CHAPTER 5

エンドツーエンド SSL の設定

（注） この章の情報は、特に記載のない限り、ACE モジュールと ACE アプライアンスの両方に適用されます。この章で説明する機能は、特に記載のない限り、IPv4 と IPv6 に適用されます。

この章では、エンドツーエンド SSL 接続を提供するように Cisco ACE アプリケーション コントロール エンジン を設定する方法について説明します。このプロセスには、SSL 開始（バック エンド）と SSL 終了（フロント エンド）を組み合わせて、クライアント、ACE、およびサーバの間の安全なリンクを提供することが含まれます。すべてのデータが暗号化され、暗号文として 3 つのデバイス間で送信されます。

この章の内容は、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、ACE が、接続の一方のエンドにあるクライアントともう一方のエンドにあるサーバとの間に SSL 接続を確立し、維持することを示します。エンドツーエンド SSL 用に ACE を設定すると、ACE は次の機能を実行します。

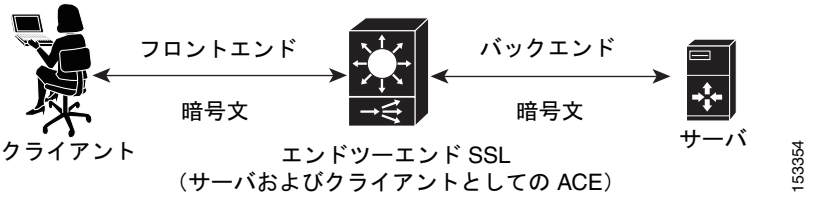
- クライアントとの SSL セッションを終了する（フロントエンド接続）
- サーバとの SSL セッションを開始する（バックエンド接続）
- バックエンド コンテンツをロード バランスする

エンドツーエンド SSL は、SSL 終了と SSL 開始用に ACE を設定するのに使用する構成を組み合わせます。エンドツーエンド SSL の場合は、次のタイプのポリシー マッ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 とサーバ間のトラフィックのバックエンド フローを指示します。
- 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 間のトラフィックのフロントエンド フローを指示します。
  - 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、関連付けられたレイヤ 7 ポリシー マップを適用します。

