IPv6 セキュリティへの IPsec の実装

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 機能により、堅牢な標準ベースのセキュリティ ソリューションが提供され、ネットワーク データを IP パケット レベルで暗号化できます。IPsec では、データ認証サービスおよびアンチリプレイ サービスの他にデータ機密保持サービスが提供されます。

IPsec は、IPv6 仕様の必須コンポーネントです。OSPF for IPv6 によって IPsec 認証のサポートと保護が提供され、IPv6 ユニキャスト トラフィックと IPv6 マルチキャスト トラフィックの保護に IPv6 IPsec トンネル モードと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。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 セキュリティへの IPsec の実装の機能情報」（P.21）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPsec for IPv6 セキュリティの実装の前提条件

- IPv4 を熟知している必要があります。IPv4 の設定およびコマンド リファレンス情報については、「関連資料」の関連資料を参照してください。
- IPv6 アドレッシングおよび基本設定を熟知している必要があります。詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。

IPsec for IPv6 セキュリティの実装に関する情報

IPsec を使用した OSPF for IPv6 認証サポート

OSPF for IPv6 パケットが変更されてルータに再送信されることにより、ルータが管理者にとって望ましくない動作をすることにならないように、OSPF for IPv6 パケットを認証する必要があります。OSPF for IPv6 では、IP Security（IPSec; IP セキュリティ）セキュア ソケット Application Program Interface（API; アプリケーション プログラム インターフェイス）を使用して、OSPF for IPv6 パケットに認証を追加します。この API は、IPv6 をサポートするように拡張されています。

OSPF for IPv6 では、認証をイネーブルにするために IPsec を使用する必要があります。認証を使用するには、暗号イメージが必要です。これは、OSPF for IPv6 での使用に必要な IPsec API は、暗号イメージにしか含まれていないためです。

OSPF for IPv6 では、認証フィールドが OSPF ヘッダーから削除されています。OSPF を IPv6 上で実行すると、OSPF は IPv6 Authentication Header（AH; 認証ヘッダー）と IPv6 Encapsulating Security Payload（ESP; カプセル化セキュリティ ペイロード）を使用して、ルーティング交換の整合性、認証、および機密性を確保します。IPv6 AH および ESP 拡張ヘッダーを使用すると、OSPF for IPv6 に認証および機密性を提供できます。

IPsec を設定するには、セキュリティ ポリシーを設定します。これは、Security Policy Index（SPI）とキーの組み合せです（このキーによって Message Digest 5（MD5）の値が作成および検証されます）。OSPF for IPv6 の IPsec は、インターフェイスまたは OSPF エリアに対して設定できます。セキュリティを強化するには、ユーザは、IPsec を設定する各インターフェイスで異なるポリシーを設定する必要があります。ユーザが OSPF エリアに対して IPsec を設定した場合、ポリシーはそのエリア内のすべてのインターフェイス（IPsec が直接設定されているインターフェイスを除く）に適用されます。OSPF for IPv6 に対して設定された IPsec は、ユーザには不可視です。

IPv6 での OSPF に対する IPsec の設定の詳細については、「*Implementing OSPF for IPv6*」を参照してください。

IPsec for IPv6

IP セキュリティ、つまり IPsec は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）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 レイヤで機能し、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かを確認できます。
- 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 受信者は再送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。

Internet Key Exchange（IKE; インターネット キー エクスチェンジ）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。

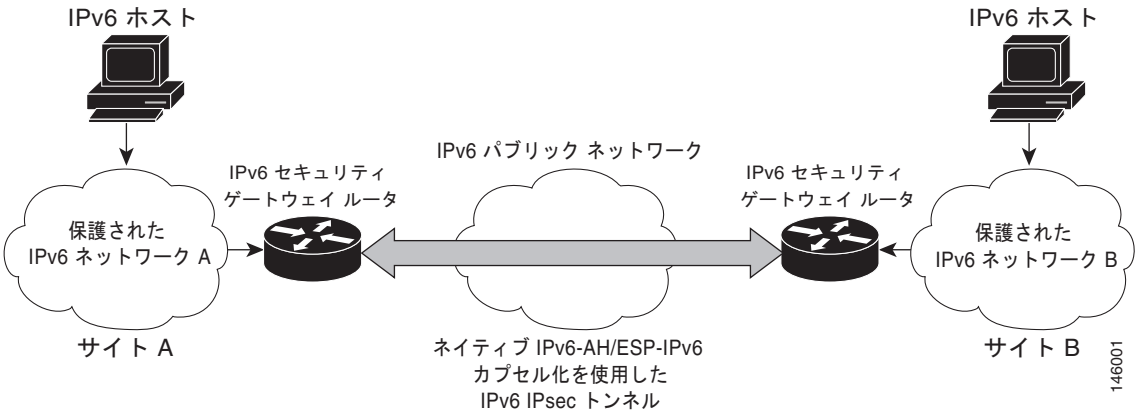
IKE は、Oakley キー交換や Skeme キー交換を Internet Security Association Key Management Protocol（ISAKMP）フレームワークの内部に実装したハイブリッド プロトコルです（ISAKMP、Oakley、および Skeme は IKE によって実装されるセキュリティ プロトコルです）。図 1 を参照してください。この機能は、IPv4 IPsec 保護を使用したセキュリティ ゲートウェイ モデルと似ています。

