IKE：アグレッシブ モードの開始

機能の履歴

リリース	変更点
12.2(8)T	この機能が追加されました。

このマニュアルでは、Cisco IOS Release 12.2(8)T における IKE：アグレッシブ モードの開始機能について説明します。次の項で構成されています。

機能の概要

IKE：アグレッシブ モードの開始機能を使用すれば、IP Security（IPSec; IP セキュリティ）の RADIUS トンネル アトリビュートとして Internet Key Exchange（IKE; インターネット キー エクスチェンジ）事前共有キーを設定できます。これにより、ハブアンドスポーク トポロジ内で IKE 事前共有キーを拡張できます。

IKE 事前共有キーは理解しやすく、簡単に導入できるものですが、ユーザの数が増えると拡張が難しくなり、セキュリティ上の脅威が発生しやすくなります。ハブ ルータに事前共有キーを保管するのではなく、この機能を利用すれば、事前共有キーを、認証、許可、およびアカウンティング（AAA）サーバに保存し、またそこから取得することによって拡張できます。事前共有キーは、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）RADIUS トンネル アトリビュートとして AAA サーバに保存され、ユーザがハブ ルータに「スピーク」を試行する際に取得されます。ハブ ルータによって AAA サーバから事前共有キーが取得され、スポーク（ユーザ）が、Internet Security Association Key Management Policy（ISAKMP）ピア ポリシー内に RADIUS トンネル アトリビュートとして指定されている事前共有キーを使用して、ハブに対してアグレッシブ モードを開始します。

RADIUS トンネル アトリビュート

IKE アグレッシブ モード ネゴシエーションを開始するには、Tunnel-Client-Endpoint（66）および Tunnel-Password（69）アトリビュートを、ISAKMP ピア ポリシー内に設定する必要があります。Tunnel-Client-Endpoint アトリビュートは、適切な IKE ID ペイロード内で符号化されることによって、サーバに伝達されます。Tunnel-Password アトリビュートは、アグレッシブ モード ネゴシエーション用 IKE 事前共有キーとして使用されます。

利点

IKE：アグレッシブ モードの開始機能を使用すれば、IPSec ピアの RADIUS トンネル アトリビュートを指定し、トンネル アトリビュートとの IKE アグレッシブ モード ネゴシエーションを開始できます。この機能は、暗号ハブアンドスポーク シナリオでの実装に最適です。これにより、スポークが、AAA サーバ上にトンネル アトリビュートとして指定され保存されている事前共有キーを使用することによって、ハブとの IKE アグレッシブ モード ネゴシエーションを開始します。このシナリオは、事前共有キーが中央リポジトリ（AAA サーバ）に保管され、複数のハブ ルータと 1 つのアプリケーションによるキーの情報の使用が可能になるので、容易に拡張できます。

制約事項

TED の制約事項

この機能は、トンネル セットアップを開始するために Tunnel Endpoint Discovery（TED）が使用されているダイナミック クリプト マップで使用するものではありません。TED は、各サイトにピアの事前共有キーを保管するための AAA サーバが必要なフル メッシュ セットアップの設定に便利ですが、この設定をこの機能と共に使用するのは実用的ではありません。

Tunnel-Client-Endpoint ID タイプ

この機能では次の ID タイプだけを使用できます。

- ID_IPV4（IPV4 アドレス）
- ID_FQDN（完全修飾ドメイン名、たとえば「foo.cisco.com」）
- ID_USER_FQDN（E メール アドレス）

関連資料

- 『*Cisco IOS Security Command Reference*』

サポートされているプラットフォーム

この機能は、IPSec および Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）がサポートされているすべてのプラットフォーム上で実行されます。

- Cisco 800 シリーズ
- Cisco 805
- Cisco 806

- Cisco 828
- Cisco 1400 シリーズ
- Cisco 1600 シリーズ
- Cisco 1600-R シリーズ
- Cisco 1710
- Cisco 1720
- Cisco 1750
- Cisco 1751
- Cisco 2400 シリーズ
- Cisco 2600 シリーズ
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100 シリーズ
- Cisco 7200 シリーズ
- Cisco 7500 シリーズ
- Cisco 7700 シリーズ
- Cisco MC3810
- Route Processor Module（RPM; ルート プロセッサ モジュール）
- Universal Route Module（URM）

Cisco Feature Navigator を使用したプラットフォーム サポートの特定

Cisco IOS ソフトウェアは、特定のプラットフォームがサポートされている機能セットにパッケージングされています。この機能のプラットフォーム サポートに関連した更新情報を取得するには、Cisco Feature Navigator にアクセスします。新しいプラットフォーム サポートが機能に追加されると、Cisco Feature Navigator によって、サポートされているプラットフォームのリストが自動的に更新されます。

Cisco Feature Navigator は Web ベースのツールであり、特定の機能セットがサポートされている Cisco IOS ソフトウェア イメージ、および、特定の Cisco IOS イメージ内でサポートされている機能を素早く特定できます。機能またはリリースごとに検索できます。リリース セクションでは、各リリースを横に並べて比較し、各ソフトウェア リリースに固有の機能と共通機能の両方を表示できます。

Cisco Feature Navigator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E メールで届きます。資格のあるユーザは、http://www.cisco.com/register にある指示に従って、Cisco.com 上にアカウントを作成できます。

