# IPsec 管理構成ガイド

**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

# 目 次

第 1 章

# 最初にお読みください

### Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと発展しています。これにより、スイッチングおよびルーティング ポートフォリオの幅広い範囲のアクセスおよびエッジ製品に 1 つのリリースで対応できます。

（注） 技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディング ページに表示されている場合は、その機能がプラットフォームでサポートされていることを示します。

第 2 章

# IPsec VPN モニタリング

IP Security VPN モニタリング機能では、VPN セッション モニタリング拡張機能によって、バーチャル プライベート ネットワーク（VPN）のトラブルシューティングを行い、エンドユーザ インターフェイスをモニタリングできます。セッション モニタリング拡張には、次のものが含まれます。

- コンフィギュレーション ファイル内のインターネット キー交換（IKE）ピアの説明を指定する機能
- 暗号セッション ステータスの一覧
- 暗号セッションのアップまたはダウン ステータスの Syslog 通知
- 1 つのコマンドライン インターフェイス（CLI）を使用して、IKE と IP Security（IPsec）の両方のセキュリティ アソシエーション（SA）をクリアする機能。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

# IP Security VPN モニタリングの前提条件

- IPSec と暗号化についての知識が必要です。
- ご使用のルータで IPSec がサポートされている必要があります。また IPsec VPN モニタリング機能を使用する前に、ルータ上で IPSec を設定しておく必要があります。

# IP Security VPN モニタリングの制限事項

- ルータ上で Cisco IOS XE k8 または k9 暗号イメージを実行する必要があります。

# IPsec VPN モニタリングに関する情報

## 暗号セッションの背景知識

暗号化セッションは、2 つの暗号エンドポイント間における一連の IPSec 接続（フロー）です。2 つの暗号エンドポイントで、IKE をキーイング プロトコルとして使用している場合、それらの暗号エンドポイントは互いに対して IKE ピアになります。一般に、暗号化セッションは、1 つの IKE セキュリティ アソシエーション（制御トラフィック用）と、少なくとも 2 つの IPSec セキュリティ アソシエーション（データ トラフィック用、各方向に 1 つ）で構成されています。キー再生成中、または両サイドから同時に設定要求が行われたことにより、同じセッションの IKE SA と IPSec SA が重複したり、IKE SA または IPSec SA が重複したりする可能性があります。

## Per-IKE ピアの説明

Per-IKE Peer Description 機能を使用すれば、IKE ピアの選択に関する説明を入力できます。一意なピアの説明（最大 80 文字）は、特定の IKE ピアを参照する場合に使用することができます。ピアの説明を追加するには、**description** コマンドを使用します。

（注） ネットワーク アドレス変換（NAT）デバイスの背後に「配置」された IKE ピアは一意に識別することができないため、同じピアの説明を共有する必要があります。

この説明フィールドの主要な利用目的はモニタリングです（たとえば、**show** コマンドを使用するときや、ロギング（Syslog メッセージ）などのためです）。説明フィールドは純粋に記述用です（たとえば、クリプト マップを定義する際のピア アドレスや FQDN の置換としては使用できません）。

# 暗号化セッション ステータスのサマリー リスト

すべてのアクティブな VPN セッションの一覧を表示するには、**show crypto session** コマンドを入力します。一覧には次の項目が含まれます。

- インターフェイス
- IKE ピアの説明（存在している場合）
- IPSec SA を作成したピアに関連付けられた IKE SA
- セッションのフローにサービスを提供する IPSec SA

同じピア（同じセッション）に対して複数の IKE または IPSec SA が確立される場合があります。その場合、IKE ピアの説明は、ピアに関連付けられている各 IKE SA に対して、また、セッションのフローにサービスを提供する各 IPSec SA に対して、異なる値で繰り返されます。

このコマンドの **show crypto session detail** バリアントを使用して、セッションに関してより詳しい情報を取得することもできます。

# 暗号化セッションのアップまたはダウンステータスに関する Syslog 通知

暗号セッションのアップまたはダウン ステータスの Syslog 通知を実行する機能では、暗号セッションがアップおよびダウンする度に Syslog 通知を行います。

次に、暗号セッションがアップしたことを示す Syslog 通知の例を示します。

```
%CRYPTO-5-SESSION_STATUS: Crypto session is UP. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20
 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

次に、暗号セッションがダウンしたことを示す Syslog 通知の例を示します。

```
%CRYPTO-5-SESSION_STATUS: Crypto session is DOWN. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20
 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

# IKE および IPsec セキュリティ交換のクリア コマンド

**clear crypto session** コマンドを使用すると、1 つのコマンドで IKE と IPSec の両方をクリアできます。特定の暗号化セッションや、すべてのセッションのサブセット（たとえば、あるリモート サイトへの単一のトンネル）をクリアするには、ローカルまたはリモート IP アドレス、ローカルまたはリモートポート、フロントドア VPN ルーティングおよび転送（FVRF）名、内部 VRF（IVRF）

名といった、セッション固有のパラメータを指定する必要があります。削除する単一のトンネルを指定する場合、リモート IP アドレスを使用するのが一般的です。

**clear crypto session** コマンドを入力するとき、パラメータとしてローカル IP アドレスを指定すると、その IP アドレスをローカルの暗号化エンドポイント（IKE ローカル アドレス）として共有するすべてのセッション（および各セッションの IKE SA と IPsec SA）がクリアされます。**clear crypto session** コマンドを使用する際に、パラメータを指定しなかった場合、ルータ内のすべての IPsec SA および IKE SA が削除されます。

# IP Security VPN モニタリングの設定方法

## IKE ピアの説明の追加

IKE ピアの説明を IPsec VPN セッションに追加するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoisakmppeer** {**ip-address** *ip-address*}
4. **description**

### 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **cryptoisakmppeer** {**ip-address** *ip-address*}<br><br>例：<br><br>`Router (config)# crypto isakmp peer address 10.2.2.9` | IPSec ピアによるアグレッシブ モードのトンネル属性に関する認証、許可、アカウンティング（AAA）の IKE クエリーをイネーブルにし、ISAKMP ピア コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **description**<br><br>例：<br><br>`Router (config-isakmp-peer)# description connection from site A` | IKE ピアの説明を追加します。 |

# ピアの記述の確認

ピアの説明を確認するには、**showcryptoisakmppeer** コマンドを使用します。

## 手順の概要

1. **enable**
2. **showcryptoisakmppeer**

## 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **showcryptoisakmppeer**<br><br>例：<br><br>`Router# show crypto isakmp peer` | ピアの説明を表示します。 |

### 例

次に、説明の例を示します。IKE ピア 10.2.2.9 の説明として「connection from site A」が追加されていることが確認できます。

```
Router# show crypto isakmp peer
Peer: 10.2.2.9 Port: 500
 Description: connection from site A
  flags: PEER_POLICY
```

アドレス 10.2.2.9 のピアが接続され、セッションがアップになると、Syslog のステータスが次のように表示されます。

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection
from site A Id: ezvpn
```

次に、説明の例を示します。IKE ピア 10.2.2.9 の説明として「connection from site A」が追加されていることが確認できます。

```
Router# show crypto isakmp peer
Peer: 10.2.2.9 Port: 500
 Description: connection from site A
  flags: PEER_POLICY
```

アドレス 10.2.2.9 のピアが接続され、セッションがアップになると、Syslog のステータスが次のように表示されます。

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection
from site A Id: ezvpn
```

# 暗号化セッションのクリア

暗号セッションをクリアするには、ルータのコマンド ラインから **clear crypto session** コマンドを使用します。このコマンドを使用するうえで、コンフィギュレーション ファイル内のコンフィギュレーション文は不要です。

## 手順の概要

1. **enable**
2. **clearcryptosession**

## 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **clearcryptosession**<br><br>例：<br><br>`Router# clear crypto session` | 暗号セッション（IPSec および IKE SA）を削除します。 |

# IP Security VPN モニタリングの設定例

## show crypto session コマンドの出力例

次に、**detail** キーワードを指定していない **show crypto session** の出力例を示します。

```
Router# show crypto session
Crypto session current status
Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.0.0.2/500
   IKE SA: local 172.0.0.1/500 remote 172.0.0.2/500 Active
   IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.30.30.0/255.255.255.0
         Active SAs: 2, origin: crypto map
```

次に、**show crypto session コマンドおよび detail** キーワードを使用した出力例を示します。

```
Router# show crypto session detail
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.1.3 port 500 fvrf: (none) ivrf: (none)
      Desc: this is my peer at 10.1.1.3:500 Green
      Phase1_id: 10.1.1.3
  IKE SA: local 10.1.1.4/500 remote 10.1.1.3/500 Active
          Capabilities:(none) connid:3 lifetime:22:03:24
  IPSEC FLOW: permit 47 host 10.1.1.4 host 10.1.1.3
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
  IPSEC FLOW: permit ip host 10.1.1.4 host 10.1.1.3
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4605665/2949
        Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4605665/2949
```

# その他の参考資料

ここでは、IPsec VPN モニタリングの関連資料について説明します。

## 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| IP セキュリティ、暗号化、および IKE | • 「Configuring Internet Key Exchange for IPsec VPNs」<br>• IPsec を使用した VPN のセキュリティの設定 |
| セキュリティ コマンド | 『*Cisco IOS Security Command Reference*』 |

# 標準

| 標準 | タイトル |
| --- | --- |
| この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。 | -- |

# MIB

| MIB | MIB のリンク |
| --- | --- |
| 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。またこの機能による既存 MIB のサポートに変更はありません。 | 選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

# RFC

| RFC | タイトル |
| --- | --- |
| この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。 | -- |

# シスコのテクニカル サポート

| 説明 | リンク |
| --- | --- |
| シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。<br>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。<br>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。 | http://www.cisco.com/en/US/support/index.html |

# IP Security VPN モニタリングの機能履歴

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：*IP Security VPN* モニタリングの機能履歴

| 機能名 | リリース | 機能情報 |
|---|---|---|
| IPsec VPN モニタリング | Cisco IOS XE Release 2.1 | IP Security VPN モニタリング機能では、VPN セッション モニタリング拡張機能によって、VPN のトラブルシューティングを行い、エンドユーザ インターフェイスをモニタリングできます。セッション モニタリング拡張には、次のものが含まれます。<br>• コンフィギュレーション ファイル内の IKE ピアの説明を指定する機能。<br>• 暗号セッション ステータスの一覧<br>• 暗号セッションのアップまたはダウン ステータスの Syslog 通知<br><br>CLI を使用して IKE と IPsec SA の両方を削除する機能<br>• 次のコマンドが、新たに導入または変更されました。**clearcryptosession**、**description(isakmppeer)**、**showcryptoisakmppeer**、**showcryptosession**。 |

第 3 章

# Cisco VRF-Aware IPsec の IPsec および IKE MIB サポート

バーチャルプライベートネットワークのルーティングと転送（VRF）対応 IP security（IPsec）機能を使用すると、MIB で VRF 対応 IPsec を管理できます。これにより、VRF ごとに IPsec 統計情報とパフォーマンス メトリックの詳細が表示されます。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

# Cisco VRF-Aware IPsec の IPsec および IKE MIB サポートに関する前提条件

- 簡易ネットワーク管理プロトコル（SNMP）の知識が必要です。

# Cisco VRF-Aware IPsec の IPsec および IKE MIB サポートに関する情報

## Cisco VRF 対応 IPsec の IPsec および IKE MIB サポート機能でサポートされる MIB

- CISCO-IPSEC-FLOW-MONITOR-MIB は、トンネル履歴と障害情報ごとに IKE および IPSEC をサポートします。この履歴と障害情報の長さは設定することができ、VRF ごとに維持する必要があります。テーブル サイズは、グローバル コンフィギュレーション モードで **crypto mib ipsec flowmib history tunnel size number** および **crypto mib ipsec flowmib history failure size** コマンドを使用して制御します。
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB はサポートされています。しかし、この MIB は、特定の VPN VRF インスタンスに対してではなくルータ全体に適用されるので、VRF 対応ではありません。そのため、この MIB に所属するオブジェクト ID（OID）は、グローバル VRF コンテキストに関連して実行されます。

## Cisco VRF-Aware IPSec の IPSec および IKE MIB サポート機能によってサポートされる SNMP トラップ

次の IKE および IPsec トンネルの開始と終了トラップは、対応する VRF と一致する必要があります。

- IPSEC_TUNNEL_STOP
- IKE_TUNNEL_STOP
- IPSEC_TUNNEL_START
- IKE_TUNNEL_START

次のトラップは、Cisco VRF-Aware IPsec 機能に合わせて変更されたグローバル トラップです。

- TOO_MANY_SAS_CREATED
- CRYPTOMAP_ADDED
- CRYPTOMAPSET_ATTACHED
- CRYPTOMAP_DELETED
- CRYPTOMAPSET_DELETED
- ISAKMP_POLICY_ADDED
- ISAKMP_POLICY_DELETED

# Cisco VRF-Aware IPSec の IPSec および IKE MIB サポートの設定方法

この機能を使用するに当たって、特別な設定は必要ありません。SNMP フレームワークを使用して、MIB を使用した VRF 対応 IPsec を管理できます。詳細については、「Cisco VRF-Aware IPSec の IPSec および IKE MIB サポートの設定例」の項を参照してください。

この機能のトラブルシューティングに関する情報は、次の項に記載されています。

## Cisco VRF-Aware IPSec の IPSec および IKE MIB サポート機能のトラブルシューティング方法

次の **debug crypto mib** コマンドおよびキーワードを使用して、Cisco VRF-aware IPsec に関連している IPsec およびインターネット キー交換（IKE）MIB に関する情報を表示できます。

