CHAPTER 5

エンドツーエンド SSL の設定

この章では、Cisco 4700 シリーズ Application Control Engine（ACE）Appliance を設定して、エンドツーエンド SSL 接続を提供する方法について説明します。このプロセスには、SSL 終了機能（フロントエンド）と SSL 開始機能（バックエンド）を結合して、クライアント、ACE、サーバの間にセキュア リンクを提供する作業が含まれます。これら 3 つのデバイス間では、すべてのデータが暗号化され、暗号文として送信されます。

この章の主な内容は、次のとおりです。

エンドツーエンド SSL の概要

エンドツーエンド SSL とは、接続の一端にあるクライアントと他端にあるサーバの間で、ACE によって SSL 接続を確立および維持することです。ACE にエンドツーエンド SSL を設定すると、ACE は次の機能を実行します。

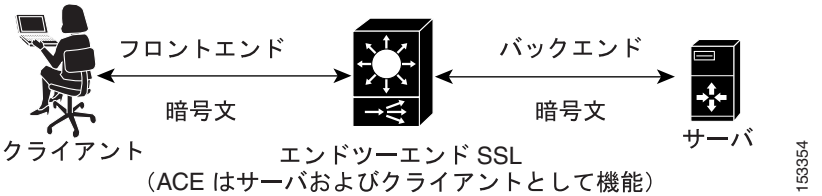
- クライアントとの SSL セッションを終了します（フロントエンド接続）。
- サーバとの SSL セッションを開始します（バックエンド接続）。
- バックエンド コンテンツのロード バランスを行います。

エンドツーエンド SSL は、ACE に SSL 終了機能と SSL 開始機能を設定する際に使用するコンフィギュレーションを結合します。エンドツーエンド SSL では、次のポリシー マップ タイプを作成する必要があります。

- レイヤ 7 ポリシー マップ — ACE とサーバの間のトラフィックのバックエンド フローを指定します。
- レイヤ 3 およびレイヤ 4 ポリシー マップ — 次の機能を実行します。
  - クライアントと ACE の間のトラフィックのフロントエンド フローを指定します。
  - 関連付けられているレイヤ 7 ポリシー マップを、レイヤ 3 およびレイヤ 4 ポリシー マップの基準を満たすトラフィックに適用します。

図 5-1 に、ACE が SSL クライアントとの SSL 接続を終了し、SSL サーバとの SSL 接続を開始するエンドツーエンド SSL アプリケーションを示します。

