CHAPTER 4

SSL 開始の設定

（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、SSL 開始の SSL クライアントとして Cisco ACE アプリケーション コントロール エンジン のコンテキストを設定する方法について説明します。

この章の内容は、次のとおりです。

（注）　サーバから ACE への SSL 接続が正常に開始されたことを確認するために、**show stats crypto client** コマンド出力のハンドシェイク カウンタを監視できます（第 6 章「SSL 情報および統計情報の表示」を参照）。接続が成功するとハンドシェイク カウンタがインクリメントします。たとえば、SSLv3 Full Handshakes カウンタはハンドシェイクが正常に完了したことを示し、SSLv3 Resumed Handshakes カウンタはセッション ID を使用してハンドシェイクが正常に再開したことを示します。トラフィックが流れていると、これらのカウントがインクリメントします。障害が発生した場合は、アラートが送信され、受信カウンタもインクリメントします。

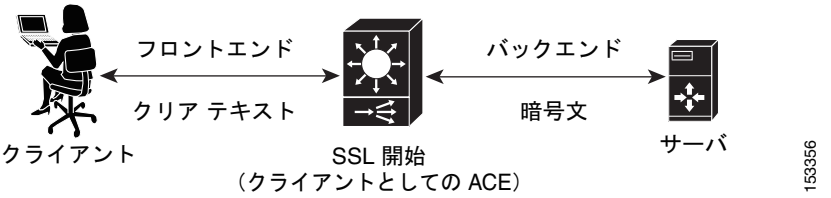
SSL 開始の概要

SSL 開始が行われるのは、SSL プロキシ クライアントとして機能する ACE が、それ自体と SSL サーバとの SSL 接続を開始し、維持するときです。この特定の用途では、ACE はクリア テキストを HTTP クライアントから受け取り、そのデータを暗号化して暗号文として 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。

図 4-1 に示すように、次のネットワーク接続において、ACE が SSL サーバとの SSL 接続を開始します。

- クライアントから ACE：ACE とクライアントとの間の HTTP 接続
- ACE からサーバ：サーバと SSL プロキシ クライアントとして機能する ACE との間の SSL 接続

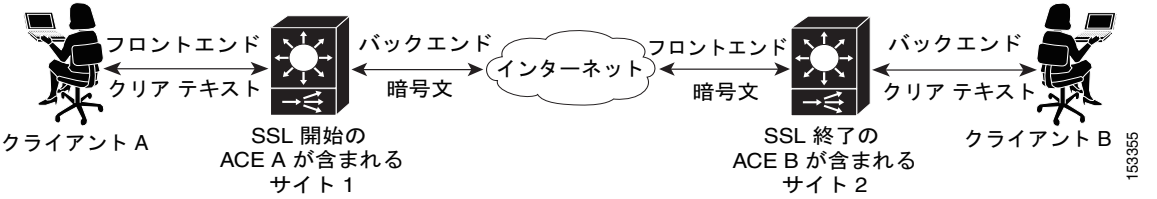
図 4-1　SSL サーバとの SSL 開始



SSL 開始により、サイト内のデバイス間でクリア テキストを最大速度で送信できるほか、インターネットを介してサイト間で、または SSL サーバに対して、暗号文を最大限のセキュリティで送信できます。クリア テキスト接続からの SSL 接続を確立する各 SSL サーバまたは ACE（SSL プロキシ サーバとして機能）用に、その SSL サーバまたは他の ACE にマップする ACE 上で、SSL 開始ポリシー サービスを設定する必要があります。

図 4-2 は、SSL 終了用に設定された他の ACE との SSL 開始フローを示します。この場合、ACE B は仮想フロントエンド SSL サーバとして機能します。

図 4-2　SSL 終了を実行している 2 番目の ACE での SSL 開始



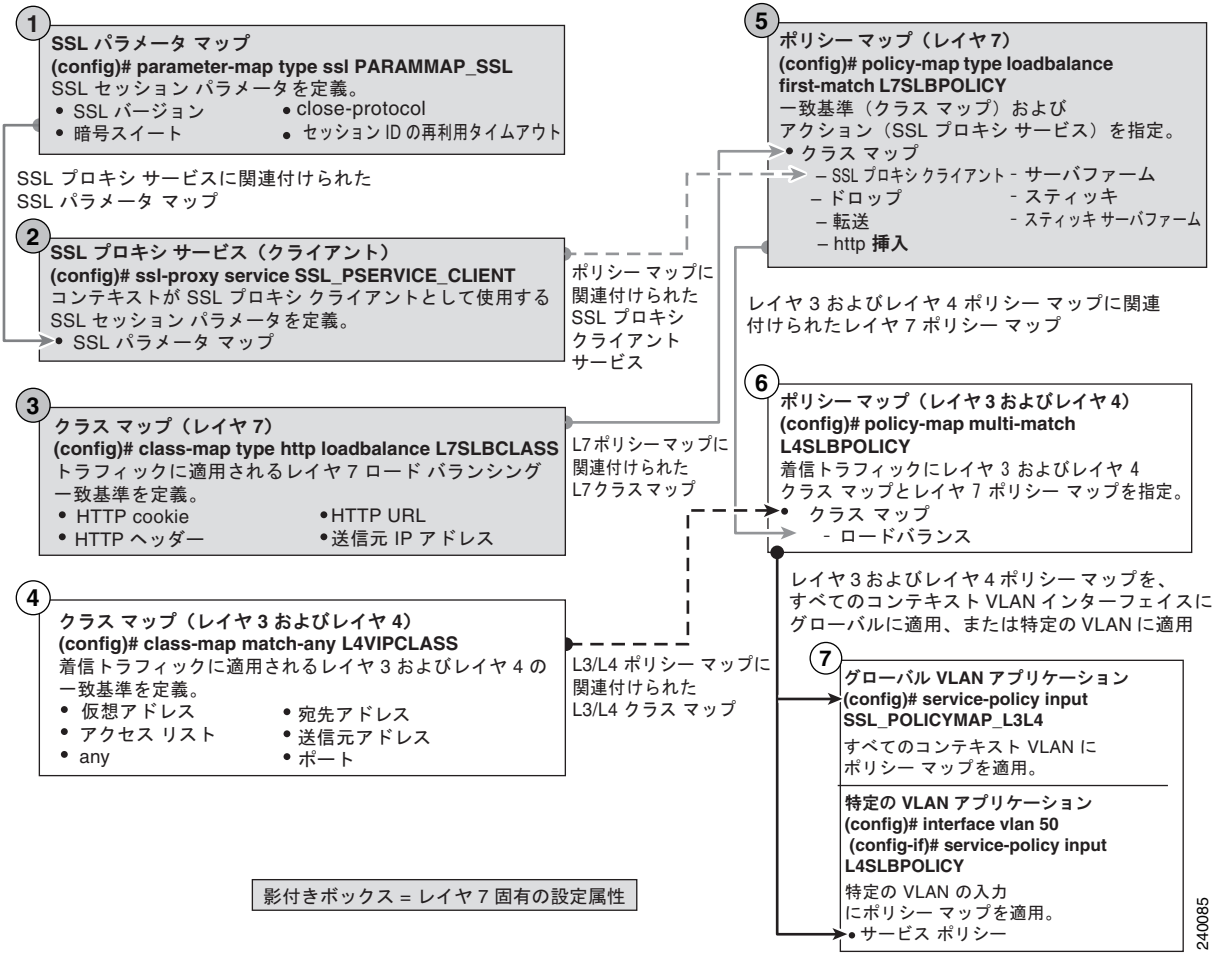
ACE は、パラメータ マップ、SSL プロキシ サービス、およびクラス マップの組み合わせを使用してポリシー マップを作成し、それによって、クライアント、ACE、および SSL サーバの間の情報フローが決まります。SSL 開始の場合は、SSL サーバによって SSL クライアントと認識されるように、ACE を設定します。これを行うには、次のタイプのポリシー マップを設定します。

- レイヤ 7 ポリシー マップ：このポリシー マップには、レイヤ 7 クラス マップおよび SSL プロキシ クライアント サービスとの関連付けが含まれます。クラス マップは、トラフィックのフィルタとして機能し、ユーザが指定したサーバ ロードバランシング（SLB）の基準を満たすトラフィックを検索します。SSL 開始の場合、一致基準は HTTP cookie や URL などの HTTP ロードバランシング属性の形式になります。SSL プロキシ クライアント サービスは、ハンドシェイクとその後の SSL セッション中に ACE が使用する SSL パラメータを定義します。
- レイヤ 3 およびレイヤ 4 ポリシー マップ：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 マップと関連付けます。ACE は、まずコンテキストのトラフィックにレイヤ 3 およびレイヤ 4 ポリシー マップを適用して、そのトラフィックが特定の宛先、ソース、仮想 IP アドレスなど、特定のレイヤ 3 およびレイヤ 4 一致基準を含んでいるかどうかを判断します。作

成するレイヤ 3 およびレイヤ 4 クラス マップに一致基準を指定し、このポリシー マップと関連付けます。一致が見つかると、ACE は、関連付けられたレイヤ 7 ポリシー マップをトラフィックに適用します。