### 手順の概要

1. **enable**
2. **debugcryptomibdetail**
3. **debugcryptomiberror**

### 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **debugcryptomibdetail**<br><br>例：<br>`Router# debug crypto mib detail` | IPsec MIB サブシステムで発生する各種イベントを表示します。<br>• **detail** キーワードの出力は非常に長くなる可能性があるので、**debug crypto mib detail** をイネーブルにすることは慎重に検討する必要があります。 |
| ステップ 3 | **debugcryptomiberror**<br><br>例：<br>`Router# debug crypto mib error` | MIB エージェント内のエラー イベントを表示します。 |

# Cisco VRF-Aware IPSec の IPSec および IKE MIB サポートの設定例

## 2 つの VRF を持つ設定の例

次に、2 つの VRF を持つハブ設定の典型的な出力例を示します。この出力は、IPsec セキュリティアソシエーション（SA）に対してポーリングを実行する場合の出力です。ルータ 3745b は VRF 対応ルータです。

### 2 つの VRF を設定

次の出力は、2 つの VRF（vrf1 および vrf2）が設定されていることを示しています。

```
Router3745b# show running-config
Building configuration...
Current configuration : 6567 bytes
!
version 12.4
service timestamps debug datetime msec localtime
service timestamps log uptime
no service password-encryption
!
hostname ipsecf-3745b
!
boot-start-marker
boot-end-marker
!
no logging console
enable password lab
!
no aaa new-model
!
resource policy
```

```
!
memory-size iomem 5
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef
!
!
ip vrf vrf1
 rd 1:101
 context vrf-vrf1-context
 route-target export 1:101
 route-target import 1:101
!
ip vrf vrf2
 rd 2:101
 context vrf-vrf2-context
 route-target export 2:101
 route-target import 2:101
!
no ip domain lookup
!
!
crypto keyring vrf1-1 vrf vrf1
  pre-shared-key address 10.1.1.1 255.255.255.0 key vrf1-1
crypto keyring vrf2-1 vrf vrf2
  pre-shared-key address 10.1.2.1 255.255.255.0 key vrf2-1
!
!
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp policy 50
 authentication pre-share
crypto isakmp key global1-1 address 10.1.151.1
crypto isakmp key global2-1 address 10.1.152.1
crypto isakmp profile vrf1-1
   keyring vrf1-1
   match identity address 10.1.1.1 255.255.255.255 vrf1
crypto isakmp profile vrf2-1
   keyring vrf2-1
   match identity address 10.1.2.1 255.255.255.255 vrf2
!
crypto ipsec security-association lifetime kilobytes 99000
crypto ipsec security-association lifetime seconds 5000
!
crypto ipsec transform-set tset ah-sha-hmac esp-des esp-sha-hmac
!
crypto map global1-1 10 ipsec-isakmp
 set peer 10.1.151.1
 set transform-set tset
 match address 151
!
crypto map global2-1 10 ipsec-isakmp
 set peer 10.1.152.1
 set transform-set tset
 match address 152
!
crypto map vrf1-1 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set tset
 set isakmp-profile vrf1-1
 match address 101
!
crypto map vrf2-1 10 ipsec-isakmp
 set peer 10.1.2.1
 set transform-set tset
 set isakmp-profile vrf2-1
 match address 102
!
!
interface FastEthernet0/0
 ip address 10.1.38.25 255.255.255.0
```

```
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 no keepalive
 serial restart-delay 0
 clock rate 128000
 no frame-relay inverse-arp
!
interface Serial1/0.1 point-to-point
 ip vrf forwarding vrf1
 ip address 10.3.1.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 21
!
interface Serial1/0.2 point-to-point
 ip vrf forwarding vrf2
 ip address 10.3.2.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 22
!
interface Serial1/0.151 point-to-point
 ip address 10.7.151.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 151
!
interface Serial1/0.152 point-to-point
 ip address 10.7.152.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 152
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 encapsulation frame-relay
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 no keepalive
 serial restart-delay 0
 no frame-relay inverse-arp
!
interface Serial1/2.1 point-to-point
 ip vrf forwarding vrf1
 ip address 10.1.1.2 255.255.255.0
```

```
 no ip route-cache
 frame-relay interface-dlci 21
 crypto map vrf1-1
!
interface Serial1/2.2 point-to-point
 ip vrf forwarding vrf2
 ip address 10.1.2.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 22
 crypto map vrf2-1
!
interface Serial1/2.151 point-to-point
 ip address 10.5.151.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 151
 crypto map global1-1
!
interface Serial1/2.152 point-to-point
 ip address 10.5.152.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 152
 crypto map global2-1
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
ip default-gateway 10.1.38.1
ip classless
ip route 10.1.1.6 255.255.255.255 10.1.151.1
ip route 10.2.1.6 255.255.255.255 10.1.152.1
ip route 10.6.2.1 255.255.255.255 10.7.151.2
ip route 10.6.2.2 255.255.255.255 10.7.152.2
ip route 172.19.216.110 255.255.255.255 FastEthernet0/0
ip route vrf vrf1 10.20.1.1 255.255.255.255 10.1.1.1
ip route vrf vrf1 10.22.1.1 255.255.255.255 10.30.1.1
ip route vrf vrf2 10.20.2.1 255.255.255.255 10.1.2.1
ip route vrf vrf2 10.22.2.1 255.255.255.255 10.30.1.2
!
!
ip http server
no ip http secure-server
!
ip access-list standard vrf-vrf1-context
ip access-list standard vrf-vrf2-context
!
access-list 101 permit ip host 10.22.1.1 host 10.20.1.1
access-list 102 permit ip host 10.22.2.1 host 10.20.2.1
access-list 151 permit ip host 10.6.2.1 host 10.1.1.6
access-list 152 permit ip host 10.6.2.2 host 10.2.1.6
snmp-server group abc1 v2c context vrf-vrf1-context read view_vrf1 notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F access vrf-vrf1-context
snmp-server group abc2 v2c context vrf-vrf2-context read view_vrf2 notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F access vrf-vrf2-context
snmp-server view view_vrf1 iso included
snmp-server view view_vrf2 iso included
snmp-server community abc1 RW
snmp-server community global1 RW
snmp-server community abc2 RW
snmp-server community global2 RW
snmp-server enable traps tty
snmp-server enable traps config
snmp-server host 172.19.216.110 version 2c abc1
snmp-server host 172.19.216.110 vrf vrf1 version 2c abc1 udp-port 2001  ipsec isakmp
snmp-server host 172.19.216.110 version 2c abc2
snmp-server host 172.19.216.110 vrf vrf2 version 2c abc2 udp-port 2002  ipsec isakmp
snmp-server context vrf-vrf1-context
snmp-server context vrf-vrf2-context
!
!
snmp mib community-map  abc1 context vrf-vrf1-context
```

```
snmp mib community-map  abc2 context vrf-vrf2-context
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

### 両方の VRF をクリア

次の出力（abc1 および abc2 の出力）は、両方の VRF が、すべてのカウンタが必ず既知の値に初期化されるように「クリア」されていることを示しています。

次の出力は、VRF abc1 がクリアされていることを示しています。

```
orcas:2> setenv SR_MGR_CONF /users/green1
orcas:3> setenv SR_UTIL_SNMP_VERSION v2c
orcas:5> setenv SR_UTIL_COMMUNITY abc1
orcas:6> setenv SR_MGR_CONF_DIR /users/green1
orcas:7> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
```

```
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
```

次の出力は、VRF abc2 がクリアされていることを示しています。

```
orcas:8> setenv SR_UTIL_COMMUNITY abc2
orcas:9> /auto/sw/packages/snmpr/14.2.0.0/solaris2bin/getmany -v2c 10.1.38.25 cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
```

```
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:10>
orcas:10>
orcas:10>
```

### VRF abc1 に対する ping の実行

次の出力は、VRF abc1 に対して ping が実行されていることを示しています。

```
Router3745a# ping
Protocol [ip]:
Target IP address: 10.22.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.20.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.22.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.1.1
```

### VRF abc1 に対するポーリングの実行

VRF abc1 に対してポーリングを実行すると次の出力が行われます。

（注） ping 実行後、カウンタにはゼロ以外の何らかの値が表示されます。

```
orcas:10>
orcas:12> setenv SR_UTIL_COMMUNITY abc1
orcas:13> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 1
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 336
cikeGlobalInPkts.0 = 2
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 1
cikeGlobalInP2Exchgs.0 = 2
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 344
cikeGlobalOutPkts.0 = 2
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 1
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cikePeerLocalAddr.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 0a 01  01 02
cikePeerRemoteAddr.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 0a 01  01 01
cikePeerActiveTime.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 13743
cikePeerActiveTunnelIndex.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 1
cikeTunLocalType.1 = ipAddrPeer(1)
cikeTunLocalValue.1 = 010.001.001.002
cikeTunLocalAddr.1 = 0a 01  01 02
cikeTunLocalName.1 = ipsecf-3745b
cikeTunRemoteType.1 = ipAddrPeer(1)
cikeTunRemoteValue.1 = 010.001.001.001
cikeTunRemoteAddr.1 = 0a 01  01 01
cikeTunRemoteName.1 =
cikeTunNegoMode.1 = main(1)
cikeTunDiffHellmanGrp.1 = dhGroup1(2)
cikeTunEncryptAlgo.1 = des(2)
cikeTunHashAlgo.1 = sha(3)
cikeTunAuthMethod.1 = preSharedKey(2)
cikeTunLifeTime.1 = 86400
cikeTunActiveTime.1 = 13752
cikeTunSaRefreshThreshold.1 = 0
cikeTunTotalRefreshes.1 = 0
cikeTunInOctets.1 = 336
cikeTunInPkts.1 = 2
cikeTunInDropPkts.1 = 0
cikeTunInNotifys.1 = 1
cikeTunInP2Exchgs.1 = 2
cikeTunInP2ExchgInvalids.1 = 0
```

```
cikeTunInP2ExchgRejects.1 = 0
cikeTunInP2SaDelRequests.1 = 0
cikeTunOutOctets.1 = 344
cikeTunOutPkts.1 = 2
cikeTunOutDropPkts.1 = 0
cikeTunOutNotifys.1 = 0
cikeTunOutP2Exchgs.1 = 1
cikeTunOutP2ExchgInvalids.1 = 0
cikeTunOutP2ExchgRejects.1 = 0
cikeTunOutP2SaDelRequests.1 = 0
cikeTunStatus.1 = active(1)
cikePeerCorrIpSecTunIndex.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1.1
 = 1
cipSecGlobalActiveTunnels.0 = 1
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 400
cipSecGlobalHcInOctets.0 = 0x0190
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 400
cipSecGlobalHcInDecompOctets.0 = 0x0190
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 4
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 4
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 4
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 704
cipSecGlobalHcOutOctets.0 = 0x02c0
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 704
cipSecGlobalHcOutUncompOctets.0 = 0x02c0
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 4
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 4
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 4
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecTunIkeTunnelIndex.1 = 1
cipSecTunIkeTunnelAlive.1 = true(1)
cipSecTunLocalAddr.1 = 0a 01  01 02
cipSecTunRemoteAddr.1 = 0a 01  01 01
cipSecTunKeyType.1 = ike(1)
cipSecTunEncapMode.1 = tunnel(1)
cipSecTunLifeSize.1 = 99000
cipSecTunLifeTime.1 = 5000
cipSecTunActiveTime.1 = 13749
cipSecTunSaLifeSizeThreshold.1 = 64
cipSecTunSaLifeTimeThreshold.1 = 10
cipSecTunTotalRefreshes.1 = 0
cipSecTunExpiredSaInstances.1 = 0
cipSecTunCurrentSaInstances.1 = 4
cipSecTunInSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunInSaEncryptAlgo.1 = des(2)
cipSecTunInSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunInSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunInSaDecompAlgo.1 = none(1)
cipSecTunOutSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunOutSaEncryptAlgo.1 = des(2)
cipSecTunOutSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaCompAlgo.1 = none(1)
cipSecTunInOctets.1 = 400
cipSecTunHcInOctets.1 = 0x0190
cipSecTunInOctWraps.1 = 0
cipSecTunInDecompOctets.1 = 400
cipSecTunHcInDecompOctets.1 = 0x0190
cipSecTunInDecompOctWraps.1 = 0
```