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 Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）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、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トラフィックに対して暗号 IPsec 保護を提供したりできます（図 1 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。

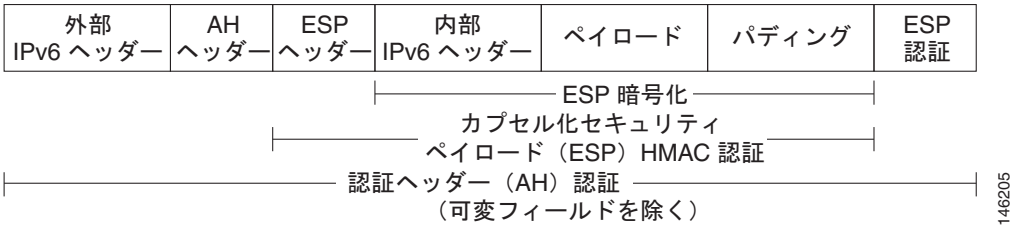
図 1　IPv6 の IPsec トンネル インターフェイス



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 Security Associations（SA; セキュリティ アソシエーション）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。

図 2 に、IPsec パケット形式を示します。

図 2　IPv6 IPsec パケット形式



IPsec VTI の詳細については、『*Cisco IOS Security Configuration Guide*』の「*IPsec Virtual Tunnel Interface*」の章を参照してください。

IPsec for IPv6 セキュリティの実装方法

- 「サイト間 IPv6 IPsec 保護用の VTI の設定」（P.4）（必須）
- 「IPsec トンネル モード設定の確認」（P.12）（任意）
- 「IPsec for IPv6 の設定と動作のトラブルシューティング」（P.14）（任意）

サイト間 IPv6 IPsec 保護用の VTI の設定

IPv6 ユニキャストおよびマルチキャスト トラフィックのサイト間 IPsec 保護のための IPsec VTI を設定するには、次の作業を実行します。この機能では、IPv6 IPsec カプセル化を使用して IPv6 トラフィックを保護できます。

- 「IPv6 における IKE ポリシーと事前共有キーの作成」（P.5）（必須）
- 「ISAKMP アグレッシブ モードの設定」（P.7）（任意）

- 「IPsec トランスフォーム セットと IPsec プロファイルの設定」（P.8）（必須）
- 「IPv6 における ISAKMP プロファイルの設定」（P.9）（任意）
- 「IPv6 IPsec VTI の設定」（P.10）（必須）

IPv6 における IKE ポリシーと事前共有キーの作成

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。

各ピアには、パラメータ値の組み合せをそれぞれ変えることで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、もう一方の装置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 ピアはプライオリティ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、2 つ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、比較している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 ピアのポリシーのライフタイムよりも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 は同じ設定にします（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）。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。

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* {**address** *peer-address* [*mask*] | **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 モードをイネーブルにします。 • 必要に応じて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 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：** `Router(config-isakmp-policy)# authentication pre-share`	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 でサポートされていません。

	コマンドまたはアクション	目的
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`	このコマンドを入力して 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** *enc-type-digit keystring* {**address** *peer-address [mask]* | **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 認証中に使用するクリプト キーリングを定義します。
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

（注） サイト間のシナリオでは、多くの場合、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*}

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。 • 必要に応じて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** {**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。

IPsec トランスフォーム セットと IPsec プロファイルの設定

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 モードをイネーブルにします。 • 必要に応じて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 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 における ISAKMP プロファイルの設定

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*}

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp profile** *profile-name* [**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。

