 11** [保存 (Save) ] をクリックします。

---

### 次のタスク

- 設定変更を展開します。 [設定変更の展開](#) を参照してください。

## 関連トピック

[7000 および 8000 シリーズ デバイス および NGIPSv の MTU 範囲](#)

[Snort® の再起動シナリオ](#)

## 論理スイッチドインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** スイッチドインターフェイスを追加するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [追加 (Add)] ドロップダウンメニューから、[論理インターフェイスの追加 (Add Logical Interface)] を選択します。

**ステップ 4** [スイッチド (Switched)] をクリックします。

**ステップ 5** [インターフェイス (Interface)] ドロップダウンリストから、VLAN タグ付きトラフィックを受信する物理インターフェイスを選択します。

**ステップ 6** [VLAN タグ (VLAN Tag)] フィールドで、このインターフェイス上のインバウンド/アウトバウンドトラフィックに割り当てるタグ値を入力します。

このタグの値には、1 ~ 4094 の任意の整数を指定できます。

**ステップ 7** セキュリティゾーンをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [セキュリティゾーン (Security Zone)] ドロップダウンリストから既存のセキュリティゾーンを選択します。
- [新規 (New)] を選択して新しいセキュリティゾーンを追加します。[セキュリティゾーンおよびインターフェイスグループオブジェクトの作成](#) を参照してください。

**ステップ 8** 仮想スイッチをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [仮想スイッチ (Virtual Switch)] ドロップダウンリストから既存の仮想スイッチを選択します。
- [新規 (New)] を選択して新しい仮想スイッチを追加します。[仮想スイッチの追加 \(8 ページ\)](#) を参照してください。

**ステップ 9** スイッチドインターフェイスにトラフィックを処理させるには、[有効 (Enabled)] チェックボックスをオンにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

**ステップ 10** [MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイスタイプによって異なる場合があります。

**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「[Snort® の再起動によるトラフィックの動作](#)」を参照してください。

**ステップ 11** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

#### 関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲](#)  
[Snort® の再起動シナリオ](#)

## 論理スイッチドインターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** 削除するスイッチドインターフェイスが含まれる管理対象デバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** 削除する論理スイッチドインターフェイスの横にある削除アイコン (🗑) をクリックします。

**ステップ 4** 入力を求められた場合、インターフェイスを削除することを確認します。

#### 次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

## 仮想スイッチの設定

レイヤ 2 展開でスイッチドインターフェイスを使用できるようにするには、その前に仮想スイッチを設定し、スイッチドインターフェイスをその仮想スイッチに割り当てる必要があります。仮想スイッチとは、ネットワークを通過するインバウンドトラフィックとアウトバウンドトラフィックを処理する複数のスイッチドインターフェイスからなるグループのことです。

### 仮想スイッチの設定に関する注意事項

仮想スイッチは、[デバイス管理 (Device Management)] ページの [仮想スイッチ (Virtual Switches)] タブから追加することができます。[仮想スイッチ (Virtual Switches)] タブには、デバイス上で設定済みのすべての仮想スイッチのリストが表示されます。このページには、各スイッチのサマリ情報が表示されます。

表 1: 仮想スイッチ テーブル ビューのフィールド

フィールド	説明
Name	仮想スイッチの名前。
Interfaces	仮想スイッチに割り当てられたすべてのスイッチ型インターフェイス。[Interfaces] タブで無効にしたインターフェイスは表示されません。
Hybrid Interface	仮想スイッチを仮想ルータに結合する、オプション設定のハイブリッドインターフェイス。
Unicast Packets	次の項目を含む、仮想スイッチのユニキャスト パケット統計： <ul style="list-style-type: none"> <li>• 受信されたユニキャスト パケット</li> <li>• 転送されたユニキャスト パケット (ホストによるドロップを除く)</li> <li>• 誤ってドロップされたユニキャスト パケット</li> </ul>

フィールド	説明
Broadcast Packets	次の項目を含む、仮想スイッチのブロードキャストパケット統計： <ul style="list-style-type: none"> <li>受信されたブロードキャストパケット</li> <li>転送されたブロードキャストパケット</li> <li>誤ってドロップされたブロードキャストパケット</li> </ul>

また、スイッチ型インターフェイスを設定するときにスイッチを追加することもできます。仮想スイッチには、スイッチ型インターフェイスだけ割り当てることができます。管理対象デバイス上でスイッチ型インターフェイスを設定する前に仮想スイッチを作成する必要がある場合は、空の仮想スイッチを作成し、あとでそれにインターフェイスを追加できます。



**ヒント** 既存の仮想スイッチを編集するには、スイッチの横にある編集アイコン (✎) をクリックします。

## 仮想スイッチの追加

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** 仮想スイッチを追加するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [仮想スイッチ (Virtual Switches)] タブをクリックします。

**ステップ 4** [仮想スイッチの追加 (Add Virtual Switch)] をクリックします。

**ステップ 5** [名前 (Name)] フィールドに名前を入力します。

**ステップ 6** [使用可能 (Available)] リストから、仮想スイッチに追加される 1 つ以上のスイッチドインターフェイスを選択します。

**ヒント** [インターフェイス (Interfaces)] タブですでに無効にしたインターフェイスは使用できません。インターフェイスを追加した後で無効にすると、設定からそれが削除されます。



- ステップ7** [追加 (Add) ]をクリックします。
- ステップ8** 仮想ルータに仮想スイッチを結びつけるには、[ハイブリッドインターフェイス (Hybrid Interface) ] ドロップダウンリストからハイブリッドインターフェイスを選択します。
- ステップ9** 必要に応じて、スイッチの詳細設定を行います。以下を参照してください。 [仮想スイッチの詳細設定 \(9 ページ\)](#)
- ステップ10** [保存 (Save) ]をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の展開](#) を参照してください。

