CHAPTER 7

HA でのロード バランシングの設定

この章では、Cisco Mobile Wireless Home Agent でのサーバ ロード バランシングに関する概念と設定の詳細について説明します。

この章は、次の内容で構成されています。

HA サーバ ロード バランシング

HA Server Load Balancing（HA-SLB; HA サーバ ロード バランシング）機能は既存の IOS サーバ ロード バランシング（SLB）機能で構築されます。Server Load Balancing（SLB; サーバ ロード バランシング）によって、ネットワーク サーバのグループ（サーバ ファーム）を単一のサーバ インスタンスとして表示し、サーバへのトラフィックを分散させ、個別のサーバへのトラフィックを制限できます。サーバ ファームを示す単一のサーバ インスタンスは仮想サーバと呼ばれます。サーバ ファームを構成するサーバは実サーバと呼ばれます。

SLB は、実サーバに対するラウンド ロビンなどのメカニズムによってトラフィックを実サーバに配信できます。さらに、Dynamic Feedback Protocol（DFP）を使用して各実サーバのヘルスをモニタリングし、最小ロードを持ったサーバを選択し、アップ状態で稼動しているサーバを選択できます。SLB アーキテクチャの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps5940/products_white_paper0900aecd802921f0.shtml

HA-SLB 機能は Cisco 7600 シリーズ プラットフォームで使用できます。この機能により、Service Application Module for IP（SAMI）でそれぞれ稼動する一連の実 Home Agent（HA）を、Cisco 7600 スーパーバイザに存在する単一の仮想サーバの IP アドレスによって特定できます。

PDSN/FA はユーザの初期登録要求を仮想サーバの IP アドレスに送信します。SUP で稼動する HA-SLB はパケットを代行受信し、登録要求を実 HA の 1 つに転送します。

一般的なコール フローには次のイベント シーケンスがあります。

ステップ 1　PDSN/FA はモバイル IP Registration Request（RRQ; 登録要求）を仮想サーバ IP アドレス（HA-SLB）に転送します。Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバが HA アドレスを PDSN/FA に戻す場合、仮想サーバ IP アドレスのアドレスを戻すよう AAA サーバを設定する必要があります。

ステップ 2　SLB は、サーバ ファームから実サーバ/HA の 1 つを選択し、モバイル IP RRQ をこのサーバに配信します。

ステップ 3　実 HA は Reply で MobileIP RRQ に応答し、メッセージは実 HA から PDSN/FA に送信されます。HA-SLB はこのパケットを代行受信しません。実 HA はバインディングとローカル トンネル エンドポイントを作成します。

ステップ 4　PDSN/FA は、ビジター テーブルとローカル トンネル エンドポイントを作成し、トンネル経由で実 HA から直接トラフィックを送受信します。

ステップ 5　PDSN/FA はライフタイム "0" を含んだモバイル IP RRQ を実 HA に送信してバインディングを終了します。

（注）　パケットは仮想 IP アドレス（HA-SLB）には送信されません。

ステップ 6　実 HA はモバイル IP RRP を PDSN/FA を送信します。HA-SLB はこのパケットを代行受信しません。実 HA は バインディングを終了します。

（注）　モバイル IP メッセージは RFC 2002 には準拠しませんが、draft-kulkarni-mobile-ip-dynamic-ha-assignment-frmwrk-00.txt に準拠します。

HA/SLB 仮想 IP アドレス宛てで、HA アドレス 0.0.0.0 または 255.255.255.255 のある RRQ は、重み付け「ラウンドロビン」、ロード バランシング アルゴリズムを使用して、実際の HA に転送されます。SLB メカニズムは、実サーバのヘルスをロード バランサに伝える機能を実サーバに与える DFP をサポートします。したがって、ロード バランシング アルゴリズムで実サーバの重みを調整します。

MN は、HA から RRP を受信する前に複数の RRQ を送信できるので（最初の RRQ を送信した後 MN の電源を再投入する、MN が最初の登録を複数送信するよう誤って設定されている、または RRP がネットワークによってドロップされる）、同じ MN から着信する登録を追跡することが重要です。これにより同じ MN が複数の HA で登録されるのを防ぐので、これらの HA では IP アドレスと他のリソースが浪費されます。この問題を解決するには、HA-SLB は RRQ を解析し、MN の Network Access Identifier（NAI; ネットワーク アクセス識別子）でインデックス化されたセッション オブジェクトを作成します。このセッション オブジェクトは、RRQ の転送先の実 HA IP アドレスを保存します。同じ MN からの以後の登録は、この同じ実 HA に転送されます。セッション オブジェクトは、設定可能な時間の間（デフォルトは 10 秒）保存されます。HA-SLB がこの時間内に MN からの RRQ を検出しない場合、セッション オブジェクトはクリアされます。HA-SLB が RRQ を検出すると、セッション オブジェクトに関連付けられたタイマーはリセットされます。

