



集約インターフェイスのセットアップ

シリーズ 3 管理対象デバイスが、ネットワーク間にパケット スイッチングを提供するレイヤ 2 展開、またはインターフェイス間にトラフィックをルーティングするレイヤ 3 展開に設定されている場合、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の 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リンク集約グループ (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、2 つの FirePOWER 管理対象デバイス (上記の図を参照)、またはサードパーティ製アクセス スイッチまたはルータに接続されている 1 つの FirePOWER 管理対象デバイスです。2 つのデバイスは一致している必要はありませんが、同じ物理構成を備え、IEEE 802.ad リンク集約標準をサポートしている必要があります。LAG の一般的な展開は、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。

仮想管理対象デバイス、Cisco ASA with FirePOWER Services デバイス、Blue Coat X-Series 向け Cisco NGIPS デバイスには集約インターフェイスを設定できないので注意してください。

集約インターフェイスの設定方法については、[LAG の設定 \(8-2 ページ\)](#) を参照してください。

LAG の設定

ライセンス:Control

サポートされるデバイス:シリーズ 3

集約インターフェイスには2つのタイプがあります。スイッチドはレイヤ2集約インターフェイス、ルーテッドはレイヤ3集約インターフェイスです。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と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適用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 [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。

- FireSIGHT 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 にまたがることは可能ですが、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 を含めることはできません。



(注)

リンク集約はデバイス クラスタではサポートされません。

詳細については、次の各項を参照してください。

- [ロード バランシング アルゴリズムの指定 \(8-3 ページ\)](#)
- [リンク選択ポリシーの指定 \(8-3 ページ\)](#)
- [LACP の設定 \(8-4 ページ\)](#)
- [集約スイッチドインターフェイスの追加 \(8-5 ページ\)](#)
- [集約ルーテッドインターフェイスの追加 \(8-8 ページ\)](#)

- [論理集約インターフェイスの追加 \(8-12 ページ\)](#)
- [集約インターフェイス統計情報の表示 \(8-14 ページ\)](#)
- [集約インターフェイスの削除 \(8-14 ページ\)](#)

ロード バランシング アルゴリズムの指定

ライセンス:Control

サポートされるデバイス:シリーズ 3

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
- 接続先ポート
- ソース IP
- 送信元 MAC
- 送信元ポート
- 送信元および宛先 IP
- 送信元および宛先 MAC
- 送信元および宛先ポート



(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 選択 ポリシーの指定

ライセンス:Control

サポートされるデバイス:シリーズ 3

リンク集約では、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 ポリシーは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ています。



(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。

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 優先度 (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 以外のデバイスである場合に適しています。

LACP が有効な場合、LACP 優先度に基づくリンク選択ポリシーでは、以下の 2 つの LACP 優先度(システム プライオリティとリンク プライオリティ)が使用されます。

- LACP システム プライオリティ。リンク集約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。動的リンク集約では、最初に、LACP システム プライオリティ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、プライオリティ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、デフォルトのプライオリティは 32768 になります。
- LACP リンク プライオリティ。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 プライオリティによって、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プライオリティが高くなります。アクティブ リンクがダウンすると、最もプライオリティの高いスタンバイ 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 プライオリティ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、デフォルトのプライオリティは 32768 になります。

LACP は、動的リンク集約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。詳細については、[LACP の設定\(8-4 ページ\)](#)を参照してください。

LACP の設定

ライセンス:Control

サポートされるデバイス:シリーズ 3

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 を有効にする場合は、LAG の両端で転送モードを選択して、デバイスの間での 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。

- [遅い (Slow)]: 30 秒
- [速い (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

ライセンス: Control

サポートされるデバイス: シリーズ 3

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。



注意

センシング インターフェイスまたはインラインセットの MTU の任意の値 (シリーズ 2) または最高値 (シリーズ 3) を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インスペクションが一時的に中断されます。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インターフェイスのタイプに応じて異なります。[Snort の再開によるトラフィックへの影響 \(1-9 ページ\)](#) を参照してください。

既存のスイッチド LAG 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 (鉛筆) をクリックします。

スイッチド LAG インターフェイスの設定方法:

アクセス: Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 スwitch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。
[インターフェイス (Interfaces)] タブが表示されます。
- 手順 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。
- 手順 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。
- 手順 5 オプションで、[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 ゾーンを選択するか、または [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。
- 手順 6 [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するか、[新規 (New)] を選択して新しい仮想スイッチを追加します。



