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

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、スイッチド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 つのスイッチド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入されるパケットは、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。

物理スイッチド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。システムがVLANタグなしのパケットを受信した場合、該当するポートに物理スイッチドインターフェイスが設定されていなければ、パケットはドロップされます。システムがVLANタグ付きのパケットを受信した場合、論理スイッチドインターフェイスが設定されていなければ、同じくパケットはドロップされます。

スイッチド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したVLANタグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。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 インスペクションが一時的に中断されます。インスペクションは、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、それ以上インスペク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	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

手順

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。

（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 インスペクションが一時的に中断されます。インスペクションは、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、それ以上インスペク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	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

手順

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 インスペクションが一時的に中断されます。インスペクションは、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、それ以上インスペク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	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

手順

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
名前（Name）]	仮想スイッチの名前。
インターフェイス	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。[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。
ハイブリッドインターフェイス（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。

フィールド	説明
ユニキャスト パケット（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： • 受信されたユニキャスト パケット • 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） • 誤ってドロップされたユニキャスト パケット
ブロードキャスト パケット（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： • 受信されたブロードキャスト パケット • 転送されたブロードキャスト パケット • 誤ってドロップされたブロードキャスト パケット

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、後でその仮想スイッチ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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

手順

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、ネットワークを介して交換され、ネットワーク ブリッジに関する情報を伝送しま

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 ループと見なします。特定のレイヤ2展開では、これによって問題が発生する場合があります。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、セッションの確立前に TCP 接続のレスポンダから送信された非 SYN-ACK/RST パケット
- 発信側または応答側のどちらかから送信された、確立された TCP 接続の 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ている仮想ルータと同じ厳格な 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	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

手順

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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	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るようになります。

手順

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。