Cisco Feature Navigator は定期的に更新されています（Cisco IOS ソフトウェアの主要なリリース時およびテクノロジー リリース時）。最新情報については、次の URL から Cisco Feature Navigator ホームページにアクセスしてください。

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

サポートされている規格、MIB、および RFC

規格

なし

MIB

なし

選択したプラットフォーム、Cisco IOS 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 2409、『*The Internet Key Exchange*』
- RFC 2868、『*RADIUS Attributes for Tunnel Protocol Support*』

前提条件

IKE：アグレッシブ モードの開始機能を設定する前に、次の作業を実行する必要があります。

- AAA の設定
- IPSec トランスフォームの設定
- スタティック クリプト マップの設定
- ISAKMP ポリシーの設定
- ダイナミック クリプト マップの設定

これらの作業の完了については、「Configuring Authentication」および「Configuring Internet Key Exchange for IPsec VPN」の各章を参照してください。

設定作業

IKE：アグレッシブ モードの開始機能の設定作業については、次の各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。

- 「RADIUS トンネル アトリビュートの設定」（必須）
- 「RADIUS トンネル アトリビュート設定の確認」（任意）

RADIUS トンネル アトリビュートの設定

ISAKMP ピア設定内の Tunnel-Client-Endpoint および Tunnel-Password アトリビュートを設定するには、グローバル コンフィギュレーション モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto map map-name isakmp authorization list list-name`	アグレッシブ モードで、トンネル アトリビュートに関する AAA の IKE クエリー生成をイネーブルにします。
ステップ 2	`Router(config)# crypto isakmp peer {ip-address ip-address | fqdn fqdn}`	アグレッシブ モードで、トンネル アトリビュートに関する AAA の IKE クエリー生成のための IPSec ピアをイネーブルにして、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。
ステップ 3	`Router(config-isakmp)# set aggressive-mode client-endpoint client-endpoint`	ISAKMP ピア設定内で、Tunnel-Client-Endpoint アトリビュートを指定します。
ステップ 4	`Router(config-isakmp)# set aggressive-mode password password`	ISAKMP ピア設定内で、Tunnel-Password アトリビュートを指定します。

RADIUS トンネル アトリビュート設定の確認

Tunnel-Client-Endpoint および Tunnel-Password アトリビュートが ISAKMP ピア ポリシー内で設定されていることを確認するには、**show running-config global configuration** コマンドを使用します。

トラブルシューティングのヒント

IKE：アグレッシブ モードの開始機能のトラブルシューティングを行うには、EXEC モードで次のデバッグ コマンドを使用します。

コマンド	目的
`Router# debug aaa authorization`	AAA 認証に関する情報を表示します。
`Router# debug crypto isakmp`	IKE イベントに関するメッセージを表示します。
`Router# debug radius`	RADIUS 関連の情報を表示します。

設定例

ここでは、次の設定例について説明します。

- 「ハブの設定例」
- 「スポークの設定例」
- 「RADIUS ユーザ プロファイル例」

ハブの設定例

次に、アグレッシブ モードがサポートされているハブアンドスポーク トポロジのハブを、RADIUS トンネル アトリビュートを使用して設定する方法の例を示します。

```
!The AAA configurations are as follows:
aaa new-model
aaa authorization network ike group radius
aaa authentication login default group radius
```

```
!
! The Radius configurations are as follows:
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key rad123
!
! The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPSec configurations are as follows:
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
!
crypto dynamic-map Dmap 10
 set transform-set trans1
!
crypto map Testtag isakmp authorization list ike
crypto map Testtag 10 ipsec-isakmp dynamic Dmap
!
interface Ethernet0
 ip address 4.4.4.1 255.255.255.0
 crypto map Testtag
!
interface Ethernet1
 ip address 2.2.2.1 255.255.255.0
```

スポークの設定例

次に、アグレッシブ モードがサポートされているハブアンドスポーク トポロジのスポークを、RADIUS トンネル アトリビュートを使用して設定する方法の例を示します。

```
!The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPSec configurations are as follows:
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
 access-list 101 permit ip 3.3.3.0 0.0.0.255 2.2.2.0 0.0.0.255
!
! Initiate aggressive mode using Radius tunnel attributes
crypto isakmp peer address 4.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
!
crypto map Testtag 10 ipsec-isakmp
 set peer 4.4.4.1
 set transform-set trans1
 match address 101
!
interface Ethernet0
 ip address 5.5.5.1 255.255.255.0
 crypto map Testtag
!
interface Ethernet1
 ip address 3.3.3.1 255.255.255.0
```

RADIUS ユーザ プロファイル例

次に、Tunnel-Client-Endpoint および Tunnel-Password アトリビュートがサポートされている RADIUS サーバ上のユーザ プロファイルの例を示します。

```
user@cisco.com  Password = "cisco", Service-Type = Outbound
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Type = :1:ESP,
    Cisco:Avpair = "ipsec:tunnel-password=cisco123",
    Cisco:Avpair = "ipsec:key-exchange=ike"
```

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。

- **crypto isakmp peer**
- **set aggressive-mode client-endpoint**
- **set aggressive-mode password**

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。