IPsec VPN モニタリング

IPSec 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、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）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 Internet Key Exchange（IKE; インターネット キー エクスチェンジ）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 ステータスのシスログ通知
- 1 つの Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、IKE と IP Security（IPSec; IP セキュリティ）の両方の Security Association（SA; セキュリティ アソシエーション）をクリアする機能

IPsec VPN モニタリングの機能履歴

リリース	変更点
12.3(4)T	この機能が追加されました。

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

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

この章の構成

IPsec 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。

IPsec VPN モニタリングの制約条件

- ルータ上で Cisco IOS の 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

IPSec 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するには、次の概念を理解しておく必要があります。

背景知識：暗号セッション

暗号セッションは、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、最低 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 Peer Description

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（Cisco IOS Release 12.3(4)T 以前は、ピアのを特定するために使用できるのは IP アドレスと完全修飾ドメイン名（FQDN）だけでした。説明文を設定する方法はありませんでした）。そのピア独自の説明（80 文字まで入力可能）は、その特定の IKE ピアを参照する際にはいつでも使用可能です。ピアの説明を追加するには、**description** コマンドを使用します。

（注） Network Address Translation（NAT; ネットワーク アドレス変換）デバイスの背後に「存在する」IKE ピアを一意に特定はできません。そのため、それらのピアでは、同じ内容の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（シスログ 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）。

暗号セッション ステータスの一覧

show crypto session コマンドを入力して、すべてのアクティブ VPN セッションの一覧を取得できます。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。

暗号セッションのアップまたはダウン ステータスのシスログ通知

暗号セッションのアップまたはダウン ステータスのシスログ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シスログ通知を行います。

次に、暗号セッションがアップしたことを示すシスログ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シスログ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 セキュリティ交換クリア コマンド

IOS の旧バージョンでは、IKE 接続と IPSec 接続（つまり、SA）の両方を単独でクリアできるコマンドはありませんでした。その代わり、IKE をクリアするには **clear crypto isakmp** コマンドを使用し、IPSec をクリアするには **clear crypto ipsec** コマンドを使用する必要がありました。新しい **clear crypto session** コマンドを使用すれば、IKE と IPSec の両方を、1 つのコマンドでクリアできます。特定の暗号セッションや、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フォワーディング（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 コマンドを使用する際にローカル IP アドレスをパラメータとして指定した場合、その IP アドレスをローカル暗号エンドポイント（IKE ローカル アドレス）として共有しているすべてのセッション（およびそれらの 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。

IPsec VPN モニタリングの設定方法

この機能の設定作業については、次の項を参照してください。一覧内の各作業は、必須と任意に分けています。

- 「IKE ピアの説明の追加」（P.4）（任意）
- 「ピアの説明の確認」（P.5）（任意）
- 「暗号セッションのクリア」（P.6）（任意）

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. **configure terminal**
3. **crypto isakmp peer** {**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** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp peer** {**ip-address** *ip-address*} **例：** `Router (config)# crypto isakmp peer address 10.2.2.9`	アグレッシブ モードで、トンネル アトリビュートの認証、許可、およびアカウンティング（AAA）に関する IKE クエリー生成のための IPSec ピアをイネーブルにして、ISAKMP ピア 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	**description** **例：** `Router (config-isakmp-peer)# description connection from site A`	IKE ピアの説明を追加します。

ピアの説明の確認

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

手順の概要

1. **enable**
2. **show crypto isakmp peer**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show crypto isakmp peer** **例：** `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、シスログ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. **clear crypto session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear crypto session** **例：** `Router# clear crypto session`	暗号セッション（IPSec および IKE SA）を削除します。

IPsec VPN モニタリングの設定例

ここでは、次の設定例について説明します。

- 「show crypto session コマンドの出力：例」（P.6）

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、**detail キーワードを指定した show crypto session** の出力例を示します。

```
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

内容	参照先
IP セキュリティ、暗号化、および IKE	• 「*Configuring Internet Key Exchange for IPsec VPNs*」 • 「*Configuring Security for VPNs with IPsec*」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

規格

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

MIB

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

RFC

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

シスコのテクニカル サポート

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

コマンド リファレンス

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

- **clear crypto session**
- **description（isakmp ピア）**
- **show crypto isakmp peer**
- **show crypto session**

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

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