CHAPTER 4

インライン ポスチャの設定

この章では、インライン ポスチャ ノードをスタンドアロン モードで、またはハイ アベイラビリティ ペアとして設定する方法を説明します。この項では、次のトピックを扱います。

Cisco ISE 展開におけるインライン ポスチャ ノードの役割

インライン ポスチャ ノードは、アクセス ポリシーを適用し、許可変更（CoA）リクエストを処理するゲートキーパーです。インライン ポスチャ ノードは、ワイヤレス LAN コントローラ（WLCs）や VPN デバイスなど、CoA 要求を処理できないネットワーク上のネットワーク アクセス デバイスの背後に配置されます。

EAP/802.1x と RADIUS プロトコルを使用したクライアントの初期認証の後に、クライアントはポスチャ評価を受ける必要があります。ポスチャ評価プロセスによって、クライアントからネットワークへのアクセスを制限するか、拒否するか、フル アクセスを許可するかが決定されます。クライアントが WLC または VPN デバイスを経由してネットワークにアクセスする場合、インライン ポスチャ ノードは、これらのデバイスが対応できないポリシー適用と CoA に対応します。

インライン ポスチャによるポリシー適用

インライン ポスチャは、コントロール プレーンの RADIUS プロキシと URL リダイレクトの機能を使用してエンドポイントのデータ プレーン トラフィックを管理します。RADIUS プロキシとしてのインライン ポスチャは、ネットワーク アクセス デバイス（NAD）と RADIUS サーバとの間の RADIUS セッションに介入することができます。NAD は、クライアント トラフィックをすべて通過させることができます。ただし、インライン ポスチャは、クライアントからの限定的なトラフィックのみを通過させます。このように帯域幅が制限されていると、クライアントでのエージェントのプロビジョニン

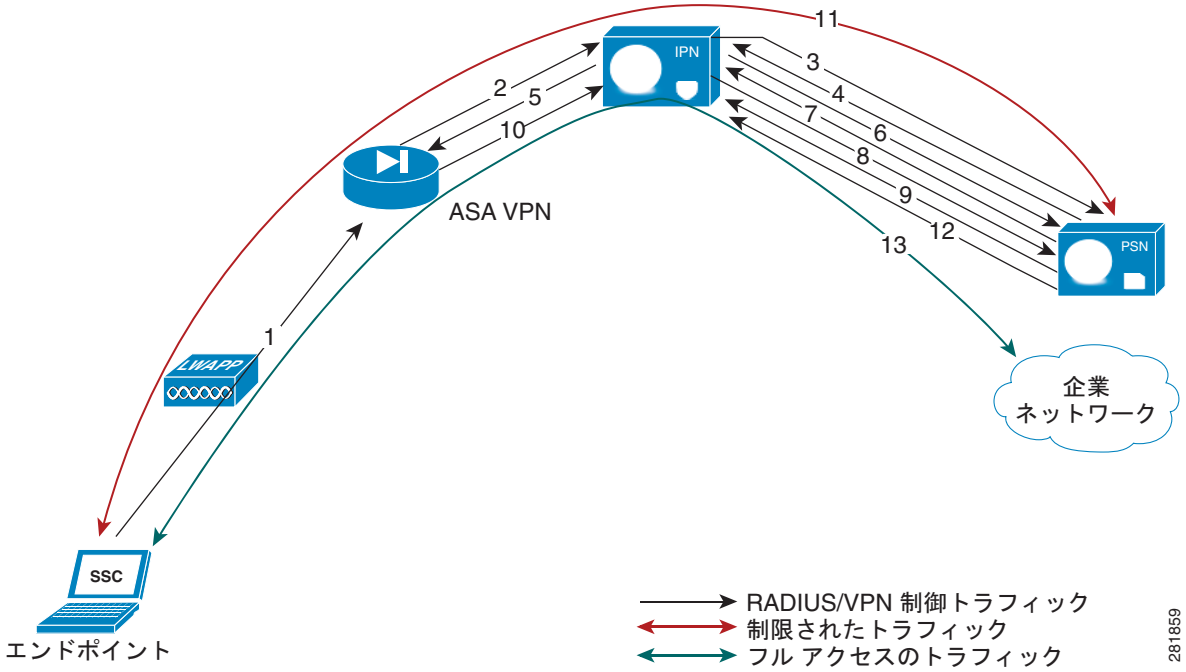
グ、ポスチャ評価、および修復完了が可能になります。このような制限を行うには、個々のクライアント フローに合わせて調整されたダウンロード可能なアクセス コントロール リスト（ACL）をダウンロードしてインストールします。

クライアントが準拠している場合は、CoA がポリシー サービス ノードからインライン ポスチャ ノードに送信され、インライン ポスチャ ノードは、準拠しているクライアント エンドポイントのすべてのトラフィックを通過させます。RADIUS プロキシによってフル アクセス DACL がダウンロードされてインストールされ、クライアント IP アドレスが関連付けられます。インストールされた DACL は、多数のユーザ グループの間で共通とすることもできるので、DACL の内容が Cisco ISE サーバ側で変更されることがなければ、何度もダウンロードする必要はありません。

インライン ポスチャ ポリシー適用のフロー

図 4-1 では、インライン ポスチャ ポリシー適用プロセスが図示され、ポリシー サービス ノードへのトラフィックに対する WLC 適用のフローが示されています。アクセスのステップは、VPN ゲートウェイがある場合のインライン展開でも同様です。

図 4-1　　インライン ポスチャ ポリシー適用のフロー



1. エンドポイントがワイヤレス ネットワークへの .1X 接続を開始します。
2. WLC（これは NAD です）が、RADIUS Access-Request メッセージを RADIUS サーバ（通常はポリシー サービス ノード）に送信します（この図では、RADIUS Access-Request メッセージはインライン ポスチャ ノードに送信されています）。
3. RADIUS プロキシとして機能するインライン ポスチャ ノードが、Access-Request メッセージを RADIUS サーバにリレーします。
4. ユーザの認証後に、RADIUS サーバは RADIUS Access-Accept メッセージをインライン ポスチャ ノードに返送します。

Access-Accept メッセージが送信される前に、エンドポイント、WLC、インライン ポスチャ ノード、および Cisco ISE RADIUS サーバの間で、多数の RADIUS トランザクションが発生することがあります。この例で説明するプロセスは、簡潔にするために、ある程度省略しています。

5. インライン ポスチャ ノードは、Access-Accept メッセージを WLC に渡し、これを受けて WLC は、メッセージに付随しているプロファイルに従ってエンドポイントにアクセスを許可します。
6. プロキシされた Access-Accept メッセージがトリガーとなり、インライン ポスチャ ノードが Authorization-Only リクエストをポリシー サービス ノードに送信し、セッションのプロファイルを取得します。
7. ポリシー サービス ノードから Access-Accept メッセージが、必要なインライン ポスチャ ノード プロファイルとともに返されます。
8. プロファイルで定義されているアクセス コントロール リスト（ACL）がまだインライン ポスチャ ノード上にない場合、インライン ポスチャ ノードは（Cisco ISE RADIUS サーバへの）RADIUS リクエストを使用してポリシー サービス ノードからダウンロードします。
9. Cisco ISE RADIUS サーバは、応答として完全な ACL を送信します。これがインライン ポスチャ データ プレーンにインストールされ、エンドポイント トラフィックが通過できるようになります。

   完全な ACL がダウンロードされる前、特に、ACL が大きすぎて 1 つのトランザクションでは送信できない場合は、多数のトランザクションが発生することがあります。
10. エンドポイント トラフィックが WLC に到着すると、WLC はセッションの RADIUS Accounting-Start メッセージをインライン ポスチャ ノードに送信します。

    エンドポイントからの実際のデータ トラフィックがインライン ポスチャ ノードの非信頼側に到着した時点では、まだインライン ポスチャ ノードが Accounting-Start メッセージを受信していないことがあります。RADIUS Accounting-Start メッセージを受信すると、インライン ポスチャ ノードはそのセッションに関与するエンドポイントの IP アドレスを学習し、このセッションですでにダウンロードおよびインストールされた ACL をエンドポイントに関連付けます。このクライアント エンドポイントの初期プロファイルではアクセスを制限しておき、クライアントにフル アクセス権を付与する前にポスチャを確認できます。
11. この制限的な ACL で許可されるのが Cisco ISE サーバへのアクセスのみであるとすると、エンドポイントに許可されるアクションは、たとえばエージェントのダウンロードやデータ プレーン上でのポスチャ評価のみとなります。
12. クライアント エンドポイントがポスチャ準拠である（Cisco ISE のサービスとのこれまでの制限的な通信の一部として）場合は、ポリシー サービス ノードによって、新しいプロファイルでの RADIUS（CoA）が開始されます。したがって、インライン ポスチャ ノードでは、新しい ACL がそのセッションに適用されます。新しい ACL は即座にインストールされて、エンドポイント トラフィックに適用されます。
13. これで、エンドポイントは企業ネットワークへのフル アクセスが可能となります。これは、インライン ポスチャ ノードに新しいプロファイルが適用された結果です。