```
cipSecTunInPkts.1 = 4
cipSecTunInDropPkts.1 = 0
cipSecTunInReplayDropPkts.1 = 0
cipSecTunInAuths.1 = 4
cipSecTunInAuthFails.1 = 0
cipSecTunInDecrypts.1 = 4
cipSecTunInDecryptFails.1 = 0
cipSecTunOutOctets.1 = 704
cipSecTunHcOutOctets.1 = 0x02c0
cipSecTunOutOctWraps.1 = 0
cipSecTunOutUncompOctets.1 = 704
cipSecTunHcOutUncompOctets.1 = 0x02c0
cipSecTunOutUncompOctWraps.1 = 0
cipSecTunOutPkts.1 = 4
cipSecTunOutDropPkts.1 = 0
cipSecTunOutAuths.1 = 4
cipSecTunOutAuthFails.1 = 0
cipSecTunOutEncrypts.1 = 4
cipSecTunOutEncryptFails.1 = 0
cipSecTunStatus.1 = active(1)
cipSecEndPtLocalName.1.1 =
cipSecEndPtLocalType.1.1 = singleIpAddr(1)
cipSecEndPtLocalAddr1.1.1 = 16 01  01 01
cipSecEndPtLocalAddr2.1.1 = 16 01  01 01
cipSecEndPtLocalProtocol.1.1 = 0
cipSecEndPtLocalPort.1.1 = 0
cipSecEndPtRemoteName.1.1 =
cipSecEndPtRemoteType.1.1 = singleIpAddr(1)
cipSecEndPtRemoteAddr1.1.1 = 14 01  01 01
cipSecEndPtRemoteAddr2.1.1 = 14 01  01 01
cipSecEndPtRemoteProtocol.1.1 = 0
cipSecEndPtRemotePort.1.1 = 0
cipSecSpiDirection.1.1 = in(1)
cipSecSpiDirection.1.2 = out(2)
cipSecSpiDirection.1.3 = in(1)
cipSecSpiDirection.1.4 = out(2)
cipSecSpiValue.1.1 = 3891970674
cipSecSpiValue.1.2 = 1963217493
cipSecSpiValue.1.3 = 3691920464
cipSecSpiValue.1.4 = 3458912974
cipSecSpiProtocol.1.1 = ah(1)
cipSecSpiProtocol.1.2 = ah(1)
cipSecSpiProtocol.1.3 = esp(2)
cipSecSpiProtocol.1.4 = esp(2)
cipSecSpiStatus.1.1 = active(1)
cipSecSpiStatus.1.2 = active(1)
cipSecSpiStatus.1.3 = active(1)
cipSecSpiStatus.1.4 = active(1)
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:14>
orcas:14>
orcas:14>
```

### VRF abc2 に対するポーリングの実行

VRF abc2 に対してポーリングを実行すると次の出力が行われます。

（注） ping は VRF abc1 に関してだけ完了しています。そのため、VRF abc2 のカウンタは初期化されたステートのままです。

```
setenv SR_UTIL_COMMUNITY abc2
orcas:15>
orcas:15> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
```

```
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:16>
```

# その他の参考資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| テクノロジーごとの Cisco IOS コマンド | 『Cisco IOS Release Command References』 |
| Cisco IOS マスター コマンド リスト | 『Master Command List』 |
| SNMP の設定 | 『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」の章 |
| VRF-Aware IPsec の設定 | 「VRF-Aware IPSec」 |

### 標準

| 標準 | タイトル |
|---|---|
| なし。 | -- |

### MIB

| MIB | MIB のリンク |
|---|---|
| • CISCO-IPSEC-FLOW-MONITOR-MIB<br>• CISCO-IPSEC-MIB<br>• CISCO-IPSEC-POLICY-MAP-MIB | 選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャ 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。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | タイトル |
|---|---|
| なし。 | -- |

### シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。<br>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。<br>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。 | http://www.cisco.com/cisco/web/support/index.html |

# Cisco VRF-Aware IPSec の IPsec および IKE MIB サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2*：*Cisco VRF-Aware IPSec* の *IPsec* および *IKE MIB* サポートに関する機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Cisco VRF-Aware IPSec の IPSec および IKE MIB サポート | IOS XE 3.1S | バーチャル プライベート ネットワークのルーティングと転送（VRF）対応 IP security（IPsec）機能を使用すると、MIB で VRF 対応 IPsec を管理できます。これにより、VRF ごとに IPsec 統計情報とパフォーマンス メトリックの詳細が表示されます。<br>この機能は、Cisco IOS Release 12.4(4)T で導入されました。<br>この機能は、Cisco IOS Release XE 3.1S に統合されました。<br>次のコマンドが、新たに導入または変更されました。<br>**debugcryptomib** |

第 4 章

# IPsec SNMP サポート

IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。

この機能のコマンドを使用すれば、IPsec MIB 機能のバージョンを確認したり、SNMP トラップをディセーブルにしたり、この機能によって使用されるバッファのサイズをモニタリングおよび制御したりできます。

（注） このマニュアルでは、Cisco IPsec MIB の Cisco IOS XE CLI サポートを中心に説明します。また、このマニュアルでは現在サポートされている MIB の要素も示します。このマニュアルでは、Cisco IPsec MIB の（ネットワーク管理ステーションからの）SNMP 設定については説明しません。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

# IPsec SNMP サポートの制限事項

- IPsec--SNMP サポート機能でサポートされるトンネル設定エラー ログは次のものだけです。
  - NOTIFY_MIB_IPSEC_PROPOSAL_INVALID
  - 「A tunnel could not be established because the peer did not supply an acceptable proposal.」
  - NOTIFY_MIB_IPSEC_ENCRYPT_FAILURE
  - 「A tunnel could not be established because it failed to encrypt a packet to be sent to a peer.」
  - NOTIFY_MIB_IPSEC_SYSCAP_FAILURE
  - 「A tunnel could not be established because the system ran out of resources.」
  - NOTIFY_MIB_IPSEC_LOCAL_FAILURE
  - 「A tunnel could not be established because of an internal error.」

これらのエラー通知はエラー テーブルに記録されますが、SNMP 通知（トラップ）としては使用できないことに注意してください。

- 次の機能は、IPsec MIB 機能ではサポートされていません。
  - チェックポインティング
  - CISCO-IPSEC-MIB の Dynamic Cryptomap テーブル
- CISCO-IPSEC-POLICY-MAP-MIB（ciscoIpSecPolMap）で定義されている通知はありません（「IPSec Policy Map Notifications Group」は空です）。

# IPsec SNMP サポートの情報

IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。

IPsec MIB を使用すれば、SNMP を使用した IPsec 設定のモニタリングおよび IPsec ステータスのモニタリングが可能です。また、IPsec MIB を各種バーチャル プライベート ネットワーク（VPN）ソリューションに統合できます。

たとえば、この機能を使用すれば、Cisco IOS XE CLI を使用して、トンネル履歴テーブルやトンネルエラーテーブルのサイズを細かく指定できます。履歴テーブルには、トンネルに関する属性

および統計情報がアーカイブされます。エラー テーブルには、トンネルのエラーの原因とエラーが発生した時刻がアーカイブされます。エラー履歴テーブルは、トンネルの終了が通常のものか異常なものかを区別するための簡単な手段として使用できます。つまり、トンネル履歴テーブル内のトンネルエントリに関連するエラー レコードがない場合、トンネルは正常に終了したことになります。ただし、すべてのエラーがトンネルのものとは限らないので、トンネル履歴テーブルがすべてのエラー テーブルを伴うわけではありません。そのため、サポート対象の設定エラーはエラー テーブルに記録されますが、関連する履歴テーブルは、トンネルが設定されていないので、記録されません。

この機能では、ネットワーク管理システムで使用される IPsec 簡易ネットワーク管理プロトコル（SNMP）通知も提供されます。

## 関連機能およびテクノロジー

IPsec--SNMP サポート機能は、VPN Device Manager（VDM）をサポートするように設計されました。VDM によって、ネットワーク管理者は、Web ブラウザから単一デバイス上のサイト間 VPN を管理および設定でき、また、リアルタイムで変更の効果を確認できます。VDM では、IPsec プロトコルを使用したサイト間 VPN の設定プロセスを簡単にするために、ウィザード ベースのグラフィカル ユーザ インターフェイス（GUI）が実装されます。VDM ソフトウェアは Cisco VPN ルータに直接インストールされます。また、VDM ソフトウェアは、次世代の Device Manager 製品で使用でき、互換性を保つように設計されています。

# IPsec SNMP サポートの設定方法

## IPsec SNMP 通知のイネーブル化

IPsec SNMP 通知をイネーブルにするには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-serverenabletrapsipseccryptomap** [**add** | **delete** | **attach** | **detach**]
4. **snmp-serverenabletrapsisakmp** [**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}]
5. **snmp-serverhost***host-address***traps***community-string***ipsec**

### 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **snmp-serverenabletrapsipseccryptomap** [**add** \| **delete** \| **attach** \| **detach**]<br><br>例：<br><br>`Router (config)# snmp-server enable traps ipsec cryptomap add` | ルータを、IPsec SNMP 通知を送信するようにルータをイネーブルにします。 |
| ステップ 4 | **snmp-serverenabletrapsisakmp** [**policy** {**add** \| **delete**} \| **tunnel** {**start** \| **stop**}]<br><br>例：<br><br>`Router (config)# snmp-server enable traps isakmp policy add` | ルータを、IPsec ISAKMP SNMP 通知を送信するようにルータをイネーブルにします。 |
| ステップ 5 | **snmp-serverhost***host-address***traps***community-string***ipsec**<br><br>例：<br><br>`Router (config)# snmp-server host my.example.com traps version2c` | IPsec SNMP 通知動作の受信者を指定します。 |

#### 次の作業

SNMP の設定の詳細については、『*Cisco IOS XE Configuration Fundamentals Configuration Guide*』の「Configuring SNMP Support」章を参照してください。

## IPsec エラー履歴テーブルのサイズの設定

デフォルトのエラー履歴テーブルのサイズは 200 です。エラー履歴テーブルのサイズを変更するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configureterminal**
3. **cryptomibipsecflowmibhistoryfailuresize***number*

### 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **cryptomibipsecflowmibhistoryfailuresize***number*<br><br>例：<br><br>`Router (config)# crypto mib ipsec flowmib history failure size 220` | IPsec エラー履歴テーブルのサイズを変更します。 |

## IPsec トンネル履歴テーブルのサイズの設定

デフォルトのトンネル履歴テーブルのサイズは 200 です。トンネル履歴テーブルのサイズを変更するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configureterminal**
3. **cryptomibipsecflowmibhistorytunnelsize***number*

### 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **cryptomibipsecflowmibhistorytunnelsize***number*<br><br>例：<br><br>`Router (config)# crypto mib ipsec flowmib history tunnel size` | IPsec トンネル履歴テーブルのサイズを変更します。 |

# IPsec MIB 設定の確認

IPsec MIB 機能が正しく設定されているかどうかを確認するには、次のタスクを実行します。

- **show crypto mib ipsec flowmib history failure size** 特権 EXEC コマンドを入力して、エラー履歴テーブルのサイズを表示します。

```
Router# show crypto mib ipsec flowmib history failure size
IPSec Failure Window Size: 140
```

- **show crypto mib ipsec flowmib history tunnel size** 特権 EXEC コマンドを入力して、トンネル履歴テーブルのサイズを表示すします。

```
Router# show crypto mib ipsec flowmib history tunnel size
IPSec History Window Size: 130
```

- **show crypto mib ipsec flowmib version** 特権 EXEC コマンドを入力して、管理アプリケーションによって使用される MIB バージョンを表示して、フィーチャ セットを識別します。

```
Router# show crypto mib ipsec flowmib version
IPSec Flow MIB version: 1
```

- **debug crypto mib** コマンドを入力して、IPsec MIB デバッグ メッセージ通知を表示します。

```
Router# debug crypto mib
Crypto IPSec Mgmt Entity debugging is on
```

# IPsec MIB のモニタおよびメンテナンス

IPsec MIB 情報のステータスをモニタリングするには、次のコマンドのいずれかを使用します。

## 手順の概要

1. **enable**
2. **showcryptomibipsecflowmibhistoryfailuresize**
3. **showcryptomibipsecflowmibhistorytunnelsize**
4. **showcryptomibipsecflowmibversion**

## 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **showcryptomibipsecflowmibhistoryfailuresize**<br><br>例：<br><br>`Router# show crypto mib ipsec flowmib history failure size` | IPsec エラー履歴テーブルのサイズを表示します。 |
| ステップ 3 | **showcryptomibipsecflowmibhistorytunnelsize**<br><br>例：<br><br>`Router# show crypto mib ipsec flowmib history tunnel size` | IPsec トンネル履歴テーブルのサイズを表示します。 |
| ステップ 4 | **showcryptomibipsecflowmibversion**<br><br>例：<br><br>`Router# show crypto mib ipsec flowmib version` | ルータによって使用される IPsec Flow MIB のバージョンを表示します。 |

# IPsec SNMP サポートの設定例

## IPsec 通知のイネーブル化の例

次に、IPsec 通知がイネーブルにされている例を示します。

```
snmp-server enable traps ipsec isakmp
```

次に、ルータが、ホスト nms1.example.com に IPsec 通知を送信するように設定されている例を示します。

```
snmp-server host nms1.example.com public ipsec isakmp
Translating "nms1.example.com"...domain server (172.00.0.01) [OK]
```

## 履歴テーブルのサイズの指定例

次に、指定したエラー履歴テーブルのサイズが 140 になっている例を示します。

```
crypto mib ipsec flowmib history failure size 140
```

次に、指定したトンネル履歴テーブルのサイズが 130 になっている例を示します。

