集約インターフェイスと LACP

以下のトピックでは、集約インターフェイスの設定について、および管理対象デバイスでLACPがどのように機能するかについて説明します。

集約インターフェイスについて

Firepower システムでは、管理対象デバイスがレイヤ 2（ネットワーク間でパケット スイッチングを行う）、またはレイヤ 3（インターフェイス間でトラフィックをルーティングする）に展開されている場合、複数の物理イーサネットインターフェイスを管理対象デバイス上で1つの論理リンクにグループ化できます。このように1つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

集約リンクを作成するには、スイッチドまたはルーテッドLink Aggregation Group（LAG）を作成します。集約グループを作成すると、集約インターフェイスと呼ばれる論理インターフェイスが作成されます。上位層エンティティである LAG は単一の論理リンクに似ており、データトラフィックは集約インターフェイスを介して送信されます。集約リンクは、複数のリンクの帯域幅をまとめて追加することによって帯域幅を増加させます。また、使用可能なすべてのリンクのトラフィックをロードバランシングすることで、冗長性を実現します。リンクの1つで障害が発生すると、トラフィックは残りのリンク全体にロードバランシングされます。

LAG のエンドポイントは、7000 または 8000 シリーズ デバイス（上記の図を参照）が 2 つの場合もあれば、一方がサードパーティ アクセス スイッチまたはルータに接続されている 7000

または 8000 シリーズ デバイスの場合もあります。2 つのデバイスは一致している必要はありませんが、同じ物理構成で、IEEE 802.ad リンク アグリゲーション標準規格をサポートしている必要があります。LAG の通常の展開では、2 つの管理対象デバイス間のアクセス リンクを集約するか、管理対象デバイスとアクセス スイッチまたはルータ間にポイントツーポイント接続を確立します。

NGIPSv デバイスや ASA FirePOWER モジュールでは集約インターフェイスを設定することはできません。

LAG 設定

集約インターフェイスには次の 2 種類があります。

- スイッチド：レイヤ 2 集約インターフェイス
- ルーテッド：レイヤ 3 集約インターフェイス

リンク集約は、リンク集約グループ（LAG）を使用して実装します。LAG を設定するには、集約スイッチドまたはルーテッドインターフェイスを作成して、一連の物理インターフェイスをリンクに関連付けます。すべての物理インターフェイスは同じ速度とメディアでなければなりません。

集約リンクは動的または静的に作成します。動的リンク集約では、IEEE 802.ad リンク集約標準のコンポーネットである Link Aggregation Control Protocol（LACP）が使用されますが、静的リンク集約では使用されません。LACP は、LAG の両端の各デバイスでリンクおよびシステムの情報を交換できるようにして、集約でアクティブに使用するリンクを決定します。静的LAG 構成では、手動でリンク集約を維持し、ロード バランシング ポリシーとリンク選択ポリシーを展開する必要があります。

スイッチドまたはルーテッド集約インターフェイスを作成すると、同じタイプのリンク集約グループが自動的に作成され、それに番号が付けられます。たとえば、最初の LAG（スイッチドまたはルーテッド）を作成すると、その集約インターフェイスは、管理対象デバイスの [インターフェイス（Interfaces）] タブの **lag0** ラベルによって識別できます。物理インターフェイスと論理インターフェイスをこの LAG に関連付けると、それらは階層ツリー メニューのプライマリ LAG の下にネスト表示されます。ただし、スイッチド LAG にはスイッチド物理インターフェイスのみを含めることができ、ルーテッド LAG にはルーテッド物理インターフェイスのみを含めることができます。

LAG を設定する際は、以下の要件を考慮してください。

- Firepower システムは、最大 14 の LAG をサポートし、各 LAG インターフェイスに 0 ～ 13 の一意の ID を割り当てます。LAG ID は設定できません。
- リンクの両側に LAG を設定し、どちらの側のインターフェイスも同じ速度に設定する必要があります。
- 各 LAG ごとに少なくとも 2 つの物理インターフェイスを関連付ける必要があります（最大 8 つ）。物理インターフェイスは複数の LAG に属することはできません。

- LAG の物理インターフェイスは、他の動作モードでインラインまたはパッシブとして使用できず、タグ付きトラフィックの別の論理インターフェイスの一部として使用することもできません。
- LAG の物理インターフェイスは複数の NetMods にまたがることが可能ですが、複数のセンサーにまたがることはできません（すべての物理インターフェイスが同じデバイス上に存在する必要があります）。
- LAG にはスタック構成の NetMod を含めることができません。

スイッチド インターフェイスの集約

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、スイッチド LAG インターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチド LAG 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。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