    特定のセッションに対する RADIUS stop メッセージが WLC から発行されると、対応するエンドポイント アクセスがインライン ポスチャ ノードにおいてリセットされます。

例に示したような展開においては、ワイヤレス ネットワークに追加のエンドポイントが接続されるときに、これらのエンドポイントは多くの場合、認証と許可が完了してネットワークに接続しているユーザが属している ID グループの 1 つに分類されます。

たとえば、従業員、役員、ゲスト ユーザのそれぞれに、これまでに説明したステップを通してアクセス権が付与されているとします。この状況では、これらの ID グループのそれぞれに対応する限定的またはフル アクセスのプロファイルが、すでにインライン ポスチャ ノードにインストールされています。それ以降のエンドポイントの認証と許可では、インライン ポスチャ ノードに存在するインストー

ル済みプロファイルが使用されます。ただし、元のプロファイルが Cisco ISE ポリシー設定中に変更された場合を除きます。後者のケースでは、変更済みのプロファイルと ACL がダウンロードされてインライン ポスチャ ノードにインストールされ、前のバージョンが置き換えられます。

信頼 / 非信頼インターフェイス

次の用語は、インライン ポスチャ展開において重要な役割を果たします。

- 信頼 : Cisco ISE ネットワークの*内側にある*ポリシー サービス ノードやその他の信頼できるデバイスと通信するインターフェイス。信頼インターフェイスの名前は常に Eth0 インターフェイスとなります。
- 非信頼 : Cisco ISE ネットワークの*外側にある* WLC、VPN、その他のデバイスと通信するインターフェイス。非信頼インターフェイスの名前は常に Eth1 インターフェイスとなります。

インライン ポスチャに必要な専用ノード

他のペルソナとは異なり、インライン ポスチャはノードを他のサービスと共有できません。ノードを共有できないため、インライン ポスチャは、ネットワーク上のプライマリ管理ノードに専用ノードとして登録されていることが必要になります。

Cisco ISE では、ハイ アベイラビリティを実現するために、最大 2 つのインライン ポスチャ ノードをアクティブ / スタンバイ ペアとして設定できます。

Cisco ISE 分散展開の詳細については、第 3 章「分散環境での Cisco ISE の設定」を参照してください。

Cisco ISE 展開におけるスタンドアロン インライン ポスチャ ノード

スタンドアロンのインライン ポスチャ ノードとは、単独でサービスを実行するインライン ポスチャ ノードであり、他のすべてのノードからは独立して動作します。単一のスタンドアロン インライン ポスチャ ノードの展開を選択するのは、たとえばネットワークが小規模であり、冗長性が大きな問題にならない場合です。

図 4-2 は単純なインライン ポスチャ スタンドアロン設定であり、クライアントのアクセスは WLC や VPN のデバイスを通過します。

インライン ポスチャのハイ アベイラビリティ

インライン ポスチャのハイ アベイラビリティ展開は、1 つのアクティブ / スタンバイ ペアとして設定された 2 つのインライン ポスチャ ノードから成ります。アクティブ ノードが RADIUS プロキシとして機能し、すべてのネットワーク パケットを転送します。このノードで障害が発生すると、スタンバイ ノードがその処理を引き継ぎます。アクティブ ノードが正しく機能している間は、スタンバイ ノードはパッシブのままです。ただし、アクティブ ノードに問題が生じた場合は、スタンバイ ノードがインライン ポスチャ機能の実行を引き継ぎます。

「プライマリ」と「セカンダリ」という用語の意味は、インライン ポスチャのハイ アベイラビリティに関する場合と Cisco ISE ノード関連の場合とで異なります。インライン ポスチャのハイ アベイラビリティの場合、プライマリとセカンダリは、アクティブ状態を引き継ぐデバイスと、競合が発生した場合（たとえば、両方のノードが同時に起動したとき）にスタンバイの役割を担うデバイスを指します。アクティブとスタンバイという用語は、ハイ アベイラビリティの状態を表します。プライマリまたはセ

カンダリのインライン ポスチャ ノードは、アクティブとスタンバイのどちらの状態にもなることができます。セカンダリのインライン ポスチャ ノードは読み取り専用であり、どのような種類の設定にも（ハイ アベイラビリティであっても）使用することはできません。

インライン ポスチャのハイ アベイラビリティ ペアを設定する場合、プライマリ ノードに編集できる多くのオプションがあります。設定の変更はすべて、プライマリ ノードで行われるからです。プライマリ ノードに対して行われた設定変更は自動的に、セカンダリ ノードに反映されます。このような理由から、セカンダリ ノードは読み取り専用となっています。

図 4-4 はルーテッド モードのハイ アベイラビリティ インライン ポスチャ設定を示しています。

インライン ポスチャのハイ アベイラビリティ ペアは、1 つのクラスタとして構成される、2 つの物理的インライン ポスチャ ノードから成ります。これらのノードは、eth2 と eth3 インターフェイスの間にハートビート リンクが存在し、専用ケーブルで接続されています。

両ノードの eth2 および eth3 インターフェイスは、ハートビート プロトコル交換を使用して通信することによって、ノードの健全性を特定します。各インライン ポスチャ ノードの、信頼と非信頼のイーサネット インターフェイスそれぞれに専用の物理 IP アドレスがありますが、それとは別のサービス IP アドレスをクラスタ全体に割り当てる必要があります。

（注） サービス IP アドレス（仮想 IP アドレスと呼ばれることもあります）は、RADIUS 認証に必要になります。サービス IP アドレスは、アクティブ/スタンバイ ペアの両ノードの、信頼と非信頼の両方のインターフェイスに割り当てます。したがって、サービス IP アドレスがクラスタのアドレスとなり、このクラスタをネットワークの他の部分に対して、1 つのエンティティとして表すことができます。

インライン ポスチャ ノードでの自動フェールオーバー

インライン ポスチャのステートレス ハイ アベイラビリティ展開には、1 つのアクティブ/スタンバイ ペア ノード設定があります。スタンバイ ノードはバックアップ ユニットとして機能し、インターフェイス間のパケット転送は行いません。ステートレスとは、アクティブ ノードにより認証および許可されたセッションがフェールオーバーの発生後に再び自動的に許可されることを意味します。

スタンバイ ノードは、ハートビート プロトコルを使用してアクティブ ノードをモニタリングします（eth2 と eth3 のインターフェイスを使用）。このプロトコルは、2 つのノード間でメッセージが一定の間隔で送信されることを必要とします。ハートビートが停止するか、割り当てられた時間内に応答がない場合は、フェールオーバーが発生し、復元アクションが実行されます。

ハートビートとは、インライン ポスチャのハイ アベイラビリティ ペアの一方のノードから他方のノードに、一定の間隔で送信されるメッセージです。ハートビートが受信されない状態が長時間にわたる場合（通常はハートビート間隔の数個分）は、ハートビートを送信しているはずのノードで障害が発生したと見なされます。障害が発生したのがプライマリのインライン ポスチャ ノードの場合は、セカンダリ ノードに引き継がれるので、サービスの中断は発生しません。

ハートビートが両方のインライン ポスチャのハイ アベイラビリティ ノードで同時に停止した場合は、その結果としてパーティショニング状態となることがあります。パーティショニング状態とは、両方のノードが他方を完全に停止しているものと見なし、両方がアクティブ コントロールを引き継ごうとしている状態です。

ハートビートのモニタリングに加えて、リンク検証メカニズムを使用することもできます（使用することを強く推奨します）。このメカニズムが使用されているときは、インライン ポスチャの信頼と非信頼のインターフェイスそれぞれが、外部 IP アドレスに対して ping を実行します。両方のノードが外部 IP アドレスに対して ping を実行できない場合は、フェールオーバーが発生します。ただし、ノードの一方が到達不可能になった場合は、機能している方のノードが自動的にアクティブ ノードになります。

フェールオーバーが発生した場合、次の処理が行われます。

1. スタンバイのインライン ポスチャ ノードが、サービス IP アドレスを引き継ぎます。

2. 障害が発生したノードを管理者が修復し、必要に応じて以前の設定に戻します。

   障害が発生したノードがオンラインに戻ったら、手動同期操作を実行してノードに最新の情報を反映する必要があります。インライン ポスチャ ノードの同期操作を実行する方法については、「インライン ポスチャのノードの同期」（P.4-19）を参照してください。

