CHAPTER 10

HA のセキュリティ

セキュリティ

この章では、Cisco IOS Mobile Wireless Home Agent ソフトウェアのセキュリティ機能における各種コンセプトについて説明します。

この章の内容は、次のとおりです。

- 3 DES 暗号化（p.10-1）
- モバイル IP の IPSec（p.10-1）
- 6 CPU SAMI 搭載 Cisco 7600 での IPSec サポート（p.10-6）
- 制約事項（p.10-7）
- 設定例（p.10-9）

3 DES 暗号化

Cisco Home Agent（HA）には、HA 上で IPSec をサポートする 3DES 暗号化が統合されています。Cisco 7600 プラットフォーム上では、SAMI は Cisco VPN-SPA IPSec アクセラレーション カードを使用します。

HA では、PDSN と HA 間にモバイル IP データ トラフィック トンネルを確立する前に、各 PDSN のパラメータを設定する必要があります。

（注） この機能の使用は、ハードウェアのサポートに限定されます。

（注） この機能を使用できるのは、Cisco 7200 および 7301 ルータのプラットフォームだけです。

モバイル IP の IPSec

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）は、加入ピア間にデータ機密保持、データ整合性、およびデータ認証を提供する IP Security（IPSec）と呼ばれるオープン標準フレームワークを開発しました。IPSec は、IP レイヤでこれらのセキュリティ サービスを提供し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）を使用して、ローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションを処理し、IPSec で使用する暗号化および認証キーを生成します。IPSec を使用することにより、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイとホスト間の 1 つ以上のデータ フローを保護できます。

HA は、スタティックに設定された任意の共有秘密を使用して、モバイル IP レジストレーション メッセージ内の認証拡張を処理します。

HA は、IS-835-B の要求に基づいて、IPSec、IKE、Authentication Header（AH; 認証ヘッダー）、および IP Encapsulating Security Payload（ESP）をサポートしています。

IS835-B は、IPSec セキュリティの提供において、3 つのメカニズムを指定しています。

- 証明書
- ダイナミックに分散された事前共有秘密
- スタティックに設定された事前共有秘密

（注）　Cisco IOS IPSec 機能は、Cisco 7600 スイッチ プラットフォーム上で使用できます。HA 2.0（以上）のリリースは、IPSec IKE について、スタティックに設定された事前共有秘密だけをサポートしています。

IS-835-B に規定されているように、HA および AAA には、PDSN の同じセキュリティ レベルを設定する必要があります。PDSN は、AAA サーバからセキュリティ レベルを受信して IKE を開始します。HA は、IKE 要求に応答して、セキュリティ ポリシーを確立します。

PDSN が AAA サーバからセキュリティ レベルを受信して IKE を開始すると、HA は IKE 要求に応答して、セキュリティ ポリシーを確立します。クリプト コンフィギュレーションのアクセスリストに指定されているすべてのトラフィックが、IPSec トンネルによって保護されます。アクセスリストは、PDSN と HA 間のすべてのトラフィックが保護されるように設定します。指定した PDSN/HA ペアに属すすべてのバインディングが保護されます。

IPSec は、コロケーション COA を使用するモバイルには適用されません。

（注）　Cisco 7600 プラットフォーム上の Cisco Home Agent Release 2.0（以上）には、Catalyst 7600 ルータ上で実行するブレードとして、Cisco IPSec Services Module（VPN-SPA）のサポートが必要です。VPN-SPA には、物理的な WAN または LAN インターフェイスはありません。VPN ポリシー用の VLAN セレクタが使用されます。Cisco 7600 インターネット ルータの詳細については、次の URL を参照してください：
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_installation_guides_list.html

IPSec ベースのセキュリティは、ホーム AAA サーバから受信するパラメータに応じて、PDSN と HA 間のトンネルに適用できます。各 PDSN/HA ペア間に、1 つのトンネルを確立できます。PDSN/HA ペア間の単一トンネルでは、3 種類のトラフィック ストリームを使用できます。コントロール メッセージ、IP-in-IP カプセル化データ、および GRE-in-IP カプセル化データです。トンネルを通過するすべてのトラフィックに、IPSec による同レベルの保護が適用されます。

IS835 には、RFC 2002 に基づくモバイル IP サービスが定義されています。Cisco HA は、モバイル IP サービスおよびプロキシ モバイル IP サービスを提供します。

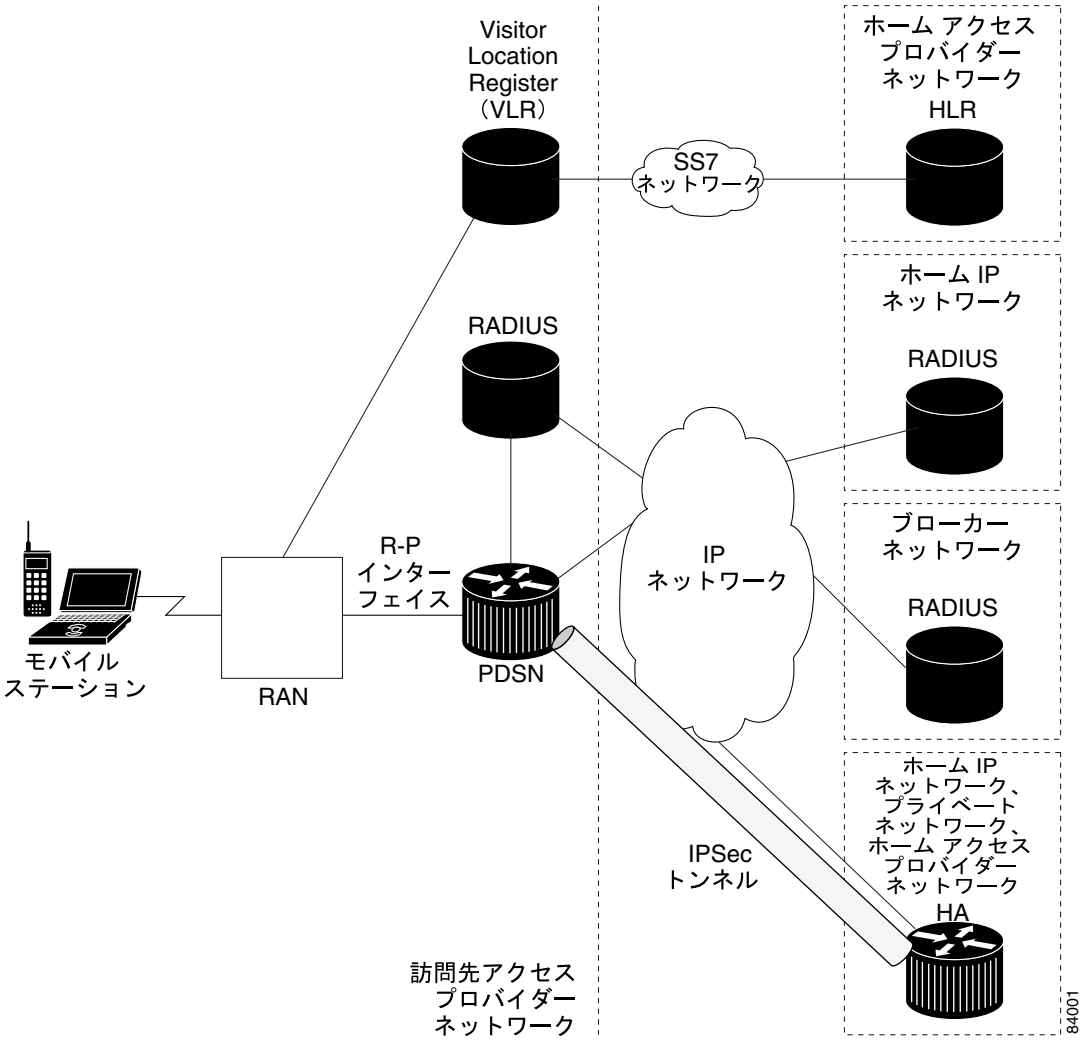
プロキシ モバイル サービスでは、Mobile-Node（MN; モバイル ノード）は簡易 IP によって PDSN/FA に接続し、PDSN/FA が HA への MN のモバイル IP プロキシとして動作します。

