SafeNet IPsec VPN Client サポート

SafeNet IPsec VPN Client サポート機能を使用すると、ローカル終端アドレスまたはインターフェイスに対する Internet Security Association and Key Management Protocol（ISAKMP）プロファイルまたは ISAKMP キーリングの設定範囲を制限できます。この機能の利点は、異なったローカル終端アドレスを使用することで、同じピア ID および ISAKMP 鍵を異なったユーザが使用できることです。

SafeNet IPsec VPN Client サポート機能の履歴

リリース	変更点
12.3(14)T	この機能が追加されました。
12.2(18)SXE	この機能は、Cisco IOS Release 12.2(18)SXE に統合されました。

プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明の場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

SafeNet IPsec VPN Client サポートの前提条件

- ISAKMP プロファイルおよび ISAKMP キーリングの設定方法を理解する必要があります。

SafeNet IPsec VPN Client サポートの制約事項

- ローカル アドレス オプションが機能するのは、インターフェイスのプライマリ アドレスに対してだけです。
- IP アドレスを設定したら、管理者は、設定した IP アドレスへのピア終端の接続を確認する必要があります。
- デバイスに IP アドレスが設定されていないか、インターフェイスに IP アドレスが設定されていない場合、ISAKMP プロファイルまたは ISAKMP キーリングが完全に無効になります。

SafeNet IPsec VPN Client サポートに関する情報

SafeNet IPsec VPN Client サポートを設定するには、次の概念を理解しておく必要があります。

- 「ISAKMP プロファイルおよび ISAKMP キーリングの設定：背景」（P.2）
- 「ローカル終端アドレスまたはインターフェイス」（P.3）

ISAKMP プロファイルおよび ISAKMP キーリングの設定：背景

Cisco IOS Release 12.3(14)T 以前は ISAKMP プロファイルおよび ISAKMP キーリングの設定はグローバルだけでした。グローバルであるということは、これらの設定の範囲は、ローカルに定義されているどのようなパラメータでも制限できないということです（VRF インスタンスを除く）。たとえば、ISAKMP キーリングにアドレス 10.11.12.13 の事前共有鍵が含まれている場合、ピアの接続先のインターフェイスまたはローカル アドレスに関係なく、ピアのアドレスが 10.11.12.13 の場合は同じ鍵が使われていました。しかし、同じキーリングを Virtual Route Forwarding（VRF; VPN ルーティングおよび転送）インスタンスとバインドするだけでなく、特定のインターフェイスにもバインドする必要がある場合があります。たとえば、VRF インスタンスがなければ仮想 LAN になり、固定の仮想 LAN（VLAN）インターフェイスを 1 つ使い、Internet Key Exchange（IKE; インターネット鍵交換）がピアのグループとネゴシエーションされます。このようなピアのグループは、単一の事前共有鍵を使用します。このため、キーリングをインターフェイスにバインドできれば、ワイルドカード鍵の定義が簡単になり、鍵が他のユーザに使用される心配もなくなります。

ピアの ID を管理者が管理できない場合がありますが、異なったユーザで同じピアがネゴシエーションする場合であっても、ローカル終端アドレスが、ピアを区別する唯一の方法になります。ピアの区別後にトラフィックが別の VRF インスタンスに送信される場合、ISAKMP プロファイルの設定が、ピアを区別する唯一の方法になります。残念ながら、すべてのこのような状況では、まったく同じ ID をピアが使用する場合、ISAKMP プロファイルではネゴシエーションでピアを区別できません。そのような場合は、ISAKMP プロファイルをローカル終端アドレスにバインドすればピアを区別できます。ローカル終端アドレスを割り当てられる場合は、ピアの ID がまったく同じであっても問題ありません。

ローカル終端アドレスまたはインターフェイス

Cisco IOS Release 12.3(14)T に導入された SafeNet IPsec VPN Client サポート機能を使用すると、ローカル終端アドレスまたはインターフェイスに対する ISAKMP プロファイルおよび ISAKMP キーリングの範囲を制限できます。

SafeNet IPsec VPN Client サポートの利点

この機能の利点は、異なったローカル終端アドレスを使用することで、同じピア ID および ISAKMP 鍵を異なったユーザが使用できることです。

SafeNet IPsec VPN Client サポートの設定方法

ここでは、次の各手順について説明します。最初の 2 つの設定はどちらを先に実行してもかまいません。

- 「ローカル終端アドレスまたはインターフェイスへの ISAKMP プロファイルの制限」（P.3）（必須）
- 「ローカル終端アドレスまたはインターフェイスへのキーリングの制限」（P.4）（必須）
- 「SafeNet IPsec VPN Client サポートのモニタおよびメンテナンス」（P.5）（任意）
- 「例」（P.6）（任意）