3. アクティブ セッションは自動的に再認証および許可されます。

インライン ポスチャ動作モード

どのインライン ポスチャ動作モードを選択するかは、主に既存のネットワークのアーキテクチャによって決まります。Cisco ISE は次の動作モードをサポートします。

- 「インライン ポスチャ ルーテッド モード」（P.4-6）
- 「インライン ポスチャ ブリッジ モード」（P.4-7）
- 「インライン ポスチャ メンテナンス モード」（P.4-8）

インライン ポスチャ ルーテッド モード

インライン ポスチャ ルーテッド モードは、レイヤ 3 の「hop in the wire」として動作し、選択的にパケットを指定のアドレスに転送します。このモードを使用すると、ネットワーク トラフィックを分離できるので、選択した宛先アドレスに対するアクセス権を持つユーザを指定できるようになります。

ルーテッド モードでは、インライン ポスチャ ノードはレイヤ 3 ルータとして動作し、非信頼ネットワークとその管理対象クライアントのデフォルト ゲートウェイとして機能します。非信頼ネットワークと信頼ネットワーク間のすべてのトラフィックは、インライン ポスチャ ノードを通過します。インライン ポスチャ ノードは、IP フィルタリング ルール、アクセス ポリシー、および設定されたその他のトラフィック処理メカニズムを適用します。

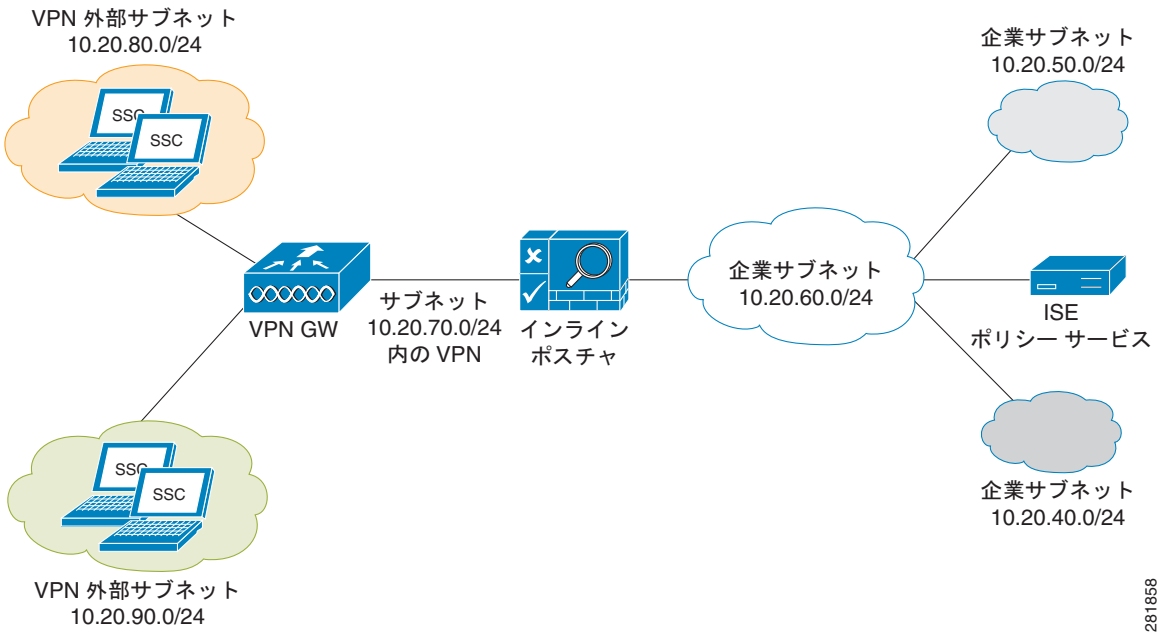
インライン ポスチャをルーテッド モードで設定する場合は、次の 2 つのインターフェイスの IP アドレスを指定する必要があります。

- 信頼できる（Eth0）
- 信頼できない（Eth1）

信頼できるアドレスと信頼できないアドレスは、異なるサブネットに属する必要があります。インライン ポスチャは、1 つまたは複数のサブネットを管理でき、非信頼インターフェイスは管理対象サブネットのゲートウェイとして機能します。

図 4-2 に、インライン ポスチャ ルーテッド モードの設定を示します。この例では、インライン ポスチャは VPN ゲートウェイ（GW）からポリシー サービス ノードに向かうクライアント トラフィックのホップの 1 つです。他のルータと同様に、インライン ポスチャも、サブネット 10.20.80.0/24 および 10.20.90.0/24 に対して、VPN ゲートウェイへのスタティック ルートが設定済みであることを必要とします。ネットワークの信頼側にある企業ルータも、同じサブネットに対して、インライン ポスチャ ノードへのスタティック ルートが設定済みであることを必要とします。

図 4-2　インライン ポスチャ ルーテッド モードの構成



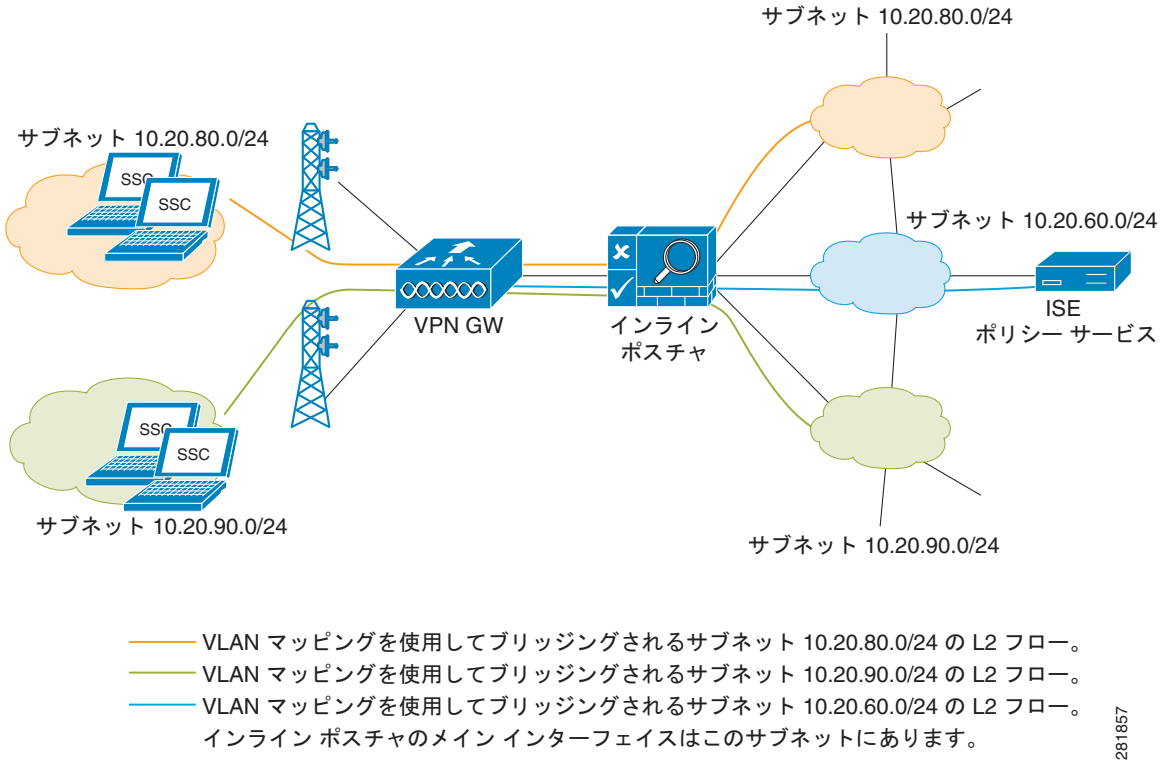
インライン ポスチャ ブリッジ モード

インライン ポスチャ ブリッジ モードは、レイヤ 2 の「bump in the wire」として動作し、パケットを宛先アドレスにかかわらず転送します。

ブリッジ モードでは、インライン ポスチャ ノードは標準のイーサネット ブリッジとして動作します。通常、この設定は、非信頼ネットワーク内にゲートウェイがすでに配置されていて、既存の設定を変更したくない場合に使用します。

図 4-3 に、WLC から Cisco ISE ネットワーク（ポリシー サービス ノードによって管理される）へのレイヤ 2 クライアント トラフィックに対してブリッジとして動作するインライン ポスチャ ノードを示します。この設定では、インライン ポスチャは、アドレス解決プロトコル（ARP）ブロードキャストに応答し、ARP ブロードキャストを適切な VLAN に送信できる、サブネット 10.20.80.0/24 と 10.20.90.0/24 に対応するサブネット エントリを必要とします。

図 4-3　インライン ポスチャ ブリッジ モードの設定



インライン ポスチャ ノードがブリッジ モードのときは、次のことが当てはまります。

- インライン ポスチャ eth0 と eth1 インターフェイスの IP アドレスを同一にすることができます
- ブリッジド サブネットのすべてのエンド デバイスは、非信頼ネットワーク上に配置する必要があります。