```
crypto mib ipsec flowmib history tunnel size 130
```

# その他の参考資料

**関連資料**

| 関連項目 | マニュアル タイトル |
|---|---|
| AAA アカウンティングの設定 | • 「Configuring Accounting」 |
| IPsec VPN アカウンティングの設定 | • 「Configuring Security for VPNs with IPsec」 |
| 基本 AAA RADIUS の設定 | • Cisco.com にある『*Cisco IOS Security Configuration Guide: User Services*』の「Configuring RADIUS」の章 |
| ISAKMP プロファイルの設定 | 「VRF Aware IPsec」 |

| 関連項目 | マニュアル タイトル |
|---|---|
| TACACS+ および RADIUS での権限レベル | • 「Configuring TACACS+」<br>• Cisco.com にある『*Cisco IOS Security Configuration Guide: User Services*』の「Configuring RADIUS」の章 |
| IP セキュリティ、RADIUS、および AAA コマンド | 『*Cisco IOS Security Command Reference*』 |
| 推奨暗号化アルゴリズム | Next Generation Encryption |

### MIB

| MIB | MIB のリンク |
|---|---|
| なし | 選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### 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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html |

# IPsec SNMP サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

**表 3**：***IPsec SNMP*** **サポートの機能情報**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| IPsec SNMP サポート | Cisco IOS XE Release 2.1 | IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。<br>次のコマンドが、新たに導入または変更されました。<br>**cryptomibipsecflowmibhistoryfailuresize**、**cryptomibipsecflowmibhistorytunnelsize**、**debugcryptomib**、**showcryptomibipsecflowmibhistoryfailuresize**、**showcryptomibipsecflowmibhistorytunnelsize**、**showcryptomibipsecflowmibversion**、**snmp-serverenabletrapsipsec**、**snmp-serverenabletrapsisakmp**、**snmp-serverhost**。 |

# 用語集

**CA**：認証局（CA）。認証局（CA）は、メッセージ暗号化用のセキュリティ証明書および公開キー（X509v3 証明書の形式）を発行および管理する、ネットワーク内のエンティティです。CA は、公開キー インフラストラクチャ（PKI）の一部として、デジタル証明書の要求側が提供した情報を確認するために登録局（RA）に問い合わせます。RA によって要求側の情報が確認されると、CA は証明書を発行できます。一般に、証明書には、オーナーの公開キー、証明書の失効日、およびそ公開キーのオーナーに関するその他の情報が含まれています。

**IP セキュリティ**：IPsec を参照してください。

**IPsec**：インターネット プロトコル セキュリティ（IPsec）。参加ピア間でのデータの機密性、整合性、および認証を提供するオープン スタンダードの枠組みです。IPsec では、これらのセキュリティ サービスが IP レイヤで実現されます。IPsec では、インターネット キー交換（IKE）によって、ローカル ポリシーに基づいたプロトコルおよびアルゴリズムのネゴシエーションが処理され、IPsec によって使用される暗号キーおよび認証キーが生成されます。IPsec は、1 組のホスト

間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

**管理情報ベース**：MIB を参照してください。

**MIB**：管理情報ベース。ネットワーク管理情報のデータベースです。これらの情報は、簡易ネットワーク管理プロトコル（SNMP）や共通管理情報プロトコル（CMIP）などのネットワーク管理プロトコルにより使用および保持されます。MIB オブジェクトの値は、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、グラフィカルユーザ インターフェイス（GUI）のネットワーク管理システム（NMS）から実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

**簡易ネットワーク管理プロトコル**：SNMP を参照してください。

**SNMP**：簡易ネットワーク管理プロトコル。アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ形式を規定します。

**トラップ**：重要なイベントを知らせるためのメッセージです。指定された重大な状況が発生したり、しきい値を超過した場合、SNMP エージェントから、ネットワーク管理システム、コンソール、または端末へ送信されます。

第 5 章

# IPsec VPN アカウンティング

IPsec VPN アカウンティング機能を使用すれば、セッションが開始される時と終了する時を指示することによって、セッションをアカウンティングできます。

VPN セッションとは、インターネット キー交換（IKE）セキュリティ アソシエーション（SA）および、IKE SA によって作成される 1 つ以上の SA ペアとして定義されます。セッションは、最初の IP セキュリティ（IPsec）ペアが作成されると開始し、すべての IPsec SA が削除されると停止します。

セッション識別情報およびセッション使用状況情報は、標準 RADIUS 属性とベンダー固有属性を介して、Remote Authentication Dial-In User Service（RADIUS）サーバに渡されます。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

# IPsec VPN アカウンティングの前提条件

- RADIUS と認証、許可、アカウンティング（AAA）アカウンティングの設定方法を理解します。
- IPsec アカウンティングの設定方法を理解します。

# IPsec VPN アカウンティングに関する情報

## 『RADIUS Accounting』

多くの大規模ネットワークでは、監査のために、ユーザ アクティビティを記録する必要があります。多く使用される方式は、RADIUS アカウンティングです。

RADIUS アカウンティングを使用すれば、セッションが開始される時と終了する時を指示することによって、セッションをアカウンティングできます。また、セッション識別情報およびセッション使用状況情報が、RADIUS 属性および VSA を介して RADIUS サーバに渡されます。

### RADIUS 開始アカウンティング

RADIUS 開始パケットには、一般的には、サービスを要求する者、およびサービスのプロパティの構成を特定する多くの属性が格納されています。次の表に、開始に必要な属性を示します。

**表 *4*：*RADIUS* アカウンティング開始パケット属性**

| RADIUS 属性<br>値 | 属性 | 説明 |
|---|---|---|
| 1 | user-name | 拡張認証（XAUTH）で使用されるユーザ名。XAUTH が使用されない場合、ユーザ名が NULL になる場合があります。 |
| 4 | nas-ip-address | ユーザにサービスを提供するネットワーク アクセス サーバ（NAS）の IP アドレスの識別。RADIUS サーバのスコープ内の NAS に対して一意である必要があります。 |

| RADIUS 属性<br>値 | 属性 | 説明 |
|---|---|---|
| 5 | nas-port | ユーザにサービスを提供する NAS の物理ポート番号。 |
| 8 | framed-ip-address | IPsec セッション用に割り当てられたプライベートアドレス。 |
| 40 | acct-status-type | ステータス タイプ。この属性では、このアカウンティング要求がマーキングするのが、セッションの開始（start）、終了（stop）、または更新のいずれかなのかを示します。 |
| 41 | acct-delay-time | クライアントが特定のレコードの送信を試行した秒数。 |
| 44 | acct-session-id | ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウンティング ID。 |
| 26 | vrf-id | Virtual Route Forwarder（VRF）の名前を表す文字列。 |
| 26 | isakmp-initiator-ip | リモート IKE の発信側（V4）のエンドポイント IP アドレス。 |
| 26 | isakmp-group-id | アカウンティングに使用される VPN グループ プロファイルの名前。 |
| 26 | isakmp-phase1-id | セッションの発信側の識別を可能にする、IKE によって使用されるフェーズ 1 識別情報（ID）（たとえば、ドメイン名（DN）、完全修飾ドメイン名（FQDN）、IP アドレスなど）。 |

## RADIUS 終了アカウンティング

RADIUS 終了パケットには、セッションの使用状況を識別する多くの属性が格納されています。表 2 に、RADIUS 終了パケットに必要な追加属性を示します。開始パケットなしで終了パケットだけを送信することは、そのように設定すれば可能です。終了パケットだけを送信すれば、これにより、AAA サーバに送信されるレコードの数を簡単に減らせます。

**表 *5*：*RADIUS* アカウンティング終了パケット属性**

| RADIUS 属性<br>値 | 属性 | 説明 |
|---|---|---|
| 42 | acct-input-octets | サービスが提供されている間に Unity クライアントから受信されたオクテット数。 |
| 43 | acct-output-octets | このサービスの配信中に Unity クライアントに送信されたオクテット数。 |
| 46 | acct-session-time | Unity クライアントがサービスを受信した時間の長さ（秒単位）。 |
| 47 | acct-input-packets | このサービスの配信中に Unity クライアントから受信したパケット量。 |
| 48 | acct-output-packets | このサービスの配信中に Unity クライアントに送信したパケット量。 |
| 49 | acct-terminate-cause | 未使用。 |
| 52 | acct-input-gigawords | このサービスの間に Acct-Input-Octets カウンタの値が 232（2 の 32 乗）を超えた回数。 |
| 52 | acct-output-gigawords | このサービスの間に Acct-Input-Octets カウンタの値が 232（2 の 32 乗）を超えた回数。 |

## RADIUS 更新アカウンティング

RADIUS 更新アカウンティングがサポートされています。パケットおよびオクテット カウントが更新内に表示されます。

# IKE および IPsec サブシステムの相互作用

## Accounting Start

IPsec アカウンティングが設定されている場合、IKE フェーズが終了すると、アカウンティング開始レコードがセッション用に生成されます。キー再生成中は、新しいアカウンティング レコードは生成されません。

次に、ルータ上で生成されており、定義されている AAA サーバに送信されるアカウント開始レコードを示します。

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 10.1.1.4:1646 id 4, len
 220
*Aug 23 04:06:20.131: RADIUS:  authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7 19
FB 3F
*Aug 23 04:06:20.135: RADIUS:  Acct-Session-Id     [44]  10  "00000001"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  31
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   25  "isakmp-group-id=cclient"
*Aug 23 04:06:20.135: RADIUS:  Framed-IP-Address   [8]   6   10.13.13.1
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=10.1.2.2"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No Progress"
*Aug 23 04:06:20.135: RADIUS:  User-Name           [1]   13  "username1"
*Aug 23 04:06:20.135: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 04:06:20.135: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 04:06:20.135: RADIUS:  NAS-IP-Address      [4]   6   10.1.1.147
*Aug 23 04:06:20.135: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 10.1.1.4:1646, Accounting-response,
 len 20
*Aug 23 04:06:20.139: RADIUS:  authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98 79
9D 5D
```

## アカウンティング終了

リモート ピアでのフロー（IPsec SA ペア）がなくなると、アカウンティング終了パケットが生成されます。

アカウンティング終了レコードには次の情報が格納されます。

- パケット出力
- パケット入力
- オクテット出力

- ギガワード入力
- ギガワード出力

次に、ルータ上で生成されたアカウント開始レコードを示します。アカウント開始レコードは、定義されている AAA サーバに送信されます。

```
*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
len 238
*Aug 23 04:20:16.519: RADIUS:  authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2 8A
3E E6
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=10.1.1.2"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No Progress"
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Time   [46]  6   709
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Octets   [42]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Octets  [43]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Packets  [47]  6   1004
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Packets [48]  6   1004
*Apr 23 04:20:16.519: RADIUS:  Acct-Input-Giga-Word[52]  6   0
*Apr 23 04:20:16.519: RADIUS:  Acct-Output-Giga-Wor[53]  6   0

*Aug 23 04:20:16.519: RADIUS:  Acct-Terminate-Cause[49]  6   none                      [0]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  32
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   26  "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS:  Acct-Status-Type    [40]  6   Stop                      [2]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 04:20:16.519: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 04:20:16.519: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 04:20:16.519: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 04:20:16.519: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646, Accounting-response,
 len 20
*Aug 23 04:20:16.523: RADIUS:  authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA B8
22 A0
```

## アカウンティング更新

アカウンティング更新がイネーブルな場合、セッションが「アップ」であればアカウンティング更新が送信されます。更新間隔は設定可能です。アカウンティング更新をイネーブルにするには、**aaa accounting update** コマンドを使用します。

次に、ルータから送信されるアカウンティング更新を示します。

```
Router#
*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
len 200
*Aug 23 21:46:05.263: RADIUS:  authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A F1
52 25
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Id     [44]  10  "00000003"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=10.1.1.2"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  36
```

```
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No Progress"
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Time   [46]  6   109
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Octets   [42]  6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Octets  [43]  6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Packets  [47]  6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Packets [48]  6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Status-Type    [40]  6   Watchdog                  [3]
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 21:46:05.263: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 21:46:05.263: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 21:46:05.263: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646, Accounting-response,
 len 20
*Aug 23 21:46:05.267: RADIUS:  authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A AC
1C
```

# IPsec VPN アカウンティングの設定方法

## IPsec VPN アカウンティングの設定

### はじめる前に

IPsec は、IPsec VPN アカウンティングを設定するより先に設定する必要があります。

## 手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaaauthenticationlogin***list-namemethod*
5. **aaaauthorizationnetwork***list-namemethod*
6. **aaaaccountingnetworklist-namestart-stop**[**broadcast**] **group** *group-name*
7. **aaasession-idcommon**
8. **cryptoisakmpprofile***profile-name*
9. **vrf***ivrf*
10. **matchidentitygroup***group-name*
11. **clientauthenticationlist***list-name*
12. **isakmpauthorizationlist***list-name*
13. **clientconfigurationaddress**[**initiate** | **respond**]
14. **accounting***list-name*
15. **exit**
16. **cryptodynamic-map***dynamic-map-name dynamic-seq-num*
17. **settransform-set***transform-set-name*
18. **setisakmp-profile***profile-name*
19. **reverse-route**[**remote-peer**]
20. **exit**
21. **cryptomap***map-name***ipsec-isakmpdynamic***dynamic-template-name*
22. **radius-serverhost***ip-address* [**auth-port** *port-number]* [**acct-port** *port-number*]
23. **radius-serverkey***string*
24. **radius-servervsasendaccounting**
25. **interface***typeslot/port*
26. **cryptomap***map-name*