Security Association（SA; セキュリティ アソシエーションまたはトンネル）は、一度確立されると、トンネルにトラフィックが存在しなくなるか、SA のライフタイムが期限切れになるまで、アクティブとして存続します。

（注）　IPSec SA は、フェールオーバー時にスタンバイに複製されないので、IPSec は HA 冗長設定とは併用できません。

図 10-1 に、IS835 の IPSec ネットワーク トポロジを示します。

図 10-1　IS835 IPSec ネットワーク



PDSN と HA 間の IPSec 相互運用性（IS-835-C）

IS-835C に基づく IPSec ルールでは、接続は常に PDSN から HA の IP アドレスに対して開始される必要があります。一部の PDSN は、IPSec コンフィギュレーションに柔軟に対応していません。これらの PDSN では、リモート IPSec の終端地点が常に HA の IP アドレスである場合を除き、リモート IPSec 終端地点のコンフィギュレーションを適用できません。

次のセクションでは、Home Agent Release 2.0 以上を使用する場合の、これらの PDSN と HA 間の IPSec 相互運用性の対処方法について説明します。

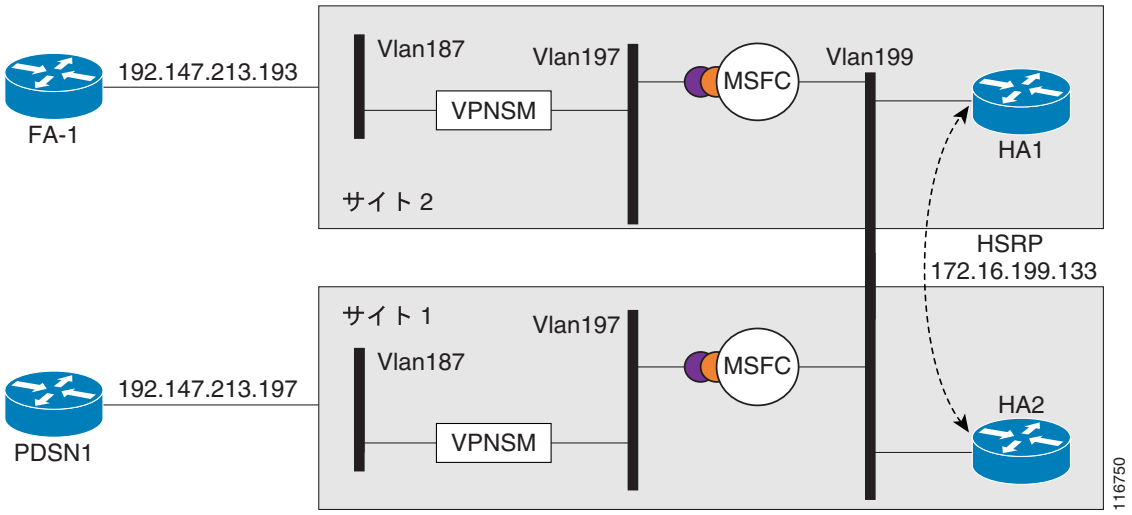
コンフィギュレーションの変更により、HA の IP アドレスへの IPSec 接続と、VPNSM による終端が可能になります。

単一 HA インスタンスの処理

このソリューションでは、SUP IOS に同じ HA IP アドレスを割り当てます。HA へのトラフィックは、ポリシーにより、正しい HA にルーティングされます。

図 10-2 に、実現可能なコンフィギュレーションを示します。

図 10-2　単一 HA の相互運用性



次に、スーパーバイザのコンフィギュレーション例を示します。PDSN の IP アドレスは 14.0.0.1、HA3 のアドレスは 13.0.0.50、HA4 のアドレスは 13.0.0.51 です。

単一 HA インスタンスの相互運用性

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 60000
crypto isakmp key cisco address 10.0.0.0 0.0.0.0
!
crypto ipsec transform-set mobile-set1 esp-3des

# Comment: testmap is used for HA3

crypto map testmap local-address Loopback21
crypto map testmap 20 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set mobile-set1
 match address 131
!

interface Loopback21
 description corresponds to ha-on-proc3
 ip address 10.0.0.50 255.255.255.255
!

interface GigabitEthernet4/1
description encrypt traffic from vlan 151 to vlan 201& 136 to 139
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,136,146,151,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet4/2
 description decrypts traffic from vlan 201 to 151, 139 to 136
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,139,149,201,1002-1005
 switchport mode trunk
 cdp enable

interface Vlan136
 description secure vlan
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap
!
interface Vlan137
 description internal vlan to HA3
 ip address 10.0.0.1 255.255.0.0
!
interface Vlan139
 no ip address
 crypto connect vlan 136
!