ローカル終端アドレスまたはインターフェイスへの ISAKMP プロファイルの制限

ISAKMP プロファイルを設定し、ローカル終端アドレスまたはインターフェイスに制限するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **keyring** *keyring-name*
5. **match identity address** *address*
6. local-address {*interface-name* | *ip-address* [*vrf-tag*]}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp profile** *profile-name* **例：** `Router (config)# crypto isakmp profile profile1`	ISAKMP プロファイルを定義し、ISAKMP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**keyring** *keyring-name* **例：** `Router (conf-isa-profile)# keyring keyring1`	（任意）ISAKMP プロファイルでキーリングを設定します。 • ローカル終端の動作には ISAKMP プロファイル内にキーリングは必要ありません。ローカル終端は RSA（Rivest、Shamir、Adelman）証明書を使用する場合でも動作します。
ステップ 5	**match identity address** *address* **例：** `Router (conf-isa-profile)# match identity address 10.0.0.0 255.0.0.0`	ISAKMP プロファイルのピアの ID を一致させます。
ステップ 6	**local-address** {*interface-name* | *ip-address* [*vrf-tag*]} **例：** `Router (conf-isa-profile)# local-address serial2/0`	ISAKMP プロファイルまたは ISAKMP キーリングの設定範囲を、ローカル終端アドレスまたはインターフェイスに制限します。

ローカル終端アドレスまたはインターフェイスへのキーリングの制限

ISAKMP キーリングを設定し、ローカル終端アドレスまたはインターフェイスに範囲を制限するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name*
4. local-address {*interface-name* | *ip-address* [*vrf-tag*]}
5. pre-shared-key address *address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto keyring** *keyring-name* **例：** `Router (config)# crypto keyring keyring1`	IKE 認証中に使用するクリプト キーリングを定義し、キーリング コンフィギュレーション モードを開始します。
ステップ 4	**local-address** {*interface-name* | *ip-address* [*vrf-tag*]} **例：** `Router (conf-keyring)# local-address serial2/0`	ISAKMP プロファイルまたは ISAKMP キーリングの設定範囲を、ローカル終端アドレスまたはインターフェイスに制限します。
ステップ 5	**pre-shared-key address** *address* **例：** `Router (conf-keyring)# pre-shared-key address 10.0.0.1`	IKE 認証に使用する事前共有鍵を定義します。

SafeNet IPsec VPN Client サポートのモニタおよびメンテナンス

次の **debug** コマンドおよび **show** コマンドを使用すれば、ISAKMP プロファイルまたは ISAKMP キーリングの範囲をローカル終端アドレスまたはインターフェイスに制限した設定をモニタおよびメンテナンスできます。

手順の概要

1. **enable**
2. **debug crypto isakmp**
3. **show crypto isakmp profile**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug crypto isakmp** **例：** `Router# debug crypto isakmp`	IKE イベントに関するメッセージを表示します。
ステップ 3	**show crypto isakmp profile** **例：** `Router# show crypto isakmp profile`	ルータに定義されている ISAKMP プロファイルをすべてリストします。

例

ローカル終端アドレスにバインドされている ISAKMP キーリングに対して実行した debug crypto isakmp コマンドの出力：例

ISAKMP の設定は次のとおりです（serial2/0 のアドレス：10.0.0.1、serial2/1 のアドレス：10.0.0.2）。

```
crypto keyring keyring1
! Scope of the keyring is limited to interface serial2/0.
  local-address serial2/0
  ! The following is the key string used by the peer.
  pre-shared-key address 10.0.0.3 key somerandomkeystring
crypto keyring keyring2
  local-address serial2/1
  ! The following is the keystring used by the peer coming into serial2/1.
   pre-shared-key address 10.0.0.3 key someotherkeystring
```

接続が serial2/0 に入ってきて、事前共有鍵の発信元として keyring1 が選択されると（keyring2 は serial2/1 にバインドされているため無視される）、出力は次のようになります。

```
Router# debug crypto isakmp

*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):Keyring keyring2 is bound to
  10.0.0.0, skipping
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):Looking for a matching key for
  10.0.0.3 in keyring1
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0): : success
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):found peer pre-shared key
  matching 10.0.0.3
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0): local preshared key found
```

