IPv6 仮想トンネル インターフェイス

シスコのネットワーク デバイス用の Cisco IOS IPv6 セキュリティ機能を利用すると、ネットワークをパフォーマンスの劣化や障害から保護するだけでなく、故意に行われる攻撃や、善意のネットワーク ユーザの意図しない危険な間違いにより生ずるデータの紛失または毀損に対しても保護できます。

Cisco IOS IPsec 機能では、IP パケット レベルのネットワーク データ暗号化を利用して、標準規格に準拠した堅牢なセキュリティが提供されています。また、IPsec では、データ機密保持サービスだけでなく、データ認証およびリプレイ攻撃防止サービスも提供されています。

IPsec は、IPv6 仕様の必須コンポーネントです。IPv6 ユニキャストおよびマルチキャスト トラフィックを保護するために、IPv6 IPsec トンネル モードおよびカプセル化が使用されます。このマニュアルでは IPv6 セキュリティへの IPsec の実装について説明します。

IPv6 仮想トンネル インターフェイスに関する情報

IPsec for IPv6

IP セキュリティ（IPsec）は Internet Engineering Task Force (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、インターネットなどの保護されていないネットワークを介して機密情報を送信する際の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 は、次のオプションのネットワーク セキュリティ サービスを提供します一般に、ローカル セキュリティ ポリシーにより、これらのサービスを 1 つ以上使用するよう指示されます。

- データ機密性：IPsec 送信者はネットワークを通じてパケットを送信する前に、パケットを暗号化できます。

- データ整合性：IPSec受信者は、IPSec送信者から送信されたパケットを認証し、伝送中にデータが変更されていないようにします。
- データ送信元認証：IPSec受信者は、送信されたIPSecパケットの送信元を認証できます。このサービスはデータ整合性サービスに依存します。
- アンチ リプレイ：IPsec 受信者はリプレイされたパケットを検出し、拒否できます。

IPsecを使用すれば、データを、観測、変更、またはスプーフィングされることなく、パブリック ネットワークを介して送信できます。IPsec 機能は IPv6 と IPv4 の両方で似ていますが、サイト間トンネル モードは IPv6 だけでサポートされています。

IPv6 では、IPsec は AH 認証ヘッダーと ESP 拡張ヘッダーを使用して実装されます。認証ヘッダーは、送信元の整合性と認証を提供します。再送されたパケットに対するオプションの保護も提供します。認証ヘッダーによって、ほとんどの IP ヘッダー フィールドの整合性が保護され、シグニチャベースのアルゴリズムに従って送信元が認証されます。ESPヘッダーは、機密性、送信元の認証、内部パケットのコネクションレス型整合性、アンチリプレイ、および制限されたトラフィック フローの機密性を提供します。

インターネット キー交換（IKE）プロトコルとは、IPsec とともに使用されるキー管理プロトコル標準です。IPsec の設定には必ずしも IKE は必要ありませんが、IKE では、IPsec 標準に対する新機能が追加されているほか、設定をより柔軟かつ容易に行えるよう、IPsec のサポートが強化されています。

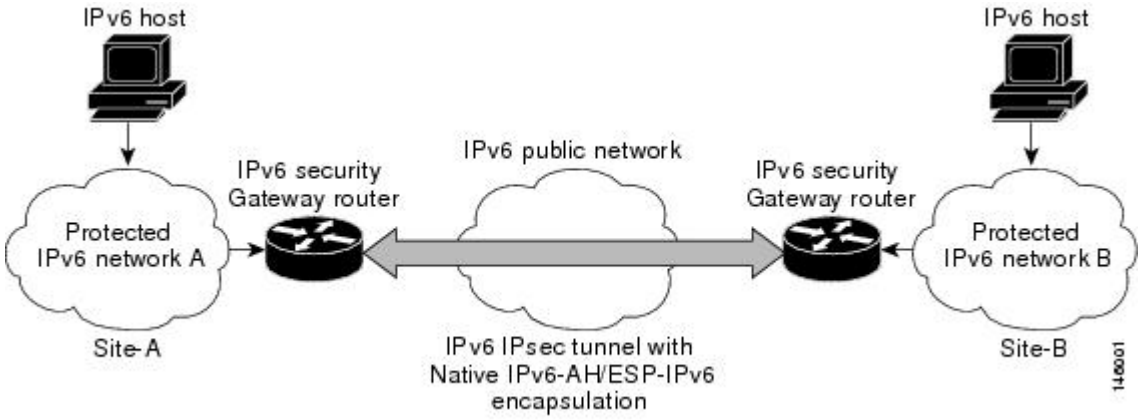
IKE は、Oakley キー交換や Skeme キー交換を Internet Security Association Key Management Protocol（ISAKMP）フレームワークの内部に実装したハイブリッドプロトコルです（ISAKMP、Oakley、および Skeme は IKE によって実装されるセキュリティ プロトコルです）。次の図を参照してください。この機能は、IPv4 IPsec 保護を使用したセキュリティ ゲートウェイ モデルと似ています。