インライン ポスチャ メンテナンス モード

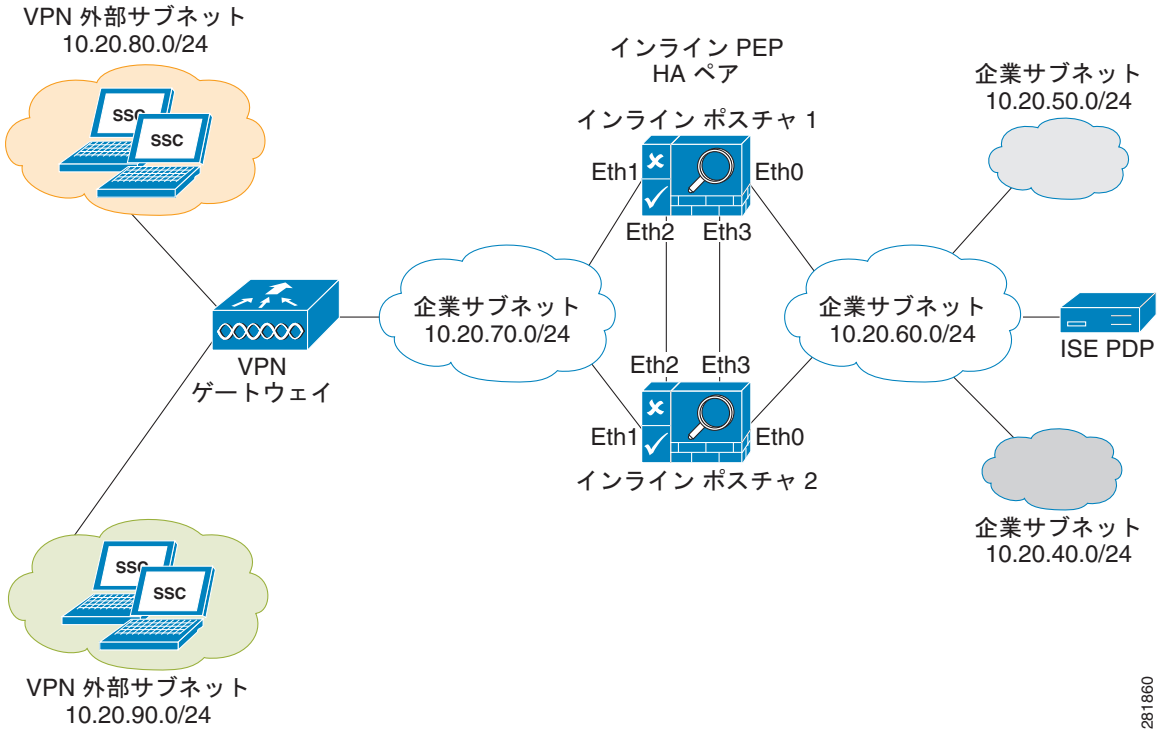
インライン ポスチャ メンテナンス モードでは、ノードがオフラインになるので、管理手順を実行できます。このモードは、ノードが初めてネットワークに接続され、他の設定がまだ行われていないときのデフォルト モードでもあります。

ルーテッド モードとブリッジ モードでのインライン ポスチャのハイ アベイラビリティ

図 4-4 に、インライン ポスチャのハイ アベイラビリティのルーテッド モード設定の例を示します。2 つのノードの eth2 と eth3 のインターフェイスを接続する専用ケーブルは、アクティブ ノードの障害の有無を調べるハートビート通信のためのものです。

この例では、インライン ポスチャ 1 の非信頼 IP アドレスを 10.20.70.101 とし、インライン ポスチャ 2 の非信頼 IP アドレスを 10.20.70.102 とします。ただし、ネットワークの非信頼側にある両方のノードのサービス IP アドレスは 10.20.70.100 です。ペアのうち、アクティブ インライン ポスチャ ノードは、どの時点でも、ネットワークの非信頼側のサービス IP アドレスを担当しています。同じことが、ネットワークの信頼側にも当てはまります。

図 4-4　インライン ポスチャのハイ アベイラビリティのルーテッド モード設定



ブリッジ モードでは、インライン ポスチャ eth0 と eth1 インターフェイスの IP アドレスは、同一サブネット内であることが必要です。IP アドレスを同一にすることを推奨します。ネットワークの信頼側にあるデバイスの IP アドレスが属するサブネットが、ブリッジ モードのインライン ポスチャによって管理されている場合は、明示的なスタティック ルートがインライン ポスチャ ノードにおいて設定されている必要があります。この設定が必要になるのは、デフォルトではインライン ポスチャが管理するサブネット（ユーザ インターフェイスの [管理対象サブネット（Managed Subnets）] ページで設定されます）全体がネットワークの非信頼側にあると見なされるからです。

インライン ポスチャ展開のベスト プラクティス

インライン ポスチャ環境を効率的に管理するには、ここでリストされているベスト プラクティスに従います。

- 「アクセス権限を定義するためのフィルタの使用」（P.4-9）
- 「管理対象サブネットおよびスタティック ルートの設定」（P.4-10）
- 「ハイ アベイラビリティ ペアの設定」（P.4-10）

アクセス権限を定義するためのフィルタの使用

インライン ポスチャのフィルタを設定するときは、次のことを考慮してください。

- 一般的な実装では、インライン ポスチャは、ネットワークにアクセスしようとしているエンドポイントに認証要件を適用します。デバイスとサブネットのフィルタは、WLC や VPN のデバイスを許可するか拒否するかを決定するのに使用されます。

- 特定のデバイスでは、認証、ポスチャ評価、ロール割り当てのうち 1 つ以上をバイパスしたい場合があります。バイパスするデバイスのタイプの一般的な例としては、プリンタ、IP Phone、サーバ、非クライアント マシン、ネットワーク デバイスがあります。

  インライン ポスチャによって、MAC アドレス、MAC と IP アドレス、またはサブネット アドレスが照合され、デバイスに対してバイパス機能が有効になっているかどうかが判断されます。管理者は、ポリシー適用をバイパスするか、強制的にアクセスをブロックするかを選択できます。

注意 直接接続された ASA VPN デバイスの MAC アドレスを MAC フィルタで設定するときは、必ず IP アドレスも入力してください。任意の IP アドレスが追加されていない場合は、VPN クライアントがポリシー適用をバイパスできてしまいます。このようにバイパスできるのは、VPN がクライアントにとってはレイヤ 3 のホップであり、デバイスは自身の MAC アドレスを送信元アドレスとして使用して、インライン ポスチャ ノードに向けてパケットをネットワークで送信するからです。

管理対象サブネットおよびスタティック ルートの設定

インライン ポスチャの管理対象サブネットを設定するときは、次のことを考慮してください。

- インライン ポスチャの管理対象サブネットを設定します。管理対象サブネットを設定すると、非信頼インターフェイス上のクライアント デバイスに対する適切な VLAN ID を指定して、インライン ポスチャ ノードからアドレス解決プロトコル（ARP）クエリーを送信できるようになります。非信頼（認証）VLAN を、管理対象サブネットの [VLAN ID] フィールドで設定してください。
- インライン ポスチャ ノードの非信頼インターフェイスにパケットを直接配信する WLC など、エンドポイント用の管理対象サブネットは、インライン ポスチャ ノードに近接するレイヤ 2 で設定します。
- IP アドレスを設定し、サブネット アドレスは設定しないでください。このようにすれば、インライン ポスチャから送信される ARP リクエストの送信元 IP アドレスが正しく設定されます。
- インライン ポスチャ ノードの信頼側のサブネットは、非信頼側のサブネットと異なることを確認します。
- 管理ノード、ポリシー サービス ノード、およびモニタリング ノードがインライン ポスチャ ノードと同一のサブネット上に存在していないことを確認します。ただし、スタティック ルートを定義済みの場合を除きます。

インライン ポスチャのスタティック ルートを設定するときは、次のことを考慮してください。

- インライン ポスチャ ノードからの距離が 1 ホップよりも大きい（レイヤ 3）エンドポイントに対しては、スタティック ルートを設定します。
- VPN アドレス プールによく見られるすべてのダウンストリーム ホスト ネットワークには、スタティック ルートを設定します。

ハイ アベイラビリティ ペアの設定

ハイ アベイラビリティを実現するためにインライン ポスチャを設定するときは、次のことを考慮してください。

- サービス IP アドレス（仮想 IP と呼ばれることもあります）を、インライン ポスチャの両側のインターフェイス、つまり信頼側（eth0）と非信頼側（eth1）のそれぞれに割り当てます。
- リンク検出 IP アドレスを、信頼（eth0）と非信頼（eth1）それぞれのインターフェイスに対して指定します。リンク検出は、任意設定としてユーザ インターフェイスに表示されますが、設定することを強く推奨します。