図 5-1　エンドツーエンド SSL

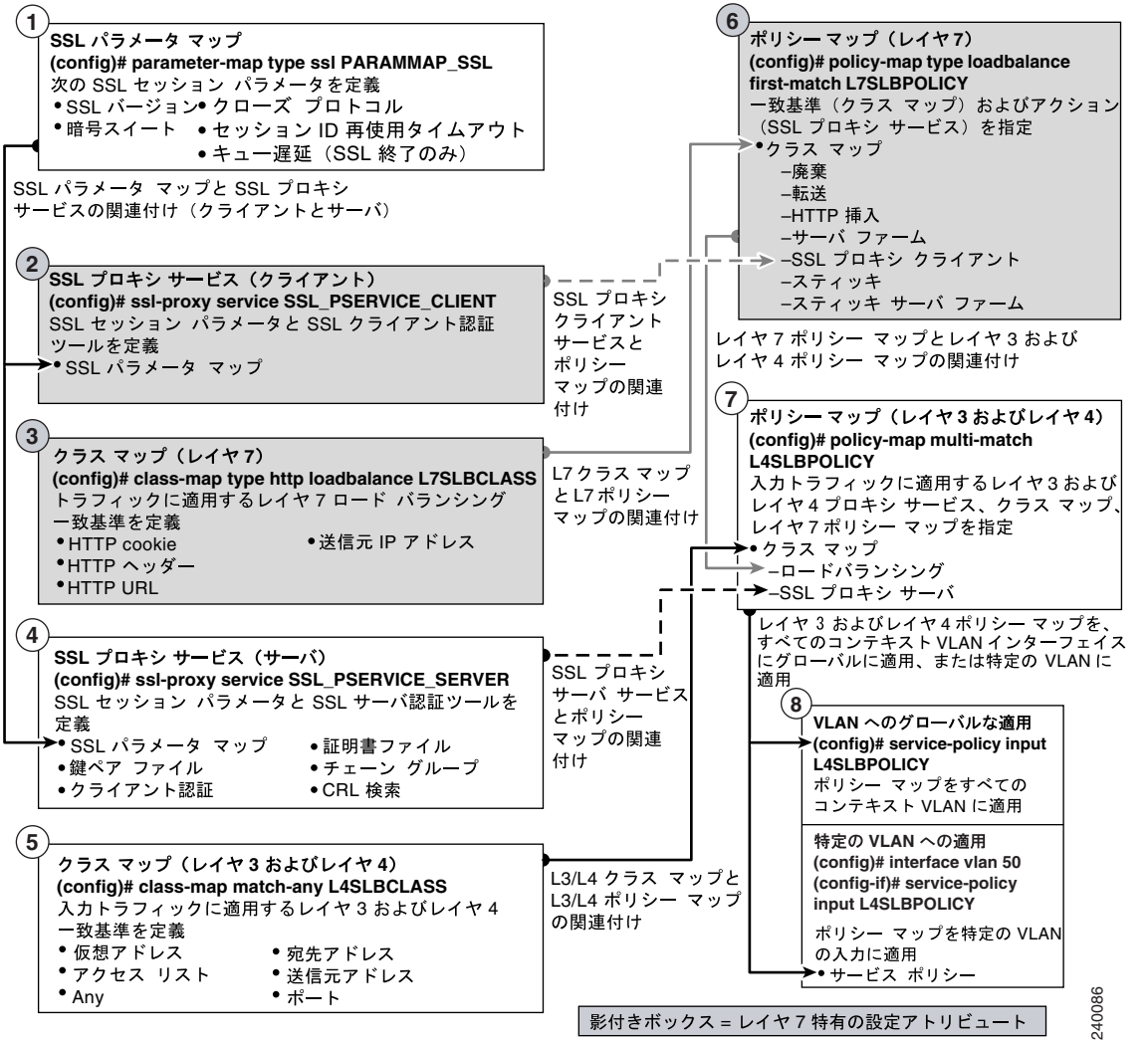


ACE は、パラメータ マップ、SSL プロキシ サービス、およびクラス マップを組み合わせることにより、クライアント、ACE、および SSL サーバ間の情報フローのポリシー マップを確立します。

図 5-2 は、レイヤ 7 ロードバランシング ポリシー マップを確立し、これをレイヤ 3 およびレイヤ 4 ポリシー マップと関連付けてエンドツーエンド SSL の設定を作成するための主なプロセスを図示したものです。レイヤ 7 と、レイヤ 3 およびレイヤ 4 の設定アトリビュートを簡単に見分けられるように、レイヤ 7 のアトリビュートにはグレーの影を付けてあります。

プロセスの最後のステップでは、レイヤ 3 およびレイヤ 4 のポリシー マップをこのコンテキストの入力トラフィックに適用します。この図には、ポリシー マップ設定のさまざまな構成要素の相互関係も示してあります。

図 5-2　エンドツーエンド SSL の基本的な設定フロー図



ACE エンドツーエンド SSL 設定の前提条件

ACE に SSL 動作を設定する前に、まず ACE にサーバ ロード バランシング（SLB）を設定する必要があります。SLB 設定プロセスでは、次の設定オブジェクトを作成します。

- レイヤ 7 クラス マップ
- レイヤ 3 およびレイヤ 4 クラス マップ
- レイヤ 7 ポリシー マップ
- レイヤ 3 およびレイヤ 4 ポリシー マップ

SLB の設定後、このガイドのエンドツーエンド SSL の説明に従って、既存の SLB クラス マップとポリシー マップを変更し、SSL 設定要件を加えます。

ACE の SLB 設定手順については、『*Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*』を参照してください。

エンドツーエンド SSL の設定

ACE にエンドツーエンド SSL を設定するための主要なプロセスを表 5-1 に示します。エンドツーエンド SSL は、SSL 終了機能と SSL 開始機能の設定プロセスを組み合わせたものなので、手順には、このガイド内で該当プロセスが詳細に記述されているセクションへのリンクが示してあります。

表 5-1　エンドツーエンド SSL 設定のクイック スタート

作業
1. ACE で SSL 開始機能を設定します（第 4 章「SSL 開始の設定」を参照）。SSL 開始機能の設定では、バックエンド動作のすべてとフロントエンド動作の一部を設定します。 この時点でこの設定を VLAN に適用しないでください。
2. ACE のフロントエンド動作用パラメータ マップを作成します（第 3 章「SSL 終了の設定」の「SSL パラメータ マップの作成と定義」を参照）。 ACE が、ステップ 1 でバックエンド動作用に作成したパラメータ マップと同じものを使用する場合は、このステップを飛ばしてください。
3. SSL プロキシ サーバ サービスを作成します（第 3 章「SSL 終了の設定」の「SSL プロキシ サービスの作成と定義」を参照）。
4. SSL プロキシ サーバ サービスを、ステップ 1 で作成したレイヤ 3 およびレイヤ 4 ポリシー マップと関連付けます。この関連付けについては、第 3 章「SSL 終了の設定」の「SSL プロキシ サーバ サービスとポリシー マップの関連付け」を参照してください。
5. レイヤ 3 およびレイヤ 4 ポリシー マップを VLAN に適用します（第 3 章「SSL 終了の設定」の「ポリシー マップの VLAN への適用」を参照）。
6. （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすることにより、設定変更をフラッシュ メモリに保存します。 `host1/Admin(config-if)# do copy running-config startup-config`