図 5-1 は、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 の適用を示します。

図 5-1　エンドツーエンド SSL

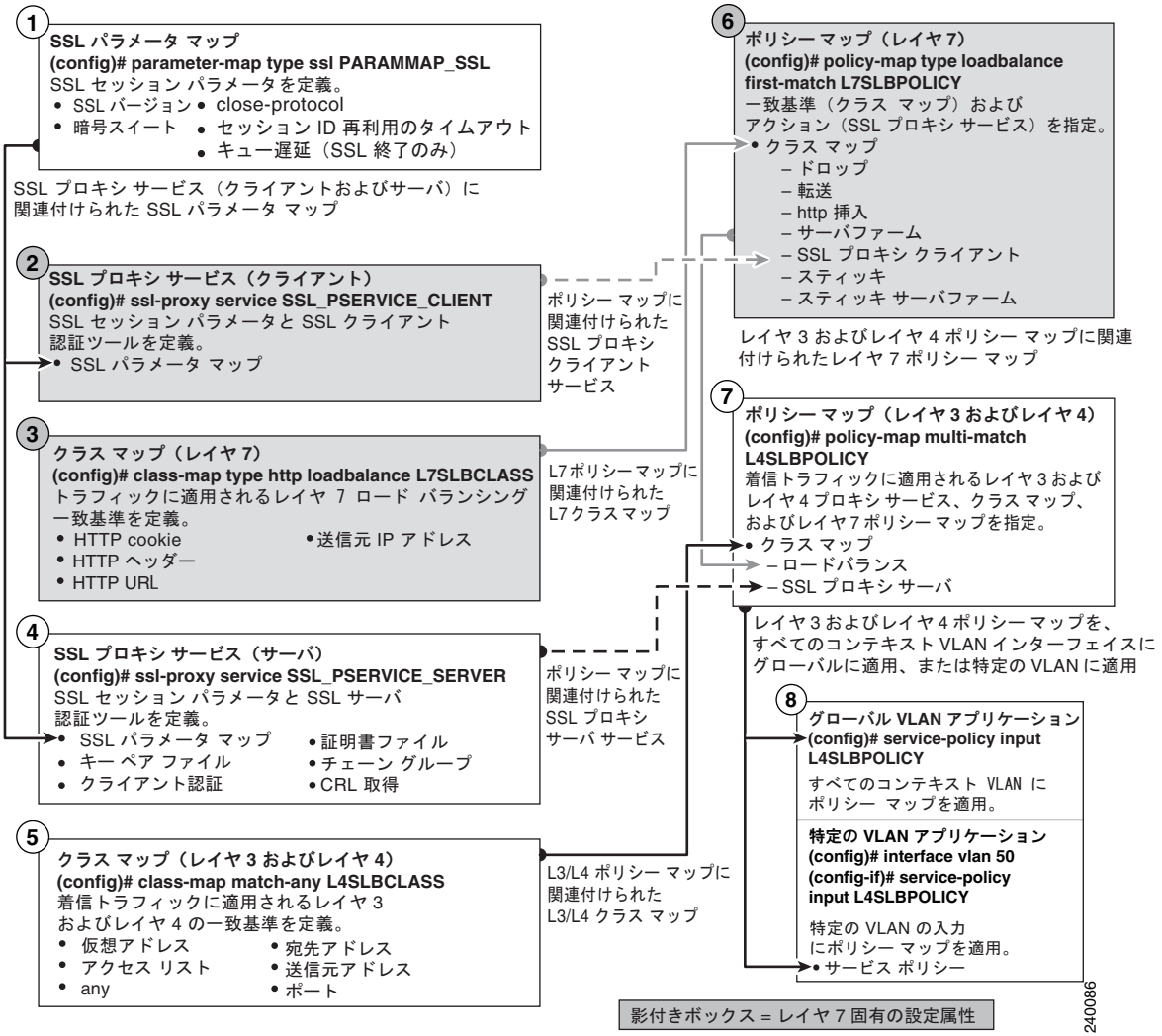


ACE は、パラメータ マップ、SSL プロキシ サービス、およびクラス マップの組み合わせを使用して、クライアント、ACE、および SSL サーバ間の情報フローを決定するポリシー マップを作成します。

図 5-2 は、レイヤ 7 ロードバランシング ポリシー マップを作成し、それをレイヤ 3 およびレイヤ 4 ポリシー マップに関連付けてエンドツーエンド SSL 設定を作成するのに必要なプロセスの概要を示します。レイヤ 7 属性と、レイヤ 3 およびレイヤ 4 属性とを容易に識別できるように、レイヤ 7 属性はグレーで塗られています。

プロセスの最後のステップでは、コンテキストの入力トラフィックにレイヤ 3 およびレイヤ 4 ポリシー マップを適用します。この図は、ポリシー マップ設定のさまざまなコンポーネントが互いにどのように関連付けられるかも示しています。

図 5-2　基本的なエンドツーエンド SSL の設定のフロー図



ACE エンドツーエンド SSL 設定の前提条件

SSL オペレーション用に ACE を設定する前に、まずサーバ ロード バランシング（SLB）用に設定する必要があります。SLB の設定プロセス中に、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 を設定したら、このガイドに記載されているエンドツーエンド SSL 用の SSL 設定要件を使用して、既存の SLB クラス マップおよびポリシー マップを変更します。

SLB 用に ACE を設定するには、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

エンドツーエンド SSL の設定

表 5-1 は、エンドツーエンド SSL 用に ACE を設定するのに必要なプロセスの概要を示します。エンドツーエンド SSL は SSL 終了と SSL 開始の設定プロセスを結合するため、この手順では、特定のプロセスを詳しく説明している項へのリンクを示します。

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. 第 4 章の「SSL 開始の設定」の説明に従って、SSL 開始用に ACE を設定します。SSL 開始の設定では、バックエンド操作のすべてと、フロントエンド操作の一部を設定します。 現時点では、VLAN に設定を適用しないでください。
2. 第 3 章「SSL 終了の設定」の「SSL パラメータ マップの作成および定義」の項の説明に従って、フロントエンド操作で ACE が使用するパラメータ マップを作成します。 手順 1 でバックエンド操作用に作成したのと同じパラメータ マップを ACE が使用する場合、この手順は省略します。