IPv6 IPsec VTI の設定

前提条件

ipv6 unicast-routing コマンドを使用して、IPv6 ユニキャスト ルーティングをイネーブルにします。

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**]

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。 • 必要に応じて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	**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。IPv6 ユニキャスト ルーティングは、設定するインターフェイス トンネルの数にかかわらず、一度だけイネーブルにする必要があります。
ステップ 4	**interface tunnel** *tunnel-number* **例：** `Router(config)# interface tunnel 0`	トンネル インターフェイスと番号を指定し、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。

	コマンドまたはアクション	目的
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。

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** [**vrf**] [*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：** `Router# show crypto isakmp peer detail`	ピアの説明を表示します。
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。

	コマンドまたはアクション	目的
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 Forwarding Information Base（FIB; 転送情報ベース）のエントリを表示します。
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** [**error**]
3. **debug crypto engine packet** [**detail**] [**error**]

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。 • 必要に応じてパスワードを入力します。

	コマンドまたはアクション	目的
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。

例

show crypto ipsec sa コマンドの出力例

次に、**show crypto ipsec sa** コマンドの出力例を示します。

```
Router# show crypto ipsec sa

interface: Tunnel0
     Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::A8BB:CCFF:FE01:9002

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (::/0/0/0)
    current_peer 3FFE:2002::A8BB:CCFF:FE01:2C02 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 133, #pkts encrypt: 133, #pkts digest: 133
     #pkts decaps: 133, #pkts decrypt: 133, #pkts verify: 133
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 60, #recv errors 0

      local crypto endpt.: 3FFE:2002::A8BB:CCFF:FE01:9002,
      remote crypto endpt.: 3FFE:2002::A8BB:CCFF:FE01:2C02
      path mtu 1514, ip mtu 1514
      current outbound spi: 0x28551D9A(676666778)

      inbound esp sas:
       spi: 0x2104850C(553944332)
         transform: esp-des ,
         in use settings ={Tunnel, }
         conn id: 93, flow_id: SW:93, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397507/148)
         IV size: 8 bytes
```

```
    replay detection support: Y
    Status: ACTIVE

  inbound ah sas:
   spi: 0x967698CB(2524354763)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 93, flow_id: SW:93, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4397507/147)
    replay detection support: Y
    Status: ACTIVE

  inbound pcp sas:

  outbound esp sas:
   spi: 0x28551D9A(676666778)
    transform: esp-des ,
    in use settings ={Tunnel, }
    conn id: 94, flow_id: SW:94, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4397508/147)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

  outbound ah sas:
   spi: 0xA83E05B5(2822636981)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 94, flow_id: SW:94, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4397508/147)
    replay detection support: Y
    Status: ACTIVE

  outbound pcp sas:
```

show crypto isakmp peer コマンドの出力例

次の出力例は、IPv6 ルータ上のピアの説明を示しています。

```
Router# show crypto isakmp peer detail

Peer: 2001:DB8:0:1::1 Port: 500 Local: 2001:DB8:0:2::1
Phase1 id: 2001:DB8:0:1::1
flags:
NAS Port: 0 (Normal)
IKE SAs: 1 IPsec SA bundles: 1
last_locker: 0x141A188, last_last_locker: 0x0
last_unlocker: 0x0, last_last_unlocker: 0x0
```

show crypto isakmp profile コマンドの出力例

次の出力例は、IPv6 ルータに定義されている ISAKMP プロファイルを示しています。

```
Router# show crypto isakmp profile

ISAKMP PROFILE tom
Identities matched are:
ipv6-address 2001:DB8:0:1::1/32
Certificate maps matched are:
Identity presented is: ipv6-address fqdn
keyring(s): <none>
trustpoint(s): <all>
```

show crypto isakmp sa コマンドの出力例

次の出力例は、アクティブな IPv6 デバイスの SA を示しています。IPv4 デバイスは非アクティブです。

```
Router# show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH
Lifetime Cap.

IPv6 Crypto ISAKMP SA

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1001  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:00 Cap: D    Engine-id:Conn-id = SW:1

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1002  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth: psk
  DH: 1  Lifetime: 23:45:01 Cap: D    Engine-id:Conn-id = SW:2
```