仮想トンネル インターフェイスを使用する IPv6 IPsec サイト間保護

IPsec 仮想トンネル インターフェイス（VTI）は、IPv6 トラフィックのサイト間 IPv6 暗号保護を提供します。IPv6 ユニキャストと IPv6 マルチキャストのあらゆるタイプのトラフィックを保護するために、ネイティブ IPv6 IPsec カプセル化が使用されます。

IPsec VTI では、IPv6 ルータがセキュリティ ゲートウェイとして機能し、他のセキュリティ ゲートウェイ ルータ間に IPsec トンネルを確立したり、トラフィックが内部ネットワークからパブリック IPv6 インターネットを介して送信された場合に暗号 IPsec 保護を提供したりできます（次の図を参照）。この機能は、IPv4 IPsec 保護を使用したセキュリティ ゲートウェイ モデルと似ています。

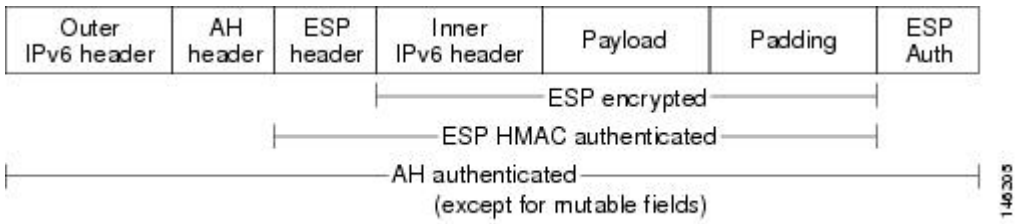
図 *1 : IPv6* の *IPsec* トンネル インターフェイス



IPsec トンネルを設定すると、トンネル インターフェイスの回線プロトコルがアップ状態に変わる前に、IKE および IPsec セキュリティ アソシエーション（SA）がネゴシエーションされ、設定されます。リモート IKE ピアは、トンネルの宛先アドレスと同じです。ローカル IKE ピアは、トンネルの宛先アドレスと同じ IPv6 アドレス スコープを持つトンネルの送信元インターフェイスから選択されたアドレスです。

次の図に、IPsec パケット形式を示します。

図 *2 : IPv6 IPsec* パケット形式



IPv6 仮想トンネル インターフェイスの設定方法

サイト間 IPv6 IPsec 保護用の VTI の設定

IPv6 での IKE ポリシーおよび事前共有キーの定義

IKE ネゴシエーションは保護する必要があるため、各 IKE ネゴシエーションは、共有（共通）の IKE ポリシーについて両ピアが同意することで開始されます。このポリシーには、次の IKE ネゴシエーションを保護するために使用するセキュリティ パラメータとピアの認証方法を記述します。

両ピアがポリシーに同意すると、各ピアに確立されている SA によってポリシーのセキュリティ パラメータが識別され、ネゴシエーションにおける以降すべての IKE トラフィックに適用されます。

パラメータ値の組み合わせをそれぞれ変えることにより各ピアにプライオリティをつけたポリシーを複数設定できます。ただし、そのうちの少なくとも 1 つのポリシーには、リモート ピアのポリシーのいずれかとまったく同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値が設定されている必要があります。作成する各ポリシーに対して、一意のプライオリティを割り当てます（1 ～ 10,000 で指定し、1 が最大のプライオリティ）。

（注） サポートされているパラメータの値が 1 つしかないデバイスを使用する場合は、もう一方のデバイスでサポートされている値を設定する必要があります。この制限を別にすれば、セキュリティとパフォーマンスには通常トレードオフの関係があり、パラメータ値の多くにはこのトレードオフがあります。ネットワークのセキュリティ リスクのレベルと、そのリスクに対する許容度を評価する必要があります。