access-list 131 permit ip host 10.0.0.1 host 10.0.0.50
access-list 131 permit ip host 10.0.0.50 host 10.0.0.1
access-list 131 permit ip 10.0.0.0 0.0.0.255 10.0.0.0 0.0.0.255

access-list 2000 permit udp any any eq mobile-ip
```

```
access-list 2000 permit ipinip any any

route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.2
!
```

6 CPU SAMI 搭載 Cisco 7600 での IPSec サポート

PDSN と HA 間のモバイル IP トンネル上に、IPSec トンネルの確立が必要になることがあります。PDSN は外部ネットワークに、HA はホーム ネットワークに常駐します。IS-835B 仕様に基づいて、IPSec 接続は常に PDSN から HA に対して開始します。したがって、IPSec トンネルのエンドポイントは、PDSN IP アドレスおよび HA IP アドレスです。

Cisco 7600 HA ソリューションでは、IPSec は SUP で終端しますが、実際の HA アプリケーションは 1 枚以上の SAMI カード上に常駐します。各 SAMI カードには 6 つの CPU があり、それぞれ 1 つの HA インスタンスを実行します。各 HA に、独自の IP アドレスがあります。IPSec エンドポイントである SUP と HA エンドポイントである SAMI の IP アドレスが異なる場合には、HA IP アドレスの PDSN によって生成された IKE メッセージは、SUP でドロップされます。

この問題を回避するには、SAMI 上に設定されている HA IP アドレスと同じ IP アドレスを SUP に使用させる必要があります。そのためには、各 PDSN/HA ペアが正しく処理されるように、異なる HA IP アドレス宛ての IPSec トラフィックを、異なる IPSec VLAN に割り当てます。このコンフィギュレーションにより、HA アプリケーションを実行する SAMI 上の 6 つのすべての CPU をサポートし、それぞれに IPSec エンドポイントとなる独自の IP アドレスを設定できます。

この場合、SUP720 上で VRF IPSec 機能を使用します。PDSN から発信されたトラフィックはすべて、HA IP アドレスに基づいて異なる VLAN に割り当てられます。各 VLAN は 1 つの VRF に対応し、SUP 上の各 HA インスタンスに 1 つの VRF が存在します。つまり、IPSec の VRF モードにより、トラフィックは SAMI 上の 6 つの異なる HA インスタンスにそれぞれ分類されます。パケットは、クリプト VLAN によって復号化されると、特定の HA に対応する内部 VLAN のポリシーに基づいて、SAMI 上の正しい HA CPU にルーティングされます。

この場合、複数のシャーシ間および単一シャーシ内での IPSec 冗長設定がサポートされます。

この動作のコール フローは、次のとおりです。

1. SUP 上で、PDSN と HA IP アドレスの各ペア間の IPSec SA が開始されます。PDSN から、PDSN IP アドレスと、特定の HA IP アドレスであるピア IP アドレスを持つ IKE メッセージが送信されます。IKE メッセージ内の PDSN IP アドレスと HA IP アドレスに基づいて、PDSN/HA ペア用の正しい ISAKMP プロファイルが選択され、各ペアに対応する VRF が指示されます。これにより、PDSN/HA ペアに対応する個別の SPI が確立されます。
2. HA IP アドレス単位で 1 つの VLAN が定義され、SUP 上のそのアドレス用に定義された VRF に割り当てられます。したがって、SUP は、PDSN の IPSec 終端地点となる HA IP アドレスを所有します。
3. 各 PDSN/HA IP アドレス ペア間に IPSec SA が確立されると、入力パケットの SPI に基づいて、暗号化パケットが正しい VRF に割り当てられます。
4. 暗号化パケットは、HA アドレスに対応する IPSec VLAN で復号化されると、SUP と MWAM 上の HA インスタンス間の内部 VLAN を使用して、HA IP アドレスをホスティングしている MWAM カード上の対応する CPU にポリシー ルーティングされます。
5. リターン パスでは、SAMI 上の HA インスタンスからのパケットが内部 VLAN に渡され、その HA に対応する IPSec VLAN に割り当てられます。これにより、パケットが暗号化され、出力インターフェイスを通じて PDSN に送出されます。

制約事項

同時バインディング

Cisco HA は、同時バインディングをサポートしていません。同じ NAI に複数のフローが確立されると、各フローに異なる IP アドレスが割り当てられます。つまり、同時バインディングは不要です。同時バインディングは、同じ IP アドレスへの複数のフローを維持する場合に使用されるからです。

セキュリティ

HA は、IS-835-B の要件に基づいて、IPSec、IKE、IPSec AH、および IP ESP をサポートしています。HA は、制御トラフィック用またはユーザ トラフィック用の個別のセキュリティはサポートしていません。両方のセキュリティを有効にするか無効にするかのどちらかです。

HA は、IS-835-B に定義されているダイナミックな鍵の割り当て、または共有秘密はサポートしていません。

モバイル IP SA の設定

モバイル ホスト、Foreign Agent（FA; 外部エージェント）、および HA の SA を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **ip mobile secure** {**host** | **visitor** | **home-agent** | **foreign-agent** | **proxy-host**} {*lower-address* [*upper-address*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key** {**hex** | **ascii**} *string* [**replay timestamp** [*number*] **algorithm md5 mode prefix-suffix**]	IP モバイル ユーザの SA を指定します。

HA の IPSec の設定

HA の IPSec を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp** **set peer** *ip address of ha* **set transform-set** transform-set-name **match address** *acl name* **crypto map** *map name* **local-address** *interface*	1 つのクリプトマップ セットに 1 つの HA のクリプト マップ エントリを作成します。 クリプト マップの定義を完了するには： **1.** 関連する ACL を定義します。 **2.** クリプト　マップをインターフェイスに割り当てます。1 つのクリプト マップ セットで、各 HA に個別のシーケンス番号を使用することにより、複数の HA のクリプト マップを設定できます。 IPSec トラフィックのクリプト マップに使用するインターフェイスを識別し、名前を指定します。
ステップ 2	Router# **access-list** *acl-name* **deny udp host** *HA IP addr* **eq mobile-ip host** *PDSN IP addr* **eq mobile-ip** **access-list** *acl-name* **permit ip host** *PDSN IP addr* **host** *HA IP addr* **access-list** *acl-name* **deny ip any any**	アクセス リストを定義します。 「acl-name」に、クリプト マップの設定と同じ ACL 名を指定します。
ステップ 3	Router# **Interface** *Physical-Interface of PI interface* **crypto map** *Crypto-Map set*	Pi インターフェイスにクリプト マップを割り当てます。HA は、このインターフェイス上で、PDSN 間とのモバイル IP トラフィックを送受信します。

アクティブ / スタンバイ HA SA の作成

アクティブ / スタンバイ HA SA を表示するには、次の IOS コマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)#**show ip mobile secure ?** **foreign-agent** **home-agent** **host** **summary**	アクティブおよびスタンバイの HA SA を表示します。 FA の SA を表示します。HA の SA を表示します。モバイル ホストの SA を表示します。SA の要約を表示します。

次に、このコマンドの例を示します。