(注) 新しい仮想スイッチを追加する場合は、スイッチド インターフェイスをセットアップした後に、[デバイス管理 (Device Management)] ページの [仮想スイッチ (Virtual Switches)] タブ ([デバイス (Devices)] > [デバイス管理 (Device Management)] > [仮想スイッチ (Virtual Switches)]) でそのスイッチを設定する必要があります。[仮想スイッチの追加 \(6-7 ページ\)](#) を参照してください。

- 手順 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。
- 手順 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 (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。モード設定は銅インターフェイスでのみ使用可能であることに注意してください。



(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。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。

- 手順 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専用であることに注意してください。

デフォルトでは、MDI/MDIX は Auto-MDIX 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。

- 手順 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。
- 設定可能な MTU の範囲は、FireSIGHT システムのデバイス 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、[管理対象デバイスの MTU の範囲 \(4-70 ページ\)](#) を参照してください。
- 手順 11** [リンク アグリゲーション (Link Aggregation)] には、LAG バンドルに追加する物理インターフェイスを選択するための 2 つのオプションがあります。
- [使用可能なインターフェイス (Available Interfaces)] の横で、1 つ以上のインターフェイスを選択し、選択項目の追加アイコン (➡) をクリックします。複数の物理インターフェイスを選択するには、**Ctrl** キーまたは **Shift** キーを使用します。
 - すべてのインターフェイス ペアを LAG バンドルに追加するには、すべてを追加アイコン (➡) をクリックします。



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。

- 手順 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、展開シナリオに対応するオプションを選択します。詳細については、[ロード バランシング アルゴリズムの指定 \(8-3 ページ\)](#) を参照してください。
- 手順 13** [リンク 選択ポリシー (Link Selection Policy)] ドロップダウン リストから、展開シナリオに対応する次のオプションを選択します。[最大ポート数 (Highest Port Count)] (冗長性)、[最大合計帯域幅 (Highest Total Bandwidth)] (速度)、[安定 (Stable)] (過剰な変更を避けて、リンク ステートを維持)、または [LACP 優先度 (LACP Priority)] (自動リンク集約)。
- [LACP 優先度 (LACP Priority)] を選択する場合は、[システム優先度 (System Priority)] の値を割り当てる必要があります。次に、[インターフェイス優先度の設定 (Configure Interface Priority)] リンクをクリックして、LAG の各インターフェイスにプライオリティ値を割り当てます。0 ~ 65535 を指定できます。値を指定しない場合、デフォルトのプライオリティは 32768 になります。詳細については、[リンク 選択ポリシーの指定 \(8-3 ページ\)](#) を参照してください。



(注) FireSIGHT システム 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 優先度 (LACP Priority)] を選択します。

- 手順 14** [トンネル レベル (Tunnel Level)] ドロップダウン リストから、展開シナリオに対応するオプション ([内部 (Inner)] または [外部 (Outer)]) を選択します。
- 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るので注意してください。外部トンネルは常に、レイヤ 2 と IPv 6 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。
- 手順 15** [LACP (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。詳細については、[LACP の設定 \(8-4 ページ\)](#) を参照してください。
- 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、FireSIGHT システム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。

- 手順 16 [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)] を選択します。
 - パケットを 1 秒ごとに受信するには、[速い (Fast)] を選択します。
- 手順 17 [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)] を選択します。
 - 受信した LACP パケットに応答するには、[パッシブ (Passive)] を選択します。
- 手順 18 [保存 (Save)] をクリックします。

スイッチド LAG インターフェイスが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは [デバイスへの変更の適用 \(4-27 ページ\)](#) を参照してください)。

集約ルーテッド インターフェイスの追加

ライセンス:Control

サポートされるデバイス:シリーズ 3

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

シリーズ 3 デバイスにルーテッド インターフェイス ペアを追加すると、変更の適用時に Snort プロセスが再起動され、トラフィック インспекションは一時的に中断されます。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 の再開によるトラフィックへの影響 \(1-9 ページ\)](#) を参照してください。

ルーテッド LAG インターフェイスに Address Resolution Protocol (ARP) スタティック エントリを追加できます。外部ホストがトラフィックを送信する、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、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と、仮想ルータは IP アドレスおよび関連付けられている MAC アドレスで応答します。

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 ポリシーにルールを追加できます。[ネットワークベースのルールによるトラフィックの制御 \(15-1 ページ\)](#) を参照してください。

管理対象デバイスの [ローカルルータ トラフィックの検査 (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。ローカルルータ トラフィックの検査の詳細については、[高度なデバイス設定について \(4-59 ページ\)](#) を参照してください。

**注意**

センシング インターフェイスまたはインラインセットの MTU の任意の値(シリーズ 2)または最高値(シリーズ 3)を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インスペクションが一時的に中断されます。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インターフェイスのタイプに応じて異なります。[Snort の再開によるトラフィックへの影響\(1-9 ページ\)](#)を参照してください。