図 4-3 は、SSL 開始用に ACE が使用する、2 種類のポリシー マップの構築および適用に必要なプロセスの概要を示します。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を互いに関連付ける方法も示します。

図 4-3　基本的な SSL 開始の設定のフロー図



ACE SSL 開始設定の前提条件

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 SSL 開始用の 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。

SSL 開始の設定のクイック スタート

図 4-1 は、SSL 開始用に ACE を設定するのに必要な手順の概要を示します。各手順には、その作業を完了するために必要な CLI コマンド、または手順の参照先が含まれています。各機能および CLI コマンドに関連付けられているすべてのオプションについての詳細は、表 4-1 以降のセクションを参照してください。

（注） このクイック スタートには、図 4-3 で示されるような、パラメータ マップを作成するための手順は含まれていません。ACE は、表 4-2 で説明するように、デフォルトのパラメータ マップ設定を使用します。

表 4-1　SSL 開始の設定のクイック スタート

作業およびコマンドの例

1. 複数のコンテキストで動作する場合は、CLI プロンプトを観察して、適切なコンテキストで動作しているかどうかを確認してください。必要に応じて、適切なコンテキストに直接ログインするか、または切り替えてください。
`host1/Admin# changeto C1`
`host1/C1#`
この表の残りの例では管理コンテキストを使用しています。コンテキスト作成の詳細については、『*Virtualization Guide, Cisco ACE Application Control Engine*』を参照してください。

2. コンフィギュレーション モードを開始します。
`host1/Admin# config`
`host1/Admin(config)#`

3. レイヤ 7 ポリシー マップと関連付ける SSL プロキシ クライアント サービスを作成します。このクイック スタートでは、プロキシ クライアント サービスのパラメータを定義しません。SSL クライアントとして機能するように ACE を設定するのに必要な作業は、ポリシー マップとこの一般的なプロキシ クライアント サービスを関連付けることだけです。
`host1/Admin(config)# ssl-proxy service SSL_PSERVICE_CLIENT`
`host1/Admin(config-ssl-proxy)# exit`

4. レイヤ 7 クラス マップを作成し、必要なロードバランシング一致基準を使用して設定します。
`host1/Admin(config)# class-map type http loadbalance L7SLBCLASS`
`host1/Admin(config-cmap-http-lb)# match url XYZ.ORG`
`host1/Admin(config-cmap-http-lb)# exit`
`host1/Admin(config)#`

表 4-1　SSL 開始の設定のクイック スタート （続き）

作業およびコマンドの例

5. レイヤ 3 およびレイヤ 4 クラス マップを作成し、必要な入力トラフィック一致基準を使用して設定します。
`host1/Admin(config)# class-map match-any L4VIPCLASS`
`host1/Admin(config-cmap)# match virtual-address 2001:DB8:1::2/64`
`or`
`host1/Admin(config-cmap)# match virtual-address 192.168.12.2 255.255.255.0`
`host1/Admin(config-cmap)# exit`
`host1/Admin(config)#`

6. レイヤ 7 ポリシー マップを作成し、手順 4 で作成したレイヤ 7 クラス マップを関連付けます。
`host1/Admin(config)# policy-map type loadbalance first-match L7SLBPOLICY`
`host1/Admin(config-pmap-lb)# class L7SLBCLASS`
`host1/Admin(config-pmap-lb-c)#`

7. 手順 3 で作成した SSL プロキシ クライアント サービスをレイヤ 7 ポリシー マップと関連付けます。
`host1/Admin(config-pmap-lb-c)# ssl-proxy client SSL_PSERVICE_CLIENT`
`host1/Admin(config-pmap-lb-c)# exit`
`host1/Admin(config-pmap-lb)# exit`
`host1/Admin(config)#`

8. レイヤ 3 およびレイヤ 4 ポリシー マップを作成し、手順 5 で作成したレイヤ 3 およびレイヤ 4 クラス マップを関連付けます。
`host1/Admin(config)# policy-map multi-match L4SLBPOLICY`
`host1/Admin(config-pmap)# class CLASSMAP_L3`
`host1/Admin(config-pmap-c)#`

9. 手順 6 で作成したロードバランシング 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 マップと関連付けます。
`host1/Admin(config-pmap-c)# loadbalance L7SLBPOLICY`
`host1/Admin(config-pmap-c)# exit`
`host1/Admin(config-pmap)# exit`
`host1/Admin(config)#`

表 4-1　SSL 開始の設定のクイック スタート （続き）

作業およびコマンドの例

10. 次のように、レイヤ 3 およびレイヤ 4 ポリシー マップを、目的のインターフェイスの入力トラフィックに適用します。
 	
コンテキスト内のすべての VLAN に、ポリシー マップをグローバルに適用します。
 	
`host1/Admin(config)# service-policy input L4SLBPOLICY`
 	
コンテキスト内の特定の VLAN に、ポリシー マップを適用します。
 	
`host1/Admin(config)# interface vlan 50`
`host1/Admin(config-if)# service-policy input L4SLBPOLICY`

11. 実行コンフィギュレーションを表示して、追加した情報が正しく設定されているか確認します。 `host1/Admin(config-if)# do show running-config`
12.（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`

SSL パラメータ マップの作成および定義

SSL パラメータ マップでは、ACE が SSL プロキシ サービスに適用する SSL セッション パラメータを定義します。SSL パラメータ マップを作成すると、同じ SSL セッション パラメータを異なるプロキシ サービスに適用できます。表 4-2 では、各 SSL セッション パラメータとそれぞれのデフォルト値について説明します。

表 4-2　SSL パラメータの SSL セッション パラメータ Map

SSL セッション パラメータ	説明	デフォルトの値/動作
Cipher suites	SSL ハンドシェイク時に ACE がサポートする暗号スイートを定義します（ACE がサポートする使用可能な暗号スイートのリストについては、表 4-3 を参照してください）。	ACE は、使用可能な暗号スイートをすべてサポートします。
Authentication-failure ignore	期限切れまたは無効なサーバ証明書を無視し、SSL 開始設定のバックエンド接続を確立し続けるように、ACE を有効化します。	ACE は、証明書の問題が発生した場合に、SSL ハンドシェイクを終了します。
CDP-errors ignore	**crl best-effort** コマンドが ACE で設定されている場合、このパラメータによって、ACE は CDP エラーによる認証の失敗を無視できます。	Disabled
Close-protocol	ACE が終了通知メッセージを実行する方法を定義します。	**none**：ACE は、セッションを終了するときに終了通知アラート メッセージをクライアント/サーバに送信しますが、クライアント/サーバからの応答は想定しません。
Purpose-check disabled	このコマンドが設定されると、ACE は認証時に証明書に対する目的確認を実行できません。	Enabled

表 4-2　SSL パラメータの SSL セッション パラメータ Map （続き）

SSL セッション パラメータ	説明	デフォルトの値 / 動作
Rehandshake	再ハンドシェイクを有効化すると、ACE は、SSL HelloRequest メッセージをピアに送信して SSL ハンドシェイク ネゴシエーションを再開できます。	Disabled
Version	SSL ハンドシェイク時に ACE でサポートされる SSL および TLS のバージョンを定義します。	ACE がサポートするバージョンは、SSL3 と TLS1 です。
Session cache timeout	ACE が新しい SSL セッションを確立するために新しい SSL ハンドシェイクが必要になるまでの、SSL セッション ID の有効期間を定義します。	Disabled
Expired CRL	CRL が期限切れになった場合に、ACE が受け取ったすべてのクライアント認証を拒否するかどうかを定義します。	Disabled

（注）　SSL プロキシ サービスが SSL セッション パラメータのデフォルト値を使用するようにする場合、SSL パラメータ マップを作成したり、プロキシ サービスと関連付けたりする必要はありません。SSL プロキシ サービスにパラメータ マップを関連付けないと、ACE は、表 4-2 にリストされているセッション パラメータのデフォルト値を自動的にプロキシ サービスに適用します。

パラメータ マップの SSL コンフィギュレーション モードには、**queue-delay timeout** コマンドが含まれます。このキュー遅延は、ACE がそのクライアントに送信する暗号化されたデータにのみ適用されます。したがって、このタイマーは ACE によって処理される SSL 開始接続には影響を与えません。

SSL パラメータ マップを作成するには、**parameter-map type ssl** コマンドをコンフィギュレーション モードで使用します。

このコマンドの構文は次のとおりです。

parameter-map type ssl *parammap_name*

parammap_name 引数は、SSL パラメータ マップの名前です。スペースを含まない最大 64 文字で、引用符で囲まれていない英数字の文字列を入力します。

たとえば、SSL パラメータ マップ PARAMMAP_SSL を作成するには、次のように入力します。

```
host1/Admin(config)# parameter-map type ssl PARAMMAP_SSL
```

SSL プロキシ パラメータ マップを作成したあと、CLI はパラメータ マップ SSL コンフィギュレーション モードになります。

```
host1/Admin(config-parammap-ssl)#
```