インライン ポスチャ ノードのガイドライン

分散展開でインライン ポスチャ ノードを設定する前に、次の内容を読んで、理解しておきます。

1. インライン ポスチャは、管理、ポリシー サービス、またはモニタリングのペルソナと同時に実行することはできないため、専用ノードとなります。
2. インライン ポスチャ ノードは、ネットワーク上のプライマリ管理ノードに対するセカンダリ ノードとして登録する必要があります。
3. スタンドアロンのインライン ポスチャ ノードを展開することも、アクティブ/スタンバイ ペアを展開することもできます。
4. ネットワークで一度に最大 2 つのインライン ポスチャ ノードを設定できます。インライン ポスチャのハイ アベイラビリティ アクティブ/スタンバイ ペアの場合は、2 つのノードを設定します。一方のノードがプライマリとして指定され、他方のノードがセカンダリ ノードとして指定されます。両方のノードが同時に稼働された場合は、プライマリ ノードがアクティブ ノードになります。
5. インライン ポスチャ アクティブ/スタンバイ ペア設定の場合は、この機能に関連する設定作業はすべて、ペアのアクティブ ノードから行う必要があります。Cisco ISE ユーザ インターフェイスでは、スタンバイ ノードのユーザ インターフェイスには基本的な設定テーブルのみが表示されます。
6. インライン ポスチャのアクティブ ノード設定をピア スタンバイ ノードに同期させる処理は、アクティブ ノードの [フェールオーバー（Failover）] タブから実行できます。詳細については、「インライン ポスチャのノードの同期」（P.4-19）を参照してください。

（注） WLC 認証、許可、アカウンティング（AAA）サーバ（Cisco 2100 または 4400 シリーズ ワイヤレス LAN コントローラ）がネットワーク上にある場合は、RADIUS 認証サーバのタイムアウト値を 30 秒以上に設定する必要があります。この最小値以上であれば、RADIUS フェールオーバーが、インライン ポスチャと組み合わせたときに確実に動作します。詳細については、WLC サーバ ハードウェアのマニュアルを参照してください。

7. インライン ポスチャ ノードが登録されると、システムが再起動します。ハイ アベイラビリティを変更した場合や、インフラストラクチャ設定、たとえば eth1 IP アドレス、インライン ポスチャ モードを変更した場合も、システム再起動が必要です。再起動は自動的に行われます。ただし、CLI から手動でノードを再起動するには、**application stop ise** コマンドと **application start ise** コマンドを使用してください。
8. インライン ポスチャ ノードを管理ノードに登録した後は、eth0（信頼）IP アドレスを管理者ポータルから変更することはできません。これは、登録済みインライン ポスチャ ノードの eth0 IP アドレスを変更すると、管理ノードと通信できないからです。インライン ポスチャ ノードと管理ノードとの間で通信しようとしても失敗し、その結果、例外が発生する可能性があります。

（注） Cisco ISE ネットワークに登録された後は、CLI からインライン ポスチャ ノードの IP アドレスを変更しないことを強く推奨します。

注意 インライン ポスチャ ノードを設定する時には、インライン ポスチャ ノードの非信頼インターフェイスを切断する必要があります。初期設定中にインライン ポスチャ ノードの信頼および非信頼インターフェイスが同じ VLAN に接続され、ペルソナの変更後にインライン ポスチャ ノードが最初に起動された場合、マルチキャスト パケット トラフィックは非信頼インターフェイスからフラッディングされます。このマルチキャスト ストームにより、同じサブネットまたは VLAN に接続されたデバイスがダウンする可能性があります。この時点でインライン ポスチャ ノードはメンテナンス モードです。

インライン ポスチャ ノードの展開

インライン ポスチャ ノードを展開するための最初のプロセスは、スタンドアロン ノードの場合でも、アクティブ/スタンバイ ペアの場合でも同じです。

（注）　インライン ポスチャは、Cisco ISE 3415、ISE 3315、ISE 3355、および ISE 3395 のプラットフォーム上でサポートされます。

インライン ポスチャ ノードを展開するには、次の作業を実行します。

1. 「インライン ポスチャ ノードの設定」（P.4-12）
2. 「インライン ポスチャのダウンロード可能アクセス コントロール リストの作成」（P.4-15）
3. 「インライン ポスチャ ノード プロファイルの作成」（P.4-16）
4. 「インライン ポスチャ許可ポリシーの作成」（P.4-17）

インライン ポスチャ ノードの設定

インライン ポスチャとは、管理ノードに登録されている専用ノードです。インライン ポスチャの設定は管理コンソールから行い、その設定内容はインライン ポスチャ ノードに複製されます。設定のコピーが、ローカルの管理データベースに保存されます。インライン ポスチャのノードが登録されたら、再起動されます。

インライン ポスチャ ノードを Cisco ISE ネットワークに導入するには、初めにインライン ポスチャ ノードをプライマリ管理ノードに登録し、インライン ポスチャの設定を指定してから、許可プロファイルとポリシーを作成する必要があります。これによって、インライン ポスチャのゲートキーピング ポリシーが確立します。

インライン ポスチャ ノードは RADIUS プロキシであり、RADIUS サーバとして NAD と連携し、これにより NAD（VPN ゲートウェイ、WLC）は RADIUS クライアントとなります。プロキシとしてのインライン ポスチャは、クライアントとしてポリシー サービス ノードと接続し、これにより、ポリシー サービス ノードはインライン ポスチャの RADIUS サーバとなります。

（注）　次に示す手順を完了すると、インライン ポスチャ ノードに対応する NAD エントリが自動的に作成されます。スタンドアロン ノードの場合は、そのノードの IP アドレスが使用されます。ハイ アベイラビリティ ペアの場合は、アクティブ ノードのサービス IP アドレスが使用されます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

インライン ポスチャは、Cisco ISE 3495 プラットフォームではサポートされていません。次のサポート対象プラットフォームのいずれかにインライン ポスチャをインストールすることを確認します。ISE 3315、ISE 3355、ISE 3395、または、ISE 3415。

インライン ポスチャ用の証明書設定のガイドラインに従い、適用します。詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

インライン ポスチャ ノードをプライマリ管理ノードに登録します。Cisco ISE 分散システムのメンバーとして動作するには、すべてのノードがプライマリ管理ノードに登録されている必要があります。

RADIUS 設定は必須です。最低でも 1 つのクライアントと 1 つのサーバ設定が必要です。この手順を完了するには、両側の対応する共有秘密情報が必要です。

インストールに必要なすべての設定情報を手元に用意してください。たとえば、信頼と非信頼の IP アドレス、サービス IP アドレス、他の Cisco ISE ノードの IP アドレス、RADIUS 設定用の共有秘密情報、管理 VLAN ID、WLC、または VPN IP アドレスなどです。必要な情報のリストについては、システム設計者に確認してください。

注意　直接接続された ASA VPN デバイスの MAC アドレスを MAC フィルタで設定するときは、必ず IP アドレスも入力してください。任意の IP アドレスが追加されていない場合は、VPN クライアントがポリシー適用をバイパスできてしまいます。このようにアクセスできるのは、VPN がクライアントにとってはレイヤ 3 のホップであり、デバイスは自身の MAC アドレスを送信元アドレスとして使用して、インライン ポスチャ ノードに向けてパケットをネットワークで送信するからです。

ステップ 1　[管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。

ステップ 2　[展開ノード（Deployment Nodes）] ページの**インライン ポスチャ ノード**のチェックボックスをオンにして [編集（Edit）] をクリックします。

ステップ 3　[全般設定（General Settings）] タブの [インライン PEP（Inline PEP）] チェックボックスをオンにします。[管理（Administration）]、[モニタリング（Monitoring）]、および [ポリシー サービス（Policy Service）] の各チェックボックスは自動的にオフになります。

タブは、[全般設定（General Settings）]、[基本情報（Basic Information）]、[展開モード（Deployment Modes）]、[フィルタ（Filters）]、[RADIUS 設定（Radius Config）]、[管理対象サブネット（Managed Subnets）]、[スタティック ルート（Static Routes）]、[ロギング（Logging）]、および [フェールオーバー（Failover）] に変化します。

（注）　新規登録されたインライン ポスチャ ノードは、デフォルト IP アドレス 192.168.1.100、サブネット マスク 255.255.255.0、およびデフォルト ゲートウェイ 192.168.1.1 が設定されています。これらの値は、実際の展開に合わせてステップ 3 で変更してください。

ステップ 4　次のタブをクリックし、タブのフィールドに対して適切な情報を入力します。フィールドの詳細については、インライン ポスチャ ノードの設定を参照してください。