IKE ネゴシエーションが開始されると、IKE は、両方のピアにある同じ IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモート ピアに送信し、リモート ピアの方では一致するポリシーを探そうとします。リモート ピアは、自分のプライオリティ 1 位のポリシーと、相手のピアから受け取ったポリシーを比較し、一致するポリシーを探します。一致するポリシーが見つかるまで、リモート ピアは優先順位が高い順に各ポリシーをチェックします。

2 つのピアのポリシーが一致するのは、両方のピアが同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値を持ち、リモート ピアのポリシーに指定されているライフタイムが、比較対象のポリシーのライフタイム以下の場合です（ライフタイムが同一でない場合は、リモート ピアのポリシーでの、より短いライフタイムが使用されます）。

一致した場合は、IKE がネゴシエーションを完了し、IPsec セキュリティ アソシエーションが作成されます。一致するポリシーが見つからなかった場合は、IKEはネゴシエーションを拒否し、IPsec は確立されません。

（注） ポリシーに指定する認証方式によっては、追加の設定が必要な場合があります。ピアのポリシーに必要な関連設定がされていないと、一致するポリシーをリモート ピアで検索するときに、ピアはポリシーを送信しません。

IKE ポリシーで事前共有キーを使用するピアそれぞれについて ISAKMP ID を設定する必要があります。

2 つのピアが IKE を使って IPsec SA を確立する場合、各ピアが自分の ID をもう一方のピア（リモート ピア）に送信します。各ピアは、ルータの ISAKMP ID の設定に従い、ホスト名または IPv6 アドレスを送信します。

デフォルトでは、ピアの ISAKMP ID はピアの IPv6 アドレスになっています。必要に応じて ID をピアのホスト名に変更します。一般的に、すべてのピアの ID は同じ設定（すべてのピアで

IPv6アドレスを設定するか、すべてのピアでホスト名を設定）にします。お互いの識別にホスト名を使うピアとIPv6アドレスを使うピアが混在していると、リモート ピアのIDが識別されない場合にDNS lookupでIDを解決できなくなり、IKEネゴシエーションが失敗することがあります。

このタスクを実行して、IPv6 での IKE ポリシーおよび事前共有キーを作成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
5. **hash** {**sha** | **md5**}
6. **group** {**1** | **2** | **5**}
7. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
8. **lifetime** *seconds*
9. **exit**
10. **crypto isakmp key** password-type keystring *keystring* **{ address** *peer-address*| **ipv6** {*ipv6-address* / *ipv6-prefix*} | **hostname** *hostname} [* **no-xauth** *]*
11. **crypto keyring** *keyring-name* [**vrf** *fvrf-name*]
12. **pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key*

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 policy** *priority* 例： `Router(config)# crypto isakmp policy 15`	IKEポリシーを定義し、ISAKMPポリシー コンフィギュレーション モードを開始します。 • ポリシー番号1は、最もプライオリティが高いポリシーを示します。*priority* 引数の値が小さいほど、プライオリティは高くなります。
ステップ 4	**authentication** {**rsa-sig**	**rsa-encr**	**pre-share**} 例：	IKE ポリシー内の認証方式を指定します。 • **rsa-sig** キーワードと **rsa-encr** キーワードはIPv6でサポートされません。

	コマンドまたはアクション	目的
	`Router(config-isakmp-policy)# authentication pre-share`	
ステップ 5	**hash** {**sha** | **md5**} 例： `Router(config-isakmp-policy)# hash md5`	IKE ポリシー内のハッシュ アルゴリズムを指定します。
ステップ 6	**group** {**1** | **2** | **5**} 例： `Router(config-isakmp-policy)# group 2`	IKE ポリシー内部での D-H グループの識別番号を指定します。
ステップ 7	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**} 例： `Router(config-isakmp-policy)# encryption 3des`	IKE ポリシー内の暗号化アルゴリズムを指定します。
ステップ 8	**lifetime** *seconds* 例： `Router(config-isakmp-policy)# lifetime 43200`	IKE SA のライフタイムを指定します。 • IKE ライフタイム値の設定は任意です。
ステップ 9	**exit** 例： `Router(config-isakmp-policy)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了し、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 10	**crypto isakmp key** password-type keystring *keystring* { **address** *peer-address*| **ipv6** {*ipv6-address* / *ipv6-prefix*} | **hostname** *hostname} [* **no-xauth** *]* 例： `Router(config)# crypto isakmp key 0 my-preshare-key-0 address ipv6 3ffe:1001::2/128`	事前共有認証キーを設定します。
ステップ 11	**crypto keyring** *keyring-name* [**vrf** *fvrf-name*] 例： `Router(config)# crypto keyring keyring1`	IKE 認証で使用される暗号キーリングを定義し、config-keyring モードを開始します。
ステップ 12	**pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key* 例： `Router (config-keyring)# pre-shared-key ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	IKE 認証に使用する事前共有キーを定義します。