リトライ カウンタは各セッション オブジェクトに関連付けられ、ロード バランサによって検出され、再送信された RRQ ごとに増加します。検出された試行回数が設定された「再割り当て」しきい値よりも大きい場合、再送信するセッションは別の実 HA に再び割り当てられ、接続障害がオリジナルの実 HA に対して記録されます。接続障害が検出され、設定されたしきい値に到達すると、実サーバはダウン状態であると見なされ、RRQ を再転送しません。HA-SLB は、設定可能なタイム インターバルの経過後、または実サーバが DFP メッセージを HA-SLB に送信すると、その実サーバへのセッションの転送を再開します。

HA-SLB でのロード バランシング

HA-SLB は、ロード バランシング アルゴリズムの重み付けラウンドロビンを使用します。このアルゴリズムは、仮想サーバへの新しい接続に使用する実サーバを、サーキュラ方式でサーバ ファームから選択するよう指定します。実サーバごとに重み *n* が割り当てられます。仮想サーバに関連付けられた他の実サーバと比較した場合、これは接続を処理する容量を示します。たとえば、実サーバ ServerA（n = 3）、ServerB（n = 1）、ServerC（n = 2）を構成するサーバ ファームがあると想定します。仮想サーバへの最初の 3 つの RRQ は ServerA に、4 番目の RRQ は ServerB に、5 番目と 6 番目の RRQ は ServerC に割り当てられます。

スタティックまたはダイナミックなロード バランシングを実行するよう IOS SLB を設定できます。サーバ ファームの各 HA に重みをスタティックに割り当てることで、スタティック ロード バランシングを実行できます。SLB の DFP マネージャと実 HA の DFP クライアントそれぞれに、DFP を設定することで、ダイナミック ロード バランシングを実行できます。

HA-SLB の動作モード

HA-SLB は 2 つのモード（dispatched モードと Direct（NAT サーバ）モード）で動作します。

dispatched モードでは、仮想サーバ アドレスは HA に通知されます。HA-SLB は Media Access Control（MAC; メディア アクセス制御）レイヤでパケットを単に HA にリダイレクトします。これにより、HA は SLB に隣接するレイヤ 2 でなければいけません。

Direct モードでは、HA-SLB は NAT サーバ モードで動作し、RRQ の宛先 IP アドレスを実サーバの IP アドレスに変更することで、RRQ を HA へルーティングします。この場合、HA は SLB に隣接するレイヤ 2 である必要はありません。

ルータにモバイル IP HA 冗長性を設定するには、次のセクションで説明する手順を実行します。

- 「HA ロード バランシングの設定」（P.7-3）
- 「サーバ ロード バランシングの設定」（P.7-3）

HA ロード バランシングの設定

HA ロード バランシング機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent dynamic-address` *ip address*	登録応答パケットの Home Agent Address フィールドを設定します。Home Agent Address フィールドを *ip address* に設定します。このコマンドは HA で設定されます。

サーバ ロード バランシングの設定

HA でモバイル IP SLB 機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip slb vserver` *name* `Router(config-slb-vserver)# virtual` *ip address* `udp 434 service` *ipmobile*	モバイル IP SLB 機能をイネーブルにします。*ip address* は、PDSN/FA からの登録要求の送信先である仮想 HA のアドレスです。これは、SLB スーパーバイザで設定されます。

HA-SLB の設定例

次に、設定の詳細の検証方法を含めた、さまざまな HA-SLB 設定を示します。

スタティックな重みが設定された dispatched モード

SLB での設定：

次のコマンドは、サーバ ファーム "HAFARM" を設定し、2 つの実サーバ（HA）とサーバ ファームを関連付けます。実サーバにはスタティックな重みが設定されます。

```
ip slb serverfarm HAFARM
 real 10.1.1.51
  weight 1
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice
```

次のコマンドは、SLB の "ipmobile" としてのサービスを仮想サーバに設定し、サーバ ファーム "HAFARM" と仮想サーバを関連付けます。任意で、**idle ipmobile request** *idle-time-val* コマンドは、セッション オブジェクトが存在する期間を設定します。