```
Router# show ip mobile secure home-agent
Security Associations (algorithm,mode,replay protection,key):
30.0.0.30:
   SPI 100,  MD5, Prefix-suffix, Timestamp +/- 7,
   Key 'red'
HA#
```

設定例

HA の IPSec 設定

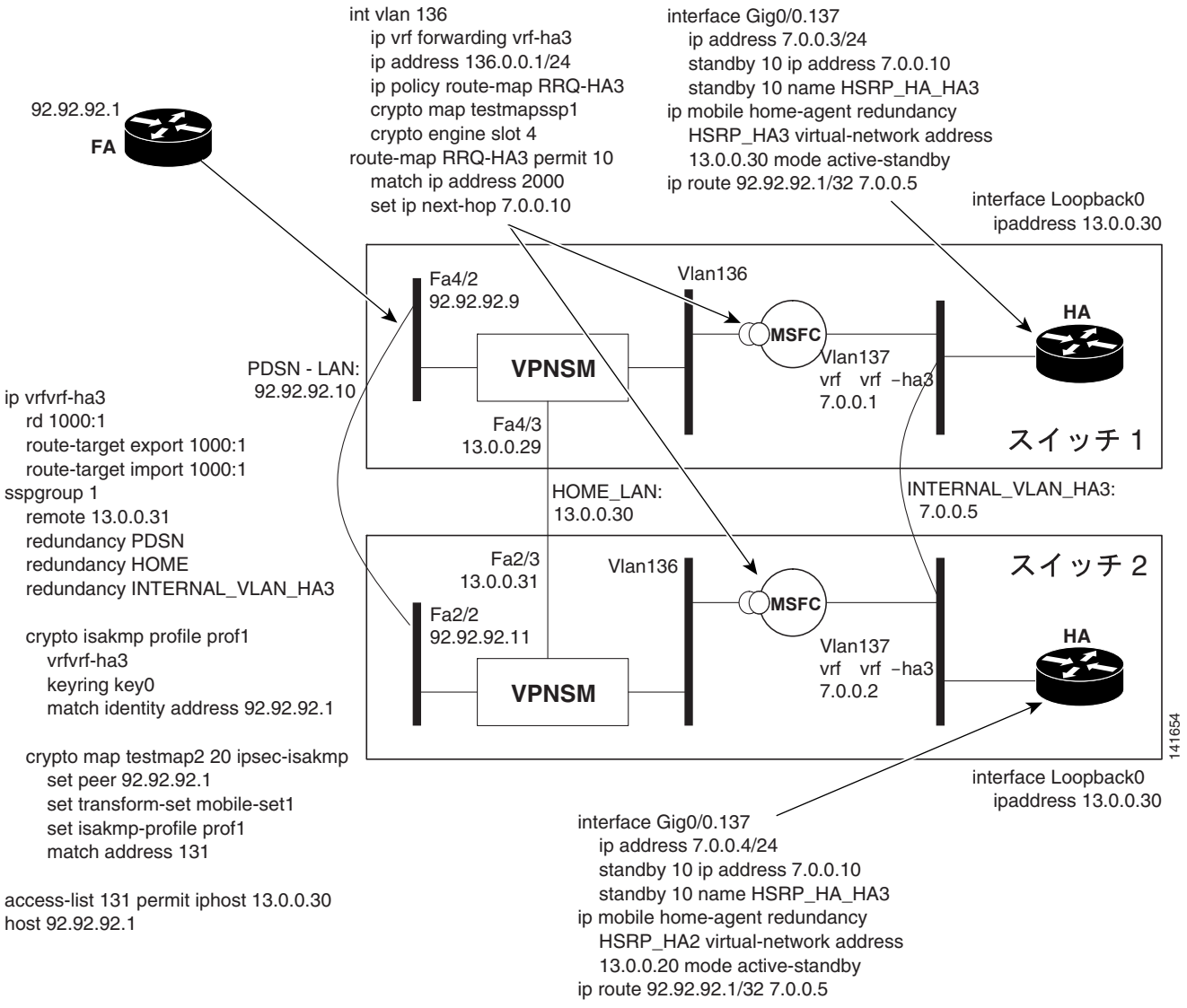
（注）　暗号化するホストおよびサブネットを許可する場合には、必ず、明示的な拒否（deny）ステートメントを指定してください。拒否ステートメントにより、他のすべてのパケットが暗号化されないように設定します。

（注）　Cisco Catalyst 6500 および 7600 の IPSec は、HA ではなく、スーパーバイザ上で設定します。

6 HA インスタンス用の SUP 720 および VRF-IPSec の設定

次に、SUP 720 および VRF-IPSec の詳細な設定例を示します。図 10-3 を参照してください。

図 10-3　SUP 720 / VRF-IPSec の設定



SUP の設定 ― スイッチ 1 :

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.31
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
  pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
   vrf vrf-ha2
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 12.0.0.30
crypto isakmp profile prof2
   vrf vrf-ha3
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 13.0.0.30
crypto isakmp profile prof4
   vrf vrf-ha4
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 14.0.0.30
crypto isakmp profile prof5
   vrf vrf-ha5
   keyring key0
```

```
   match identity address 92.92.92.1 255.255.255.255
   local-address 15.0.0.30
crypto isakmp profile prof6
   vrf vrf-ha6
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet4/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet4/4
crypto map testmap1 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof1
 match address 121
!
crypto map testmap4 local-address FastEthernet4/7
crypto map testmap4 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof4
 match address 141
!
crypto map testmap5 local-address FastEthernet4/9
crypto map testmap5 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof5
 match address 151
!
crypto map testmap6 local-address FastEthernet4/11
crypto map testmap6 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof6
 match address 161
!
crypto engine mode vrf
!
interface FastEthernet4/2
 ip address 92.92.92.9 255.255.0.0
 ip policy route-map RRQ-HA10
 speed 100
 duplex half
 standby delay minimum 30 reload 60
 standby 1 ip 92.92.92.10
 standby 1 preempt
 standby 1 name PDSN-LAN
 standby 1 track FastEthernet4/2
 standby 1 track FastEthernet4/3
 standby 1 track FastEthernet4/4
 standby 1 track FastEthernet4/7
 standby 1 track FastEthernet4/9
 standby 1 track FastEthernet4/11
 standby 1 track GigabitEthernet6/1
 standby 1 track Vlan136
 standby 1 track Vlan137
 standby 1 track Vlan127
 standby 1 track Vlan126
 standby 1 track Vlan146
 standby 1 track Vlan147
```

```
 standby 1 track Vlan156
 standby 1 track Vlan157
 standby 1 track Vlan166
 standby 1 track Vlan167
 standby 1 track Vlan200
 crypto engine slot 6
!
interface FastEthernet4/3
 ip address 13.0.0.29 255.255.0.0
 standby delay minimum 30 reload 60
 standby 3 ip 13.0.0.30
 standby 3 preempt
 standby 3 name HOME-LAN
 standby 3 track FastEthernet4/2
 standby 3 track FastEthernet4/3
 standby 3 track FastEthernet4/4
 standby 3 track FastEthernet4/7
 standby 3 track FastEthernet4/9
 standby 3 track FastEthernet4/11
 standby 3 track GigabitEthernet6/1
 standby 3 track Vlan136
 standby 3 track Vlan137
 standby 3 track Vlan127
 standby 3 track Vlan126
 standby 3 track Vlan146
 standby 3 track Vlan147
 standby 3 track Vlan156
 standby 3 track Vlan157
 standby 3 track Vlan166
 standby 3 track Vlan167
 standby 3 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/4
 ip address 12.0.0.29 255.255.255.0
 duplex half
 standby delay minimum 30 reload 60
 standby 2 ip 12.0.0.30
 standby 2 preempt
 standby 2 name HOME-LAN-2
 standby 2 track FastEthernet4/2
 standby 2 track FastEthernet4/3
 standby 2 track FastEthernet4/4
 standby 2 track FastEthernet4/7
 standby 2 track FastEthernet4/9
 standby 2 track FastEthernet4/11
 standby 2 track GigabitEthernet6/1
 standby 2 track Vlan136
 standby 2 track Vlan137
 standby 2 track Vlan127
 standby 2 track Vlan126
 standby 2 track Vlan146
 standby 2 track Vlan147
 standby 2 track Vlan156
 standby 2 track Vlan157
 standby 2 track Vlan166
 standby 2 track Vlan167
 standby 2 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/5
 switchport
 switchport access vlan 137
 switchport mode access
 no ip address
!
interface FastEthernet4/6
 switchport
 switchport access vlan 127
```

```
 switchport mode access
 no ip address
 speed 100
 duplex half
!
interface FastEthernet4/7
 ip address 14.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 4 ip 14.0.0.30
 standby 4 preempt
 standby 4 name HOME-LAN-4
 standby 4 track FastEthernet4/2
 standby 4 track FastEthernet4/3
 standby 4 track FastEthernet4/4
 standby 4 track FastEthernet4/7
 standby 4 track FastEthernet4/9
 standby 4 track FastEthernet4/11
 standby 4 track Vlan136
 standby 4 track Vlan137
 standby 4 track Vlan127
 standby 4 track Vlan126
 standby 4 track GigabitEthernet6/1
 standby 4 track Vlan146
 standby 4 track Vlan147
 standby 4 track Vlan156
 standby 4 track Vlan157
 standby 4 track Vlan166
 standby 4 track Vlan167
 standby 4 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/8
 switchport
 switchport access vlan 147
 switchport mode access
 no ip address
!
interface FastEthernet4/9
 ip address 15.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 5 ip 15.0.0.30
 standby 5 preempt
 standby 5 name HOME-LAN-5
 standby 5 track FastEthernet4/2
 standby 5 track FastEthernet4/3
 standby 5 track FastEthernet4/4
 standby 5 track FastEthernet4/7
 standby 5 track FastEthernet4/9
 standby 5 track FastEthernet4/11
 standby 5 track Vlan136
 standby 5 track Vlan137
 standby 5 track Vlan127
 standby 5 track Vlan126
 standby 5 track GigabitEthernet6/1
 standby 5 track Vlan146
 standby 5 track Vlan147
 standby 5 track Vlan156
 standby 5 track Vlan157
 standby 5 track Vlan166
 standby 5 track Vlan167
 standby 5 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/10
 switchport
 switchport access vlan 157
 switchport mode access
 no ip address
!
```

```
interface FastEthernet4/11
 ip address 16.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 6 ip 16.0.0.30
 standby 6 preempt
 standby 6 name HOME-LAN-6
 standby 6 track FastEthernet4/2
 standby 6 track FastEthernet4/3
 standby 6 track FastEthernet4/4
 standby 6 track FastEthernet4/7
 standby 6 track FastEthernet4/9
 standby 6 track FastEthernet4/11
 standby 6 track Vlan136
 standby 6 track Vlan137
 standby 6 track Vlan127
 standby 6 track Vlan126
 standby 6 track GigabitEthernet6/1