ISAKMP アグレッシブ モードの設定

一般的には、サイト間シナリオではアグレッシブ モードを設定する必要はありません。通常、デフォルト モードが使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer** {**address** {*ipv4-address* | **ipv6** *ipv6-address ipv6-prefix-length*} | **hostname** *fqdn-hostname*}
4. **set aggressive-mode client-endpoint** {*client-endpoint* | **ipv6** *ipv6-address*}
5. **end**

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** {**address** {*ipv4-address* | **ipv6** *ipv6-address ipv6-prefix-length*} | **hostname** *fqdn-hostname*} 例： `Router(config)# crypto isakmp peer address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	IPsec ピアによるトンネル属性の IKE クエリーをイネーブルにします。
ステップ 4	**set aggressive-mode client-endpoint** {*client-endpoint* | **ipv6** *ipv6-address*} 例： `Router(config-isakmp-peer)# set aggressive mode client-endpoint ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	リモート ピアの IPv6 アドレスを定義します。このアドレスは、アグレッシブ モードのネゴシエーションで使用されます。通常、リモート ピアのアドレスはクライアント側のエンドポイント アドレスです。
ステップ 5	**end** 例： `Router(config-isakmp-peer)# end`	crypto ISAKMP ピア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec トランスフォーム セットおよび IPsec プロファイルの定義

このタスクを実行して、IPsec トランスフォーム セットを定義します。トランスフォーム セットは、IPsec ルータに受け入れられるセキュリティ プロトコルとアルゴリズムの組み合わせです。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
4. **crypto ipsec profile** *name*
5. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*

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 ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] 例： `Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des`	トランスフォームセットを定義し、ルータを暗号化トランスフォーム コンフィギュレーション モードにします。
ステップ 4	**crypto ipsec profile** *name* 例： `Router(config)# crypto ipsec profile profile0`	2 つの IPsec ルータ間における IPsec 暗号化のために使用される IPsec パラメータを定義します。
ステップ 5	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6* 例： `Router (config-crypto-transform)# set-transform-set myset0`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。

IPv6 での ISAKMP プロファイルの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name* [**accounting** *aaalist*
4. **self-identity** {**address** | **address ipv6**] | **fqdn** | **user-fqdn** *user-fqdn*}
5. **match identity** {**group** *group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6** *ipv6-address*} | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}
6. **end**

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 profile** *profile-name* [**accounting** *aaalist* 例： `Router(config)# crypto isakmp profile profile1`	ISAKMP プロファイルを定義し、IPsec ユーザ セッションを監査します。
ステップ 4	**self-identity** {**address**	**address ipv6**]	**fqdn**	**user-fqdn** *user-fqdn*} 例： `Router(config-isakmp-profile)# self-identity address ipv6`	ローカル IKE がリモート ピアに対して IKE 自身を識別させるために使用する ID を定義します。
ステップ 5	**match identity** {**group** *group-name*	**address** {*address* [*mask*] [*fvrf*]	**ipv6** *ipv6-address*}	**host** *host-name*	**host domain** *domain-name*	**user** *user-fqdn*	**user domain** *domain-name*} 例： `Router(config-isakmp-profile)# match identity address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	ISAKMP プロファイルでリモート ピアの ID を照合します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-isakmp-profile)# end`	ISAKMP プロファイル コンフィギュレーション モードを終了し、特権 sEXEC モードに戻ります。

IPv6 IPsec VTI の設定

始める前に

ipv6 unicast-routing コマンドを使用して、IPv6 ユニキャストルーティングを有効化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface tunnel** *tunnel-number*
5. **ipv6 address** *ipv6-address/prefix*
6. **ipv6 enable**
7. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
8. **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
9. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
10. **tunnel protection ipsec profile** *name* [**shared**]
11. **end**

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	**ipv6 unicast-routing** 例： `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト ルーティングをイネーブルにします。設定するインターフェイス トンネルの数に関係なく、IPv6 ユニキャスト ルーティングを有効化する必要があるのは 1 回だけです。