## 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**<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **aaanew-model**<br><br>例：<br><br>`Router (config)# aaa new-model` | アカウンティングサーバに送信される定期的中間アカウンティングレコードをイネーブルにします。 |
| ステップ 4 | **aaaauthenticationlogin***list-namemethod*<br><br>例：<br><br>`Router (config)# aaa authentication login cisco-client group radius` | RADIUS またはローカル経由で、認証、許可、および拡張認可（XAUTH）のアカウンティング（AAA）認証を実行します。 |
| ステップ 5 | **aaaauthorizationnetwork***list-namemethod*<br><br>例：<br><br>`Router (config)# aaa authorization network cisco-client group radius` | RADIUS またはローカルから、リモートクライアント上の AAA 認証パラメータを設定します。 |
| ステップ 6 | **aaaaccountingnetworklist-namestart-stop**[**broadcast**] **group** *group-name*<br><br>例：<br><br>`Router (config)# aaa accounting network acc start-stop broadcast group radius` | RADIUS または TACACS+ を使用する場合の課金またはセキュリティのために、要求されたサービスのAAAアカウンティングをイネーブルにします。 |
| ステップ 7 | **aaasession-idcommon**<br><br>例：<br><br>`Router (config)# aaa session-id common` | コール内の各 AAA アカウンティングサービス タイプに、同じセッション ID を使用するかどうか、または、各アカウンティングサービスタイプに対して異なるセッション ID を割り当てるかどうかを指定します。 |
| ステップ 8 | **cryptoisakmpprofile***profile-name*<br><br>例：<br><br>`Route (config)# crypto isakmp profile cisco` | IPsec ユーザ セッションを監査し、isakmp-profile サブモードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 9 | **vrf***ivrf*<br><br>例：<br>`Router (conf-isa-prof)# vrf cisco` | オンデマンド アドレス プールを、バーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF）インスタンス名に関連付けます。 |
| ステップ 10 | **matchidentitygroup***group-name*<br><br>例：<br>`Router(conf-isa-prof)# match identity group cisco` | ISAKMP プロファイルのピアの ID を一致させます。 |
| ステップ 11 | **clientauthenticationlist***list-name*<br><br>例：<br>`Router(conf-isa-prof)# client authentication list cisco` | Internet Security Association and Key Management Protocol（ISAKMP）プロファイル内の IKE 拡張認証（XAUTH）を設定します。 |
| ステップ 12 | **isakmpauthorizationlist***list-name*<br><br>例：<br>`Router(conf-isa-prof)# isakmp authorization list cisco-client` | ISAKMP プロファイル内の AAA サーバを使用して、IKE 共有秘密およびその他のパラメータを設定します。一般に、共有秘密およびその他のパラメータは、モード設定（MODECFG）を介して、リモート ピアへプッシュされます。 |
| ステップ 13 | **clientconfigurationaddress**[**initiate** \| **respond**]<br><br>例：<br>`Router(conf-isa-prof)# client configuration address respond` | ISAKMP プロファイル内で IKE モード設定（MODECFG）を設定します。 |
| ステップ 14 | **accounting***list-name*<br><br>例：<br>`Router(conf-isa-prof)# accounting acc` | この ISAKMP プロファイルを介して接続しているすべてのピアの AAA アカウンティング サービスをイネーブルにします。 |
| ステップ 15 | **exit**<br><br>例：<br>`Router(conf-isa-prof)# exit` | isakmp-profile サブモードを終了します。 |
| ステップ 16 | **cryptodynamic-map***dynamic-map-name dynamic-seq-num*<br><br>例：<br>`Router(config)# crypto dynamic-map mymap 10 ipsec-isakmp` | ダイナミック クリプトマップテンプレートを作成し、クリプト マップ コンフィギュレーション コマンドモードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 17 | **settransform-set***transform-set-name*<br><br>例：<br><br>`Router(config-crypto-map)# set transform-set aswan` | クリプトマップテンプレートで使用可能なトランスフォーム セットを指定します。 |
| ステップ 18 | **setisakmp-profile***profile-name*<br><br>例：<br><br>`Router(config-crypto-map)# set isakmp-profile cisco` | ISAKMP プロファイル名を設定します。 |
| ステップ 19 | **reverse-route**[**remote-peer**]<br><br>例：<br><br>`Router(config-crypto-map)# reverse-route` | ルート（IP アドレス）を、VPN リモートトンネルエンドポイントの背後の宛先に対して注入できるようにします。また、トンネル エンドポイント自体に対するルートを設定することも可能です（クリプト マップの **remote-peer** キーワードを使用します）。 |
| ステップ 20 | **exit**<br><br>例：<br><br>`Router(config-crypto-map)# exit` | ダイナミック クリプト マップ コンフィギュレーション モードを終了します。 |
| ステップ 21 | **cryptomap***map-name***ipsec-isakmpdynamic***dynamic-template-name*<br><br>例：<br><br>`Router(config)# crypto map mymap ipsec-isakmp dynamic dmap` | クリプトマップ コンフィギュレーション モードを開始します。 |
| ステップ 22 | **radius-serverhost***ip-address* [**auth-port** *port-number]* [**acct-port** *port-number*]<br><br>例：<br><br>`Router(config)# radius-server host 172.16.1.4` | RADIUS サーバ ホストを指定します。 |
| ステップ 23 | **radius-serverkey***string*<br><br>例：<br><br>`Router(config)# radius-server key nsite` | ルータおよびRADIUSデーモン間のすべてのRADIUSコミュニケーションの認証キーおよび暗号キーを指定します。 |
| ステップ 24 | **radius-servervsasendaccounting**<br><br>例：<br><br>`Router(config)# radius-server vsa send accounting` | ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 25 | **interface***typeslot/port*<br><br>例：<br>`Router(config)# interface FastEthernet 1/0` | インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 26 | **cryptomap***map-name*<br><br>例：<br>`Router(config-if)# crypto map mymap` | インターフェイスに対して以前に定義されたクリプト マップ セットを適用します。 |

# アカウンティング更新の設定

セッションが「up」中にアカウンティング更新を送信するには、次の任意の作業を実行します。

### はじめる前に

IPSec VPN アカウンティングは、アカウンティング更新の設定前に設定する必要があります。詳細については、IPsec VPN アカウンティングの設定, （49 ページ）を参照してください。

### 手順の概要

1. **enable**
2. **configureterminal**
3. **aaaaccountingupdateperiodic***number*

### 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**<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **aaaaccountingupdateperiodic***number*<br><br>例：<br><br>`Router (config)# aaa accounting update periodic 1-2147483647` | （任意）アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。 |

# IPsec VPN アカウンティングのトラブルシューティング

IPsec アカウンティング イベントに関するメッセージを表示するには、次の任意の作業を実行します。

## 手順の概要

1. **enable**
2. **debugcryptoisakmpaaa**

## 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **debugcryptoisakmpaaa**<br><br>例：<br><br>`Router# debug crypto isakmp aaa` | IKE に関するメッセージを表示します。<br><br>• **aaa** キーワードによって、アカウンティング イベントが指定されます。 |

# IPsec VPN アカウンティングの設定例

## アカウンティングおよび ISAKMP プロファイル例

次に、アカウンティングおよび ISAKMP プロファイルを持つリモート アクセス クライアントをサポートするための設定する例を示します。

```
version 2.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto isakmp policy 10
hash md5
authentication pre-share
lifetime 200
crypto isakmp key cisco address 172.31.100.2
crypto iakmp client configuration group cclient
 key jegjegjhrg
 pool addressA

crypto-isakmp profile groupA
 vrf cisco
 match identity group cclient
 client authentication list cisco-client
 isakmp authorization list cisco-client
 client configuration address respond
 accounting acc
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto dynamic-map remotes 1
set peer 172.31.100.2
set security-association lifetime seconds 120
set transform-set esp-des-md5
reverse-route
!
crypto map test 10 ipsec-isakmp dynamic remotes
!
voice call carrier capacity active
!
```

```
interface Loopback0
ip address 10.20.20.20 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0
ip address 10.2.80.203 255.255.255.0
no ip mroute-cache
load-interval 30
duplex full
!
interface FastEthernet1/0
ip address 192.168.219.2 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.28.100.1 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.20.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
ip local pool addressA 192.168.1.1 192.168.1.253
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 5 15
 ntp server 172.31.150.52
end
```

# ISAKMP プロファイルなしのアカウンティング例

次に、ISAKMP プロファイルが使用されていない時にアカウンティング リモート アクセス ピアをサポートする Cisco IOS XE 設定全体の例を示します。

```
version 2.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
 lifetime 200
crypto isakmp key cisco address 172.31.100.2
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto map test client accounting list ipsecaaa
crypto map test 10 ipsec-isakmp
 set peer 172.31.100.2
 set security-association lifetime seconds 120
 set transform-set esp-des-md5
 match address 101
!
voice call carrier capacity active
!
interface Loopback0
 ip address 10.20.20.20 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.2.80.203 255.255.255.0
 no ip mroute-cache
 load-interval 30
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.219.2 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/1
```

```
 ip address 172.28.100.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.30.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
 permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 5 15
!
exception core-file ioscrypto/core/sheep-core
exception dump 172.25.1.129
ntp clock-period 17208229
ntp server 172.71.150.52
!
end
```

# その他の参考資料

## 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| AAA アカウンティングの設定 | 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』の「Configuring Accounting」モジュール |

| 関連項目 | マニュアル タイトル |
|---|---|
| IPsec VPN アカウンティングの設定 | 『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」モジュール |
| 基本 AAA RADIUS の設定 | 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』の「Configuring RADIUS」モジュール |
| ISAKMP プロファイルの設定 | 『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「VRF-Aware IPsec」モジュール |
| TACACS+ および RADIUS での権限レベル | • 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』の「Configuring TACACS+」モジュール<br>• 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』の「Configuring RADIUS」モジュール |
| IP セキュリティ、RADIUS、および AAA コマンド | 『*Cisco IOS Security Command Reference*』 |

# 標準

| 標準 | タイトル |
|---|---|
| なし。 | -- |

# MIB

| MIB | MIB のリンク |
|---|---|
| なし。 | 選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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。<br>http://www.cisco.com/go/mibs |

## RFC

| RFC | タイトル |
|---|---|
| なし。 | |

## シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。<br>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。<br>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。 | http://www.cisco.com/cisco/web/support/index.html |

# IPsec VPN アカウンティングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6*：***IPsec VPN*** アカウンティングの機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| IPsec VPN アカウンティング | Cisco IOS XE Release 2.1 | IPsec VPN アカウンティング機能を使用すれば、セッションが開始される時と終了する時を指示することによって、セッションをアカウンティングできます。<br>VPN セッションとは、IKE SA および、IKE SA によって作成される 1 つ以上の SA ペアとして定義されます。セッションは、最初の IPsec ペアが作成されると開始し、すべての IPsec SA が削除されると停止します。<br>セッション識別情報およびセッション使用状況情報が、標準的な RADIUS 属性および VSA を介して、RADIUS サーバに渡されます。<br>次のコマンドが、新たに導入または変更されました。**clientauthenticationlist**、**clientconfigurationaddress**、**cryptoisakmpprofile**、**cryptomap(globalIPsec)**、**debugcryptoisakmp**、**isakmpauthorizationlist**、**matchidentity**、**setisakmp-profile**、**vrf**。 |

# 用語集

**IKE**：インターネット キー エクスチェンジ。IKE によって、キーが必要なサービス（IP セキュリティ（IPsec）など）のための共有セキュリティ ポリシーおよび認証キーが確立されます。IPsec トラフィックを通過させる前に、ルータ、ファイアウォール、ホストそれぞれでピアの ID を検証する必要があります。それには、事前共有キーを両ホストに手動で入力するか、認証局（CA）サービスを使用します。

**IPsec**：IP セキュリティ。IPsec はオープン規格のフレームワークであり、これにより、参加ピア間でデータ機密性、データ整合性、およびデータ認証が提供されます。IPsec では、これらのセキュリティ サービスが IP レイヤで実現されます。IPsec では、ローカル ポリシーに基づいたプロトコルやアルゴリズムのネゴシエーションの処理や、IPsec に使用される暗号キーや認証キーの生成が、IKE を通じて行われます。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

**ISAKMP**：インターネット セキュリティ アソシエーションおよびキー管理プロトコル。ISAKMP は、セキュリティ アソシエーションのネゴシエーション、確立、変更、および削除を行うインターネット IPsec プロトコル（RFC 2408）です。また、キー生成および認証データ（特定のキー生成メカニズムとは独立しています）、キー確立プロトコル、暗号化アルゴリズム、または認証メカニズムも交換されます。

**L2TP セッション**：レイヤ 2 転送プロトコル。L2TP は、単一の PPP 接続のトンネリングがサポートされた、L2TP アクセス コンセントレータ（LAC）と L2TP ネットワーク サーバ（LNS）の間における通信トランザクションです。PPP 接続、L2TP セッション、および L2TP コールの間に 1 対 1 の関係があります。

**NAS**：ネットワーク アクセス サーバ。NAS は、パケットの世界（インターネットなど）と回線の世界（公衆電話交換網（PSTN））との間のインターフェイスとなるシスコのプラットフォーム（または複数のプラットフォームの集まり。AccessPath システムなど）です。

**PFS**：Perfect Forward Secrecy（完全転送秘密）。PFS は、導き出される共有秘密値に関連する暗号特性です。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。

**QM**：キュー マネージャ。Cisco IP Queue Manager（IP QM）は、インテリジェントで、IP ベースの、コール処理およびルーティング ソリューションであり、Cisco IP Contact Center（PCC）ソリューションの一部として、強力なコール処理オプションが提供されます。

**RADIUS**：リモート認証ダイヤルイン ユーザ サービス。RADIUS は、モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

**RSA**：Rivest、Shamir、および Adelman。Rivest、Shamir、および Adelman は、暗号化および認証に使用可能な公開キー暗号化システムの発明者たちです。

**SA**：セキュリティ アソシエーション。SA は、データ フローに適用されるセキュリティ ポリシーおよびキー関連情報のインスタンスです。

**TACACS+**：Terminal Access Controller Access Control System Plus。TACACS+ は、ユーザによるルータまたはネットワーク アクセス サーバへのアクセス試行の集中的な確認を可能にするセキュリティ アプリケーションです。