既存のルーテッド LAG 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。

ルーテッド LAG インターフェイスの設定方法:

アクセス: Admin/Network Admin

- 手順 1 [デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。
[デバイス管理(Device Management)] ページが表示されます。
- 手順 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。
デバイスの [インターフェイス(Interfaces)] タブが表示されます。
- 手順 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。
- 手順 4 [ルーテッド(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。
- 手順 5 オプションで、[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するか、または [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。
- 手順 6 [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するか、または [新規(New)] を選択して新しい仮想ルータを追加します。

**(注)**

新しい仮想ルータを追加する場合は、ルーテッド インターフェイスをセットアップした後に、[デバイス管理(Device Management)] ページの [仮想ルータ(Virtual Routers)] タブ([デバイス(Devices)] > [デバイス管理(Device Management)] > [仮想ルータ(Virtual Routers)]) でそのルータを設定する必要があります。[仮想ルータの追加\(7-11 ページ\)](#)を参照してください。

- 手順 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。
- 手順 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(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。モード設定は銅インターフェイスでのみ使用可能であることに注意してください。



(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。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。

手順 9 [MDI/MDIX (MDI/MDIX)] ドロップダウン リストから、LAG 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専用であることに注意してください。

通常、[MDI/MDIX] は [Auto-MDIX] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

手順 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 はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではないことに注意してください。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス 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、[管理対象デバイスの MTU の範囲 \(4-70 ページ\)](#) を参照してください。

手順 11 [ICMP (ICMP)] の横にある [応答の有効化 (Enable Responses)] チェック ボックスをオンにして、LAG インターフェイスが ping や traceroute などの ICMP トラフィックに応答できるようにします。

手順 12 [IPv6 NDP (IPv6 NDP)] の横にある [ルータ アドバタイズメントの有効化 (Enable Router Advertisement)] チェック ボックスをオンにして、LAG インターフェイスがルータ アドバタイズメントを送信できるようにします。

手順 13 IP アドレスを追加するには、[追加 (Add)] をクリックします。

[IP アドレスの追加 (Add IP Address)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 15 (任意) 組織で IPv6 アドレスを使用している場合は、[IPv6 (IPv6)] フィールドの横にある [アドレス自動設定 (Address Autoconfiguration)] チェック ボックスをオンにすると、LAG インターフェイスの IP アドレスが自動的に設定されます。

手順 16 [種類 (Type)] には、[ノーマル (Normal)] または [SFRP] を選択します。

SFRP オプションの詳細については [SFRP の設定 \(7-9 ページ\)](#) を参照してください。

手順 17 [OK] をクリックします。

IP アドレスが追加されます。

IP アドレスを編集するには、編集アイコン () をクリックします。IP アドレスを削除するには、削除アイコン () をクリックします。



(注) IP アドレスをクラスタ デバイスのルーテッド インターフェイスに追加する場合、クラスタ 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。

- 手順 18 スタティック ARP エントリを追加するには、[追加(Add)] をクリックします。
[スタティック ARP エントリの追加(Add Static ARP Entry)] ポップアップ ウィンドウが表示されます。
- 手順 19 [IP アドレス (IP Address)] フィールドに、スタティック ARP エントリの IP アドレスを入力します。
- 手順 20 [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。2 桁の 16 進数の 6 個のグループをコロンで区切る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)。
- 手順 21 [OK] をクリックします。
スタティック ARP エントリが追加されます。



ヒント スタティック ARP エントリを編集するには、編集アイコン(✎)をクリックします。スタティック ARP エントリを削除するには、削除アイコン(🗑)をクリックします。

- 手順 22 [リンク アグリゲーション(Link Aggregation)] には、LAG バンドルに追加する物理インターフェイスを選択するための 2 つのオプションがあります。
- [使用可能なインターフェイス (Available Interfaces)] の横で、1 つ以上のインターフェイスを選択し、選択項目の追加アイコン(➡)をクリックします。複数の物理インターフェイスを選択するには、**Ctrl** キーまたは **Shift** キーを使用します。
 - すべてのインターフェイス ペアを LAG バンドルに追加するには、すべてを追加アイコン(➡)をクリックします。