SSL セッション パラメータを定義せずにパラメータ マップ SSL コンフィギュレーション モードを終了すると、ACE は、表 4-2 にリストされているデフォルト値を使用してパラメータ マップを設定します。

既存の SSL パラメータ マップを削除するには、次のように入力します。

```
host1/Admin(config)# no parameter-map type ssl PARAMMAP_SSL
```

ここでは、次の内容について説明します。

- SSL パラメータ マップの説明の定義
- 暗号スイートの追加
- 期限切れまたは無効なサーバ証明書の無視
- CDP エラーによる認証の失敗を無視する ACE 設定
- close-protocol 動作の定義
- 証明書での目的確認の無効化
- SSL セッションの再ハンドシェイクの有効化
- SSL および TLS のバージョンの定義
- SSL セッション キャッシュ タイムアウトの設定
- 期限切れの CRL サーバ証明書の拒否

SSL パラメータ マップの説明の定義

SSL パラメータ マップ コンフィギュレーション モードで **description** コマンドを使用して、SSL パラメータ マップの簡単な説明を記述できます。このコマンドの構文は次のとおりです。

description *text*

text 引数には、スペースを含め最大 240 文字の英数字からなるテキスト文字列を引用符で囲まずに入力します。

たとえば、SSL パラメータ マップの説明を指定するには、次のコマンドを入力します。

```
host1/Admin(config)# parameter-map type ssl PARAMMAP_SSL
host1/Admin(config-parammap-conn)# description SSL parameter map
```

SSL パラメータ マップから説明を削除するには、次のように入力します。

```
host1/Admin(config-parammap-conn)# no description
```

暗号スイートの追加

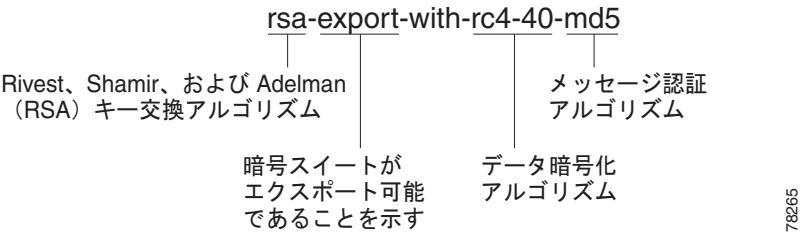
SSL プロトコルは、以下のような操作で使用する、さまざまな暗号化アルゴリズムをサポートします。

- サーバとクライアントを相互に認証する
- 証明書を送信する
- セッション キーを確立する

サポートする SSL バージョン、使用できる暗号化強度に関する企業ポリシー、SSL 対応ソフトウェアの輸出に関する政府規制などのさまざまな要因によって、クライアントとサーバがサポートする暗号スイート（暗号セット）が異なる可能性があります。また、SSL ハンドシェイク プロトコルによって、サーバとクライアントが相互認証、証明書の送信、およびセッション キーの確立に使用する暗号スイートをどのようにネゴシエートするかが決まります。

図 4-4 に示すように、暗号スイートは、キー交換アルゴリズム、データ暗号化アルゴリズム、メッセージ認証（ハッシュ）アルゴリズムという、3 種類のアルゴリズムで構成されます。

図 4-4　暗号スイートのアルゴリズム



（注） 輸出可能な暗号スイートは、米国のソフトウェア製品輸出規制で定義されている他の暗号スイート（128 ビット暗号化の 3DES や RC4 など）ほどの強度はない暗号スイートです。輸出可能な暗号スイートは、米国からほとんどの国に輸出され、輸出可能な製品に強力な暗号化を提供します。

SSL パラメータ マップ コンフィギュレーション モードで **cipher** コマンドを使用すると、安全なセッション中に ACE がサポートする暗号スイートを定義できます。ユーザが選択する暗号スイートはユーザの環境およびセキュリティ要件によって異なり、ACE にロードした証明書とキーに関連付けられている必要があります。

（注） デフォルトでは、ACE は、表 4-3 にリストされているすべての暗号スイートをサポートします。このデフォルト設定は、特定の暗号を使用して SSL パラメータ マップを設定しない場合にのみ有効です。すべての暗号スイートを使用する設定に戻すには、コマンドの **no** 形式を使用して、定義した暗号をすべてパラメータ マップから削除する必要があります。

このコマンドの構文は次のとおりです。

cipher *cipher_name* [**priority** *cipher_priority*]

次のキーワードと引数があります。

- *cipher_name*：ACE がサポートするように指定する暗号スイートの名前です。表 4-3 のリストは、ACE がサポートする暗号スイートを示しています。この表から、サポートされている暗号スイートの 1 つを入力します。
- **priority**：暗号スイートにプライオリティ レベルを割り当てます。プライオリティ レベルは、最も高い 10 から最も少ない 1 までで、暗号スイートの優先順位を表します。デフォルトでは、すべての設定された暗号スイートに 1 のプライオリティ レベルが付けられます。ACE は、どの暗号スイートを使用するかをネゴシエートする際に、最も高いプライオリティ レベルで設定されている暗号スイートに基づいて、クライアント リストから選択します。より高いプライオリティ レベルは、指定された暗号スイートに偏ります。SSL 終了アプリケーションの場合、ACE は、クライアントの ClientHello ハンドシェイク メッセージの暗号スイートに一致するプライオリティ レベルを使用します。SSL 開始アプリケーションの場合、プライオリティ レベルは、ACE がサーバへの ClientHello ハンドシェイク メッセージに暗号スイートを配置する順序を表します。
- *cipher_priority*：暗号スイートの優先度レベルです。1 ～ 10 の値を入力します。デフォルトのプライオリティ値は 1 です。

たとえば、暗号スイート rsa_with_aes_128_cbc_sha を追加し、プライオリティ レベル 2 を割り当てるには、次のように入力します。

```
host1/Admin(config)# parameter-map type ssl PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# cipher rsa_with_aes_128_cbc_sha
priority 2
```

SSL パラメータ マップに含める各暗号スイートについて、**cipher** コマンドを繰り返します。

SSL パラメータ マップから暗号スイートを削除するには、次のように入力します。

```
host1/Admin(config-parammap-ssl)# no cipher rsa_with_aes_128_cbc_sha
```

表 4-3 は、ACE がサポートする使用可能な暗号化スイートを示します。また、サポートされている暗号スイートのうち、ACE からエクスポート可能なものを示します。この表では、各暗号スイートに必要な認証証明書および暗号キーも示します。

ACE が表 4-3 にリストされているすべての暗号スイートをサポートするデフォルトの設定を使用する場合、ACE は、表に表示されるのと同じ順序（RSA_WITH_RC4_128_MD5 で開始する順序）で暗号スイートをそのピアに送信します。

注意　タイトルに「export」が含まれている暗号スイートは、米国以外での使用を目的としており、キー サイズが制限さている暗号化アルゴリズムを持ちます。

表 4-3　ACE でサポートされる SSL 暗号スイート

暗号スイート	輸出可能	使用される認証証明書	使用するキー交換アルゴリズム
RSA_WITH_RC4_128_MD5	No	RSA 証明書	RSA キー交換
RSA_WITH_RC4_128_SHA	No	RSA 証明書	RSA キー交換
RSA_WITH_DES_CBC_SHA	No	RSA 証明書	RSA キー交換
RSA_WITH_3DES_EDE_CBC_SHA	No	RSA 証明書	RSA キー交換
RSA_EXPORT_WITH_RC4_40_MD5	Yes	RSA 証明書	RSA キー交換
RSA_EXPORT_WITH_DES40_CBC_SHA	Yes	RSA 証明書	RSA キー交換
RSA_EXPORT1024_WITH_RC4_56_MD5	Yes	RSA 証明書	RSA キー交換
RSA_EXPORT1024_WITH_DES_CBC_SHA	Yes	RSA 証明書	RSA キー交換
RSA_EXPORT1024_WITH_RC4_56_SHA	Yes	RSA 証明書	RSA キー交換
RSA_WITH_AES_128_CBC_SHA	No	RSA 証明書	RSA キー交換
RSA_WITH_AES_256_CBC_SHA	No	RSA 証明書	RSA キー交換

期限切れまたは無効なサーバ証明書の無視

期限切れまたは無効なサーバ証明書を無視し、SSL 開始設定のバック エンド接続を確立し続けるように ACE を有効化するには、パラメータ マップ SSL コンフィギュレーション モードで **authentication-failure ignore** コマンドを使用します。このコマンドを使用すると、ACE がサーバ証明書に関する次の重大でないエラーを無視できます。

- Certificate not yet valid
- Certificate has expired
- Unable to get issuer certificate
- Certificate revoked

このコマンドの構文は次のとおりです。

authentication-failure ignore

たとえば、期限切れまたは無効なサーバ証明書を無視するには、次のように入力します。

```
host1/Admin(config)# parameter-map type ssl SSL_PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# authentication-failure ignore
```

デフォルト設定の disabled に戻すには、このコマンドの **no** 形式を使用します。

```
host1/Admin(config-parammap-ssl)# no authentication-failure ignore
```