 standby 6 track Vlan146
 standby 6 track Vlan147
 standby 6 track Vlan156
 standby 6 track Vlan157
 standby 6 track Vlan166
 standby 6 track Vlan167
 standby 6 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/12
 switchport
 switchport access vlan 167
 switchport mode access
 no ip address
!
interface GigabitEthernet6/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,136,146,156,166
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan126
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha2
 ip address 126.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA2
 no mop enabled
 crypto map testmap1 ssp 1
 crypto engine slot 6
!
interface Vlan127
 description internal vlan to HA2
 ip vrf forwarding vrf-ha2
 ip address 6.0.0.1 255.255.0.0
 standby 12 ip 6.0.0.5
```

```
 standby 12 preempt
 standby 12 name INTERNAL_VLAN_HA2
 standby 12 track FastEthernet4/2
 standby 12 track FastEthernet4/3
 standby 12 track FastEthernet4/4
 standby 12 track FastEthernet4/7
 standby 12 track FastEthernet4/9
 standby 12 track FastEthernet4/11
 standby 12 track Vlan136
 standby 12 track Vlan137
 standby 12 track Vlan127
 standby 12 track Vlan126
 standby 12 track GigabitEthernet6/1
 standby 12 track Vlan146
 standby 12 track Vlan147
 standby 12 track Vlan156
 standby 12 track Vlan157
 standby 12 track Vlan166
 standby 12 track Vlan167
 standby 12 track Vlan200
!
interface Vlan136
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha3
 ip address 136.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap ssp 1
 crypto engine slot 6
!
interface Vlan137
 description internal vlan to HA3
 ip vrf forwarding vrf-ha3
 ip address 7.0.0.1 255.255.0.0
 standby 13 ip 7.0.0.5
 standby 13 preempt
 standby 13 name INTERNAL_VLAN_HA3
 standby 13 track FastEthernet4/2
 standby 13 track FastEthernet4/3
 standby 13 track FastEthernet4/4
 standby 13 track FastEthernet4/7
 standby 13 track FastEthernet4/9
 standby 13 track FastEthernet4/11
 standby 13 track Vlan136
 standby 13 track Vlan137
 standby 13 track Vlan127
 standby 13 track Vlan126
 standby 13 track GigabitEthernet6/1
 standby 13 track Vlan146
 standby 13 track Vlan147
 standby 13 track Vlan156
 standby 13 track Vlan157
 standby 13 track Vlan166
 standby 13 track Vlan167
 standby 13 track Vlan200
!
interface Vlan146
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha4
 ip address 146.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA4
 no mop enabled
 crypto map testmap4 ssp 1
```

```
 crypto engine slot 6
!
interface Vlan147
 description internal vlan to HA4
 ip vrf forwarding vrf-ha4
 ip address 8.0.0.1 255.255.0.0
 standby 14 ip 8.0.0.5
 standby 14 preempt
 standby 14 name INTERNAL_VLAN_HA4
 standby 14 track FastEthernet4/2
 standby 14 track FastEthernet4/3
 standby 14 track FastEthernet4/4
 standby 14 track FastEthernet4/7
 standby 14 track FastEthernet4/9
 standby 14 track FastEthernet4/11
 standby 14 track Vlan136
 standby 14 track Vlan137
 standby 14 track Vlan127
 standby 14 track Vlan126
 standby 14 track GigabitEthernet6/1
 standby 14 track Vlan146
 standby 14 track Vlan147
 standby 14 track Vlan156
 standby 14 track Vlan157
 standby 14 track Vlan166
 standby 14 track Vlan167
 standby 14 track Vlan200
!
interface Vlan156
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha5
 ip address 156.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA5
 no mop enabled
 crypto map testmap5 ssp 1
 crypto engine slot 6
!
interface Vlan157
 description internal vlan to HA5
 ip vrf forwarding vrf-ha5
 ip address 9.0.0.1 255.255.0.0
 standby 15 ip 9.0.0.5
 standby 15 preempt
 standby 15 name INTERNAL_VLAN_HA5
 standby 15 track FastEthernet4/2
 standby 15 track FastEthernet4/3
 standby 15 track FastEthernet4/4
 standby 15 track FastEthernet4/7
 standby 15 track FastEthernet4/9
 standby 15 track FastEthernet4/11
 standby 15 track Vlan136
 standby 15 track Vlan137
 standby 15 track Vlan127
 standby 15 track Vlan126
 standby 15 track GigabitEthernet6/1
 standby 15 track Vlan146
 standby 15 track Vlan147
 standby 15 track Vlan156
 standby 15 track Vlan157
 standby 15 track Vlan166
 standby 15 track Vlan167
 standby 15 track Vlan200
!
interface Vlan166
 description secure vlan
 ethernet point-to-point
```

```
 ip vrf forwarding vrf-ha6
 ip address 166.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA6
 no mop enabled
 crypto map testmap6 ssp 1
 crypto engine slot 6
!
interface Vlan167
 description internal vlan to HA6
 ip vrf forwarding vrf-ha6
 ip address 10.0.0.1 255.255.0.0
 standby 16 ip 10.0.0.5
 standby 16 preempt
 standby 16 name INTERNAL_VLAN_HA6
 standby 16 track FastEthernet4/2
 standby 16 track FastEthernet4/3
 standby 16 track FastEthernet4/4
 standby 16 track FastEthernet4/7
 standby 16 track FastEthernet4/9
 standby 16 track FastEthernet4/11
 standby 16 track Vlan136
 standby 16 track Vlan137
 standby 16 track Vlan127
 standby 16 track Vlan126
 standby 16 track GigabitEthernet6/1
 standby 16 track Vlan146
 standby 16 track Vlan147
 standby 16 track Vlan156
 standby 16 track Vlan157
 standby 16 track Vlan166
 standby 16 track Vlan167
 standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.2 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
 standby 250 track FastEthernet4/2
 standby 250 track FastEthernet4/3
 standby 250 track FastEthernet4/4
 standby 250 track FastEthernet4/7
 standby 250 track FastEthernet4/9
 standby 250 track FastEthernet4/11
 standby 250 track Vlan136
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet6/1
 standby 250 track Vlan146
 standby 250 track Vlan147
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
 standby 250 track Vlan167
!
ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
```

```
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!
route-map RRQ-HA4 permit 10
 match ip address 2000
 set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
 match ip address 2000
 set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
 match ip address 2001
 continue 11
 set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
 match ip address 2002
 continue 12
 set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
 match ip address 2003
 continue 13
 set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
 match ip address 2004
 continue 14
 set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
 match ip address 2005
 set ip next-hop 200.0.0.45
```