- 基本情報
- [展開モード（Deployment Modes）] : 新規登録されたインライン ポスチャ ノードは、メンテナンス モードとなっています。実稼働目的の場合は、ルーテッド モードまたはブリッジ モードを選択する必要があります。
- [フィルタ（Filters）] : クライアント デバイスのサブネット アドレスとサブネット マスクを入力するか、フィルタリングするデバイスの MAC アドレスと IP アドレスを入力します。MAC とサブネットのフィルタを使用すると、ネットワークの非信頼側にある特定のエンドポイントやデバイスについて、インライン ポスチャ適用をバイパスすることができます。たとえば、VPN または WLC の管理トラフィックがインライン ポスチャを通過できるようにする必要がある場合に、その NAD を Cisco ISE のポリシー適用対象外とします。その NAD の MAC アドレスと IP アドレスをフィルタで指定しておくと、インライン ポスチャ経由でユーザ インターフェイスや設定ターミナルに、制約なくアクセスできるようになります。
- [RADIUS 設定（RADIUS Config）] : RADIUS 設定は必須です。インライン ポスチャには、最低でも 1 つのクライアントと 1 つのサーバの設定が必要です。
- [管理対象サブネット（Managed Subnets）] : インライン ポスチャ ノードと近接するレイヤ 2 にあるエンドポイントのサブネットについては（たとえば WLC）、管理対象サブネットを設定する必要があります。このように設定するには、管理対象サブネットと同じサブネットにある未使用の

IP アドレスが 1 つとサブネットの VLAN（ある場合）が必要になります。複数の管理対象サブネット エントリを指定できます。次の値を入力する必要があります。IP アドレス、サブネット マスク、VLAN ID、および説明。

- [スタティック ルート（Static Routes）] : サブネット アドレスとサブネット マスクを入力し、[インターフェイス タイプ（Interface Type）] ドロップダウン リストで [信頼（Trusted）] または [非信頼（Untrusted）] を選択します。このステップを、実際の設定に合わせて必要なだけ繰り返します。

  Cisco ISE の制御下にあるエンドポイントのサブネットがインライン ポスチャ ノードからレイヤ 3 分離れている場合は、スタティック ルート エントリが必要です。たとえば、VPN ゲートウェイ デバイス（管理対象サブネット トラフィックをインライン ポスチャ非信頼インターフェイスに送信するデバイス）が 2 ホップ離れている場合は、そのクライアント サブネットに対してはインライン ポスチャのためのスタティック ルートが定義されている必要があります。信頼側のネットワークは、トラフィックをインライン ポスチャ信頼インターフェイスに送信すべきということを認識している必要があります。

- [ロギング（Logging）] : [ロギング（Logging）] タブをクリックし、ロギング サーバ（一般的にはモニタリング ノード）の IP アドレスとポート番号を入力します。

  インライン ポスチャのイベントをログに記録するための IP アドレスとポート（デフォルト 20514）は必須です。この要件が守られていれば、インライン ポスチャ ノードの動作ステータスが Cisco ISE ダッシュボードの [システム概要（System Summary）] ダッシュレットに表示されるようになり、そのノードに関するその他のログ情報も利用できるようになります。

- [フェールオーバー（Failover）] : このタブは、インライン ポスチャのハイ アベイラビリティ設定用です。

ステップ 5　[保存（Save）] をクリックします。インライン ポスチャのノードが自動的に再起動します。

ステップ 6　自動生成されたインライン ポスチャ NAD リスティングを確認するには、[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [デフォルト デバイス（Default Device）] に移動します。

スタンドアロン ノードの場合は、そのノードの IP アドレスが使用されます。ハイ アベイラビリティ ペアの場合は、アクティブ ノードのサービス IP アドレスが使用されます。

次の作業

インライン ポスチャ ノードの展開を完了するには、不明、準拠、非準拠の 3 つの DACL、許可プロファイル、および許可ポリシー ルールを作成する必要があります。

（注）　適切なダウンロード可能アクセス コントロール リスト（DACL）を、対応するプロファイルに関連付けることが重要です。たとえば、不明 DACL には不明許可プロファイルを関連付けます。

関連項目

- 「インライン ポスチャ ノードの設定」（P.A-7）
- 「インライン ポスチャ ノードの登録」（P.3-14）
- 「ハイ アベイラビリティ ペアの設定」（P.4-18）
- 「インライン ポスチャのダウンロード可能アクセス コントロール リストの作成」（P.4-15）
- 「インライン ポスチャ ノード プロファイルの作成」（P.4-16）
- 「インライン ポスチャ許可ポリシーの作成」（P.4-17）

インライン ポスチャのダウンロード可能アクセス コントロール リストの作成

ダウンロード可能アクセス コントロール リスト（DACL）とは、許可プロファイルの構築ブロックであり、プロファイルはこのリストで定められたルールに従うことになります。アクセス コントロール リスト（ACL）は、望ましくないトラフィックがネットワークに入るのを防ぐためのものであり、具体的には送信元と宛先の IP アドレス、トランスポート プロトコル、およびその他の変数を、RADIUS プロトコルを使用してフィルタリングします。

名前付き権限オブジェクトとして作成した DACL を許可プロファイルに追加します。その後、これらの許可プロファイルを許可ポリシーの結果として指定します。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　DACL の名前と説明を入力します。

ステップ 4　次の DACL を作成します。

- ipn-compliant（すべて許可）：次の構文を使用します。permit ip any any。
- ipn-noncompliant（すべて拒否）：次の構文を使用します。deny ip any any。
- ipn-unknown（ポスチャ前）：1 つ以上の ACL を使用して、サプリカントとポリシー サービス ノードに、ポスチャ評価のための相互アクセスを許可します。この DACL を使用すると、認証を通過していないユーザをブロックまたは隔離することができます。次に構文の例を示します。

  deny tcp any any eq 80
  deny tcp any any eq 443
  permit ip any 10.1.2.4 0.0.0.0
  permit udp any any eq 53
  deny ip any any

ステップ 5　DACL を保存します。

次の作業

「インライン ポスチャ ノード プロファイルの作成」（P.4-16）

関連項目

「Cisco ISE 許可プロファイル」（P.20-1）

インライン ポスチャ ノード プロファイルの作成

インライン ポスチャ許可プロファイルを 3 つ作成し、さらに NAD 用の許可プロファイルを 1 つ作成する必要があります。

すべてのインライン ポスチャ インバウンド プロファイルは自動的に、cisco-av-pair=ipep-authz=true に設定されます。これで、インライン ポスチャ ノードによってそのルールが適用されるようになります（プロキシとしてそのまま NAD にプロキシするのではなく）。URL リダイレクトはクライアント プロビジョニングに欠かせないものであり、エージェント検出リダイレクションにも必要です。

はじめる前に

次のタスクを実行するには、スーパー管理者、システム管理者、またはポリシー管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [インライン ポスチャ ノード プロファイル（Inline Posture Node Profiles）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　許可プロファイルの名前および説明を入力します。[名前（name）] フィールドでサポートされる文字は次のとおりです。スペース、!# $ % & ' ( ) * + , - ./ ; = ?@ _ {。

（注）　RADIUS 応答メッセージ = NAD プロファイルと設定すると、*NAD プロファイル*がインライン ポスチャの RADIUS ログ メッセージに表示されるようになります。この設定は、後でトラブルシューティングするときに役立つ可能性があります。

ステップ 4　作成した DACL に対応する、インライン ポスチャの次の許可プロファイルを作成します。次の許可プロファイルのそれぞれについて、適切な DACL を指定します。

- IPN-Unknown-Compliant（ポスチャ前）：このプロファイルには、URL リダイレクトを入力する必要があります。入力するには、[URL リダイレクト（URL Redirect）] チェックボックスをオンにします。

  この URL リダイレクトは、[属性詳細（Attributes Details）] フィールドに表示されます。

  ユーザは、エージェントをダウンロードしてインストールするための Web ページにリダイレクトされます。このエージェントが、ユーザのシステムをスキャンします。システムが合格の場合、ユーザにはフル アクセス権が自動的に付与されます。システムが不合格の場合は、ユーザはアクセスを拒否されます。
- IPN-Compliant（すべて許可）
- IPN-Noncompliant（すべて拒否）

ステップ 5　[送信（Submit）] をクリックします。

次の作業

「インライン ポスチャ許可ポリシーの作成」（P.4-17）

関連項目

- 「Cisoc ISE の許可プロファイル」（P.20-1）
- 「Cisco ISE 許可プロファイル」（P.20-1）

インライン ポスチャ許可ポリシーの作成

許可ポリシーは、ネットワークおよびそのリソースに対するアクセスを制御する手段となります。Cisco ISE では、許可ポリシーを作成するときに多数のルールを定義できるようになっています。