CDP エラーによる認証の失敗を無視する ACE 設定

デフォルトでは、サーバ証明書失効用に **crl best-effort** コマンドを設定すると、ACE が提示された証明書内の CRL 分散ポイント（CDP）エラー、または CRL ダウンロード時に発生したエラーを検出した場合、ACE はその SSL 接続を拒否します。

cdp-errors ignore コマンドでは、**crl best-effort** コマンドが設定されている場合に、SSL パラメータ マップが CDP エラーやダウンロード エラーを無視するように設定できます。**cdp-errors ignore** コマンドを設定する場合、ACE では、提示された証明書内に CDP エラーを検出した場合や、有効な証明書失効リスト（CRL）を証明書上の有効な CDP からダウンロードできない場合に、SSL 接続が許可されます。

パラメータ マップ SSL コンフィギュレーション モードでのこのコマンドの構文は次のとおりです。

cdp-errors ignore

たとえば、CDP エラーを無視するように ACE を設定する場合は、次のように入力します。

```
host1/Admin(config)# parameter-map type ssl PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# cdp-errors ignore
```

CDP エラーが発生した場合に ACE が SSL 接続を拒否するデフォルトの動作をリセットするには、**no** 形式の **cdp-errors ignore** コマンドを使用します。例を示します。

```
host1/Admin(config-parammap-ssl)# no cdp-errors ignore
```

提示された SSL 証明書内にある CDP エラーを ACE が無視し、SSL 接続を許可した回数を表示するには、**show crypto cdp-errors** コマンドを使用します。このコマンドは、[Best Effort CDP Errors Ignored] フィールドの出力を表示します。

close-protocol 動作の定義

SSL パラメータ マップ コンフィギュレーション モードで **close-protocol** コマンドを使用して、ACE が終了通知メッセージの送信を処理する方法を設定できます。

このコマンドの構文は次のとおりです。

close-protocol {**disabled** | **none**}

キーワードは次のとおりです。

- **disabled** : セッションを閉じるときに ACE が終了通知アラート メッセージをクライアント / サーバに送信しないように指定します。クライアント / サーバからの応答は想定しません。
- **none** : セッションを閉じるときに ACE が終了通知アラート メッセージをクライアント / サーバに送信するように指定します。クライアント / サーバからの応答は想定しません。

たとえば、close-protocol を disabled に設定するには、次のように入力します。

```
host1/Admin(config)# parameter-map type ssl PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# close-protocol disabled
```

close-protocol コマンドをデフォルト設定に設定して、終了通知アラート メッセージをクライアントやサーバに送信するには、次のように入力します。

```
host1/Admin(config-parammap-ssl)# no close-protocol
```

証明書での目的確認の無効化

デフォルトでは、証明書チェーンのサーバ認証中に、ACE は次の場合に basicContraint フィールドの目的確認を実行します。

- サーバ証明書に CA FALSE 設定がある場合。
- 中間証明書に CA TRUE 設定がある場合。

このフィールドにこれらの設定がない場合、証明書の認証は失敗します。

証明書の認証時に ACE が目的確認をする必要がないと判断した場合は、パラメータ マップ SSL コンフィギュレーション モードで **purpose-check disabled** コマンドを使用して無効にすることができます。

このコマンドの構文は次のとおりです。

purpose-check disabled

たとえば、目的確認を無効にするには、次のように入力します。

```
host1/Admin(config)# parameter-map type ssl SSL_PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# purpose-check disabled
```

目的確認を実行するデフォルト設定を再度有効にするには、このコマンドの **no** 形式を使用します。

```
host1/Admin(config-parammap-ssl)# no purpose-check disabled
```

SSL セッションの再ハンドシェイクの有効化

SSL セッションの再ハンドシェイクでは、ACE がクライアントに SSL HelloRequest メッセージを送信して SSL ハンドシェイク ネゴシエーションを再開できるようにします。再ハンドシェイクは、SSL セッションを再確立してセキュリティを保障する場合に役立ちます。

デフォルトでは、SSL の再ハンドシェイクは無効になっています。セッション中に SSL セッションの再ハンドシェイク機能を有効化するには、パラメータ マップ SSL コンフィギュレーション モードで **rehandshake enable** コマンドを使用します。

このコマンドの構文は次のとおりです。

rehandshake enable

たとえば、SSL の再ハンドシェイク機能を有効にするには、次のように入力します。

```
host1/Admin(config)# parameter-map type ssl PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# rehandshake enable
```

再ハンドシェイク機能を無効にするには、次のように入力します。

```
host1/Admin(config-parammap-ssl)# no rehandshake enable
```

rehandshake enable コマンドのステータスを表示するには、**show parameter-map** コマンドを使用します。

SSL および TLS のバージョンの定義

ピアとの SSL ハンドシェイク時に ACE がサポートするセキュリティ プロトコルのバージョンを指定するには、SSL パラメータ マップ コンフィギュレーション モードで **version** コマンドを使用します。

このコマンドの構文は次のとおりです。

version {**all** | **ssl3** | **tls1**}

キーワードは次のとおりです。

- **all**：（デフォルト）ACE は、SSL バージョン 3.0 と TLS バージョン 1.0 の両方をサポートします。
- **ssl3**：ACE は、SSL バージョン 3.0 だけをサポートします。
- **tls1**：ACE は、TLS バージョン 1.0 だけをサポートします。

たとえば、パラメータ マップ用に SSL バージョン 3.0 を指定するには、次のように入力します。

```
host1/Admin(config)# parameter-map type ssl PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# version ssl3
```

SSL プロキシ パラメータ マップからセキュリティ プロトコルのバージョンを削除するには、次のように入力します。

```
host1/Admin(config-parammap-ssl)# no version tlsl
```

SSL セッション キャッシュ タイムアウトの設定

クライアントおよび ACE が完全な SSL キー交換を実行し、新しいマスター秘密キーを確立するたびに、SSL セッション ID が作成されます。クライアントと ACE との SSL ネゴシエーション プロセスを迅速化するため、SSL セッション ID の再利用機能により、ACE はセッション キャッシュ内の秘密キー情報を再利用できます。クライアントのその後の接続では、ACE が、最後のネゴシエートされたセッションでキャッシュに格納されたキーを再利用します。

デフォルトでは、SSL セッション ID の再利用は、ACE で無効になっています。ACE で新しいセッションを確立するために完全な SSL ハンドシェイクが必要になるまで SSL セッション ID が有効になる時間の合計について、セッション キャッシュ タイムアウト値を設定することによって、セッション ID の再利用を有効にできます。

パラメータ マップ SSL コンフィギュレーション モードで **session-cache timeout** コマンドを使用して、セッション キャッシュ タイムアウトを設定できます。このコマンドの構文は次のとおりです。

session-cache timeout *seconds*

seconds 引数は、ACE がセッション ID を削除する前にキャッシュ内に格納されているキーを再利用する秒単位の時間です。0 ～ 72000（20 時間）の整数を入力します。デフォルトでは、セッション ID の再利用は無効です。値が 0 の場合、キャッシュが満杯になると ACE がキャッシュからセッション ID を削除し、Least Recently Used（LRU）タイムアウト ポリシーを適用します。

たとえば、600 秒にセッション キャッシュ タイムアウトを設定するには、次のように入力します。

```
host1/Admin(config-parammap-ssl)# session-cache timeout 600
```

タイマーを無効にし、ACE との新しい接続ごとに SSL 完全ハンドシェイクが発生するようにするには、次のように入力します。

```
host1/Admin(config-parammap-ssl)# no session-cache timeout
```

コンテキストのセッション キャッシュ情報をクリアするには、**clear crypto session-cache** コマンドを使用します。このコマンドの構文は次のとおりです。

clear crypto session-cache [**all**]

オプションのキーワード **all** では、すべてのコンテキストのすべてのセッション キャッシュ情報がクリアされます。このオプションを使用できるのは、管理コンテキストのみです。

期限切れの CRL サーバ証明書の拒否

「サーバ認証中の CRL の使用」に説明されているように、サーバ認証用に証明書失効リスト（CRL）を ACE 上で設定すると、この CRL には、新しいバージョンが使用可能になる日付を指定するための更新フィールドが含まれます。デフォルトでは、ACE は更新フィールドが期限切れの日付になっている CRL を使用しません。そのため、CRL を使用したサーバ証明書の受け取りを拒否しません。

使用されている CRL が期限切れの場合にサーバ証明書が失効していると判断するように ACE を設定するには、パラメータ マップ SSL コンフィギュレーション モードで **expired-crl reject** コマンドを使用します。このコマンドの構文は次のとおりです。

expired-crl reject

例を示します。

```
host1/Admin(config-parammap-ssl)# expired-crl reject
```

使用されている CRL が期限切れになった後に証明書が失効したと判断しない、ACE のデフォルト動作にリセットするには、次のように入力します:

```
host1/Admin(config-parammap-ssl)# no expired-crl reject
```

SSL プロキシ サービスの作成および定義

SSL プロキシ サービスは、ACE が SSL ハンドシェイク時に使用する SSL パラメータ マップを定義します。SSL 開始の場合は、SSL プロキシ クライアント サービスで ACE を設定します。これは、ACE が SSL クライアントとして機能するためです。