SUP の設定 — スイッチ 2 :

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.29
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
  pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
   vrf vrf-ha2
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 12.0.0.30
crypto isakmp profile prof2
   vrf vrf-ha3
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 13.0.0.30
crypto isakmp profile prof4
   vrf vrf-ha4
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 14.0.0.30
crypto isakmp profile prof5
   vrf vrf-ha5
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
```

```
   local-address 15.0.0.30
crypto isakmp profile prof6
   vrf vrf-ha6
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet2/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet2/5
crypto map testmap1 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof1
 match address 121
!
crypto map testmap4 local-address FastEthernet2/7
crypto map testmap4 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof4
 match address 141
!
crypto map testmap5 local-address FastEthernet2/9
crypto map testmap5 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof5
 match address 151
!
crypto map testmap6 local-address FastEthernet2/11
crypto map testmap6 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof6
 match address 161
!
crypto engine mode vrf
!
interface FastEthernet2/2
 ip address 92.92.92.11 255.255.0.0
 ip policy route-map RRQ-HA10
 speed 100
 duplex full
 standby delay minimum 30 reload 60
 standby 1 ip 92.92.92.10
 standby 1 preempt
 standby 1 name PDSN-LAN
 standby 1 track FastEthernet2/2
 standby 1 track FastEthernet2/3
 standby 1 track FastEthernet2/5
 standby 1 track FastEthernet2/7
 standby 1 track FastEthernet2/9
 standby 1 track FastEthernet2/11
 standby 1 track GigabitEthernet4/1
 standby 1 track Vlan136
 standby 1 track Vlan137
 standby 1 track Vlan127
 standby 1 track Vlan126
 standby 1 track Vlan146
 standby 1 track Vlan156
 standby 1 track Vlan157
```

```
 standby 1 track Vlan166
 standby 1 track Vlan167
 standby 1 track Vlan147
 standby 1 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/3
 ip address 13.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 3 ip 13.0.0.30
 standby 3 preempt
 standby 3 name HOME-LAN
 standby 3 track FastEthernet2/2
 standby 3 track FastEthernet2/3
 standby 3 track FastEthernet2/5
 standby 3 track FastEthernet2/7
 standby 3 track FastEthernet2/9
 standby 3 track FastEthernet2/11
 standby 3 track GigabitEthernet4/1
 standby 3 track Vlan136
 standby 3 track Vlan137
 standby 3 track Vlan127
 standby 3 track Vlan126
 standby 3 track Vlan146
 standby 3 track Vlan156
 standby 3 track Vlan157
 standby 3 track Vlan166
 standby 3 track Vlan167
 standby 3 track Vlan147
 standby 3 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/4
 switchport
 switchport access vlan 137
 switchport mode access
 no ip address
!
interface FastEthernet2/5
 ip address 12.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 2 ip 12.0.0.30
 standby 2 preempt
 standby 2 name HOME-LAN-2
 standby 2 track FastEthernet2/2
 standby 2 track FastEthernet2/3
 standby 2 track FastEthernet2/5
 standby 2 track FastEthernet2/7
 standby 2 track FastEthernet2/9
 standby 2 track FastEthernet2/11
 standby 2 track GigabitEthernet4/1
 standby 2 track Vlan136
 standby 2 track Vlan137
 standby 2 track Vlan127
 standby 2 track Vlan126
 standby 2 track Vlan146
 standby 2 track Vlan156
 standby 2 track Vlan157
 standby 2 track Vlan166
 standby 2 track Vlan167
 standby 2 track Vlan147
 standby 2 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/6
 switchport
 switchport access vlan 127
 switchport mode access
 no ip address
```