ローカル終端アドレスにバインドされている ISAKMP プロファイルに対して実行した debug crypto isakmp コマンドの出力：例

設定は次のとおりです。

```
crypto isakmp profile profile1
  keyring keyring1
  match identity address 10.0.0.0 255.0.0.0
  local-address serial2/0
```

```
crypto isakmp profile profile2
  keyring keyring1
  keyring keyring2
  self-identity fqdn
  match identity address 10.0.0.1 255.255.255.255
  local-address serial2/1
```

この設定でローカル終端アドレス serial2/0 を通って接続が入ってくると、出力は次のようになります。

```
Router# debug crypto isakmp

*Feb 11 15:01:29.935: ISAKMP:(0:0:N/A:0):

Profile profile2 bound to 10.0.0.0 skipped

*Feb 11 15:01:29.935: ISAKMP:(0:1:SW:1):: peer matches profile1 profile
```

show crypto isakmp profile コマンドの出力：例

次に、**show** コマンドの一般的な出力で、serial2/0 にバインドされている ISAKMP プロファイルに対して実行した例を示します。

```
Router# show crypto isakmp profile

ISAKMP PROFILE profile1
  Identities matched are:
    ip-address 10.0.0.0 255.0.0.0
  Certificate maps matched are:
  keyring(s): keyring1
  trustpoint(s): <all>
  Interface binding: serial2/0 (10.20.0.1:global)
```

SafeNet IPsec VPN Client サポートのトラブルシューティング

ISAKMP プロファイルまたは ISAKMP キーリングを選択できなかった場合は、ISAKMP プロファイルまたは ISAKMP キーリングの設定でバインドされているローカル アドレスをダブルクリックし、IKE デバッグの出力に従い、そのアドレスでピアが正しく終端されているかを確認します。ローカル アドレスのバインドを解除し（プロファイルまたはキーリングの範囲をグローバルにするため）、プロファイルまたはキーリングの選択をチェックして状況を確認します。

SafeNet IPsec VPN Client サポートの設定例

ここでは、次の設定、**debug** コマンド、**show** コマンドそれぞれの例を示します。

- 「ローカル インターフェイスにバインドされている ISAKMP プロファイル：例」（P.8）
- 「ローカル インターフェイスにバインドされている ISAKMP キーリング：例」（P.8）
- 「ローカル IP アドレスにバインドされている ISAKMP キーリング：例」（P.8）
- 「IP アドレスにバインドされ、VRF に限定されている ISAKMP キーリング：例」（P.8）

ローカル インターフェイスにバインドされている ISAKMP プロファイル：例

次に、ローカル インターフェイスにバインドされている ISAKMP プロファイルの例を示します。

```
crypto isakmp profile profile1
   keyring keyring1
   match identity address 10.0.0.0 255.0.0.0
  local-address serial2/0
```

ローカル インターフェイスにバインドされている ISAKMP キーリング：例

次に、インターフェイス serial2/0 だけにバインドされている ISAKMP キーリングの例を示します。

```
crypto keyring
   local-address serial2/0
  pre-shared-key address 10.0.0.1
```

ローカル IP アドレスにバインドされている ISAKMP キーリング：例

次に、IP アドレス 10.0.0.2 だけにバインドされている ISAKMP キーリングの例を示します。

```
crypto keyring keyring1
   local-address 10.0.0.2
  pre-shared-key address 10.0.0.2 key
```

IP アドレスにバインドされ、VRF に限定されている ISAKMP キーリング：例

次に、ISAKMP キーリングが IP アドレス 10.34.35.36 にバインドされており、範囲を VRF examplevrf1 に限定している場合の例を示します。

```
ip vrf examplevrf1
   rd 12:3456
crypto keyring ring1
   local-address 10.34.35.36 examplevrf1
interface ethernet2/0
   ip vrf forwarding examplevrf1
   ip address 10.34.35.36 255.255.0.0
```

その他の参考資料

ここでは、SafeNet IPsec VPN Client サポート関連の参考資料を示します。

関連資料と標準

内容	参照先
ISAKMP プロファイルおよび ISAKMP キーリングの設定	「*VRF-Aware IPSec*」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

規格	タイトル
この機能によってサポートされる新しい規格や変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **local-address**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『*Master Command List*』を参照してください。