（注） SSL 開始の設定でキーおよび証明書をインポートまたは関連付ける必要はありません。

コンフィギュレーション モードで **ssl-proxy service** コマンドを使用して、SSL プロキシ クライアント サービスを作成できます。

このコマンドの構文は次のとおりです。

ssl-proxy service *pservice_name*

pservice_name 引数は、SSL プロキシ クライアント サービスの名前です。スペースを含まない最大 64 文字で、引用符で囲まれていない英数字の文字列を入力します。

たとえば、SSL プロキシ クライアント サービス PSERVICE _CLIENT を作成するには、次のように入力します。

```
host1/Admin(config)# ssl-proxy service PSERVICE_CLIENT
```

SSL プロキシ クライアント サービスを作成したあと、CLI は SSL プロキシ コンフィギュレーション モードになります。

```
host1/Admin(config-ssl-proxy)#
```

既存の SSL プロキシ クライアント サービスを削除するには、次のように入力します。

```
host1/Admin(config)# no ssl-proxy PSERVICE_CLIENT
```

ここでは、次の内容について説明します。

- SSL プロキシ クライアント サービスと SSL パラメータ マップの関連付け
- サーバ認証の認証グループの設定
- サーバ認証中の CRL の使用
- CRL のダウンロード場所の設定
- CRL での署名確認の設定

SSL プロキシ クライアント サービスと SSL パラメータ マップの関連付け

SSL プロキシ クライアント サービスと SSL パラメータ マップを関連付けるには、**ssl advanced-options** コマンドを SSL プロキシ コンフィギュレーション モードで使用します。

このコマンドの構文は次のとおりです。

ssl advanced-options *parammap_name*

parammap_name 引数は、既存の SSL パラメータ マップの名前です（「SSL パラメータ マップの作成および定義」の項を参照）。スペースを含まない最大 64 文字で、引用符で囲まれていない英数字の文字列を入力します。

たとえば、パラメータ マップ PARAMMAP_SSL を SSL プロキシ サービスと関連付けるには、次のように入力します。

```
host1/Admin(config)# ssl-proxy service PSERVICE_CLIENT
host1/Admin(config-ssl-proxy)# ssl advanced-options PARAMMAP_SSL
```

SSL プロキシ サービスと SSL パラメータ マップの関連付けを削除するには、次のように入力します。

```
host1/Admin(config-ssl-proxy)# no ssl advanced-options PARAMMAP_SSL
```

サーバ認証の認証グループの設定

デフォルトでは、サーバ認証は SSL 開始の設定で常に有効になります。サーバは ACE に証明書を送信する必要があります。ACE は、それがサーバ証明書であり、期限が切れていないことを確認して、その証明書を認証します。ただし、ACE は、その証明書が承認済み CA によって署名されていることは確認しません。サーバ証明書の有効期限が切れている場合、ACE は、サーバにリセット（RST）を送信することにより、バック エンド接続を拒否します。そうでない場合、ACE はサーバとの SSL 接続を通常どおりにセット アップします。

この動作は、パラメータ マップ SSL コンフィギュレーション モードで **authentication-failure ignore** コマンドを使用して上書きできます。このコマンドの詳細については、「期限切れまたは無効なサーバ証明書の無視」を参照してください。

認証グループは、証明書の署名者として信頼されている証明書で構成されます（第 2 章「証明書およびキーの管理」の「認証のための証明書グループの設定」の項を参照）。認証グループを SSL 開始設定で SSL プロキシ サーバに割り当てると、ACE は、サーバ証明書をグループ内の証明書と比較してチェックします。これには、そのサーバ証明書の発行者および署名のチェックが含まれます。

この SSL プロキシ サービスのサーバ認証のために認証グループを使用するには、SSL プロキシ コンフィギュレーション モードで **authgroup** コマンドを使用します。**authgroup** コマンドの構文は次のとおりです。

authgroup *group_name*

group_name 引数は、既存の証明書認証グループの名前です。スペースを含まない最大 64 文字で、引用符で囲まれていない英数字の文字列を入力します。

（注）　サーバ認証を有効にすると、ACE のパフォーマンスが大きく低下することがあります。

たとえば、証明書認証グループ AUTH-CERT1 を指定するには、次のように入力します。

```
host1/Admin(config-ssl-proxy)# authgroup AUTH-CERT1
```

SSL プロキシ サービスから証明書認証グループを削除するには、次のように入力します。

```
host1/Admin(config-ssl-proxy)# no authgroup AUTH-CERT1
```

サーバ認証中の CRL の使用

デフォルトでは、ACE は、サーバ認証中に証明書失効リスト（CRL）を使用しません。ACE は、HTTP または LDAP を介した CRL のダウンロードをサポートします。次のいずれかの方法で、CRL を使用するように SSL プロキシ サービスを設定できます。

- ACE は、サービス用の各サーバ証明書をスキャンして、認証拡張内の CRL をポイントする CRL 分散ポイント（CDP）が含まれているかどうかを判断し、その後で、CDP が有効な場合はその場所からその CRL を取得することができます。CDP に http:// または ldap:// ベースの URL がある場合は、その URL を使用して、CRL を ACE にダウンロードします。
- ACE が CRL を取得する CRL のダウンロード場所を手動で設定できます（「CRL のダウンロード場所の設定」の項を参照）。

（注）　デフォルトでは、使用されている CRL がその更新日を過ぎた場合、ACE はサーバ証明書を拒否しません。CRL が期限切れになった場合に証明書を拒否するように ACE を設定するには、**expired-crl reject** コマンドを使用します。詳細については、「期限切れの CRL サーバ証明書の拒否」のセクションを参照してください。

ベスト エフォート CRL が設定されている場合に CRL のダウンロードを試みると、以下のようになります。

- ACE は、証明書内、または ACE で設定されている最初の 4 つの CDP のみを考慮します。証明書から取得された CDP の場合、ACE は、CRL のダウンロード用に、有効で完全な CDP だけを考慮します。1 つの CDP で CRL が正常にダウンロードされた場合、ACE は、CRL のダウンロード用に後続の CDP は考慮しません。
- 最初の 4 つの CDP のいずれも有効ではなく CRL のダウンロードを続行できない場合、パラメータ マップ SSL コンフィギュレーション モードで **authentication-failure ignore** コマンドを設定していない限り、ACE はその証明書を失効と判断します。
- ACE が 4 つの有効な CDP を試したあとで CRL のダウンロードに失敗した場合、パラメータ マップ SSL コンフィギュレーション モードで **authentication-failure ignore** コマンドを設定していない限り、ACE は開始した SSL 接続を中止します。
- 提示された証明書内に CDP エラーを検出した場合や、CRL のダウンロード中に発生したエラーを検出した場合、ACE は、パラメータ マップ SSL コンフィギュレーション モードで **cdp-errors ignore** コマンドが設定されていない限り、SSL 接続を拒否します。
- ACE は、形式が正しくない CDP をスキップし、後続の CDP を処理します。形式が正しくない CDP を含む CDP エラー統計情報を表示するには、**show crypto cdp-errors** コマンドを使用します。

詳細な CRL ダウンロード統計情報については、第 6 章「SSL 情報および統計情報の表示」の「CRL 情報の表示」の項を参照してください。

SSL プロキシ コンフィギュレーション モードで **crl** コマンドを使用して、サーバ認証にどの CRL 情報を使用するかを判断できます。このコマンドの構文は次のとおりです。

crl {*crl_name* | **best-effort**}

引数とキーワードは次のとおりです。

- *crl_name*：コンフィギュレーション モードで **crypto crl** コマンドを使用して、CRL をダウンロードするときに CRL に割り当てた名前です。「CRL のダウンロード場所の設定」の項を参照してください。
- **best-effort**：ACE が各サーバ証明書をスキャンして、認証拡張内にある CRL をポイントする CDP が含まれているかどうかを判断し、その CDP が有効な場合は、その場所から CRL を取得するように指定します。

たとえば、SSL プロキシ サービスのサーバ認証に CRL1 CRL を有効にするには、次のコマンドを入力します。

```
host1/Admin(config-ssl-proxy)# crl CRL1
```

CRL 情報のクライアント証明書をスキャンするには、次のように入力します。

```
host1/Admin(config-ssl-proxy)# crl best-effort
```

ACE が、ダウンロードされた CRL データベース内のサーバ証明書を受け入れると、SSL の実サーバへの正常な SSL 接続により、次の **show stats crypto client** カウンタがインクリメントします。

- SSL サーバ認証の合計
- SSL スタティック CRL の参照

ACE がベスト エフォート CRL が有効になっている接続上でサーバ証明書を受け入れ、ダウンロードした CRL データベース内にその証明書が見つからない場合は、SSL の実サーバへの正常な SSL 接続により、次の **show stats crypto client** カウンタがインクリメントします。

- SSL サーバ認証の合計
- SSL ベスト エフォート CRL の参照

証明書が検証され、ACE にキャッシュされたあと、同じ SSL サーバへのセッションの再利用なしで SSL 接続が行われると、次の **show stats crypto client** カウンタがインクリメントします。