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。

- 手順 23 [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、展開シナリオに対応するオプションを選択します。詳細については、[ロードバランシング アルゴリズムの指定 \(8-3 ページ\)](#) を参照してください。
- 手順 24 [リンク選択ポリシー (Link Selection Policy)] ドロップダウン リストから、展開シナリオに対応する次のオプションを選択します。[最大ポート数 (Highest Port Count)] (冗長性)、[最大合計帯域幅 (Highest Total Bandwidth)] (速度)、[安定 (Stable)] (過剰な変更を避けて、リンク ステートを維持)、または [LACP 優先度 (LACP Priority)] (自動リンク集約)。
- [LACP 優先度 (LACP Priority)] を選択する場合は、[システム優先度 (System Priority)] の値を割り当てる必要があります。次に、[インターフェイス優先度の設定 (Configure Interface Priority)] リンクをクリックして、LAG の各インターフェイスにプライオリティ値を割り当てます。0 ~ 65535 を指定できます。値を指定しない場合、デフォルトのプライオリティは 32768 になります。詳細については、[リンク選択ポリシーの指定 \(8-3 ページ\)](#) を参照してください。



(注) FireSIGHT システム 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 優先度 (LACP Priority)] を選択します。

- 手順 25 [トンネル レベル(Tunnel Level)] ドロップダウン リストから、展開シナリオに対応するオプション([内部(Inner)] または [外部(Outer)]) を選択します。
- 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 IPv4 トラフィックにのみ適用されるので注意してください。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。
- 手順 26 [LACP(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。詳細については、[LACP の設定 \(8-4 ページ\)](#) を参照してください。
- 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、FireSIGHT システム はすべての物理インターフェイスを集約に使用します。
- 手順 27 [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)] を選択します。
 - パケットを 1 秒ごとに受信するには、[速い(Fast)] を選択します。
- 手順 28 [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)] を選択します。
 - 受信した LACP パケットに応答するには、[パッシブ(Passive)] を選択します。
- 手順 29 [保存(Save)] をクリックします。
- ルーテッド LAG インターフェイスが設定されます。デバイス設定を適用するまで、変更は有効になりません。[デバイスへの変更の適用 \(4-27 ページ\)](#) を参照してください。

論理集約インターフェイスの追加

ライセンス:Control

サポートされるデバイス:シリーズ 3

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 つが必要です。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。FireSIGHT システムは 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、SFRP を設定することもできます。詳細については、[SFRP の設定 \(7-9 ページ\)](#) を参照してください。

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ルールを追加できます。[ネットワークベースのルールによるトラフィックの制御\(15-1 ページ\)](#)を参照してください。

管理対象デバイスの[ローカルルータトラフィックの検査(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。ローカルルータトラフィックの検査の詳細については、[高度なデバイス設定について\(4-59 ページ\)](#)を参照してください。



注意

センシングインターフェイスまたはインラインセットのMTUの任意の値(シリーズ2)または最高値(シリーズ3)を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシングインターフェイスに対する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。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インターフェイスのタイプに応じて異なります。[Snortの再開によるトラフィックへの影響\(1-9 ページ\)](#)を参照してください。

既存の論理LAG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LAGインターフェイスの追加方法:

アクセス:Admin/Network Admin

-
- 手順 1** [デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。
[デバイス管理(Device Management)] ページが表示されます。
- 手順 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。
[インターフェイス(Interfaces)] タブが表示されます。
- 手順 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。
[インターフェイスの追加(Add Interface)] ポップアップウィンドウが表示されます。
- 手順 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。
LAGの論理インターフェイスを作成するときは、[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 **lagn** ラベルによって識別されます(n は 0 ~ 13 の整数)。
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については、[論理スイッチドインターフェイスの追加\(6-4 ページ\)](#)を参照してください。
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については、[論理ルーテッドインターフェイスの追加\(7-5 ページ\)](#)を参照してください。



(注)

集約インターフェイスを無効化すると、集約インターフェイスに関連付けられる論理インターフェイスも無効になります。

集約インターフェイス統計情報の表示

ライセンス:Control

サポートされるデバイス:シリーズ 3

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。事前定義されたウィジェットについて(55-8 ページ)を参照してください。

集約インターフェイス統計情報の表示方法:

アクセス:Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
 - 手順 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。
デバイスの [インターフェイス (Interfaces)] タブが表示されます。
 - 手順 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。
[統計情報 (Statistics)] ポップアップ ウィンドウが表示されます。
 - 手順 4 [OK] をクリックしてウィンドウを閉じます。
-

集約インターフェイスの削除

ライセンス:Control

サポートされるデバイス:シリーズ 3

以下の手順は、集約インターフェイスの削除方法を示しています。

集約インターフェイスの削除方法:

アクセス:Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
 - 手順 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。
デバイスの [インターフェイス (Interfaces)] タブが表示されます。

- 手順 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。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 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。インターフェイスが削除されます。デバイス設定を適用するまで、変更は有効になりません。[デバイスへの変更の適用\(4-27 ページ\)](#)を参照してください。
-