**VPN**：バーチャル プライベート ネットワークVPN を使用すると、ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN は「トンネリング」を使用して、IP レベルですべての情報を暗号化します。

**VRF**：VPN ルーティング/転送（VRF）インスタンス。VRF は、IP ルーティング テーブル、取得されたルーティングテーブル、そのルーティングテーブルを使用する一連のインターフェイス、ルーティングテーブルに登録されるものを決定する一連のルールおよびルーティングプロトコル

で構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。

**VSA**：ベンダー固有属性。VSA は、特定のベンダーによって実装された属性です。Vendor-Specific 属性が使用された結果、AV ペアがカプセル化されます。基本的には、Vendor-Specific = プロトコル:Attribute = 値となります。

**XAUTH**：拡張認証。XAUTH は、IKE フェーズ 1 と IKE フェーズ 2 の間における任意の交換です。XAUTH では、ルータが、（ピアの認証ではなく）実際のユーザの認証試行において、追加の認証情報を要求します。

第 6 章

# IPsec Usability Enhancements

IPsec Usability Enhancements 機能では、IPsec バーチャル プライベート ネットワーク（VPN）の設定およびモニタリングを簡単にする機能が導入されています。この機能の利点としては、IPsec およびインターネット キー交換（IKE）のインテリジェントなデフォルト、および IPsec VPN を簡単に確認およびトラブルシューティングできる機能などがあります。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

# IPsec Usability Enhancements の前提条件

- IPsec、IKE、および暗号化の知識が必要です。
- IPsec を設定し、ルータ上の IKE をイネーブルにしておく必要があります。
- ルータ上で Cisco IOS XE k9 暗号イメージを実行する必要があります。

# IPsec Usability Enhancements に関する情報

## IPsec の概要

IPsec は、インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークであり、パブリック ネットワークを介して機密性の高い情報を送信する際にセキュリティを確保します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。

IPsec では、2 つのピア間におけるセキュアなトンネルが提供されます。機密性の高いパケットを定義し、そのパケットをこれらのセキュアなトンネルを介して送信されるように定義できます。また、トンネルの特性を指定することによって、このように機密性の高いパケットを保護するために使用されるパラメータを定義できます。IPsec ピアによってこのように機密性の高いパケットが検出されたら、そのピアによって、適切かつセキュアなトンネルが設定され、そのパケットがトンネルからリモート ピアに送信されます。

## IPsec の動作

IPsec の動作は 5 つの基本的な手順で構成されています。対象となるトラフィックの識別、IKE フェーズ 1、IKE フェーズ 2、トンネルまたは IPsec セッションの確立、そして最後にトンネルの切断です。

### ステップ 1：対象となるトラフィックの識別

VPN デバイスによって、検出対象のトラフィック、つまり機密性の高いパケットが認識されます。IPsec が機密性の高いパケットに適用されるか、パケットがバイパスされるか、または、パケットが廃棄されます。トラフィックのタイプに基づき、IPsec が適用されると、IKE フェーズ 1 が開始されます。

### ステップ 2：IKE フェーズ 1

IKE セキュリティ ポリシーのネゴシエーションを行い、セキュアなチャネルを確立するために、VPN デバイス間で 3 回の交換が実行されます。

最初の交換の間、VPN デバイスによって、IKE 交換を保護するための IKE トランスフォーム セットのマッチングのネゴシエーションが行われ、その結果、使用する Internet Security Association and Key Management Protocol（ISAKMP）ポリシーが確立されます。ISAKMP ポリシーは、暗号化アルゴリズム、ハッシュ アルゴリズム、認証アルゴリズム、デフィーヘルマン（DH）グループ、およびライフタイム パラメータで構成されています。

8 種類のデフォルト ISAKMP ポリシーがサポートされています。デフォルト ISAKMP ポリシーの詳細については、IKE フェーズ 1 ISAKMP デフォルト ポリシーの確認,（67 ページ）を参照してください。

2 番目の交換は Diffie-Hellman 交換です。共有秘密が確立されます。

3 番目の交換では、ピアのアイデンティティが認証されます。ピアが認証されると、IKE フェーズ 2 が開始されます。

#### ステップ 3：IKE フェーズ 2

VPN デバイスによって、IPsec データの保護に使用される IPsec セキュリティ ポリシーのネゴシエーションが行われます。IPsec トランスフォーム セットがネゴシエートされます。

トランスフォーム セットは、ネットワーク トラフィックのセキュリティ ポリシーを制定するアルゴリズムおよびプロトコルの組み合わせです。デフォルト トランスフォーム セットの詳細については、デフォルト IPsec トランスフォーム セットの確認,（72 ページ）を参照してください。VPN トンネル確立の準備ができました。

#### ステップ 4：Tunnel--IPsec の確立

VPN デバイスによって、セキュリティ サービスが IPsec トラフィックに適用され、次に、IPsec データが送信されます。セキュリティ アソシエーション（SA）がピア間で交換されます。IPsec セッションがアクティブの間、ネゴシエートされたセキュリティ サービスがトンネル トラフィックに適用されます。

#### ステップ 5：トンネルの終了

IPsec SA ライフタイムのタイムアウトが発生するか、パケット カウンタが超過すると、トンネルが切断されます。IPsec SA が削除されます。

# IPsec Usability Enhancements の活用方法

## IKE フェーズ 1 ISAKMP デフォルト ポリシーの確認

IKE ネゴシエーションが開始されると、ピアによって共通ポリシーの検出が試行され、検出はリモート ピア上で指定された最も高いプライオリティを持つポリシーから開始されます。一致が存在するまで、ピアによって、ポリシー セットのネゴシエーションが行われます。各ピアに共通のポリシー セットが複数存在する場合、最も低いプライオリティを持つ番号が使用されます。

IKE フェーズ 1、ISAKMP、ポリシーのプライオリティの範囲および動作によって定義された各種ポリシーの 3 つのグループがあります。

- デフォルト ISAKMP ポリシー。自動的にイネーブルにされます。
- ユーザ ISAKMP 設定ポリシー。**crypto isakmp policy** コマンドを使用して設定できます。
- Easy VPN ISAKMP ポリシー。Easy VPN 設定中に使用可能にされます。

この項では、ISAKMP ポリシーの 3 つのグループに関して、互いの関係の中での動作、使用中のポリシーを適切な **show** コマンドを使用して特定する方法、および、デフォルト ISAKMP ポリシーをディセーブルにする方法について説明します。

## デフォルト IKE フェーズ 1 ポリシー

8 種類のデフォルト IKE フェーズ 1、ISAKMP、各種ポリシーがサポートされています（下表を参照）。自動的にイネーブルにされます。**cryptoisakmppolicy** コマンドを使用して IKE ポリシーを手動で設定していない場合、または **nocryptoisakmpdefaultpolicy** コマンドを使用してデフォルト IKE ポリシーを無効にしていない場合、ピア IKE ネゴシエーション中はデフォルトの IKE ポリシーが使用されます。**showcryptoisakmppolicy** コマンドまたは **showcryptoisakmpdefaultpolicy** コマンドのいずれかを発行して、デフォルトの IKE ポリシーが使用されていることを確認できます。

（注） セキュリティの脅威と、それに対抗するための暗号化技術は常に変化しています。シスコの最新の暗号化に関する推奨事項については、『Next Generation Encryption（NGE）』ホワイトペーパーを参照してください。

デフォルト IKE ポリシーによって、次のポリシー セット パラメータが定義されます。

- プライオリティ、65507 ～ 65514。65507 が最も高いプライオリティで、65514 が最も低いプライオリティ。
- 認証方式、Rivest、Shamir、および Adelman（RSA）または事前共有キー（PSK）。
- 暗号方式、Advanced Encryption Standard（AES）または Triple Data Encryption Standard（3DES）。
- ハッシュ関数、Secure Hash Algorithm（SHA-1）または Message-Digest algorithm 5（MD5）。
- DH グループ仕様 DH2 または DH5。
  - DH2 では、768 ビット DH グループが指定されます。
  - DH5 では、1536 ビット DH グループが指定されます。

（注） 3DES、MD5、および DH グループ 1、2、5 の使用は推奨しません。シスコの最新の暗号化に関する推奨事項については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。IKE 設定の詳細については、『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の「Configuring Internet Key Exchange for IPsec VPNs」の章を参照してください。

表 *7*：デフォルト *IKE* フェーズ *1*、*ISAKMP*、ポリシー

| プライオリティ | 認証 | 暗号化 | ハッシュ | Diffie-Hellman |
|---|---|---|---|---|
| 65507 | RSA | AES | SHA | DH5 |
| 65508 | PSK | AES | SHA | DH5 |
| 65509 | RSA | AES | MD5 | DH5 |
| 65510 | PSK | AES | MD5 | DH5 |
| 65511 | RSA | 3DES | SHA | DH2 |
| 65512 | PSK | 3DES | SHA | DH2 |
| 65513 | RSA | 3DES | MD5 | DH2 |
| 65514 | PSK | 3DES | MD5 | DH2 |

## ユーザ設定 IKE ポリシー

**crypto isakmp policy** コマンドを使用して、IKE ポリシーを設定できます。ユーザ設定 IKE ポリシーは一意に識別され、1 ～ 10000 の範囲のプライオリティ番号が使用されて設定されます。1 が最も高いプライオリティで、10000 は最も低いプライオリティです。

1 ～ 10000 のプライオリティを持つ 1 つ以上の IKE ポリシーを設定した結果は次のとおりです。

- ピア IKE ネゴシエーション中にユーザ設定ポリシーが使用されます。
- ピア IKE ネゴシエーション中にデフォルト IKE ポリシーが使用されます。
- **show crypto isakmp policy** コマンドを発行することによって、ユーザ設定ポリシーを表示できます。

## Easy VPN ISAKMP ポリシー

Easy VPN（「Easy VPN ISAKMP ポリシー，（69 ページ）」を参照）を設定した場合、使用中のデフォルト Easy VPN ISAKMP ポリシーは、65515 ～ 65535 の範囲のプライオリティ番号で一意に識別されます。65515 が最も高いプライオリティで、65535 は最も低いプライオリティです。

ユーザが Easy VPN を設定した結果は次のとおりです。

- ピア Easy VPN ISAKMP ネゴシエーション中に、デフォルト EzVPN ISAKMP ポリシーおよびデフォルト IKE ポリシーが使用されます。
- **showcryptoisakmppolicy** コマンドを発行することによって、Easy VPN ISAKMP ポリシーおよびデフォルト IKE ポリシーを表示できます。
- デフォルト ISAKMP ポリシーは、**nocryptoisakmpdefaultpolicy** コマンドを発行して無効にしない限り、**showcryptoisakmpdefaultpolicy** コマンドを発行すると表示されます。

## 手順の概要

1. **enable**
2. **showcryptoisakmpdefaultpolicy**
3. **configureterminal**
4. **nocryptoisakmpdefaultpolicy**

## 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **showcryptoisakmpdefaultpolicy**<br><br>例：<br><br>`Router# show crypto isakmp default policy` | （任意）1 ～ 10000 のプライオリティを持つポリシーが設定されていない場合、デフォルト ISAKMP ポリシーを表示します。 |
| ステップ 3 | **configureterminal**<br><br>例：<br><br>`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 4 | **nocryptoisakmpdefaultpolicy**<br><br>例：<br><br>`Router(config)# no crypto isakmp default policy` | （任意）65507 ～ 65514 のプライオリティを持つデフォルト ISAKMP ポリシーをオフにします。 |

### 例

次に、**showcryptoisakmpdefaultpolicy** コマンドのサンプル出力を示します。デフォルト ポリシーがディセーブルにされていないので、デフォルト ポリシーが表示されています。

```
Router# show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

次に、デフォルト IKE ポリシーがディセーブルにされてからの、**showcryptoisakmpdefaultpolicy** コマンドの出力結果の例を示します。ここでは、結果は空白になっています。

```
Router# configure terminal
Router(config)# no crypto isakmp default policy
Router(config)# exit
Router# show crypto isakmp default policy
Router#
!There is no output since the default IKE policies have been disabled.
```

次に、デフォルト ISAKMP ポリシーが使用中の時はいつでも生成されるシステム ログ メッセージの例を示します。

```
%CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

# デフォルト IPsec トランスフォーム セットの確認

トランスフォームセットは、特定のセキュリティプロトコルとアルゴリズムを組み合わせたものです。IPsec SA のネゴシエーション中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

IKE との IPsec SA のネゴシエーション中に、ピアは両方のピア上で同じトランスフォーム セットを検索します。同一のトランスフォームセットが検出された場合、そのトランスフォームセットが選択され、両方のピアの IPsec SA の一部として、保護するトラフィックに適用されます。

## デフォルト トランスフォーム セット

他のトランスフォームセットが設定されておらず、次の条件が満たされている場合、1つのデフォルト トランスフォーム セットがすべてのクリプト マップまたは IPsec プロファイルによって使用されます。

- デフォルト トランスフォーム セットが、**nocryptoipsecdefaulttransform-set** コマンドによってディセーブルにされていない。
- 使用中の暗号化エンジンで、暗号化アルゴリズムがサポートされている。

下図に示すとおり、2つのデフォルト トランスフォーム セットのそれぞれによって、Encapsulation Security Protocol（ESP）暗号化トランスフォーム タイプおよび ESP 認証トランスフォーム タイプが定義されます。