- SSL サーバ認証の合計
- SSL ベスト エフォート CRL の参照
- SSL CRL 参照キャッシュのヒット
- SSL 認証キャッシュのヒット

有効な、期限切れでない CRL が ACE にキャッシュされた場合、CRL の参照は発生せず、次の **show stats crypto client** カウンタは、同じ接続によって一緒にインクリメントしません。

- SSL ベスト エフォート CRL の参照
- SSL CRL 参照キャッシュのヒット

サーバ証明書が失効しているために SSL の実サーバへの SSL 接続が失敗すると、次の **show stats crypto client** カウンタがインクリメントします。

- SSL アラート CERTIFICATE_REVOKED の送信

- SSL サーバ認証の合計
- 失敗した SSL サーバ認証
- SSL のベスト エフォート CRL の参照、または SSL スタティック CRL の参照

サーバ認証時にダウンロードされた CRL の使用を無効にするには、次のコマンドを入力します。

```
host1/Admin(config-ssl-proxy)# no crl CRL1
```

サーバ認証時に CRL 情報のサーバ証明書の使用を無効にするには、次のコマンドを入力します。

```
host1/Admin(config-ssl-proxy)# no crl best-effort
```

CRL のダウンロード場所の設定

ACE がサーバ認証用に SSL プロキシ サービスに CRL をダウンロードするときに使用する場所を設定できます。サービスがポリシー マップで設定されていない場合や、ポリシー マップがアクティブでない場合、ACE は CRL をダウンロードしません。ACE は、次の条件下で CRL をダウンロードします。

- 最初に CRL を設定し、アクティブ レイヤ 4 ポリシー マップにアクションとして適用する場合（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）。
- ACE を再ロードする場合。
- CRL 自体で指定される NextUpdate CRL に到達すると、ACE はこの情報を読み取り、それに基づいて CRL を更新します。ACE は、次のサーバ認証要求時に、更新された CRL をダウンロードします。

コンテキストごとに最大 8 つの CRL を設定できます。CRL を設定したら、サーバ認証用に SSL プロキシ サービスに割り当てます（「サーバ認証中の CRL の使用」の項を参照）。

ACE は、ユーザが設定したドメイン ネーム システム（DNS）クライアントを使用して、CRL 内のホスト名を IP アドレスに変換します。DNS クライアントの設定の詳細については、「DNS クライアントの設定」の項を参照してください。

ダウンロードされた CRL を設定するには、コンフィギュレーション モードで **crypto crl** コマンドを使用します。このコマンドの構文は次のとおりです。

crypto crl *crl_name url*

引数は次のとおりです。

- *crl_name* : CRL に割り当てる名前です。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。
- *url* : ACE が CRL を取得する URL（CDP）です。最大 255 文字、引用符なしの英数字文字列で、CRL ファイル名を含む URL のフル パスを入力します。HTTP と LDAP の両方の URL がサポートされます。http:// プレフィックスまたは ldap:// プレフィックスで始まる URL を指定します。

  ldap:/// プレフィックスは、サーバ証明書の CDP 部分で有効な LDAP CRL リンクとは見なされません。LDAP URL の有効な形式は次のとおりです。

  - ldap://10.10.10.1:389/dc=cisco,dc=com?o=bu?certificateRevocationList
  - ldap://10.10.10.1/dc=cisco,dc=com?o=bu?certificateRevocationList
  - ldap://ldapsrv.cisco.com/dc=cisco,dc=com?o=bu?certificateRevocationList
  - ldap://ldapsrv.cisco.com:389/dc=cisco,dc=com?o=bu?certificateRevocationList

  URL の一部として疑問符（?）文字を使用するには、入力する前に Ctrl+V キーを押します。押さないと、ACE は help コマンドとして疑問符を解釈します。

（注） ldap:// リンク内のホスト名は、DNS 設定を使用して解決されます。LDAP では、TCP ポート 389 が使用されます。CRL を発行する LDAP サーバが標準ではない LDAP ポートでリッスンする場合は、標準ではない LDAP ポートを CDP で設定する必要があります。

たとえば、CRL1 という名前を付ける CRL を http://crl.verisign.com/class1.crl から設定するには、次のように入力します。

```
host1/Admin(config)# crypto crl CRL1
http://crl.verisign.com/class1.crl
```

CRL を削除するには、次のように入力します。

```
host1/Admin(config)# no crypto crl CRL1
```

CRL での署名確認の設定

証明書失効リスト（CRL）で署名確認を設定して、それが信頼できる認証局からのものであることを判断できます。これを行うには、EXEC コマンド モードで **crypto crlparams** コマンドを使用します。このコマンドの構文は次のとおりです。

crypto crlparams *crl_name* **cacert** *ca_cert_filename*

引数は次のとおりです。

- *crl_name*：既存の CRL の名前です。
- *ca_cert_filename*：署名確認に使用する CA 証明書ファイルの名前です。

たとえば、CRL で署名確認を設定するには、次のように入力します。

```
host1/Admin(config)# crypto crlparams CRL1 cacert MYCERT.PEM
```

CRL から署名確認を削除するには、次のように入力します。

```
host1/Admin(config)# no crypto crlparams CRL1
```

SSL 開始用のレイヤ 7 クラス マップの作成

ポリシー マップと関連付けるレイヤ 7 クラス マップは、指定するサーバ ロードバランシング（SLB）の基準を満たすトラフィックのフィルタとして機能します。SSL 開始の場合、一致基準は次の HTTP ロードバランシング属性の形式になります。

- Cookie
- HTTP ヘッダー
- URL
- 送信元 IP アドレス

コンフィギュレーション モードで **class-map type http loadbalance** コマンドを使用して、レイヤ 7 クラス マップを作成できます。レイヤ 7 クラス マップの設定の詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

SSL 開始用のレイヤ 7 ポリシー マップの作成

レイヤ 7 ポリシー マップは、ACE でサーバ ロード バランシングを有効にします。このポリシー マップには、レイヤ 7 クラス マップおよび SSL プロキシ クライアント サービスとの関連付けが含まれます。レイヤ 7 SLB ポリシー マップを使用するには、最初にポリシー マップを作成してから、**match** ステートメントとポリシー アクションを定義します。レイヤ 7 ポリシー マップは子ポリシーであるため、レイヤ 7 ポリシー マップを適切なレイヤ 3 およびレイヤ 4 ポリシー マップに関連付けて、レイヤ 7 SLB トラフィック分類のエントリ ポイントを用意する必要があります。インターフェイスに直接レイヤ 7 ポリシー マップを適用することはできません。レイヤ 3 およびレイヤ 4 ポリシー マップを、1 つのインターフェイスに適用するか、または 1 つのコンテキストのすべてのインターフェイスにグローバルに適用することのみが可能です。

ここでは、次の内容について説明します。

レイヤ 7 ポリシー マップの作成

コンフィギュレーション モードで **policy-map** コマンドを使用して、レイヤ 7 SLB ポリシー マップを作成できます。

このコマンドの構文は次のとおりです。

policy-map type loadbalance first-match *map_name*

次のキーワードと引数があります。

- **type loadbalance** - ロード バランシング ポリシー マップを指定します。
- **first-match** - レイヤ 7 ロード バランシング ポリシー マップの実行を定義します。ACE が実行するのは、最初に一致した分類に指定されているアクションだけです。
- *map_name* - ポリシー マップに割り当てる識別情報。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

たとえば、ポリシー マップ L7SLBPOLICY を作成するには、次のように入力します。

```
host1/Admin(config)# policy-map type loadbalance first-match
L7SLBPOLICY
```

レイヤ 7 ポリシー マップを作成したあと、CLI はポリシー マップ ロードバランシング コンフィギュレーション モードになります。

```
host1/Admin(config-pmap-lb)#
```

既存のポリシー マップを削除するには、次のように入力します。

```
host1/Admin(config)# no policy-map L7SLBPOLICY
```

レイヤ 7 クラス マップとレイヤ 7 ポリシー マップの関連付け

クラス マップとポリシー マップを関連付けるには、ポリシー マップ ロードバランシング コンフィギュレーション モードで **class** コマンドを使用します。

このコマンドの構文は次のとおりです。

class {*name1* | **class-default**} [**insert-before** *name2*]

キーワード、引数、およびオプションは次のとおりです。

- *name1* - トラフィック ポリシーにトラフィックを関連付ける、**class-map** コマンドで設定した定義済みのトラフィック クラス名です。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **class-default** - ACE が作成した予約済みの Well-known クラス マップを指定します。このクラスの削除または変更はできません。指定されたクラス マップで他の一致基準を満たせなかったすべてのトラフィックは、デフォルト トラフィック クラスに割り当てられます。指定された分類がトラフィックと一致しない場合、ACE は、指定されたアクションを **class class-default** コマンドを使用して実行します。**class-default** クラス マップには、すべてのトラフィックと一致する暗黙の **match any** ステートメントがあります。
- **insert-before** *name2* - （任意）ポリシー マップ コンフィギュレーションの *name2* 引数で指定された既存のクラス マップまたは match 文の前に、現在のクラス マップを配置します。ACE では、コンフィギュレーションの一部として順序の並べ替えを保存しません。

