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。

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. **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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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`	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。
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。

ピアの記述の確認

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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、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. **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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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。

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** キーボードを使用しない場合の **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 command and the detail** キーワードを使用する場合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

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」 • 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。 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。 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。 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/techsupport

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。 • 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。 • 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 CLI を使用して IKE と IPsec SA の両方を削除する機能 • 次のコマンドが導入または変更されました。**clear crypto session**、 **description (isakmp peer)**、 **show crypto isakmp peer**、 **show crypto session**。

翻訳について
このドキュメントは、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。