	コマンドまたはアクション	目的
ステップ 4	**interface tunnel** *tunnel-number* 例： `Router(config)# interface tunnel 0`	トンネル インターフェイスおよび番号を指定し、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 5	**ipv6 address** *ipv6-address/prefix* 例： `Router(config-if)# ipv6 address 3FFE:C000:0:7::/64 eui-64`	IPv6 トラフィックをこのトンネルにルーティングできるように、このトンネル インターフェイスに対する IPv6 アドレスを指定します。
ステップ 6	**ipv6 enable** 例： `Router(config-if)# ipv6 enable`	このトンネル インターフェイスに対して IPv6 をイネーブルにします。
ステップ 7	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} 例： `Router(config-if)# tunnel source ethernet0`	トンネル インターフェイスの送信元アドレスを設定します。
ステップ 8	**tunnel destination** {*host-name* | *ip-address* | *ipv6-address*} 例： `Router(config-if)# tunnel destination 2001:DB8:1111:2222::1`	トンネル インターフェイスの宛先を指定します。
ステップ 9	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**} 例： `Router(config-if)# tunnel mode ipsec ipv6`	トンネル インターフェイスのカプセル化モードを設定します。IPsec では、**ipsec ipv6** キーワードだけがサポートされています。
ステップ 10	**tunnel protection ipsec profile** *name* [**shared**] 例： `Router(config-if)# tunnel protection ipsec profile profile1`	トンネル インターフェイスを IPsec プロファイルに関連付けます。IPv6 では、**shared** キーワードはサポートされていません。
ステップ 11	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec トンネル モード設定の確認

手順の概要

1. **show adjacency** [**summary** [*interface-type interface-number*]] | [**prefix**] [**interface** *interface-number*] [**connectionid** *id*] [**link** {**ipv4**| **ipv6** | **mpls**}] [**detail**]
2. **show crypto engine** {**accelerator** | **brief** | **configuration** | **connections** [**active** | **dh** | **dropped-packet** | **show**] | **qos**}
3. **show crypto ipsec sa** [**ipv6**] [*interface-type interface-number*] [**detailed**]
4. **show crypto isakmp peer** [**config** | **detail**]
5. **show crypto isakmp policy**
6. **show crypto isakmp profile** [**tag** *profilename* | **vrf** *vrfname*]
7. **show crypto map** [**interface** *interface* | **tag** *map-name*]
8. **show crypto session** [**detail**] | [**local** *ip-address* [**port** *local-port*] | [**remote** *ip-address* [**port** *remote-port*]] | **detail**] | **fvfr** *vrf-name* | **ivrf** *vrf-name*]
9. **show crypto socket**
10. **show ipv6 access-list** [*access-list-name*]
11. **show ipv6 cef** [*ipv6-prefix / prefix-length*] | [*interface-type interface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]]
12. **show interface** *type number* **stats**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show adjacency** [**summary** [*interface-type interface-number*]]	[**prefix**] [**interface** *interface-number*] [**connectionid** *id*] [**link** {**ipv4**	**ipv6**	**mpls**}] [**detail**] 例： `Router# show adjacency detail`	シスコ エクスプレス フォワーディングの隣接関係テーブルまたはハードウェア レイヤ 3 スイッチングの隣接関係テーブルに関する情報を表示します。
ステップ 2	**show crypto engine** {**accelerator**	**brief**	**configuration**	**connections** [**active**	**dh**	**dropped-packet**	**show**]	**qos**} 例： `Router# show crypto engine connection active`	暗号化エンジンの設定情報の要約を表示します。
ステップ 3	**show crypto ipsec sa** [**ipv6**] [*interface-type interface-number*] [**detailed**] 例： `Router# show crypto ipsec sa ipv6`	IPv6 で現在の SA によって使用されている設定を表示します。
ステップ 4	**show crypto isakmp peer** [**config**	**detail**] 例：	ピアの説明を表示します。