たとえば、クラス マップ L7SLBCLASS をポリシー マップと関連付けるには、次のように入力します。

```
host1/Admin(config-pmap-lb)# class L7SLBCLASS
```

クラス マップをポリシー マップに関連付けた後、CLI はポリシー マップ ロード バランシング クラス コンフィギュレーション モードになります。

```
host1/Admin(config-pmap-lb-c)#
```

次の例は、**insert-before** オプションを使用してポリシー マップ内のクラス マップの位置を定義する方法を示しています。

```
host1/Admin(config-pmap-lb)# class L7SLBCLASS insert-before HTTP_CLASS
host1/Admin(config-pmap-lb-c)#
```

次の例は、**class class-default** コマンドの使用方法を示しています。

```
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)#
```

ポリシー マップとクラス マップの関連付けを削除するには、次のように入力します。

```
(config-pmap-lb)# no class L7SLBCLASS
```

レイヤ 7 SLB ポリシー アクションの指定

レイヤ 7 SLB クラス マップをレイヤ 7 SLB ポリシー マップに関連付けたあとで、またはインライン **match** コマンドを指定したあとで、ネットワーク トラフィックがクラス マップまたはインライン **match** コマンドに一致する場合に ACE が実行する必要がある、次のアクションの 1 つまたは複数を指定する必要があります。

- 要求を廃棄する
- ロード バランシングなしで要求を転送する
- HTTP ヘッダー情報を有効にする
- サーバ ファームに対するロード バランシングを有効にする
- スティッキ サーバ ファームを設定する
- パケットの IP DiffServ コード ポイントを指定する
- SSL プロキシ サービスを関連付ける

ここでは、ポリシー マップと SSL プロキシ サービスを関連付ける手順について説明します。追加のポリシー アクションの設定の詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

ポリシー マップ ロードバランシング クラス コンフィギュレーション モードで **ssl-proxy** コマンドを使用して、SSL プロキシ クライアント サービスをポリシー マップと関連付けることができます。

このコマンドの構文は次のとおりです。

ssl-proxy client *name*

name 引数は、既存の SSL プロキシ クライアント サービスの識別情報です。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

たとえば、SSL クライアント プロキシ サービス PSERVICE_CLIENT をクラス マップと関連付けるには、次のように入力します。

```
host1/Admin(config)# policy-map type loadbalance first-match
L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# ssl-proxy client PSERVICE_CLIENT
```

SSL クライアント プロキシ サービスとクラス マップの関連付けを削除するには、次のように入力します。

```
host1/Admin(config-pmap-lb-c)# no ssl-proxy client PSERVICE_CLIENT
```

SSL 開始用のレイヤ 3 およびレイヤ 4 クラス マップの作成

レイヤ 3 およびレイヤ 4 ポリシー マップに関連付けるレイヤ 3 およびレイヤ 4 クラス マップは、指定した基準に一致するトラフィックのフィルタとして機能します。SSL 開始の場合は、次のトラフィック特性の 1 つ以上に基づいて、一致基準を定義できます。

- アクセス リスト
- 仮想 IP アドレス
- 送信元 IP アドレスおよびサブネット マスク
- 宛先 IP アドレスおよびサブネット マスク
- TCP/UDP ポート番号またはポート範囲

コンフィギュレーション モードで **class-map** コマンドを使用して、レイヤ 3 およびレイヤ 4 クラス マップを作成できます。レイヤ 3 およびレイヤ 4 クラス マップの作成および設定の詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

SSL 開始用のレイヤ 3 およびレイヤ 4 ポリシー マップの作成

ユーザが SSL 開始用に作成したレイヤ 3 およびレイヤ 4 ポリシー マップには、ACE がロード バランシングに使用するレイヤ 7 ポリシー マップとの関連付けが含まれています。コンテキスト インターフェイスに直接適用できるのはレイヤ 3 およびレイヤ 4 ポリシー マップのみであるため、レイヤ 3 およびレイヤ 4 クラス マップをレイヤ 7 ポリシー マップに関連付ける必要があります。

ここでは、次の内容について説明します。

- レイヤ 3 およびレイヤ 4 ポリシー マップの作成
- レイヤ 3 およびレイヤ 4 クラス マップとポリシー マップの関連付け
- レイヤ 7 ポリシー マップとクラス マップの関連付け

レイヤ 3 およびレイヤ 4 ポリシー マップの作成

コンフィギュレーション モードで **policy-map** コマンドを使用して、レイヤ 3 およびレイヤ 4 ポリシー マップを作成できます。

このコマンドの構文は次のとおりです。

policy-map multi-match *policy_name*

policy_name 引数は、ポリシー マップに割り当てる名前です。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

たとえば、ポリシー マップ L4SLBPOLICY を作成するには、次のように入力します。

```
host1/Admin(config)# policy-map multi-match L4SLBPOLICY
```

ポリシー マップを作成すると、CLI はポリシー マップ コンフィギュレーション モードになります。

```
host1/Admin(config-pmap)#
```

既存のポリシー マップを削除するには、次のように入力します。

```
host1/Admin(config)# no policy-map L4SLBPOLICY
```

SSL クラス マップとポリシー マップの関連付けの詳細については、「レイヤ 7 クラス マップとレイヤ 7 ポリシー マップの関連付け」の項を参照してください。

レイヤ 3 およびレイヤ 4 クラス マップとポリシー マップの関連付け

ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用して、レイヤ 3 およびレイヤ 4 クラス マップをポリシー マップに関連付けることができます。

このコマンドの構文は次のとおりです。

class *class-map*

class-map 引数は、既存のクラス マップの名前です。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

たとえば、クラス マップ L4SLBCLASS をポリシー マップに関連付けるには、次のように入力します。

```
host1/Admin(config)# policy-map multi-match L4SLBPOLICY
host1/Admin(config-pmap)# class L4SLBCLASS
```

クラス マップをポリシー マップに関連付けた後、CLI はポリシー マップ クラス コンフィギュレーション モードになります。

```
host1/Admin(config-pmap-c)#
```

ポリシー マップとクラス マップの関連付けを削除するには、次のように入力します。

```
host1/Admin(config-pmap)# no class L4SLBCLASS
```

レイヤ 7 ポリシー マップとクラス マップの関連付け

ポリシー マップ クラス コンフィギュレーション モードで **loadbalance** コマンドを使用して、レイヤ 7 ポリシー マップをレイヤ 3 およびレイヤ 4 クラス マップと関連付けることができます。この関連付けでは、ACE がトラフィックに直接適用するレイヤ 3 およびレイヤ 4 ポリシー マップ内にレイヤ 7 ポリシー マップをネストします。

このコマンドの構文は次のとおりです。

loadbalance policy *policymap*

policy *policymap* キーワードおよび引数は、既存のレイヤ 7 ポリシー マップの名前を指定します。最大 64 文字の英数字からなる、引用符で囲まれていない、スペースを含まないテキスト文字列を入力します。

たとえば、レイヤ 7 ポリシー マップ L7SLBPOLICY をクラス マップと関連付けるには、次のように入力します。

```
host1/Admin(config)# policy-map multi-match L4SLBPOLICY
host1/Admin(config-pmap)# class L4SLBCLASS
host1/Admin(config-pmap-c)# loadbalance policy L7SLBPOLICY
```

クラス マップとレイヤ 7 ポリシー マップの関連付けを削除するには、次のように入力します。

```
host1/Admin(config-pmap-c)# no loadbalance policy L7SLBPOLICY
```

VLAN へのポリシー マップの適用

ここでは、VLAN トラフィックにレイヤ 3 およびレイヤ 4 ポリシー マップを適用する方法を説明します。ACE では、ポリシーを現在のコンテキスト内のすべての VLAN にグローバルに適用することも、コンテキスト内の特定の VLAN に適用することもできます。

ここでは、次の内容について説明します。

- ポリシー マップのグローバルな適用
- 特定の VLAN へのポリシー マップの適用

ポリシー マップのグローバルな適用

コンフィギュレーション モードで **service-policy** コマンドを使用して、ポリシー マップをコンテキスト内のすべての VLAN にグローバルに適用できます。

このコマンドの構文は次のとおりです。

service-policy input *policy_name*

policy_name 引数は、既存のポリシー マップの名前です。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

たとえば、ポリシー マップ L4SLBPOLICY をすべてのコンテキスト VLAN にグローバルに適用するには、次のように入力します。

```
host1/Admin(config)# service-policy input L4SLBPOLICY
```

ポリシー マップをすべての VLAN からグローバルに削除するには、次のように入力します。

```
host1/Admin(config)# no service-policy input L4SLBPOLICY
```

特定の VLAN へのポリシー マップの適用

特定の VLAN インターフェイスにポリシー マップを適用するには、コンフィギュレーション モードで **interface** コマンドを使用して、インターフェイス コンフィギュレーション モードにする必要があります。

