IKE アグレッシブ モードの開始

IKE アグレッシブ モードの開始機能を使用すれば、IP Security（IPsec）ピアの RADIUS トンネル属性を指定して、トンネル属性とのインターネット キー エクスチェンジ（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属性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。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IKE アグレッシブ モードの開始の前提条件

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
- 静的暗号マップの設定
- Internet Security Association and Key Management Protocol（ISAKMP）ポリシーの設定

- ダイナミック暗号マップの設定

IKE アグレッシブ モードの開始の制約事項

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（「foo.cisco.com」などの完全修飾ドメイン名）
- ID_USER_FQDN（E メール アドレス）

IKE アグレッシブ モードの開始に関する情報

概要

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 トンネル属性として IKE 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、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）RADIUS トンネル属性として 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 トンネル属性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 トンネル属性

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）属性を、ISAKMP ピア ポリシー内に設定する必要があります。

Tunnel-Client-Endpoint 属性は、該当する 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 属性は、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。

IKE アグレッシブ モードの開始の設定方法

RADIUS トンネル属性の設定

ISAKMP ピア設定内の Tunnel-Client-Endpoint および Tunnel-Password 属性を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* **isakmp authorization list** *list-name*
4. **crypto isakmp peer** {**ip-address** *ip-address* | **fqdn** *fqdn*}
5. **set aggressive-mode client-endpoint** *client-endpoint*
6. **set aggressive-mode password** *password*

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 map** *map-name* **isakmp authorization list** *list-name* 例： `Router (config)# crypto map testmap10 isakmp authorization list list ike`	アグレッシブ モードで、トンネル属性に関する AAA の IKE クエリー生成をイネーブルにします。
ステップ 4	**crypto isakmp peer** {**ip-address** *ip-address*	**fqdn** *fqdn*} 例： `Router (config)# crypto isakmp peer ip address 10.10.10.1`	アグレッシブ モードで、トンネル属性に関する AAA の IKE クエリー生成のための IPsec ピアを有効化して、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。

	コマンドまたはアクション	目的
ステップ 5	**set aggressive-mode client-endpoint** *client-endpoint* 例： `Router (config-isakmp)# set aggressive-mode client-endpoint user-fqdn user@cisco.com`	ISAKMP ピア設定内で、Tunnel-Client-Endpoint 属性を指定します。
ステップ 6	**set aggressive-mode password** *password* 例： `Router (config-isakmp)#set aggressive-mode password cisco123`	ISAKMP ピア設定内で、Tunnel-Password 属性を指定します。

RADIUS トンネル属性設定の確認

Tunnel-Client-Endpoint 属性および Tunnel-Password 属性が 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** グローバル コンフィギュレーション 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、次の手順を実行します。

手順の概要

1. **enable**
2. **debug aaa authorization**
3. **debug crypto isakmp**
4. **debug radius**

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 aaa authorization** 例： `Router# debug aaa authorization`	AAA 認証の情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**debug crypto isakmp** 例： `Router# debug crypto isakmp`	IKE イベントに関するメッセージを表示します。
ステップ 4	**debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。

IKE アグレッシブ モードの開始の設定例

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 トンネル属性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 10.1.1.1 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-aes 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 FastEthernet0
 ip address 10.4.4.1 255.255.255.0
 crypto map Testtag
!
interface FastEthernet1
 ip address 10.2.2.1 255.255.255.0
```

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 トンネル属性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-aes esp-sha-hmac
 access-list 101 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
!
! Initiate aggressive mode using Radius tunnel attributes
crypto isakmp peer address 10.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
!
crypto map Testtag 10 ipsec-isakmp
 set peer 10.4.4.1
 set transform-set trans1
 match address 101
!
interface FastEthernet0
 ip address 10.5.5.1 255.255.255.0
 crypto map Testtag
!
interface FastEthernet1
 ip address 10.3.3.1 255.255.255.0
```

RADIUS ユーザ プロファイルの例

次に、Tunnel-Client-Endpoint および Tunnel-Password 属性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"
```

その他の参考資料

次の項では、IKE アグレッシブ モードの開始機能に関連した関連資料を示します。

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*』
認証の設定	「Configuring Authentication」

関連項目	マニュアル タイトル
IKE の設定	「Configuring Internet Key Exchange for IPsec VPNs」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

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
• RFC 2409 • RFC 2868	• RFC 2409、『*The Internet Key Exchange*』 • RFC 2868、『*RADIUS Attributes for Tunnel Protocol Support*』

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/en/US/support/index.html

IKE アグレッシブ モードの開始の機能情報

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: IKE* アグレッシブ モードの開始の機能情報

機能名	リリース	機能情報
IKE：アグレッシブ モードの開始	Cisco IOS XE Release 2.1	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 トンネル属性を指定し、トンネル属性での 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。 次のコマンドが導入または変更されました。**crypto isakmp peer**、**set aggressive-mode client-endpoint**、**set aggressive-mode password**。

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。