#### 関連トピック

[論理ハイブリッドインターフェイス](#)

## 仮想スイッチの詳細設定

### スタティック MAC エントリを追加する (Adding Static MAC Entries)

仮想スイッチは、ネットワークからのリターントラフィックにタグを付けることで、時間の経過と共に MAC アドレスを学習します。手動でスタティック MAC エントリを追加できます。そのようにすることで、MAC アドレスが特定のポート上にあることを指定します。そのポートからトラフィックを受信するかどうかに関わらず、MAC アドレスはテーブル内でスタティックアドレスとして保持されます。仮想スイッチごとに1つ以上のスタティック MAC アドレスを指定できます。

### スパンニング ツリー プロトコル (STP) を有効にしてブリッジ プロトコル データ ユニット (BPDU) をドロップする (Enabling Spanning Tree Protocol (STP) and Dropping Bridge Protocol Data Units (BPDU))

STP は、ネットワーク ループを防止するために使用されるネットワーク プロトコルです。BPDU は、ネットワーク ブリッジに関する情報を伝送し、ネットワークを介して交換されます。ネットワーク内に冗長リンクがある場合、プロトコルはBPDUを使用して最も高速なネットワーク リンクを識別し、選択します。ネットワーク リンクで障害が発生した場合、スパンニング ツリーは既存の代替リンクにフェールオーバーします。



- (注) Cisco では、高可用性ペアで 7000 または 8000 シリーズ デバイスに展開する予定の仮想スイッチを設定する場合は、STP を有効にすることを強く推奨しています。仮想スイッチが複数のネットワーク インターフェイス間のトラフィックを切り替える場合は、STP のみを有効にします。

仮想スイッチが複数の VLAN 間のトラフィックをルーティングする場合、ルータ オン ア スティックと同様に、BPDUはさまざまな論理スイッチドインターフェイスを介してデバイスを

出入りしますが、物理スイッチドインターフェイスは同じです。その結果、STPはデバイスを冗長ネットワークループとして識別します。特定のレイヤ2配置ではこれにより問題が生じる場合があります。それを防ぐため、トラフィックのモニタリング時にデバイスがBPDUをドロップするようにドメインレベルで仮想スイッチを設定することができます。STPを無効にする場合は、BPDUをドロップするしかありません。



(注) 仮想スイッチが1つの物理インターフェイス上のVLAN間でトラフィックをルーティングする場合にのみ、BPDUをドロップしてください。

### 厳格なTCP強制を有効にする (Enabling Strict TCP Enforcement)

最大限のTCPセキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3ウェイハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3ウェイハンドシェイクが完了していない接続の非SYN TCPパケット
- 応答側がSYN-ACKを送信する前にTCP接続の発信側から送信された非SYN/RSTパケット
- SYNの後ではあるがセッションの確立前にTCP接続の応答側から送信された非SYN-ACK/RSTパケット
- イニシエータまたはレスポンドからの、確立済みのTCP接続上のSYNパケット

仮想スイッチを論理ハイブリッドインターフェイスに関連付けると、そのスイッチでは、論理ハイブリッドインターフェイスに関連付けられた仮想ルータと同じ厳密なTCP強制設定が使用されることに注意してください。その場合、スイッチで厳格なTCP強制を指定することはできません。

## 仮想スイッチの詳細設定の設定

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ1 [Devices] > [Device Management]を選択します。

ステップ2 編集する仮想スイッチが含まれるデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ3 [仮想スイッチ (Virtual Switches)] タブをクリックします。

- ステップ 4** 編集する仮想スイッチの横にある編集アイコン (✎) をクリックします。
- ステップ 5** [Advanced] タブをクリックします。
- ステップ 6** スタティック MAC エントリを追加するには、[追加 (Add)] をクリックします。
- ステップ 7** [MAC アドレス (MAC Address)] フィールドで、2 桁の 16 進数 6 組をコロンで区切った標準形式を使用して、アドレスを入力します (たとえば 01:23:45:67:89:AB)。
- (注) ブロードキャストアドレス (00:00:00:00:00:00 と FF:FF:FF:FF:FF:FF) をスタティック MAC アドレスとして追加することはできません。
- ステップ 8** [インターフェイス (Interface)] ドロップダウン リストから、MAC アドレスを割り当てるインターフェイスを選択します。
- ステップ 9** [OK] をクリックします。
- ステップ 10** スパニングツリープロトコルを有効にする場合は、[スパニングツリープロトコルを有効にする (Enable Spanning Tree Protocol)] チェックボックスをオンにします。
- ステップ 11** 厳密な TCP 強制を有効にするには、[厳密な TCP 強制 (Strict TCP Enforcement)] チェックボックスをオンにします。
- 仮想スイッチを論理ハイブリッドインターフェイスに関連付けると、このオプションは表示されず、論理ハイブリッドインターフェイスに関連付けられた仮想ルータと同じ設定がスイッチで使用されます。
- ステップ 12** ドメインレベルで BPDU をドロップするには、[BPDU のドロップ (Drop BPDUs)] チェックボックスをオンにします。
- ステップ 13** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

## 仮想スイッチの削除


スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

仮想スイッチを削除すると、そのスイッチに割り当てられたスイッチドインターフェイスを別のスイッチに含めることができますようになります。

- ステップ 1** [Devices] > [Device Management] を選択します。
- ステップ 2** 削除する仮想スイッチが含まれる管理対象デバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ3** [仮想スイッチ (Virtual Switches) ] タブをクリックします。

**ステップ4** 削除する仮想スイッチの横にある削除アイコン (  ) をクリックします。

**ステップ5** プロンプトが表示されたら、仮想スイッチを削除することを確認します。

---

### 次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。