	コマンドまたはアクション	目的
	`Router# show crypto isakmp peer detail`	
ステップ 5	**show crypto isakmp policy** 例： `Router# show crypto isakmp policy`	各 IKE ポリシーのパラメータを表示します。
ステップ 6	**show crypto isakmp profile** [**tag** *profilename* | **vrf** *vrfname*] 例： `Router# show crypto isakmp profile`	ルータに定義されている ISAKMP プロファイルをすべてリストします。
ステップ 7	**show crypto map** [**interface** *interface* | **tag** *map-name*] 例： `Router# show crypto map`	クリプト マップの設定内容を表示します。 このコマンド出力で表示されるクリプトマップは、ダイナミックに生成されます。ユーザはクリプトマップを設定する必要はありません。
ステップ 8	**show crypto session** [**detail**] | [**local** *ip-address* [**port** *local-port*] | [**remote** *ip-address* [**port** *remote-port*]] | **detail**] | **fvfr** *vrf-name* | **ivrf** *vrf-name*] 例： `Router# show crypto session`	アクティブな暗号セッションのステータス情報を表示します。 IPv6 では、**fvfr** キーワード、**ivrf** キーワード、または *vrf-name* 引数はサポートされていません。
ステップ 9	**show crypto socket** 例： `Router# show crypto socket`	暗号ソケットのリストを表示します。
ステップ 10	**show ipv6 access-list** [*access-list-name*] 例： `Router# show ipv6 access-list`	現在のすべての IPv6 アクセスリストの内容を表示します。
ステップ 11	**show ipv6 cef** [*ipv6-prefix* / *prefix-length*] | [*interface-type interface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]] 例： `Router# show ipv6 cef`	IPv6 転送情報ベース（FIB）のエントリを表示します。

	コマンドまたはアクション	目的
ステップ 12	**show interface** *type number* **stats** 例： `Router# show interface fddi 3/0/0 stats`	プロセススイッチング、ファーストスイッチング、および分散スイッチングされたパケットの数を表示します。

IPsec for IPv6 の設定と動作のトラブルシューティング

手順の概要

1. **enable**
2. **debug crypto ipsec**
3. **debug crypto engine packet** [**detail**]

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	**debug crypto ipsec** 例： `Router# debug crypto ipsec`	IPsec ネットワーク イベントを表示します。
ステップ 3	**debug crypto engine packet** [**detail**] 例： `Router# debug crypto engine packet`	IPv6 パケットの内容を表示します。 **注意** 複数のパケットが暗号化される場合、このコマンドを使用すると、システムのフラッディングが発生し、CPU 使用率が高くなる可能性があります。

IPv6 仮想トンネル インターフェイスの設定例

例：サイト間 IPv6 IPsec 保護用の VTI の設定

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
```

```
!
crypto isakmp key myPreshareKey0 address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128
crypto isakmp keepalive 30 30
!
crypto ipsec transform-set Trans1 ah-sha-hmac esp-aes
!
crypto ipsec profile profile0
  set transform-set Trans1
!
ipv6 cef
!
interface Tunnel0
  ipv6 address 3FFE:1001::/64 eui-64
  ipv6 enable
  ipv6 cef
  tunnel source Ethernet2/0
  tunnel destination 3FFE:2002::A8BB:CCFF:FE01:2C02
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile profile0
```

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
セキュリティ コマンド	『Cisco IOS Security Command Reference』
QoS コマンド	『Cisco IOS Quality of Service Solutions Command Reference』
重み付け均等化キューイング	「Configuring Weighted Fair Queueing」機能モジュール

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。 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

IPv6 仮想トンネル インターフェイスの機能情報

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 *1 : IPv6* 仮想トンネル インターフェイスの機能情報

機能名	リリース	機能情報
IPv6 仮想トンネル インターフェイス	Cisco IOS XE Release 2.4	IPsecは、インターネットなどの保護されていないネットワーク上の機密情報の送信にセキュリティを提供します。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。 次のコマンドが導入または変更されました。**authentication (IKE policy)**、**crypto ipsec profile**、**crypto isakmp key**、**crypto isakmp peer**、**crypto isakmp policy**、**crypto isakmp profile**、**crypto keyring**、**debug crypto ipv6 ipsec**、**encryption (IKE policy)**、**group (IKE policy)**、**hash (IKE policy)**、**lifetime (IKE policy)**、**match identity**、**pre-shared-key**、**self-identity**、**set aggressive-mode client-endpoint**、**set transform-set**、**show adjacency**、**show crypto engine**、**show crypto ipsec sa**、**show crypto isakmp peers**、**show crypto isakmp policy**、**show crypto isakmp profile**、**show crypto map**、**show crypto session**、**show crypto socket**、**show ipv6 access-list**、**show ipv6 cef**、**tunnel destination**、**tunnel mode**、**tunnel source**。

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。