このコマンドの構文は次のとおりです。

interface vlan *vlan*

vlan 引数は、コンテキスト VLAN 番号です。2 ～ 4094 の整数を入力します。

たとえば、VLAN 10 のインターフェイス コンフィギュレーション モードにするには、次のように入力します。

```
host1/Admin(config)# interface vlan 10
host1/Admin(config-if)#
```

インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用できます。

このコマンドの構文は次のとおりです。

service-policy input *policy-name*

policy-name 引数は、既存のポリシー マップの名前です。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

たとえば、VLAN 10 にポリシー マップ L4SLBPOLICY を適用するには、次のように入力します。

```
host1/Admin(config)# interface vlan 10
host1/Admin(config-if)# service-policy input L4SLBPOLICY
```

インターフェイスからポリシーを削除するには、次のように入力します。

```
host1/Admin(config-if)# no service-policy input L4SLBPOLICY
```

SSL 開始の設定例

次の例は、SSL プロキシ クライアントとして機能し、それ自体と SSL サーバとの間の SSL 接続を開始および維持する ACE の実行コンフィギュレーションを示します。ACE は HTTP クライアントからクリア テキストを受け取り、そのデータを暗号化して、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。この例では、SSL 開始設定は太字で示されています。

IPv6 の例

```
access-list ACL1 line 10 extended permit ip anyv6 anyv6

probe http GEN-HTTP
  port 80
  interval 50
  faildetect 5
  expect status 200 200

serverfarm host SFARM1
  description SERVER FARM 1 FOR SSL INITIATION
  probe GEN_HTTP
  rserver SERVER1 443
    inservice
  rserver SERVER2 443
    inservice
  rserver SERVER3 443
    inservice
  rserver SERVER4 443
    inservice
```

```
serverfarm host SFARM2
  description SERVER FARM 2 FOR SSL TERMINATION
  probe GEN_HTTP
  rserver SERVER5 443
    inservice
  rserver SERVER6 443
    inservice
  rserver SERVER7 443
    inservice
  rserver SERVER8 443
    inservice

parameter-map type http PARAMMAP_HTTP
  server-conn reuse
  case-insensitive
  persistence-rebalance
parameter-map type ssl PARAMMAP_SSL_INITIATION
  cipher RSA_WITH_RC4_128_MD5
  cipher RSA_WITH_RC4_128_SHA
  cipher RSA_WITH_DES_CBC_SHA
  cipher RSA_WITH_3DES_EDE_CBC_SHA
  cipher RSA_WITH_AES_128_CBC_SHA
  cipher RSA_WITH_AES_256_CBC_SHA
  cipher RSA_EXPORT_WITH_RC4_40_MD5
  cipher RSA_EXPORT1024_WITH_RC4_56_MD5
  cipher RSA_EXPORT_WITH_DES40_CBC_SHA
  cipher RSA_EXPORT1024_WITH_DES_CBC_SHA
  cipher RSA_EXPORT1024_WITH_RC4_56_SHA
  version all
parameter-map type connection TCP_PARAM
  syn-data drop
  exceed-mss allow

ssl-proxy service SSL_PSRVICE_CLIENT
  ssl advanced-options PARAMMAP_SSL_INITIATION

class-map type http loadbalance match-all L7_SERVER_CLASS
  description Sticky for SSL Testing
  2 match http url .*.jpg
  3 match source-address 2001:DB8:130::1/64
class-map type http loadbalance match-all L7_SLB-HTTP_CLASS
  2 match http url .*
  3 match source-address 2001:DB8:130::1/64
class-map match-all L4_SSL-INIT_CLASS
  description SSL Initiation VIP
  2 match virtual-address 2001:DB8:130::C tcp eq www
policy-map type loadbalance first-match L7_SSL-INIT_POLICY
```

```
  class L7_SERVER_CLASS
    serverfarm SFARM1
    insert-http SRC_IP header-value "%is"
    insert-http I_AM header-value "SSL_INIT"
    insert-http SRC_Port header-value "%ps"
    insert-http DEST_IP header-value "%id"
    insert-http DEST_Port header-value "%pd"
    ssl-proxy client SSL_PSERVICE_CLIENT
  class L7_SLB-HTTP_CLASS
    serverfarm SFARM2
    insert-http SRC_IP header-value "%is"
    insert-http I_AM header-value "SSL_INIT"
    insert-http DEST_Port header-value "%pd"
    insert-http DEST_IP header-value "%id"
    insert-http SRC_Port header-value "%ps"
    ssl-proxy client SSL_PSERVICE_CLIENT
policy-map multi-match L4_SSL-VIP_POLICY
  class L4_SSL-INIT_CLASS
    loadbalance vip inservice
    loadbalance policy L7_SSL-INIT_POLICY
    loadbalance vip icmp-reply active
    appl-parameter http advanced-options PARAMMAP_HTTP
    connection advanced-options TCP_PARAM

interface vlan 120
  description Upstream VLAN_120 - Clients and VIPs
  ip address 2001:DB8:120::1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  access-group input ACL1
  nat-pool 1 192.168.120.70 192.168.120.80 netmask 255.255.255.0 pat
  service-policy input L4_SSL-VIP_POLICY
  no shutdown
ip route 2001:DB8:1::1/64 2001:DB8:120::200
```

IPv4 の例

```
access-list ACL1 line 10 extended permit ip any any

probe http GEN-HTTP
  port 80
  interval 50
  faildetect 5
  expect status 200 200

serverfarm host SFARM1
  description SERVER FARM 1 FOR SSL INITIATION
  probe GEN_HTTP
```

```
  rserver SERVER1 443
    inservice
  rserver SERVER2 443
    inservice
  rserver SERVER3 443
    inservice
  rserver SERVER4 443
    inservice

serverfarm host SFARM2
  description SERVER FARM 2 FOR SSL TERMINATION
  probe GEN_HTTP
  rserver SERVER5 443
    inservice
  rserver SERVER6 443
    inservice
  rserver SERVER7 443
    inservice
  rserver SERVER8 443
    inservice

parameter-map type http PARAMMAP_HTTP
  server-conn reuse
  case-insensitive
  persistence-rebalance
parameter-map type ssl PARAMMAP_SSL_INITIATION
  cipher RSA_WITH_RC4_128_MD5
  cipher RSA_WITH_RC4_128_SHA
  cipher RSA_WITH_DES_CBC_SHA
  cipher RSA_WITH_3DES_EDE_CBC_SHA
  cipher RSA_WITH_AES_128_CBC_SHA
  cipher RSA_WITH_AES_256_CBC_SHA
  cipher RSA_EXPORT_WITH_RC4_40_MD5
  cipher RSA_EXPORT1024_WITH_RC4_56_MD5
  cipher RSA_EXPORT_WITH_DES40_CBC_SHA
  cipher RSA_EXPORT1024_WITH_DES_CBC_SHA
  cipher RSA_EXPORT1024_WITH_RC4_56_SHA
  version all
parameter-map type connection TCP_PARAM
  syn-data drop
  exceed-mss allow

ssl-proxy service SSL_PSRVICE_CLIENT
  ssl advanced-options PARAMMAP_SSL_INITIATION

class-map type http loadbalance match-all L7_SERVER_CLASS
  description Sticky for SSL Testing
  2 match http url .*.jpg
```

```
  3 match source-address 192.168.130.0 255.255.255.0
class-map type http loadbalance match-all L7_SLB-HTTP_CLASS
  2 match http url .*
  3 match source-address 192.168.130.0 255.255.255.0
class-map match-all L4_SSL-INIT_CLASS
  description SSL Initiation VIP
  2 match virtual-address 192.168.130.12 tcp eq www
policy-map type loadbalance first-match L7_SSL-INIT_POLICY
  class L7_SERVER_CLASS
    serverfarm SFARM1
    insert-http SRC_IP header-value "%is"
    insert-http I_AM header-value "SSL_INIT"
    insert-http SRC_Port header-value "%ps"
    insert-http DEST_IP header-value "%id"
    insert-http DEST_Port header-value "%pd"
    ssl-proxy client SSL_PSERVICE_CLIENT
  class L7_SLB-HTTP_CLASS
    serverfarm SFARM2
    insert-http SRC_IP header-value "%is"
    insert-http I_AM header-value "SSL_INIT"
    insert-http DEST_Port header-value "%pd"
    insert-http DEST_IP header-value "%id"
    insert-http SRC_Port header-value "%ps"
    ssl-proxy client SSL_PSERVICE_CLIENT
policy-map multi-match L4_SSL-VIP_POLICY
  class L4_SSL-INIT_CLASS
    loadbalance vip inservice
    loadbalance policy L7_SSL-INIT_POLICY
    loadbalance vip icmp-reply active
    appl-parameter http advanced-options PARAMMAP_HTTP
    connection advanced-options TCP_PARAM

interface vlan 120
  description Upstream VLAN_120 - Clients and VIPs
  ip address 192.168.120.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  access-group input ACL1
  nat-pool 1 192.168.120.70 192.168.120.80 netmask 255.255.255.0 pat
  service-policy input L4_SSL-VIP_POLICY
  no shutdown
ip route 10.1.0.0 255.255.255.0 192.168.120.254
```