```
!
interface FastEthernet2/7
 ip address 14.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 4 ip 14.0.0.30
 standby 4 preempt
 standby 4 name HOME-LAN-4
 standby 4 track FastEthernet2/2
 standby 4 track FastEthernet2/3
 standby 4 track FastEthernet2/5
 standby 4 track FastEthernet2/7
 standby 4 track FastEthernet2/9
 standby 4 track FastEthernet2/11
 standby 4 track Vlan136
 standby 4 track Vlan137
 standby 4 track Vlan127
 standby 4 track Vlan126
 standby 4 track GigabitEthernet4/1
 standby 4 track Vlan146
 standby 4 track Vlan156
 standby 4 track Vlan157
 standby 4 track Vlan166
 standby 4 track Vlan167
 standby 4 track Vlan147
 standby 4 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/8
 switchport
 switchport access vlan 147
 switchport mode access
 no ip address
!
interface FastEthernet2/9
 ip address 15.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 5 ip 15.0.0.30
 standby 5 preempt
 standby 5 name HOME-LAN-5
 standby 5 track FastEthernet2/2
 standby 5 track FastEthernet2/3
 standby 5 track FastEthernet2/5
 standby 5 track FastEthernet2/7
 standby 5 track FastEthernet2/9
 standby 5 track FastEthernet2/11
 standby 5 track Vlan136
 standby 5 track Vlan137
 standby 5 track Vlan127
 standby 5 track Vlan126
 standby 5 track GigabitEthernet4/1
 standby 5 track Vlan146
 standby 5 track Vlan156
 standby 5 track Vlan157
 standby 5 track Vlan166
 standby 5 track Vlan167
 standby 5 track Vlan147
 standby 5 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/10
 switchport
 switchport access vlan 157
 switchport mode access
 no ip address
!
interface FastEthernet2/11
 ip address 16.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 6 ip 16.0.0.30
```

```
 standby 6 preempt
 standby 6 name HOME-LAN-6
 standby 6 track FastEthernet2/2
 standby 6 track FastEthernet2/3
 standby 6 track FastEthernet2/5
 standby 6 track FastEthernet2/7
 standby 6 track FastEthernet2/9
 standby 6 track FastEthernet2/11
 standby 6 track Vlan136
 standby 6 track Vlan137
 standby 6 track Vlan127
 standby 6 track Vlan126
 standby 6 track GigabitEthernet4/1
 standby 6 track Vlan146
 standby 6 track Vlan156
 standby 6 track Vlan157
 standby 6 track Vlan166
 standby 6 track Vlan167
 standby 6 track Vlan147
 standby 6 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/12
 switchport
 switchport access vlan 167
 switchport mode access
 no ip address
!
interface GigabitEthernet4/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,136,146,156,166
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan126
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha2
 ip address 126.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA2
 no mop enabled
 crypto map testmap1 ssp 1
 crypto engine slot 4
!
interface Vlan127
 description internal vlan to HA2
 ip vrf forwarding vrf-ha2
 ip address 6.0.0.2 255.255.0.0
 standby 12 ip 6.0.0.5
 standby 12 preempt
 standby 12 name INTERNAL_VLAN_HA2
 standby 12 track FastEthernet2/2
 standby 12 track FastEthernet2/3
```

```
 standby 12 track FastEthernet2/5
 standby 12 track FastEthernet2/7
 standby 12 track FastEthernet2/9
 standby 12 track FastEthernet2/11
 standby 12 track Vlan136
 standby 12 track Vlan137
 standby 12 track Vlan127
 standby 12 track Vlan126
 standby 12 track GigabitEthernet4/1
 standby 12 track Vlan146
 standby 12 track Vlan156
 standby 12 track Vlan157
 standby 12 track Vlan166
 standby 12 track Vlan167
 standby 12 track Vlan147
 standby 12 track Vlan200
!
interface Vlan136
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha3
 ip address 136.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap ssp 1
 crypto engine slot 4
!
interface Vlan137
 description internal vlan to HA3
 ip vrf forwarding vrf-ha3
 ip address 7.0.0.2 255.255.0.0
 standby 13 ip 7.0.0.5
 standby 13 preempt
 standby 13 name INTERNAL_VLAN_HA3
 standby 13 track FastEthernet2/2
 standby 13 track FastEthernet2/3
 standby 13 track FastEthernet2/5
 standby 13 track FastEthernet2/7
 standby 13 track FastEthernet2/9
 standby 13 track FastEthernet2/11
 standby 13 track Vlan136
 standby 13 track Vlan137
 standby 13 track Vlan127
 standby 13 track Vlan126
 standby 13 track GigabitEthernet4/1
 standby 13 track Vlan146
 standby 13 track Vlan156
 standby 13 track Vlan157
 standby 13 track Vlan166
 standby 13 track Vlan167
 standby 13 track Vlan147
 standby 13 track Vlan200
!
interface Vlan146
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha4
 ip address 146.0.0.2 255.0.0.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA4
 no mop enabled
 crypto map testmap4 ssp 1
 crypto engine slot 4
!
interface Vlan147
 description internal vlan to HA4
```