**表 *8*：デフォルト トランスフォーム セットおよびパラメータ**

| デフォルト トランスフォーム名 | ESP 暗号化トランスフォームおよび説明 | ESP 認証トランスフォームおよび説明 |
|---|---|---|
| #$!default_transform_set_0 | esp-3des<br>（168 ビット 3DES またはトリプル DES 暗号化アルゴリズムを持つ EDP） | esp-sha-hmac |
| #$!default_transform_set_1 | esp-aes<br>（128 ビット AES 暗号化アルゴリズムを持つ ESP） | esp-sha-hmac<br>（SHA-1、ハッシュ メッセージ認証コード [HMAC] バリアント認証アルゴリズムを持つ ESP） |

## 手順の概要

1. **enable**
2. **showcryptoipsecdefaulttransform-set**
3. **configureterminal**
4. **nocryptoipsecdefaulttransform-set**

## 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**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **showcryptoipsecdefaulttransform-set**<br><br>例：<br><br>`Router# show crypto ipsec default transform-set` | （任意）IKE によって現在使用中のデフォルト IPsec トランスフォーム セットを表示します。 |
| ステップ 3 | **configureterminal**<br><br>例：<br><br>`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 4 | **nocryptoipsecdefaulttransform-set**<br><br>例：<br><br>`Router(config)# no crypto ipsec default transform-set` | （任意）デフォルト IPsec トランスフォーム セットを表示します。 |

### 例

```
The following example displays output from the show crypto ipsec default transform-set
 command when the default transform sets are enabled, the default setting:
Router# show crypto ipsec default transform-set
Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

次に、**nocryptoipsecdefaulttransform-set** コマンドを使用してデフォルト トランスフォーム セットを無効にした場合の、**showcryptoipsecdefaulttransform-set** コマンドの出力例を示します。

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set
! There is no output.
Router#
```

次に、IPsec SA がデフォルト トランスフォーム セットでネゴシエーションを行った時はいつでも生成されるシステム ログ メッセージ例を示します。

```
%CRYPTO-5-IPSEC_DEFAULT_TRANSFORM: Using Default IPsec transform-set
```

# IPsec VPN 確認および IPsec VPN のトラブルシューティング

IKE フェーズ 1 または IKE フェーズ 2 を確認したいのか、または IPsec VPN のトラブルシューティングを行いたいのかによって、この項における次の任意の作業のいずれかを実行します。

## IKE フェーズ 1 ISAKMP の確認

ISAKMP トンネルの統計情報を表示するには、次のオプション コマンドを使用します。

### 手順の概要

1. **showcryptomibisakmpflowmibfailure[vrf***vrf-name***]**
2. **showcryptomibisakmpflowmibglobal[vrf***vrf-name***]**
3. **showcryptomibisakmpflowmibhistory[vrf***vrf-name***]**
4. **showcryptomibisakmpflowmibpeer[index***peer-mib-index***][vrf***vrf-name***]**
5. **showcryptomibisakmpflowmibtunnel[index***tunnel-mib-index***][vrf***vrf-name***]**

### 手順の詳細

**ステップ 1** **showcryptomibisakmpflowmibfailure[vrf***vrf-name***]**

ISAKMP トンネルにエラーが発生した場合、このコマンドでイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib failure
 vrf Global
  Index:                        1
  Reason:                       peer lost
  Failure time since reset:     00:07:27
  Local type:                   ID_IPV4_ADDR
  Local value:                 192.0.2.1
  Remote type:                  ID_IPV4_ADDR
  Remote Value:                 192.0.2.2
  Local Address:                192.0.2.1
```

```
  Remote Address:              192.0.2.2
  Index:                       2
  Reason:                      peer lost
  Failure time since reset:    00:07:27
  Local type:                  ID_IPV4_ADDR
  Local value:                192.0.3.1
  Remote type:                 ID_IPV4_ADDR
  Remote Value:                192.0.3.2
  Local Address:               192.0.3.1
  Remote Address:              192.0.3.2
  Index:                       3
  Reason:                      peer lost
  Failure time since reset:    00:07:32
  Local type:                  ID_IPV4_ADDR
  Remote type:                 ID_IPV4_ADDR
  Remote Value:                192.0.2.2
  Local Address:               192.0.2.1
  Remote Address:              192.0.2.2
```

**ステップ 2** **showcryptomibisakmpflowmibglobal[vrf***vrf-name***]**

このコマンドを発行することによって、グローバルISAKMPトンネル統計情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib global
vrf Global
  Active Tunnels:                          3
  Previous Tunnels:                        0
  In octets:                               2856
  Out octets:                              3396
  In packets:                              16
  Out packets:                             19
  In packets drop:                         0
  Out packets drop:                        0
  In notifys:                              4
  Out notifys:                             7
  In P2 exchg:                             3
  Out P2 exchg:                            6
  In P2 exchg invalids:                    0
  Out P2 exchg invalids:                   0
  In P2 exchg rejects:                     0
  Out P2 exchg rejects:                    0
  In IPSEC delete:                         0
  Out IPSEC delete:                        0
  SAs locally initiated:                   3
  SAs locally initiated failed:            0
  SAs remotely initiated failed:           0
  System capacity failures:                0
  Authentication failures:                 0
  Decrypt failures:                        0
  Hash failures:                           0
  Invalid SPI:                             0
```

**ステップ 3** **showcryptomibisakmpflowmibhistory[vrf***vrf-name***]**

アクティブにならないISAKMPトンネルの情報については、このコマンドによって、トンネルが終了した原因を含むイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib history
vrf Global
  Reason:                             peer lost
  Index:                              2
```

```
Local type:                          ID_IPV4_ADDR
Local address:                       192.0.2.1
Remote type:                         ID_IPV4_ADDR
Remote address:                      192.0.2.2
Negotiation mode:                    Main Mode
Diffie Hellman Grp:                  2
Encryption algo:                     des
Hash algo:                           sha
Auth method:                         psk
Lifetime:                            86400
Active time:                         00:06:30
Policy priority:                     1
Keepalive enabled:                   Yes
In octets:                           3024
In packets:                          22
In drops:                            0
In notifys:                          18
In P2 exchanges:                     1
In P2 exchg invalids:                0
In P2 exchg rejected:                  0
In P2 SA delete reqs:                  0
Out octets:                            4188
Out packets:                           33
Out drops:                             0
Out notifys:                           28
Out P2 exchgs:                         2
Out P2 exchg invalids:                 0
Out P2 exchg rejects:                  0
Out P2 Sa delete requests:             0
Reason:                                peer lost
Index:                                 3
Local type:                            ID_IPV4_ADDR
Local address:                         192.0.3.1
Remote type:                           ID_IPV4_ADDR
Remote address:                        192.0.3.2
Negotiation mode:                      Main Mode
Diffie Hellman Grp:                    2
Encryption algo:                       des
Hash algo:                             sha
Auth method:                           psk
Lifetime:                              86400
Active time:                           00:06:25
Policy priority:                       1
Keepalive enabled:                     Yes
In octets:                             3140
In packets:                            23
In drops:                              0
In notifys:                            19
In P2 exchanges:                       1
In P2 exchg invalids:                  0
In P2 exchg rejected:                  0
In P2 SA delete reqs:                  0
Out octets:                            4304
Out packets:                           34
Out drops:                             0
Out notifys:                           29
Out P2 exchgs:                         2
Out P2 exchg invalids:                 0
Out P2 exchg rejects:                  0
Out P2 Sa delete requests:             0
```

**ステップ 4** **showcryptomibisakmpflowmibpeer[index***peer-mib-index***][vrf***vrf-name***]**

アクティブな ISAKMP ピア アソシエーションについては、このコマンドによって、インデックス、接続タイプ、およびIPアドレスを含む情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib peer
```

```
vrf Global
  Index:              1
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.2.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.2.2
  Index:              2
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.3.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.3.1
  Index:              3
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.4.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.4.1
```

**ステップ 5** **showcryptomibisakmpflowmibtunnel[index***tunnel-mib-index***][vrf***vrf-name***]**

アクティブな ISAKMP トンネルについては、このコマンドによって、トンネルの統計情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib tunnel
vrf Global
  Index:                      1
  Local type:                 ID_IPV4_ADDR
  Local address:              192.0.2.1
  Remote type:                ID_IPV4_ADDR
  Remote address:             192.0.2.2
  Negotiation mode:           Main Mode
  Diffie Hellman Grp:         2
  Encryption algo:            des
  Hash algo:                  sha
  Auth method:                psk
  Lifetime:                   86400
  Active time:                00:03:08
  Policy priority:            1
  Keepalive enabled:          Yes
  In octets:                  2148
  In packets:                 15
  In drops:                   0
  In notifys:                 11
  In P2 exchanges:            1
  In P2 exchg invalids:       0
  In P2 exchg rejected:       0
  In P2 SA delete reqs:       0
  Out octets:                 2328
  Out packets:                16
  Out drops:                  0
  Out notifys:                12
  Out P2 exchgs:              2
  Out P2 exchg invalids:      0
  Out P2 exchg rejects:       0
  Out P2 Sa delete requests:  0
```

## IKE フェーズ 2 の確認

IPsec フェーズ 2 トンネルの統計情報を表示するには、次のオプション コマンドを使用します。

## 手順の概要

1. **showcryptomibipsecflowmibendpoint[vrf***vrf-name***]**
2. **showcryptomibipsecflowmibfailure[vrf***vrf-name***]**
3. **showcryptomibipsecflowmibglobal[vrf***vrf-name***]**
4. **showcryptomibipsecflowmibhistory[vrf***vrf-name***]**
5. **showcryptomibipsecflowmibspi[vrf***vrf-name***]**
6. **showcryptomibipsecflowmibtunnel**[**index***tunnel-mib-index*][**vrf***vrf-name***]**

## 手順の詳細

**ステップ 1** **showcryptomibipsecflowmibendpoint[vrf***vrf-name***]**

このコマンドを発行することによって、IPsec フェーズ 2 トンネルに関連付けられた、各アクティブ エンドポイント、ローカルまたはリモートデバイスの情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router#  show crypto mib ipsec flowmib endpoint
vrf Global
  Index:                1
  Local type:           Single IP address
  Local address:        192.1.2.1
  Protocol:             0
  Local port:           0
  Remote type:          Single IP address
  Remote address:       192.1.2.2
  Remote port:          0
  Index:                2
  Local type:           Subnet
  Local address:        192.1.3.0 255.255.255.0
  Protocol:             0
  Local port:           0
  Remote type:          Subnet
  Remote address:       192.1.3.0 255.255.255.0
  Remote port:          0
```

**ステップ 2** **showcryptomibipsecflowmibfailure[vrf***vrf-name***]**

ISAKMP トンネルにエラーが発生した場合、このコマンドでイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib failure
vrf Global
  Index:                        1
  Reason:                       Operation request
  Failure time since reset:     00:25:18
  Src address:                  192.1.2.1
  Destination address:          192.1.2.2
  SPI:                          0
```

**ステップ 3** **showcryptomibipsecflowmibglobal[vrf***vrf-name***]**

このコマンドを発行することによって、グローバルIKEフェーズ2トンネルの統計情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib global
 vrf Global
  Active Tunnels:                     2
  Previous Tunnels:                   0
  In octets:                          800
  Out octets:                         1408
  In packets:                         8
  Out packets:                        8
  Uncompressed encrypted bytes:    1408
  In packets drops:                   0
  Out packets drops:                  2
  In replay drops:                    0
  In authentications:                 8
  Out authentications:                8
  In decrypts:                        8
  Out encrypts:                       8
  Compressed bytes:                   0
  Uncompressed bytes:                 0
  In uncompressed bytes:              0
  Out uncompressed bytes:             0
  In decrypt failures:                0
  Out encrypt failures:               0
  No SA failures:                     0
! Number of SA Failures.
  Protocol use failures:              0
  System capacity failures:           0
  In authentication failures:         0
  Out authentication failures:        0
```

**ステップ 4** **showcryptomibipsecflowmibhistory[vrf***vrf-name***]**

アクティブにならないIKEフェーズ2トンネルの情報については、このコマンドによって、トンネルが終了した原因を含むイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib history
vrf Global
  Reason:                      Operation request
  Index:                       1
  Local address:               192.1.2.1
  Remote address:              192.1.2.2
  IPSEC keying:                IKE
  Encapsulation mode:          1
  Lifetime (KB):               4608000
  Lifetime (Sec):              3600
  Active time:                 00:24:32
  Lifetime threshold (KB):     423559168
  Lifetime threshold (Sec):    3590000
  Total number of refreshes:   0
  Expired SA instances:        4
  Current SA instances:        4
  In SA DH group:              14
  In sa encrypt algorithm      aes
  In SA auth algorithm:        rsig
  In SA ESP auth algo:         ESP_HMAC_SHA
  In SA uncompress algorithm:  None
  Out SA DH group:             14
  Out SA encryption algorithm: aes
  Out SA auth algorithm:       ESP_HMAC_SHA
```

```
  Out SA ESP auth algorithm:   ESP_HMAC_SHA
  Out SA uncompress algorithm: None
  In octets:                   400
  Decompressed octets:         400
  In packets:                  4
  In drops:                        0
  In replay drops:                 0
  In authentications:              4
  In authentication failures:      0
  In decrypts:                     4
  In decrypt failures:             0
  Out octets:                      704
  Out uncompressed octets:         704
  Out packets:                     4
  Out drops:                       1
  Out authentications:             4
  Out authentication failures:     0
  Out encryptions:                 4
  Out encryption failures:         0
  Compressed octets:               0
  Decompressed octets:             0
  Out uncompressed octets:         704
```

**ステップ 5** **showcryptomibipsecflowmibspi[vrf***vrf-name***]**

security protection index（SPI）テーブルには、アクティブおよび期限切れの各セキュリティ IKE フェーズ 2 アソシエーションのエントリが格納されます。次に、このコマンドのサンプル出力を示します。SPI テーブルが表示されています。

例：