許可ポリシーを定義する要素は、ポリシー ルールを作成するときに参照されます。選択した条件と属性によって、許可プロファイルが定義されます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [許可（Authorization）] を選択します。

ステップ 2　デフォルトのルールはそのまま残します。

ステップ 3　不明ポスチャ ステータス ルールを次のとおりに作成します。

- [ID グループ（Identity Group）] : [任意（Any）]
- [条件（Condition）] : [Session:PostureStatus] [等しい（EQUALS）] = [不明（Unknown）]
- [権限（Permissions）] : IPN-Unknown-Compliant + nad-authorization-profile

ステップ 4　準拠ポスチャ ルールを次のとおりに作成します。

- [ID グループ（Identity Group）] : [任意（Any）]
- [条件（Condition）] : [Session:PostureStatus] [等しい（EQUALS）] = [準拠（Compliant）]
- [権限（Permissions）] : IPN-Compliant + nad-authorization-profile

ステップ 5　非準拠ポスチャ ルールを次のとおりに作成します。

- [ID グループ（Identity Group）] : [任意（Any）]
- [条件（Condition）] : [Session:PostureStatus] [等しい（EQUALS）] = [非準拠（Noncompliant）]
- [権限（Permissions）] : IPN-Noncompliant + nad-authorization-profile

ステップ 6　ポリシーを保存します。インライン ポスチャ ノードの展開は、これで完了です。

次の作業

「管理ノードでの RADIUS クライアントとしてのインライン ポスチャ ノードの設定」（P.4-20）.

関連項目

- 「Cisoc ISE の許可プロファイル」（P.20-1）
- 「Cisco ISE 許可プロファイル」（P.20-1）

ハイ アベイラビリティ ペアの設定

ハイ アベイラビリティのために 2 つのインライン ポスチャ ノードを設定する場合、一方のノードをペアのプライマリ ユニットとして指定し、デフォルトではこのノードがアクティブになります。他方がセカンダリ ノードとなり、デフォルトでスタンバイ ユニットとなります。

ハイ アベイラビリティ ノードのフェールオーバーが発生すると、スタンバイ ノードがサービス IP アドレスを引き継ぎます。このプロセスが発生した後で、管理者は障害が発生したインライン ポスチャ ノードを修復する必要があります。必要に応じて、以前の設定に戻します。ハイ アベイラビリティ フェールオーバーはステートレスであるため、すべてのアクティブ セッションは自動的に、フェールオーバーの発生後に再び許可されます。

ここに示す例では、ブリッジ モードのハイ アベイラビリティ ペアに使用されるサービス IP アドレスは、インライン ポスチャ ノードの物理 IP アドレスとは異なるものであり、実質的にクラスタが作成されます。このクラスタは 1 つのユニットとして、サービス IP アドレスを使用して WLC と相互作用します。このような理由から、サービス IP は信頼と非信頼それぞれのネットワークに対して定義されます。

（注） ハイ アベイラビリティ ペアの両方のノードが、同一のモード（ブリッジまたはルータ）を使用する必要があります。混合モードは、インライン ポスチャのハイ アベイラビリティ ペアではサポートされません。

はじめる前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- インライン ポスチャ ノード 2 つが正常に設定され、Cisco ISE ネットワーク上で登録されている必要があります。
- インライン ポスチャのハイ アベイラビリティ ペア（プライマリとセカンダリ）の両ノードの eth2 および eth3 インターフェイスは、ハートビート プロトコル交換を使用して通信することによって、ノードの健全性を特定します。ハートビートが機能するには、プライマリ インライン ポスチャ ノードの eth2 インターフェイスを、イーサネット ケーブルを使用してセカンダリ ノードの eth2 インターフェイスに接続する必要があります。同様に、プライマリ インライン ポスチャ ノードの eth3 インターフェイスを、イーサネット ケーブルを使用してセカンダリ ノードの eth3 インターフェイスに接続する必要があります。図 4-4 は、この原則を表したものです。
- RADIUS 用に、サービス IP アドレスが必要です。このアドレスは、この手順の中で、インライン ポスチャ アクティブ / スタンバイ クラスタの信頼と非信頼の両方のインターフェイスに割り当てるためのものです。
- インストールに必要なすべてのネットワーク設定情報を手元に用意してください。必要な情報のリストについては、システム設計者に確認してください。

ステップ 1　[管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。

ステップ 2　プライマリ ノードとして指定するインライン ポスチャ ノードの横のチェックボックスをオンにして [編集（Edit）] をクリックします。

ステップ 3　[全般設定（General Settings）] タブで、ノード名を確認し、[インライン PEP（Inline PEP）] チェックボックスがオンであることを確認してから、[HA 役割（HA Role）] ドロップダウン リストで [アクティブ（Active）] を選択します。

ステップ 4　[フェールオーバー（Failover）] タブをクリックし、[HA 有効（HA Enabled）] チェックボックスをオンにします。

ステップ 5　フィールドに、適切な情報を入力します。

ステップ 6　[保存（Save）] をクリックします。両方のインライン ポスチャ ノードが再起動します。ノードが再び起動したときは、指定された設定に応じて、プライマリおよびセカンダリとして設定された状態になっています。

ステップ 7　ノード ステータスの横にあるチェックボックスをオンにし、[フェールオーバー（Failover）] タブをクリックして、ノード ステータスを確認します。プライマリとセカンダリのインライン ポスチャ ノードが正しく設定されていることを確認します。

次の作業

「管理ノードでの RADIUS クライアントとしてのインライン ポスチャ ノードの設定」（P.4-20）を実行します。

関連項目

- 「インライン ポスチャ ノードの設定」（P.A-7）
- 「インライン ポスチャ ノードの設定」（P.4-12）
- 「インライン ポスチャのノードの同期」（P.4-19）

インライン ポスチャのノードの同期

ハイ アベイラビリティ ペアのノードの 1 つが停止しているときに、ただ 1 つのアクティブなノードに対して設定変更が行われた場合に、停止していたノードが起動したときに新しい設定を自動的に反映するメカニズムはありません。アクティブ ノードでのインライン ポスチャのハイ アベイラビリティ ユーザ インターフェイスにある [ピア ノードを同期（Sync-up Peer Node）] ボタンを使用すると、スタンバイ ノードを、アクティブ ノードからの最新のインライン ポスチャ データベースと手動で同期できます。

はじめる前に

- スーパー管理者またはシステム管理者である必要があります。
- 2 つのインライン ポスチャ ノードを設定する必要があります。
- 2 つのノード間の関係を確立する必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。

ステップ 2　他方のノードを同期させるインライン ポスチャ ノード（通常はアクティブ ノード）の横のチェックボックスをオンにして [編集（Edit）] アイコンをクリックします。

ステップ 3　[フェールオーバー（Failover）] タブをクリックします。このタブのフィールドの説明については、展開設定を参照してください。

ステップ 4　[ピア ノードを同期（Sync Peer Node）] をクリックします。選択したノードからのデータが自動的に、ピア ノードに転送されます。

関連項目

- 「インライン ポスチャ ノードの設定」（P.4-12）
- 「ハイ アベイラビリティ ペアの設定」（P.4-18）

管理ノードでの RADIUS クライアントとしてのインライン ポスチャ ノードの設定

インライン ポスチャ ノードが RADIUS プロキシとして機能するには、RADIUS クライアントとして管理ノードに追加する必要があります。

はじめる前に

- スーパー管理者またはシステム管理者である必要があります。
- Cisco ISE 展開にインライン ポスチャを展開する必要があります。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　[ネットワーク デバイス（Network Devices）] ナビゲーション パネルの [ネットワーク デバイス（Network Devices）] をクリックします。

ステップ 3　デバイスの名前と説明を入力します。

ステップ 4　インライン ポスチャのノードの IP アドレスを入力します。

- スタンドアロン インライン ポスチャ ノードの場合は、信頼インターフェイスの IP アドレスを入力します。
- ハイ アベイラビリティ ペアの場合は、信頼インターフェイスのサービス IP アドレスを入力します。

ステップ 5　必要に応じて [モデル名（Model Name）] と [ソフトウェア バージョン（Software Version）] に入力します。

ステップ 6　[ネットワーク デバイス グループ（Network Device Group）] では、[場所（Location）] と [デバイス タイプ（Device Type）] を必要に応じて指定します。

ステップ 7　[認証設定（Authentication Settings）] チェックボックスをオンにして、RADIUS 共有秘密情報を入力します。

ステップ 8　[保存（Save）] をクリックします。

展開からのインライン ポスチャ ノードの削除

インライン ポスチャ ノードを展開から削除するには、初めにその展開をメンテナンス モードに変更し、次に、ノードを登録解除する必要があります。メンテナンス モードとはニュートラル状態であり、そのノードをスムーズにネットワークに、または展開から移動することができます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。