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。

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

ルーテッド インターフェイスの集約

7000 または 8000 シリーズ デバイスの 2 ～ 8 つの物理ポートを組み合わせて、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

ルーテッド LAG インターフェイスにスタティック Address Resolution Protocol（ARP）エントリを追加できます。外部ホストは、トラフィックの送信先となるローカル ネットワーク上の宛先 IP アドレスの MAC アドレスを知る必要がある場合は、ARP 要求を送信します。スタティック ARP エントリを設定する場合、仮想ルータは IP アドレスや関連付けられた MAC アドレスに応答します。

ルーテッド LAG インターフェイスの [ICMP 対応の応答数（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。引き続き、アクセス コントロール ルールを使用して、宛先 IP がルーテッド インターフェイスの IP であり、プロトコルが ICMP である接続を処理することができます。ポートおよび ICMP コードの条件を参照してください。

[ローカル ルータ トラフィックを検査する（Inspect Local Router Traffic）] オプションを有効にすると、パケットはホストに到達する前にドロップされるため、あらゆる応答が抑制されます。ローカル ルータ トラフィックの検査の詳細については、デバイスの詳細設定を参照してください。

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。

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

論理集約インターフェイス

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理スイッチドインターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理 LAG 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。物理スイッチドまたはルーテッドインターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。

（注） LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lag*n.0*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。動作させるには、各 LAG にこの論理インターフェイスが少なくとも 1 つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLAN タグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。Firepower System は 1 ～ 4094 の VLAN タグをサポートします。

論理ルーテッド インターフェイスには、シスコ冗長プロトコル（SFRP）を設定することもできます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。

論理ルーテッド LAG インターフェイスの [ICMP 有効応答（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。宛先 IP がルーテッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの詳細設定である [ローカル ルータ トラフィックの検閲（Inspect Local Router Traffic）] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。

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。

関連トピック

SFRP
デバイスの詳細設定
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

ロード バランシング アルゴリズム

LAG バンドルのメンバー リンクへのトラフィックの分散方法を決定する出口ロード バランシング アルゴリズムを LAG に割り当てます。ロード バランシング アルゴリズムは、レイヤ 2 MAC アドレス、レイヤ 3 IP アドレス、レイヤ 4 ポート番号（TCP/UDP トラフィック）など、さまざまなパケット フィールドの値に基づいてハッシュを決定します。選択したロード バランシング アルゴリズムは、LAG バンドルのメンバー リンクすべてに適用されます。

LAG を設定する場合は、次のオプションから展開シナリオに対応するロード バランシング アルゴリズムを選択します。

- 宛先 IP（Destination IP）
- [宛先 MAC（Destination MAC）]
- [接続先ポート（Destination Port）]

- ソース IP
- [送信元 MAC（Source MAC）]
- 送信元ポート
- [送信元/宛先 IP（Source and Destination IP）]
- [送信元/宛先 MAC（Source and Destination MAC）]
- [送信元/宛先ポート（Source and Destination Port）]

（注） LAG の両端に同じロード バランシング アルゴリズムを設定する必要があります。必要に応じて、上位層のアルゴリズムが下位層のアルゴリズムにバックオフされます（例：ICMP トラフィックに対してレイヤ 3 にバックオフされるレイヤ 4 アルゴリズムなど）。

リンク セレクション ポリシー

リンク アグリゲーションでは、両方のエンドポイントで各リンクの速度とメディアが同じである必要があります。リンク プロパティを動的に変更できるので、リンク選択ポリシーは、システムによるリンク選択プロセスの管理方法を決定する上で役立ちます。最大ポート数を最大化するリンク選択ポリシーはリンク冗長性をサポートし、総帯域幅を最大化するリンク選択ポリシーを全体的なリンク速度をサポートします。安定したリンク選択ポリシーは、リンク状態の過剰な変更を最小限に抑えようとします。

（注） LAG の両端に同じリンク選択ポリシーを設定する必要があります。

次のオプションから展開シナリオに対応するリンク選択ポリシーを選択します。

- [最大ポート数（Highest Port Count）]：冗長性を向上させる最大アクティブ ポート数を割り当てるには、このオプションを選択します。
- [最大合計帯域幅（Highest Total Bandwidth）]：集約リンクに最大合計帯域幅を割り当てるには、このオプションを選択します。
- [安定（Stable）]：最大の課題がリンクの安定性と信頼性である場合は、このオプションを選択します。LAG を設定すると、アクティブ リンクは、ポート数や帯域幅が追加された場合ではなく、どうしても必要な場合（リンク障害などの場合）にのみ変更されます。
- [LACP 優先順位（LACP Priority）]：LAG でアクティブにするリンクを LACP アルゴリズムにより決定するには、このオプションを選択します。この設定は、展開目標が未定義の場合や、LAG の一端のデバイスが Firepower Management Center によって管理されていない場合に適しています。