```
Router# show crypto mib ipsec flowmib spi
vrf Global
  Tunnel Index:          1
  SPI Index:            1
  SPI Value:            0xCC57D053
  SPI Direction:        In
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            2
  SPI Value:            0x68612DF
  SPI Direction:        Out
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            3
  SPI Value:            0x56947526
  SPI Direction:        In
  SPI Protocol:         ESP
  SPI Status:           Active
  SPI Index:            4
  SPI Value:            0x8D7C2204
  SPI Direction:        Out
  SPI Protocol:         ESP
  SPI Status:           Active
```

**ステップ 6** **showcryptomibipsecflowmibtunnel[index***tunnel-mib-index***][vrf***vrf-name***]**

アクティブな IKE フェーズ 2 トンネルについては、このコマンドによって、トンネルの統計情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib tunnel
vrf Global
  Index:                            1
```

```
Local address:                      192.0.2.1
Remote address:                     192.0.2.2
IPSEC keying:                       IKE
Encapsulation mode:                 1
Lifetime (KB):                      4608000
Lifetime (Sec):                     3600
Active time:                        00:05:46
Lifetime threshold (KB):            64
Lifetime threshold (Sec):           10
Total number of refreshes:          0
Expired SA instances:               0
Current SA instances:               4
In SA DH group:                     14
In sa encrypt algorithm:            aes
In SA auth algorithm:               rsig
In SA ESP auth algo:                ESP_HMAC_SHA
In SA uncompress algorithm:         None
Out SA DH group:                    14
Out SA encryption algorithm:        aes
Out SA auth algorithm:              ESP_HMAC_SHA
Out SA ESP auth algorithm:          ESP_HMAC_SHA
Out SA uncompress algorithm:        None
In octets:                             400
Decompressed octets:                   400
In packets:                            4
In drops:                              0
In replay drops:                       0
In authentications:                    4
In authentication failures:            0
In decrypts:                           4
In decrypt failures:                   0
Out octets:                            704
Out uncompressed octets:               704
Out packets:                           4
Out drops:                             1
Out authentications:                   4
Out authentication failures:           0
Out encryptions:                       4
Out encryption failures:               0
Compressed octets:                     0
Decompressed octets:                   0
Out uncompressed octets:               704
```

## IPsec VPN のトラブルシューティング

問題のトラブルシューティングを行う場合、**show tech-support ipsec** コマンドを使用すれば、IPsec 関連情報の収集が簡単にできます。

### 手順の概要

1. **showtech-supportipsec**

### 手順の詳細

**showtech-supportipsec**

**show tech-support ipsec** コマンドには、3 つのバリエーションがあります。

- **showtech-supportipsec**

- **showtech-supportipsecpeer***ipv4address*
- **showtech-supportipsecvrf***vrf-name*

各バリエーションについて次に示す個々の **show** コマンドに関する **show tech-support ipsec** コマンドからの出力のサンプル表示については、「IPsec VPN のトラブルシューティング，（81 ページ）」を参照してください。

**show tech-support ipsec コマンドの出力**

キーワードを何も指定しないで **show tech-support ipsec** コマンドを入力すると、コマンドの出力には、次の **show** コマンドが出力順に表示されます。

- **showversion**
- **showrunning-config**
- **showcryptoisakmpsacount**
- **showcryptoipsecsacount**
- **showcryptosessionsummary**
- **showcryptosessiondetail**
- **showcryptoisakmpsadetail**
- **showcryptoipsecsadetail**
- **showcryptoisakmppeers**
- **showcryptorulesetdetail**
- **showprocessesmemory|includeCryptoIKMP**
- **showprocessescpu|includeCryptoIKMP**
- **showcryptoeli**
- **showcryptoengineacceleratorstatistic**

**show tech-support ipsec peer コマンドの出力**

**peer** キーワードと *ipv4address* 引数を指定して **show tech-support ipsec** コマンドを入力すると、出力に次の **show** コマンドが、指定したピアの出力順に表示されます。

- **showversion**
- **showrunning-config**
- **showcryptosessionremote***ipv4address***detail**
- **showcryptoisakmpsapeer***ipv4address***detail**
- **showcryptoipsecsapeer***ipv4address***detail**
- **showcryptoisakmppeers***ipv4address*
- **showcryptorulesetdetail**
- **showprocessesmemory|includeCryptoIKMP**

- **showprocessescpu|includeCryptoIKMP**
- **showcryptoeli**
- **showcryptoengineacceleratorstatistic**

**show tech-support ipsec vrf コマンドの出力**

**vrf** キーワードと *vrf-name* 引数を指定して **show tech-support ipsec** コマンドを入力すると、出力に次の **show** コマンドが、指定した Virtual Routing and Forwarding（VRF）の出力順に表示されます。

- **showversion**
- **showrunning-config**
- **showcryptoisakmpsacountvrf***vrf-name*
- **showcryptoipsecsacountvrf***vrf-name*
- **showcryptosessionivrf***ivrf-name***detail**
- **showcryptosessionfvrf***fvrf-name***detail**
- **showcryptoisakmpsavrf***vrf-name***detail**
- **showcryptoipsecsavrf***vrf-name***detail**
- **showcryptorulesetdetail**
- **showprocessesmemory|includeCryptoIKMP**
- **showprocessescpu|includeCryptoIKMP**
- **showcryptoeli**
- **showcryptoengineacceleratorstatistic**

例：

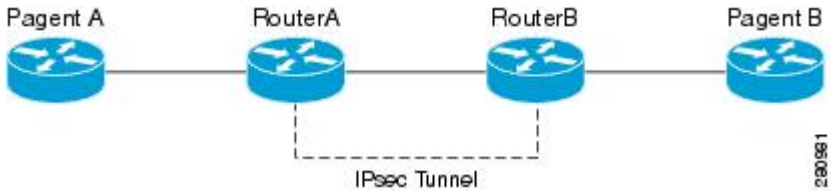
# IPsec Usability Enhancements の設定例

## IKE デフォルト ポリシーの例

次に、クリプト マップが RouterA および RouterB 上で設定されており、デフォルト IKE ポリシーが使用中になっている例を示します。トラフィックは Pagent A から Pagent B にルーティングされ

ます。Peer A および Peer B のシステム ログをチェックすると、デフォルトの IKE ポリシーが両方のピアで使用中であることを確認できます（下図を参照）。

図 *1*：サイトツーサイト トポロジーの例




```
! Configuring RouterA.
RouterA(config)# crypto isakmp key identity address 209.165.200.226
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
 and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.226
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
RouterA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.226
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.225
RouterA(config)# end
RouterA(config)# interface FastEthernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterA(cfg-crypto-trans)# mode tunnel
RouterA(cfg-crypto-trans)# end
RouterA(config)# crypto map testmap 10
RouterA(config-crypto-map)# set transform-set test_transf
RouterA(config-crypto-map)# end
! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.228
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.228
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterB(cfg-crypto-trans)# mode tunnel
RouterB(cfg-crypto-trans)# end
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# set transform-set test_transf
RouterB(config-crypto-map)# end
! Routing traffic from PagentA to PagentB.
PagentA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.229
PagentA(config)# end
! Routing traffic from PagentB to PagentA.
PagentB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.230
PagentB(config)# end
! Checking the system log on RouterA confirms that the default IKE policies are in use.
RouterA# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
Jun  5 09:17:59.251 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
! Checking the system log on RouterB confirms that the default IKE policies are in use.
RouterB# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
Jun  5 09:17:59.979 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

# デフォルト トランスフォーム セットの例

次に、スタティック クリプト マップが RouterA 上で設定され、ダイナミック クリプト マップが RouterB 上で設定されている例を示します。トラフィックは Pagent A から Pagent B にルーティングされます。IPsec SA はデフォルト トランスフォーム セットとネゴシエーションを行い、トラフィックは暗号化されます。両方のピアで **show crypto map** コマンドを実行すると、デフォルト トランスフォーム セットが使用中であることを確認できます（デフォルト トランスフォーム セットの例, （85 ページ）を参照）。

```
! Configuring RouterA.
RouterA(config)# crypto isakmp key identify address 209.165.200.225
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
 and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.225
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
RouterA(config)# ip route 209.165.200.226 255.255.255.255 209.165.200.225
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
RouterA(config)# end
RouterA(config)# interface FastEthernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto isakmp policy 10
RouterA(config-isakmp)# encryption aes
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# hash sha
RouterA(config-isakmp)# group 5
RouterA(config-isakmp)# end
! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.229
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.255 209.165.200.229
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto isakmp policy 10
RouterB(config-isakmp)# encryption aes
RouterB(config-isakmp)# authentication pre-share
RouterB(config-isakmp)# hash sha
RouterB(config-isakmp)# group 5
RouterB(config-isakmp)# end
! The SA is using the default transform set and traffic is encrypted on RouterA.
RouterA# show crypto isakmp sa detail | include 209.165.200.229.*209.165.200.225.*ACTIVE
13007  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  23:59:56
13006  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  0
13005  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  0
! The SA is using the default transform set and traffic is encrypted on RouterB.
RouterB# show crypto isakmp sa detail | include 209.165.200.225.*209.165.200.229.*ACTIVE
7007  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  23:59:55
7006  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  0
7005  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  0
! Verifying that the default transform sets are in use on RouterA.
RouterA# show crypto map
Crypto Map "testmap" 10 ipsec-isakmp
 Peer = 209.165.200.225
 Extended IP access list 101
     access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
 Current peer: 209.165.200.225
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
```

```
  #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
  #$!default_transform_set_0:  { esp-3des esp-sha-hmac  } ,
 }
 Interfaces using crypto map testmap:
  FastEthernet1/2
! Verifying that the default transform sets are in use on RouterB.
RouterB# show crypto map
Crypto Map "testmap" 10 ipsec-isakmp
 Dynamic map template tag: dyn_testmap
Crypto Map "testmap" 65536 ipsec-isakmp
 Peer = 209.165.200.229
 Extended IP access list
     access-list permit ip host 209.165.200.226 host 209.165.200.227
     dynamic (created from dynamic map dyn_testmap/10)
 Current peer: 209.165.200.229
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
  #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
 }
 Interfaces using crypto map testmap:
  GigabitEthernet0/1
```

# その他の参考資料

次の項では、IPsec Usability Enhancement 機能の関連資料を示します。

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| IKE 設定 | 『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール |
| IPsec の設定 | 『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」モジュール |
| Easy VPN サーバ | 『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Easy VPN Server」モジュール |
| Cisco IOS XE セキュリティ コマンド | 『*Cisco IOS Security Command Reference*』 |

### 標準

| 標準 | タイトル |
|---|---|
| この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。 | -- |

### MIB

| MIB | MIB のリンク |
|---|---|
| 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。またこの機能による既存 MIB のサポートに変更はありません。 | 選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | タイトル |
|---|---|
| この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。 | -- |

### シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。<br>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。<br>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。 | http://www.cisco.com/en/US/support/index.html |

# IPsec Usability Enhancements の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *9*：*IPsec Usability Enhancements* の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| IPsec Usability Enhancements | Cisco IOS XE Release 2.4 | この機能では、IKEおよびIPsecのインテリジェントなデフォルト、および、MIB統計情報にアクセスするためおよびトラブルシューティングを支援するための各種 **show** コマンドが導入されています。<br>次のコマンドが、新たに導入または変更されました。<br>**cryptoipsecdefaulttransform-set**、**cryptoisakmpdefaultpolicy**、**cryptoisakmppolicy**、**showcryptoipsecdefaulttransform-set**、**showcryptoipsectransform-set**、**showcryptoisakmpdefaultpolicy**、**showcryptoisakmppolicy**、**showcryptomap(IPsec)**、**showcryptomibipsecflowmibendpoint**、**showcryptomibipsecflowmibfailure**、**showcryptomibipsecflowmibglobal**、**showcryptomibipsecflowmibhistory**、**showcryptomibipsecflowmibspi**、**showcryptomibipsecflowmibtunnel**、**showcryptomibisakmpflowmibfailure**、**showcryptomibisakmpflowmibglobal**、**showcryptomibisakmpflowmibhistory**、**showcryptomibisakmpflowmibpeer**、**showcryptomibisakmpflowmibtunnel**、**showtech-supportipsec**。 |

# 用語集

ピア：ここでのピアとは、IPsec に参加するルータまたはその他の装置です。

SA：セキュリティ アソシエーション。2 つ以上のエンティティが、特定のデータ フローにおいて安全に通信するために、特定のセキュリティ プロトコル（AH または ESP）と関連してセキュリティ サービスを使用する方法を記述します。トラフィックを保護するために、トランスフォームと共有秘密キーが使用されます。

トランスフォーム：データ認証、データ機密性、およびデータ圧縮を実現するためにデータ フローで実行される処理のリスト。たとえば、トランスフォームには、HMAC MD5 認証アルゴリズムを使用する ESP プロトコル、56 ビット DES 暗号規格アルゴリズムを使用する AH プロトコルおよび HMAC-SHA 認証アルゴリズムを使用する ESP プロトコルなどがあります。

トンネル：ここで使用するトンネルとは、2 つのピア間（2 台のルータなど）の安全な通信パスです。トンネル モードで IPsec を使用することではありません。

# 索 引

## C



## I