ステップ 2　展開から削除するインライン ポスチャ ノードの横のチェックボックスをオンにして [編集（Edit）] をクリックします。

ステップ 3　[展開モード（Deployment Modes）] タブをクリックします)。

ステップ 4　[メンテナンス モード（Maintenance Mode）] オプション ボタンをクリックしてから [保存（Save）] をクリックします。

ステップ 5　左側のペインの [展開（Deployment）] をクリックし、展開から削除するインライン ポスチャ ノードの横のチェックボックスをオンにします。

ステップ 6　[登録解除（Deregister）] をクリックします。

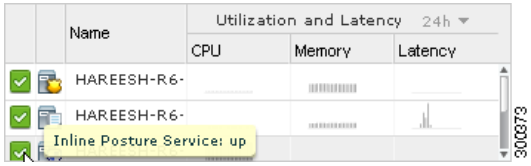
ステップ 7　[OK] をクリックします。

インライン ポスチャのノードの健全性

展開済みのインライン ポスチャ ノードの健全性のモニタリングは、管理ノードで実行されている Cisco ISE ダッシュボードから行うことができます。インライン ポスチャ ノードは、[システム概要（System Summary）] ダッシュレットに表示されます。チェック マーク付きの緑色のアイコンは、システムが正常に動作していることを示します。黄色のアイコンは警告を示し、赤色のアイコンは深刻なシステム障害を示します。スパークラインは、CPU とメモリの使用率および遅延の経時変化を示します。データ表示範囲は、過去 24 時間と過去 60 分から選択できます。

健全性のアイコンにマウス カーソルを合わせると、クイック ビュー ダイアログに、システム健全性の詳細情報が表示されます。

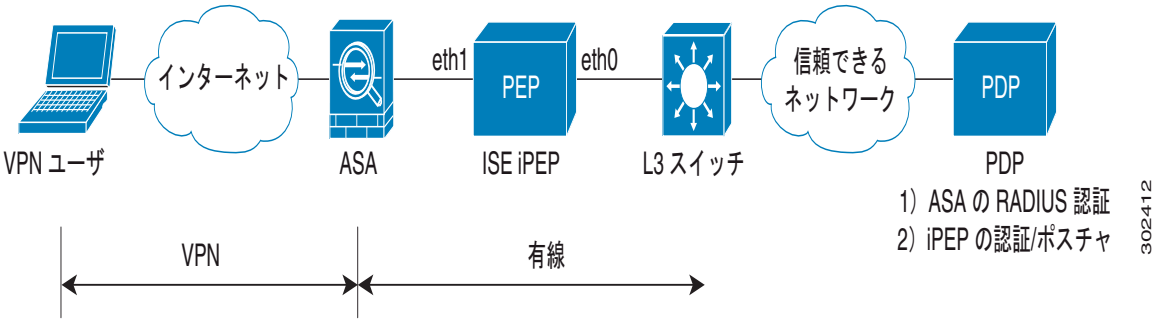
図 4-5　システム概要のステータス クイック ビュー



リモート アクセス VPN の使用例

ここでは、インライン ポスチャ ノードを Cisco ISE ネットワーク内の VPN デバイス（たとえば ASA）とともに使用する方法を説明します。図 4-6 に、インライン ポスチャ ノードをリモート VPN アクセス用に使用する Cisco ISE 展開を示します。この図の iPEP という用語はインライン ポスチャ ノードを指し、PDP はポリシー サービス ノードを指します。VPN ゲートウェイからのトラフィックはすべて、インライン ポスチャ ノードを通過する必要があります。確実に Cisco ISE によってポリシーを適用し、ネットワークのセキュリティを保護するためです。

図 4-6　インライン ポスチャ ノードを使用する Cisco ISE 展開



プロセス フロー

1. リモート ユーザは VPN ゲートウェイ（ASA）に対する認証を、RADIUS プロトコルを使用して行います。
2. RADIUS クライアントである ASA は、認証リクエストを AAA サーバ（インライン ポスチャ ノード）に送信します。
3. RADIUS プロキシであるインライン ポスチャ ノードは、この RADIUS 認証リクエストを、RADIUS サーバの役割を持つ Cisco ISE ノード（ポリシー サービス ノード）にリレーします。
4. Cisco ISE ポリシー サービス ノードは、設定済みの ID ストアを使用してリモート ユーザの認証を行い、RADIUS 応答をインライン ポスチャ ノードに返します。この応答は、ASA（ネットワーク アクセス デバイス（NAD））にリレーされます。
5. ユーザに適用される許可ポリシーに基づいて、ポリシー サービス ノードは該当する属性をインライン ポスチャ ノードに返します。さらに、ASA に返すこともできます。
6. インライン ポスチャ ノード プロファイルと NAD（標準許可プロファイル）のどちらについても、許可ポリシー ルール エントリごとに別の許可プロファイルを参照することができます。
   a. インライン ポスチャ ノード プロファイル：インライン ポスチャ ノードに適用される RADIUS 属性を指定します。たとえば、クライアント プロビジョニング サービスへのリダイレクト用の URL や、インライン ポスチャ ノードによるポリシー適用のためのダウンロード可能なアクセス コントロール リスト（DACL）です。
   b. 標準許可プロファイル：NAD（この例では ASA）のための任意の RADIUS 属性を指定します。
7. 許可ポリシーによる判定の結果、エンドポイントがポスチャ ポリシーに「非準拠」である場合や、ポスチャ ステータスが「不明」の場合は、ポリシー サービス ノードから URL リダイレクト属性値がインライン ポスチャ ノードに返されます。このときに、許可されるトラフィックを指定する DACL も返されます。DACL によって拒否された HTTP/HTTPS トラフィックはすべて、指定の URL にリダイレクトされます。
8. ポスチャが「準拠」になると、再許可が行われてポリシー サービス ノードから新しい DACL がインライン ポスチャ ノードに送信されます。これで、内部ネットワークへのユーザ特権アクセスができるようになります。

関連項目

「VPN デバイスを伴うインライン ポスチャ ノードの設定」（P.4-23）

VPN デバイスを伴うインライン ポスチャ ノードの設定

はじめる前に

インライン ポスチャ ノードやそのダウンストリーム ネットワークとの間で送受信されるトラフィックが正しくルーティングまたはスイッチングされるように、ネットワーク インフラストラクチャが設定されていることを確認します。

ステップ 1　スタンドアロンの Cisco ISE ノードを設定します。詳細については、「Cisco ISE ノードの設定」（P.3-11）を参照してください。

ステップ 2　このスタンドアロン Cisco ISE ノードをインライン ポスチャ ノードとして、既存のプライマリ管理ノードに登録し、インライン ポスチャ ノードの設定をプライマリ管理ノードから行います。詳細については、「インライン ポスチャ ノードの展開」（P.4-12）を参照してください。

ステップ 3　必要に応じて、もう 1 つのインライン ポスチャ ノードを設定し、アクティブ/スタンバイ ペアを設定します。詳細については、「インライン ポスチャのハイ アベイラビリティ」（P.4-4）を参照してください。

ステップ 4　ポリシー サービス ノードがインライン ポスチャ ノードの RADIUS サーバとなるように設定します。インライン ポスチャ ノードで設定されているものと同一の RADIUS 共有秘密を、ポリシー サービス ノードでも設定します。

ステップ 5　インライン ポスチャ ノードによって使用される許可プロファイル（インライン ポスチャ ノード プロファイル）を設定します。

ステップ 6　（任意）NAD に使用するための標準許可プロファイルを設定することもできます。詳細については、「インライン ポスチャ ノード プロファイルの作成」（P.4-16）および「インライン ポスチャのダウンロード可能アクセス コントロール リストの作成」（P.4-15）を参照してください。

ステップ 7　アイデンティティとポスチャ ステータスに基づいてインライン ポスチャ ノード プロファイルをリモート VPN ユーザに適用するための許可ポリシーを設定します。詳細については、「インライン ポスチャ許可ポリシーの作成」（P.4-17）を参照してください。

ステップ 8　VPN ゲートウェイの内部 IP アドレスを RADIUS クライアントとして、インライン ポスチャ ノードの RADIUS 設定に、NAD（この例では ASA）の RADIUS 共有秘密とともに追加します。

ステップ 9　RADIUS サーバとして設定済みのインライン ポスチャ ノードとの間で RADIUS 認証および許可を行うための、VPN ゲートウェイ（ASA）を設定します。手順は次のとおりです。

a.　[ポリシー（Policy）] > [認証（Authentication）] を選択します。

b.　ユーザ レコードに記録されている ID ソースに対してユーザを認証するように、デフォルト ルールが設定されていることを確認します。

c.　[保存（Save）] をクリックします。