表 5-1　エンドツーエンド SSL 設定のクイック スタート （続き）

作業
3. 第 3 章「SSL 終了の設定」の「SSL プロキシ サービスの作成および定義」の項の説明に従って、SSL プロキシ サーバ サービスを作成します。
4. 手順 1 で作成したレイヤ 3 およびレイヤ 4 ポリシー マップに、SSL プロキシ サーバ サービスを関連付けます。この関連付けについては、第 3 章「SSL 終了の設定」の「ポリシー マップと SSL プロキシ サーバ サービスの関連付け」の項を参照してください。
5. 第 3 章「SSL 終了の設定」の「VLAN へのポリシー マップの適用」の項の説明に従って、VLAN にレイヤ 3 およびレイヤ 4 ポリシー マップを適用します。
6. （任意）スタートアップ コンフィギュレーションに実行コンフィギュレーションをコピーして、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`

エンドツーエンド SSL 設定の例

次の例は、フロントエンド SSL とバックエンド SSL を組み合わせる、エンドツーエンド SSL 設定を示します。ACE は、HTTP クライアントから暗号化テキストを受信し、また、暗号化データを暗号文として SSL サーバに送信します。一方、ACE は SSL サーバから受け取った暗号文を復号化し、そのデータをクリア テキストとしてクライアントに送信します。例では、SSL 固有の設定要素が太字で示されています。

IPv6 の例

```
access-list ACL line 10 extended permit ip anyv6 anyv6

rserver host TEST4
  ip address 2001:DB8:20::9
  inservice

serverfarm host TEST
  rserver TEST4
    inservice
```

```
parameter-map type ssl PM1
  session-cache timeout 300
  queue-delay timeout 1

ssl-proxy service SSL_CLIENT
  ssl advanced-options PM1

ssl-proxy service SSL_SERVER
  key KEY12.PEM
  cert CERT12.PEM
  ssl advanced-options PM1

class-map type http loadbalance match-any SSL
  2 match http url .*
class-map match-any SSL_C1
  2 match virtual-address 2001:DB8:2::101 tcp eq https
  3 match virtual-address 2001:DB8:2::101 tcp any

policy-map type loadbalance first-match SSL_BACK
  class SSL
    serverfarm TEST
    ssl-proxy client SSL_CLIENT

policy-map multi-match L7_1
  class SSL_C1
    loadbalance vip inservice
    loadbalance policy SSL_BACK
    loadbalance vip icmp-reply
    ssl-proxy server SSL_SERVER

interface vlan 210
  ip address 2001:DB8:1::1/64
  service-policy input L7_1
  access-group input ACL
  no shutdown
interface vlan 220
  ip address 2001:DB8:2::1/64
  no shutdown
interface vlan 226
  ip address 2001:DB8:F::27/64
  no shutdown

ip route ::/0 2001:DB8:F::1
```

IPv4 の例

```
access-list ACL line 10 extended permit ip any any

rserver host TEST4
  ip address 20.20.2.11
  inservice

serverfarm host TEST
  rserver TEST4
    inservice

parameter-map type ssl PM1
  session-cache timeout 300
  queue-delay timeout 1

ssl-proxy service SSL_CLIENT
  ssl advanced-options PM1

ssl-proxy service SSL_SERVER
  key KEY12.PEM
  cert CERT12.PEM
  ssl advanced-options PM1

class-map type http loadbalance match-any SSL
  2 match http url .*
class-map match-any SSL_C1
  2 match virtual-address 10.10.2.101 tcp eq https
  3 match virtual-address 10.10.2.101 tcp any

policy-map type loadbalance first-match SSL_BACK
  class SSL
    serverfarm TEST
    ssl-proxy client SSL_CLIENT

policy-map multi-match L7_1
  class SSL_C1
    loadbalance vip inservice
    loadbalance policy SSL_BACK
    loadbalance vip icmp-reply
    ssl-proxy server SSL_SERVER

interface vlan 210
  ip address 10.10.2.1 255.255.255.0
  service-policy input L7_1
  access-group input ACL
  no shutdown
```

```
interface vlan 220
  ip address 20.20.2.1 255.255.255.0
  no shutdown
interface vlan 226
  ip address 10.90.15.27 255.255.255.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.90.15.1
```