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

HA での設定

次のコマンドは、HA にループバック アドレスとして仮想サーバ アドレスを設定します。この設定は、dispatched モードにだけ必要です。

```
interface Loopback1
ip address 10.1.1.10 255.255.255.0
```

次のコマンドは、実 HA のアドレスに対して、RRP の送信元アドレスおよび HA address フィールドを設定します。この設定は、dispatched モードにだけ必要です。

```
ip mobile home-agent dynamic-address 10.1.1.51
```

SLB での出力表示：

次のコマンドは、サーバ ファーム "HAFARM" のステータス、関連付けられた実サーバ、およびそのステータスを示します。各実サーバに割り当てられた接続の数も示します。

次の出力表示は、HA-SLB が 2 つの実 HA（HA ごとに 2 の接続）上で等しくロード バランシングした、4 つの MIP セッションを開始した後に取得されました。

```
SLB-7600#show ip slb reals

real                 farm name        weight  state          conns
-------------------------------------------------------------------
20.1.1.51            HAFARM           1       OPERATIONAL    2
20.1.1.52            HAFARM           1       OPERATIONAL    2
```

次のコマンドは、実行時またはセッション オブジェクトが存在する場合のセッションをすべて表示します。

```
SLB-7600#show ip slb sessions ipmobile

vserver         NAI hash           client             real                       state
-------------------------------------------------------------------------------------
-
MIPSLB          A984DF0A00000000 15.1.1.51      20.1.1.52              IPMOBILE_ESTAB
MIPSLB          1DC0E31400000000 15.1.1.51       20.1.1.52              IPMOBILE_ESTAB
MIPSLB          2BDEE91100000000 15.1.1.51       20.1.1.51              IPMOBILE_ESTAB
MIPSLB          47E2FD1B00000000 15.1.1.51       20.1.1.51              IPMOBILE_ESTAB
SLB-7600#
```

HA での出力表示：

次のコマンドは、HA1 および HA2 で開始していた 2 つのバインディングを示します。

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7600#
```

DFP を使用した dispatched モード

SLB での設定：

次のコマンドは、サーバ ファーム "HAFAR" を設定し、2 つの実サーバ（HA）とサーバ ファームを関連付けます。

```
ip slb serverfarm HAFARM
 real 10.1.1.51
  inservice
 !
 real 10.1.1.52
  inservice
!
```

次のコマンドは、SLB の "ipmobile" としてのサービスを仮想サーバに設定し、サーバ ファーム HAFARM と仮想サーバを関連付けます。次の任意の idle ipmobile request *idle-time-val* コマンドは、セッション オブジェクトが存在する期間を設定します。

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

次のコマンドは、HA-SLB に DFP マネージャを設定し、HA-SLB の接続先の 2 つの DFP エージェント（クライアント）を割り当てます。

```
ip slb dfp
 agent 10.1.1.51 500
 agent 10.1.1.52 500
!
```

HA での設定

次のコマンドは、HA にループバック アドレスとして仮想サーバ アドレスを設定します。この設定は、dispatched モードにだけ必要です。

```
interface Loopback1
ip address 10.1.1.10 255.255.255.0
!
```

次のコマンドは、実 HA に DFP エージェントを設定します。ここで設定されたポート番号は DFP マネージャで指定されたポート番号と一致する必要があります。

```
ip dfp agent ipmobile
 port 500
 inservice
!
```

次のコマンドは、実 HA のアドレスに対して、RRP の送信元アドレスおよび HA address フィールドを設定します。この設定は、dispatched モードにだけ必要です。

```
ip mobile home-agent dynamic-address 10.1.1.51
```

SLB での出力表示：

次のコマンドは、DFP の設定時に HA が最初の重み 25（デフォルトの重み）を報告することを検証します。

```
SLB-7600#show ip slb dfp weights
   Real IP Address: 10.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.51:500 at 14:59:23 UTC 04/21/03
   Real IP Address: 10.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-7600#
```

次のコマンドは、サーバ ファーム HAFARM のステータス、関連付けられた実サーバ、およびそのステータスを示します。各実サーバに割り当てられた接続の数も示します。

次の出力表示は、HA-SLB が 2 つの実 HA（HA ごとに 50 の接続）上で等しくロード バランシングした、100 の MIP セッションを開始した後に取得されました。