LACPは、動的リンクアグリゲーションをサポートするリンク選択方式の自動化における主要部分です。LACP を有効にすると、LACP の優先度に基づいたリンク選択ポリシーは LACP の次のプロパティを使用します。

LACP システム プライオリティ

リンクアグリゲーションにおいて優位なデバイスを判断するには、LACPを実行している各パートナー デバイスにこの値を設定します。値が小さいシステムほど、システム プライオリティが高くなります。動的リンクアグリゲーションでは、最初に、LACPシステム優先順位の高いシステム側でメンバー リンクに選択された状態が設定され、次に、優先順位の低いシステムでメンバー リンクが適宜設定されます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトの優先順位は 32768 になります。

LACP リンク優先順位。

集約グループに属する各リンクにこの値を設定します。リンク優先順位によって、LAG におけるアクティブ リンクとスタンバイ リンクが決まります。値が小さいリンクほど優先順位が高くなります。アクティブ リンクがダウンすると、最も優先順位の高いスタンバイ リンクが選択され、ダウンしたリンクと交換されます。ただし、複数のリンクのLACP リンク優先順位が同じである場合は、物理ポート番号が最も小さいリンクがスタンバイ リンクとして選択されます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトの優先順位は 32768 になります。

リンク集約制御プロトコル（LACP）

IEEE 802.3ad のコンポーネントであるリンク集約制御プロトコル（LACP）は、LAG バンドルを作成して維持するためにシステムおよびポートの情報を交換する 1 つの方式です。LACP を有効にすると、LAG の両端の各デバイスは LACP を使用して、集約においてアクティブに使用されているリンクを特定します。LACP は、リンク間で LACP パケット（または制御メッセージ）を交換することによって、アベイラビリティと冗長性を実現します。このプロトコルは、リンクの能力を動的に学習し、他のポートに通知します。LACP は、適合するリンクを特定すると、それらのリンクを LAG にグループ化します。あるリンクで障害が発生した場合、トラフィックは他のリンクで継続されます。リンクを機能させるには、LAG の両端で LACP を有効にする必要があります。

LACP

LACPを有効にする場合は、LAGの両端で転送モードを指定して、ペアになったデバイス間での LACP パケットの交換方法を指定する必要があります。LACP モードには次の 2 つのオプションがあります。

- [アクティブ（Active）] : デバイスをアクティブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスはLACPパケットを送信することにより、リモート リンクとのネゴシエーションを開始します。

- [パッシブ（Passive）]：デバイスをパッシブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスは受信したLACPパケットには応答しますが、LACP ネゴシエーションを開始しません。

（注） どちらのモードでも、LACP はリンク間でネゴシエートして、それらのリンクがポート速度などの基準に基づいてリンク バンドルを形成可能かどうかを判定できます。ただし、パッシブ対パッシブの構成は避けるようにしてください。そのような構成では、基本的に LAG の両端がリスニング モードになります。

LACPには、デバイス間でのLACPパケットの送信頻度を定義するタイマーがあります。LACPは次のレートでパケットを交換します。

- [低速（Slow）]：30 秒
- [高速（Fast）]：1 秒

このオプションが適用されたデバイスは、LAG の反対側のパートナー デバイスからこの頻度で LACP パケットを受信することを予期します。

（注） LAG がデバイス スタック内の管理対象デバイスに設定されている場合は、プライマリ デバイスだけがパートナー システムとのLACP通信に参加します。すべてのセカンダリ デバイスは、LACP メッセージをプライマリ デバイスに転送します。プライマリ デバイスは、動的な LAG の変更をセカンダリ デバイスにリレーします。

集約スイッチド 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

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、スイッチド LAG インターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチド LAG 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。管理対象デバイスは、最大14の LAG インターフェイスをサポートできます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 スイッチドLAG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 [追加（Add）] ドロップダウン メニューから [集約インターフェイスの追加（Add Aggregate Interface）] を選択します。

ステップ 4 [スイッチド（Switched）] をクリックして、スイッチドLAGインターフェイスのオプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、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）] をクリック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 仮想スイッチを指定します。

- [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 を参照してください。

ステップ 7 [有効（Enabled）] チェックボックスをオンにして、スイッチド LAG インターフェイスがトラフィックを処理できるようにします。

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、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）] 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 [Autonegotiation] 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。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブ リンクが選択されます。