show crypto map コマンドの出力例

次の出力例は、アクティブな IPv6 デバイスのダイナミックに生成されたクリプト マップを示しています。

```
Router# show crypto map

Crypto Map "Tunnel1-head-0" 65536 ipsec-isakmp
        Profile name: profile0
        Security association lifetime: 4608000 kilobytes/300 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }

Crypto Map "Tunnel1-head-0" 65537
        Map is a PROFILE INSTANCE.
        Peer = 2001:1::2

IPv6 access list Tunnel1-head-0-ACL (crypto)
    permit ipv6 any any (61445999 matches) sequence 1
        Current peer: 2001:1::2
        Security association lifetime: 4608000 kilobytes/300 seconds
        PFS (Y/N): N
        Transform sets={
          ts,
        }
        Interfaces using crypto map Tunnel1-head-0:
        Tunnel1
```

show crypto session コマンドの出力例

次の show crypto session 情報の出力は、現在アクティブな暗号セッションの詳細を示しています。

```
Router# show crypto session detail

Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection K - Keepalives, N -
NAT-traversal, X - IKE Extended Authentication

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 2001:1::1 port 500 fvrf: (none) ivrf: (none)
       Phase1_id: 2001:1::1
       Desc: (none)
   IKE SA: local 2001:1::2/500
            remote 2001:1::1/500 Active
            Capabilities:(none) connid:14001 lifetime:00:04:32
   IPSEC FLOW: permit ipv6 ::/0 ::/0
         Active SAs: 4, origin: crypto map
         Inbound:  #pkts dec'ed 42641 drop 0 life (KB/Sec) 4534375/72
         Outbound: #pkts enc'ed 6734980 drop 0 life (KB/Sec) 2392402/72
```

IPsec for IPv6 セキュリティの設定例

例：サイト間 IPv6 IPsec 保護のための VTI の設定

```
crypto isakmp policy 1
  authentication pre-share
!
crypto isakmp key myPreshareKey0 address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128
crypto isakmp keepalive 30 30
!
crypto ipsec transform-set 3des ah-sha-hmac esp-3des
!
crypto ipsec profile profile0
  set transform-set 3des
!
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
```

その他の関連資料

関連資料

関連項目	参照先
IPsec を使用した OSPF for IPv6 認証サポート	「*Implementing OSPF for IPv6*」
IPsec VTI 情報	「*IPsec Virtual Tunnel Interface*」
IPv6 のサポート機能リスト	「*Start Here: Cisco IOS Software Release Specifics for IPv6 Features*」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
IPv4 セキュリティの設定作業	『*Cisco IOS Security Configuration Guide*』
IPv4 セキュリティ コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*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または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB 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

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2404	『*The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2407	『*The Internet Security Domain of Interpretation for ISAKMP*』

RFC	タイトル
RFC 2408	『*Internet Security Association and Key Management Protocol (ISAKMP)*』
RFC 2409	『*Internet Key Exchange (IKE)*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』
RFC 3576	『*Change of Authorization*』
RFC 4109	『*Algorithms for Internet Key Exchange version 1 (IKEv1)*』
RFC 4302	『*IP Authentication Header*』
RFC 4306	『*Internet Key Exchange (IKEv2) Protocol*』
RFC 4308	『*Cryptographic Suites for IPsec*』

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 セキュリティへの IPsec の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア 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 を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 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。

表 1　IPv6 セキュリティへの IPsec の実装の機能情報

機能名	リリース	機能情報
Open Shortest Path First for IPv6（OSPFv3）を認証する IPv6 IPsec	12.3(4)T 12.4 12.4(2)T	OSPF for IPv6 では、IPsec のセキュア ソケット Application Program Interface（API; アプリケーション プログラム インターフェイス）を使用して認証を OSPF for IPv6 パケットに追加します。この API は、IPv6 をサポートするように拡張されています。 この機能に関する詳細については、次の各項を参照してください。 • 「IPsec を使用した OSPF for IPv6 認証サポート」（P.2） • 「IPsec for IPv6 セキュリティの実装方法」（P.4）
IPv6 IPsec VPN	12.4(4)T	この機能に関する詳細については、次の各項を参照してください。 • 「IPsec for IPv6 セキュリティの実装に関する情報」（P.2） • 「IPsec for IPv6 セキュリティの実装方法」（P.4）
IPsec IPv6 フェーズ 2 サポート	12.4(4)T	このフェーズの機能は、IPv6 トラフィックのサイト間 IPsec 保護のトンネル モードをサポートします。この機能では、IPv6 IPsec カプセル化を使用して 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できます。 この機能に関する詳細については、次の各項を参照してください。 • 「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」（P.3） • 「サイト間 IPv6 IPsec 保護用の VTI の設定」（P.4）