```
SLB-7600#show ip slb reals

real                  farm name        weight  state          conns
--------------------------------------------------------------------
10.1.1.51             HAFARM           24      OPERATIONAL    50
10.1.1.52             HAFARM           24      OPERATIONAL    50
SLB-7600#
```

HA での出力表示：

次のコマンドは、HA1 および HA2 で開始していた 50 のバインディングを検証します。

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7600#
```

現在、バインディングの数とメモリ使用量は、HA-SLB のロード バランシングを計算するためのものと見なされます。各実サーバ（HA）の frequency of calls per second（CPS; 秒単位のコールの周波数）およびスループット パラメータを考慮することで、既存の DFP の重み計算式を修正できます。

毎分計算された HA での CPS は Usage CPS と呼ばれ、HA が処理できる最大値の一部（使用可能な CPS）に設定できます。Usage CPS が使用可能な CPS に到達したら、HA 実サーバは低い重みを SLB に戻します。

ルータでスループットを計算することは困難です。これはパケット処理のための割り込み CPU を使用することで解決できます。

上記の 2 つのパラメータから次の式が得られます。

dfp_weight = （Maxbindings – NumberofBindings）×（cpu+mem）×
（Available cps – Usage cps）× dftp_max_weight ÷（Maxbindings × 32 × Available cps）

（注） 現在、メトリックを含んだ MIB アイテムは使用できません。

スタティックな重みが設定された Direct モード

SLB での設定：

次のコマンドは、サーバ ファーム "HAFARM" を設定し、2 つの実サーバ（HA）とサーバ ファームを関連付けます。実サーバにはスタティックな重みが設定されます。**nat server** コマンドは、HA-SLB を動作の Direct（NAT サーバ）モードに設定します。

```
ip slb serverfarm HAFARM
nat server
real 10.1.1.51
  weight 1
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice

ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

SLB での出力表示：

次に、サーバ ファーム HAFARM のステータス、関連付けられた実サーバ、およびそのステータスの例を示します。各実サーバに割り当てられた接続の数も示します。

次の出力表示は、HA-SLB が 2 つの実 HA（HA ごとに 2 つの接続）上で等しくロード バランシングした、4 つの MIP セッションを開始した後に取得されました。

```
SLB-7600#show ip slb reals

real                 farm name        weight  state          conns
-------------------------------------------------------------------
10.1.1.51            HAFARM           1       OPERATIONAL    2
10.1.1.52            HAFARM           1       OPERATIONAL    2
```

次のコマンドは、実行時またはセッション オブジェクトが存在する場合のセッションをすべて表示します。

```
SLB-7600#show ip slb sessions ipmobile

vserver         NAI hash         client          real                    state
------------------------------------------------------------------------------
MIPSLB          A984DF0A00000000 15.1.1.51       10.1.1.52               IPMOBILE_ESTAB
MIPSLB          1DC0E31400000000 15.1.1.51       10.1.1.52               IPMOBILE_ESTAB
MIPSLB          2BDEE91100000000 15.1.1.51       10.1.1.51               IPMOBILE_ESTAB
MIPSLB          47E2FD1B00000000 15.1.1.51       10.1.1.51               IPMOBILE_ESTAB

SLB-7600#
```

HA での出力表示：

次に、HA1 および HA2 で開始していた 2 つのバインディングの例を示します。

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7600#
```

イネーブルである次のデバッグは、NAT サーバ モードが動作中であることを示します。

```
SLB-7600#debug ip slb sessions ipmobile
SLB-7600#
*Apr 21 15:25:58: %SYS-5-CONFIG_I: Configured from console by console
*Apr 21 15:26:03: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwts-mip-np-user1@ispxyz.com, length: 28
*Apr 21 15:26:03: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:26:03: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 10.1.1.51, NAT= S
*Apr 21 15:26:03: SLB_SESSION: client= 15.1.1.51:434 session_key= 47E2FD1B00000000
SLB-7600#
```

DFP を使用した Direct モード

SLB での設定：

次のコマンドは、サーバ ファーム "HAFARM" を設定し、2 つの実サーバ（HA）とサーバ ファームを関連付けます。**nat server** コマンドは、HA-SLB を動作の Direct（NAT サーバ）モードに設定します。

```
ip slb serverfarm HAFARM
nat server
real 10.1.1.51
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice
!
```

次のコマンドは、SLB の "ipmobile" としてのサービスを仮想サーバに設定し、サーバ ファーム HAFARM と仮想サーバを関連付けます。任意の **idle ipmobile request** *idle-time-val* コマンドは、セッション オブジェクトが存在する期間を設定します。