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 Auto-MDIX のいずれかを指定するオプションを選択します。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチング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）を入力します。

設定可能な MTU の範囲は、Firepower System のデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲を参照してください。

ステップ 11 [リンク アグリゲーション（Link Aggregation）] で、LAG バンドルに追加する物理インターフェイスを [使用できるインターフェイス（Available Interfaces）] から 1 つまたは複数選択します。

ヒント LAG バンドルから物理インターフェイスを削除するには、1 つ以上の物理インターフェイスを選択して、選択項目の削除アイコン（  ）をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン（  ）をクリックします。[インターフェイス（Interfaces）] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

ステップ 12 [ロードバランシング アルゴリズム（Load-Balancing Algorithm）] ドロップダウン リストからオプションを選択します。

ステップ 13 ドロップダウンリストから [リンク選択ポリシー（Link Selection Policy）] を選択します。

ヒント Firepower System デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP 優先（LACP Priority）] を選択します。

ステップ 14 [リンク選択ポリシー（Link Selection Policy）] に [LACP 優先（LACP Priority）] を選択した場合は、[システム優先度（System Priority）] に値を割り当て、[インターフェイスの優先度の設定（Configure Interface Priority）] リンクをクリックして優先度の値を LAG の各インターフェイスに割り当てます。

ステップ 15 [トンネルレベル（Tunnel Level）] ドロップダウン リストから [内部（Inner）] または [外部（Outer）] を選択します。

（注） レイヤ 3 ロード バランシングが設定されている場合、トンネル レベルは IPv 4 トラフィックにのみ適用されます。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[トンネル レベル（Tunnel Level）] が明示的に設定されていない場合、デフォルトは [外部（Outer）] になります。

ステップ 16 [LACP] で [有効（Enabled）] チェックボックスをオンにして、スイッチド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。

このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、Firepower System は選択されたすべての物理インターフェイスを集約に使用します。

ステップ 17 [レート（Rate）] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[遅い（Slow）] をクリックします。
- パケットを 1 秒ごとに受信するには、[速い（Fast）] をクリックします。

ステップ 18 [モード（Mode）] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモート リンクとのネゴシエーションを開始するには、[アクティブ（Active）] をクリックします。

- 受信した LACP パケットに応答するには、[パッシブ（Passive）] をクリックします。

ステップ 19 [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。設定変更の導入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

集約ルーテッド 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

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中に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トラフィックの処理方法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。 でのルーテッド インターフェイス ペアの追加

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 ルーテッドLAG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 [追加（Add）] ドロップダウン メニューから [集約インターフェイスの追加（Add Aggregate Interface）] を選択します。

ステップ 4 [Routed] をクリックして、ルーテッド LAG インターフェイス オプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、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 仮想ルータを指定します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して新しい仮想ルータ 仮想ルータの追加を追加します。

ステップ 7 [有効（Enabled）] チェックボックスをオンにして、ルーテッド LAG インターフェイスがトラフィックを処理できるようにします。

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、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 [Autonegotiation] 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 LAG 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。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブ リンクが選択されます。

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 Auto-MDIX のいずれかを指定するオプションを選択します。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチング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 LAG インターフェイスが ping や traceroute のような ICMP トラフィックに応答できるようにするには、[ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにします。

ステップ 12 LAG インターフェイスがルータアドバタイズメントをブロードキャストできるようにするには、[IPv6 NDP] の横にある [ルータアドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにします。

ステップ 13 [追加（Add）] をクリックして、IP アドレスを追加します。

ステップ 14 [アドレス（Address）] フィールドで、CIDR 表記を使用して、ルーテッド LAG インターフェイスの IP アドレスとサブネット マスクを入力します。

次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 IPv6 を使用した環境で、LAG インターフェイスの IP アドレスを自動設定するには、[IPv6] フィールドの横にある [アドレスの自動設定（Address Autoconfiguration）] チェックボックスをオンにします。

ステップ 16 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

ステップ 17 [タイプ（Type）] に SFRP を選択した場合は、SFRPの説明に従いオプションを設定してください。

ステップ 18 [OK] をクリックします。

（注） IP アドレスを 7000 または 8000 シリーズ デバイスの高可用性ペアのルーテッド インターフェイスに追加する場合、高可用性ピアのルーテッドインターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 19 [追加（Add）] をクリックして、スタティック ARP エントリを追加します。

ステップ 20 [IP アドレス（IP Address）] フィールドに IP アドレスを入力します。

ステップ 21 [MAC アドレス（MAC Address）] フィールドに IP アドレスに関連付ける MAC アドレスを入力します。標準形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 22 [OK] をクリックします。