```
 ip vrf forwarding vrf-ha4
 ip address 8.0.0.2 255.255.0.0
 standby 14 ip 8.0.0.5
 standby 14 preempt
 standby 14 name INTERNAL_VLAN_HA4
 standby 14 track FastEthernet2/2
 standby 14 track FastEthernet2/3
 standby 14 track FastEthernet2/5
 standby 14 track FastEthernet2/7
 standby 14 track FastEthernet2/9
 standby 14 track FastEthernet2/11
 standby 14 track Vlan136
 standby 14 track Vlan137
 standby 14 track Vlan127
 standby 14 track Vlan126
 standby 14 track GigabitEthernet4/1
 standby 14 track Vlan146
 standby 14 track Vlan156
 standby 14 track Vlan157
 standby 14 track Vlan166
 standby 14 track Vlan167
 standby 14 track Vlan147
 standby 14 track Vlan200
!
interface Vlan156
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha5
 ip address 156.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA5
 no mop enabled
 crypto map testmap5 ssp 1
 crypto engine slot 4
!
interface Vlan157
 description internal vlan to HA5
 ip vrf forwarding vrf-ha5
 ip address 9.0.0.2 255.255.0.0
 standby 15 ip 9.0.0.5
 standby 15 preempt
 standby 15 name INTERNAL_VLAN_HA5
 standby 15 track FastEthernet2/2
 standby 15 track FastEthernet2/3
 standby 15 track FastEthernet2/5
 standby 15 track FastEthernet2/7
 standby 15 track FastEthernet2/9
 standby 15 track FastEthernet2/11
 standby 15 track Vlan136
 standby 15 track Vlan137
 standby 15 track Vlan127
 standby 15 track Vlan126
 standby 15 track GigabitEthernet4/1
 standby 15 track Vlan146
 standby 15 track Vlan156
 standby 15 track Vlan157
 standby 15 track Vlan166
 standby 15 track Vlan167
 standby 15 track Vlan147
 standby 15 track Vlan200
!
interface Vlan166
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha6
 ip address 166.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
```

```
 ip policy route-map RRQ-HA6
 no mop enabled
 crypto map testmap6 ssp 1
 crypto engine slot 4
!
interface Vlan167
 description internal vlan to HA2
 ip vrf forwarding vrf-ha6
 ip address 10.0.0.2 255.255.0.0
 standby 16 ip 10.0.0.5
 standby 16 preempt
 standby 16 name INTERNAL_VLAN_HA6
 standby 16 track FastEthernet2/2
 standby 16 track FastEthernet2/3
 standby 16 track FastEthernet2/5
 standby 16 track FastEthernet2/7
 standby 16 track FastEthernet2/9
 standby 16 track FastEthernet2/11
 standby 16 track Vlan136
 standby 16 track Vlan137
 standby 16 track Vlan127
 standby 16 track Vlan126
 standby 16 track GigabitEthernet4/1
 standby 16 track Vlan146
 standby 16 track Vlan156
 standby 16 track Vlan157
 standby 16 track Vlan166
 standby 16 track Vlan167
 standby 16 track Vlan147
 standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.1 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
 standby 250 track FastEthernet2/2
 standby 250 track FastEthernet2/3
 standby 250 track FastEthernet2/5
 standby 250 track FastEthernet2/7
 standby 250 track FastEthernet2/9
 standby 250 track FastEthernet2/11
 standby 250 track Vlan136
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet4/1
 standby 250 track Vlan146
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
 standby 250 track Vlan167
 standby 250 track Vlan147

ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
```

```
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!
route-map RRQ-HA4 permit 10
 match ip address 2000
 set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
 match ip address 2000
 set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
 match ip address 2001
 continue 11
 set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
 match ip address 2002
 continue 12
 set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
 match ip address 2003
 continue 13
 set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
 match ip address 2004
 continue 14
 set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
 match ip address 2005
 set ip next-hop 200.0.0.45
```

HA の設定 — スイッチ 1：

HA1:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
 encapsulation dot1Q 126
 ip address 126.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.127
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 127
 ip address 6.0.0.3 255.255.255.0
 standby 10 ip 6.0.0.10
 standby 10 preempt
 standby 10 name HSRP_HA_HA2
 standby 10 track GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.4 255.0.0.0
 no snmp trap link-status
 standby 200 ip 200.0.0.5
 standby 200 preempt
 standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA2:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
 encapsulation dot1Q 136
 ip address 136.0.0.83 255.255.255.0
!
interface GigabitEthernet0/0.137
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 137
 ip address 7.0.0.3 255.255.255.0
 standby 20 ip 7.0.0.10
 standby 20 preempt
 standby 20 name HSRP_HA_HA3
 standby 20 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.14 255.0.0.0
 no snmp trap link-status
 standby 201 ip 200.0.0.15
 standby 201 preempt
 standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA3:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
 encapsulation dot1Q 146
 ip address 146.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.147
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 147
 ip address 8.0.0.3 255.255.255.0
 standby 30 ip 8.0.0.10
 standby 30 preempt
 standby 30 name HSRP_HA_HA4
 standby 30 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.24 255.0.0.0
 no snmp trap link-status
 standby 202 ip 200.0.0.25
 standby 202 preempt
 standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA4:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
 encapsulation dot1Q 156
 ip address 156.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.157
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 157
 ip address 9.0.0.3 255.255.255.0
 standby 40 ip 9.0.0.10
 standby 40 preempt
 standby 40 name HSRP_HA_HA5
 standby 40 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.34 255.0.0.0
 no snmp trap link-status
 standby 203 ip 200.0.0.35
 standby 203 preempt
 standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA5:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 16.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.3 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.44 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 99.99.99.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA の設定 — スイッチ 2 :

HA1:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
 encapsulation dot1Q 126
 ip address 126.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.127
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 127
 ip address 6.0.0.4 255.255.255.0
 standby 10 ip 6.0.0.10
 standby 10 preempt
 standby 10 name HSRP_HA_HA2
 standby 10 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.6 255.0.0.0
 no snmp trap link-status
 standby 200 ip 200.0.0.5
 standby 200 preempt
 standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA2:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
 encapsulation dot1Q 136
 ip address 136.0.0.33 255.255.255.0
!
interface GigabitEthernet0/0.137
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 137
 ip address 7.0.0.4 255.255.255.0
 standby 20 ip 7.0.0.10
 standby 20 preempt
 standby 20 name HSRP_HA_HA3
 standby 20 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.16 255.0.0.0
 no snmp trap link-status
 standby 201 ip 200.0.0.15
 standby 201 preempt
 standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA3:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
 encapsulation dot1Q 146
 ip address 146.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.147
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 147
 ip address 8.0.0.4 255.255.255.0
 standby 30 ip 8.0.0.10
 standby 30 preempt
 standby 30 name HSRP_HA_HA4
 standby 30 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.26 255.0.0.0
 no snmp trap link-status
 standby 202 ip 200.0.0.25
 standby 202 preempt
 standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA4:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
 encapsulation dot1Q 156
 ip address 156.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.157
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 157
 ip address 9.0.0.4 255.255.255.0
 standby 40 ip 9.0.0.10
 standby 40 preempt
 standby 40 name HSRP_HA_HA5
 standby 40 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.36 255.0.0.0
 no snmp trap link-status
 standby 203 ip 200.0.0.35
 standby 203 preempt
 standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA5:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 16.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.4 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.46 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```