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
!
```

次のコマンドは、HA-SLB に DFP マネージャを設定し、HA-SLB の接続先の 2 つの DFP エージェント（クライアント）を割り当てます。

```
ip slb dfp
 agent 10.1.1.51 500
 agent 10.1.1.52 500
```

HA での設定

次のコマンドは、実 HA に DFP エージェントを設定します。設定されたポート番号は DFP マネージャで指定されたポート番号と一致する必要があります。

```
ip dfp agent ipmobile
 port 500
 inservice
!
```

SLB での出力表示：

次のコマンドは、DFP の設定時に HA が最初の重み 25（デフォルトの重み）を報告することを検証します。

```
SLB-7600#show ip slb dfp weights
   Real IP Address: 10.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.51:500 at 14:59:23 UTC 04/21/03
   Real IP Address: 10.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-7600#
```

次のコマンドは、サーバ ファーム "HAFARM" のステータス、関連付けられた実サーバ、およびそのステータスを示します。各実サーバに割り当てられた接続の数も示します。

次の出力表示は、HA-SLB が 2 つの実 HA（HA ごとに 50 の接続）上で等しくロード バランシングした、100 の MIP セッションを開始した後に取得されました。

```
SLB-7600#show ip slb reals

real                 farm name        weight  state          conns
-------------------------------------------------------------------
10.1.1.51            HAFARM           24      OPERATIONAL    50
10.1.1.52            HAFARM           24      OPERATIONAL    50
SLB-7600#
```

HA での出力表示：

次のコマンドは、HA1 および HA2 で開始していた 50 のバインディングを示します。

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7600#
```

イネーブルである次のデバッグは、NAT サーバ モードが動作中であることを示します。

```
SLB-7600#debug ip slb sessions ipmobile
SLB-7600#
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 10.1.1.51, NAI:
mwts-mip-np-user1@ispxyz.com, length: 28
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:47:16: SLB_SESSION: v_ip= 10.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 10.1.1.51:434 session_key= 47E2FD1B00000000
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwts-mip-np-user2@ispxyz.com, length: 28
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:47:16: SLB_SESSION: v_ip= 10.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 10.1.1.51:434 session_key= 1DC0E31400000000
```

動作の Direct モードおよび暗号転送モードが Tunnel である場合

```
Configuration on SLB:
ip slb serverfarm FARM1
 nat server
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 15.1.1.10 udp 434 service ipmobile
 serverfarm FARM1
 inservice
```

次のコマンドは、HA-SLB で IPSEC を設定します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.51
 set transform-set esp-des-sha-transport
 match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,15,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2       (outside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
```

```
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
!
interface Vlan15
 ip address 10.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 10.1.1.10 host 10.1.1.51
```

PDSN での設定：

```
The following commands configure IPSEC on PDSN:
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 10.1.1.51 host 10.1.1.10
```

clear crypto isakmp および **clear crypto sa** を PDSN および SLB で実行します。複数の MIP フローを開きます。

PDSN での出力表示：

次のコマンドを使用して、PDSN から送信されたパケットが暗号化されているか確認します。

```
PDSN-7600#sh crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0
```

```
     local crypto endpt.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
     path mtu 1500, media mtu 1500
     current outbound spi: 1A274E9D

     inbound esp sas:
      spi: 0xD3D5F08B(3554013323)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3026)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0x7FEE86C3(2146338499)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3026)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1A274E9D(438783645)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3026)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0x5F9A83(6265475)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3026)
        replay detection support: Y

     outbound pcp sas:


PDSN-7600#
```

SLB での出力表示：

次のコマンドを使用して、HA-SLB が受信したパケットが復号化されているか確認します。

```
SLB1-7600#sh crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 15.1.1.51
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

```
      local crypto endpt.: 15.1.1.15, remote crypto endpt.: 10.1.1.51
      path mtu 1500, media mtu 1500
      current outbound spi: D6C550E1

      inbound esp sas:
       spi: 0x267FCD46(645909830)
         transform: esp-des ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 11027, flow_id: 63, crypto map: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4607999/3581)
         IV size: 8 bytes
         replay detection support: Y

      inbound ah sas:
       spi: 0xF779A01E(4151943198)
         transform: ah-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 11025, flow_id: 63, crypto map: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4607999/3581)
         replay detection support: Y

      inbound pcp sas:

      outbound esp sas:
       spi: 0xD6C550E1(3603255521)
         transform: esp-des ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 11028, flow_id: 64, crypto map: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4608000/3581)
         IV size: 8 bytes
         replay detection support: Y

      outbound ah sas:
       spi: 0x325BEB84(844884868)
         transform: ah-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 11026, flow_id: 64, crypto map: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4608000/3581)
         replay detection support: Y

      outbound pcp sas:

SLB1-7600#sh ip slb sessions ipmobile

vserver         NAI hash         client          real                  state
-------------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       10.99.11.12           IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       10.99.11.12           IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       10.99.11.11           IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       10.99.11.11           IPMOBILE_ESTAB
SLB1-7600#
SLB1-7600#sh ip slb
SLB1-7600#sh ip slb rea
SLB1-7600#sh ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
10.99.11.11           FARM1            1       OPERATIONAL    2
10.99.11.12           FARM1            1       OPERATIONAL    2
SLB1-7600

Show output on SLB:
HA5-2#sh ip mob binding summary
```

```
Mobility Binding List:
Total 2
HA5-2#

HA5-3#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```

SLB でのデバッグの出力：

イネーブルである次のデバッグは、NAT サーバ モードが動作中であることを示します。

```
SLB1-7600#debug ip slb sessions ipmobile
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
*Jul  1 05:25:25.513: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 99.99.11.12, NAT= S
*Jul  1 05:25:25.513: SLB_SESSION: client= 15.1.1.51:434 session_key= A984DF0A00000000
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
*Jul  1 05:25:25.513: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 99.99.11.11, NAT= S
*Jul  1 05:25:25.513: SLB_SESSION: client= 15.1.1.51:434 session_key= 2BDEE91100000000
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
```

動作の Direct モードおよび暗号転送モードが Transport である場合

SLB での設定：

```
ip slb serverfarm FARM1
 nat server
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm FARM1
 inservice
```

次のコマンドは、HA-SLB で IPSEC を設定します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
 mode transport    (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.51
 set transform-set esp-des-sha-transport
 match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,15,1002-1005
```

```
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2       (outside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
!
interface Vlan15
 ip address 15.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 15.1.1.10 host 15.1.1.51
```

PDSN での設定：

次のコマンドは、PDSN で IPSEC を設定します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport           (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 15.1.1.51 host 15.1.1.10
```

clear crypto isakmp および **clear crypto sa** を PDSN および SLB で実行します。複数の MIP フローを開きます。

PDSN での出力表示：

次のコマンドを使用して、PDSN から送信されたパケットが暗号化されているか確認します。

```
PDSN-7600#sh crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
     path mtu 1500, media mtu 1500
     current outbound spi: 6A0EBD82

     inbound esp sas:
      spi: 0x13E0E556(333505878)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3535)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0xEFEEE153(4025409875)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3535)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6A0EBD82(1779350914)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3535)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0x49BE92A3(1237226147)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3535)
        replay detection support: Y

     outbound pcp sas:


PDSN-7600#
```

SLB での出力表示：

```
SLB1-7600#sh ip slb sessions ipmobile

vserver         NAI hash         client          real                  state
-------------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       99.99.11.12           IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       99.99.11.12           IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       99.99.11.11           IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       99.99.11.11           IPMOBILE_ESTAB
SLB1-7600#
SLB1-7600#sh ip slb rea
SLB1-7600#sh ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
99.99.11.11           FARM1            1       OPERATIONAL    2
99.99.11.12           FARM1            1       OPERATIONAL    2
SLB1-7600#
SLB1-7600#
```

次のコマンドを使用して、HA-SLB が受信したパケットが復号化されているか確認します。

```
SLB1-7600#sh crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 10.1.1.51
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 15.1.1.15, remote crypto endpt.: 15.1.1.51
     path mtu 1500, media mtu 1500
     current outbound spi: 13E0E556

     inbound esp sas:
      spi: 0x6A0EBD82(1779350914)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11031, flow_id: 65, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3527)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0x49BE92A3(1237226147)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11029, flow_id: 65, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3527)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x13E0E556(333505878)
        transform: esp-des ,
```

```
        in use settings ={Tunnel, }
        slot: 0, conn id: 11032, flow_id: 66, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3527)
        IV size: 8 bytes
        replay detection support: Y

      outbound ah sas:
       spi: 0xEFEEE153(4025409875)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11030, flow_id: 66, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3524)
        replay detection support: Y

      outbound pcp sas:


SLB1-7600#
```

HA での出力表示：

```
HA5-2#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-2#

HA5-3#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```