ステップ 23 [リンク アグリゲーション（Link Aggregation）] で、LAG バンドルに追加する物理インターフェイスを [使用できるインターフェイス（Available Interfaces）] から 1 つまたは複数選択します。

ヒント LAG バンドルから物理インターフェイスを削除するには、1 つ以上の物理インターフェイスを選択して、選択項目の削除アイコン（  ）をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン（  ）をクリックします。[インターフェイス（Interfaces）] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

ステップ 24 ドロップダウンリストから [ロードバランシング アルゴリズム（Load-Balancing Algorithm）] を選択します。

ステップ 25 ドロップダウンリストから [リンク選択ポリシー（Link Selection Policy）] を選択します。

ヒント Firepower System デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP 優先（LACP Priority）] を選択します。

ステップ 26 [リンク選択ポリシー（Link Selection Policy）] に [LACP 優先（LACP Priority）] を選択した場合は、[システム優先度（System Priority）] に値を割り当て、[インターフェイスの優先度の設定（Configure Interface Priority）] リンクをクリックして優先度の値を LAG の各インターフェイスに割り当てます。

ステップ 27 [トンネルレベル（Tunnel Level）] ドロップダウン リストから [内部（Inner）] または [外部（Outer）] を選択します。

（注） レイヤ 3 ロード バランシングが設定されている場合、トンネル レベルは IPv 4 トラフィックにのみ適用されます。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[トンネル レベル（Tunnel Level）] が明示的に設定されていない場合、デフォルトは [外部（Outer）] になります。

ステップ 28 [LACP] で [有効（Enabled）] チェックボックスをオンにして、ルーテッド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。

このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、Firepower System はすべての物理インターフェイスを集約に使用します。

ステップ 29 [レート（Rate）] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[遅い（Slow）] をクリックします。
- パケットを 1 秒ごとに受信するには、[速い（Fast）] をクリックします。

ステップ 30 [モード（Mode）] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモート リンクとのネゴシエーションを開始するには、[アクティブ（Active）] をクリックします。
- 受信した LACP パケットに応答するには、[パッシブ（Passive）] をクリックします。

ステップ 31 [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。設定変更の導入を参照してください。

関連トピック

デバイスの詳細設定

論理集約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

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理インターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理 LAG 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。物理スイッチドまたはルーテッドインターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。

（注） LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lag*n.0*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。動作させるには、各 LAG にこの論理インターフェイスが少なくとも 1 つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLAN タグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。Firepower System は 1 ～ 4094 の VLAN タグをサポートします。

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中に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トラフィックの処理方法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。 でのルーテッド インターフェイス ペアの追加

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 論理 LAG 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）]をクリックしてスイッチドインターフェイス オプションを表示するか、[ルーテッド（Routed）] をクリックしてルーテッド インターフェイス オプションを表示します。

ステップ 5 [インターフェイス（Interface）] ドロップダウン リストから使用可能な LAG を選択します。集約インターフェイスは **lag*n*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。

ステップ 6 選択したインターフェイスのタイプに適した残りの設定を行います。

- スイッチド：スイッチドインターフェイスへの論理インターフェイスの追加方法の詳細については、論理スイッチドインターフェイスの追加を参照してください。
- ルーテッド：ルーテッドインターフェイスへの論理インターフェイスの追加方法の詳細については、論理ルーテッドインターフェイスの追加を参照してください。

関連トピック

SFRP
デバイスの詳細設定
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

集約インターフェイス統計情報の表示

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

各集約インターフェイスのプロトコルおよびトラフィックの統計情報を表示できます。統計情報には、LACP キーとパートナー情報などの LACP プロトコル情報、受信パケット、転送パケット、ドロップ パケットが表示されます。統計情報は、メンバー インターフェイスごとに詳細化されており、ポート単位でトラフィックとリンクの情報が表示されます。

集約インターフェイス情報は、事前定義されたウィジェットを介してダッシュボードにも表示されます。[現在のインターフェイス ステータス（Current Interface Status）] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Interface Traffic ウィジェットには、ダッシュボードの時間範囲においてアプライアンスのインターフェイスで送受信された受信（Rx）トラフィックと送信（Tx）トラフィックの割合が示されます。定義済みダッシュボード ウィジェットを参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 論理集約インターフェイス統計情報を表示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 インターフェイス統計情報を表示するインターフェイスの横にある、表示アイコン（）をクリックします。

集約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

集約インターフェイスは **lag*n*** ラベルによって識別できます（***n*** は 0 ～ 13 の整数）。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 集約インターフェイスを削除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 削除する集約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 プロンプトが表示されたら、集約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。設定変更の導入を参照してください。