IPsec トンネル ピアの Real-Time Resolution

リモート IP Security（IPsec; IP セキュリティ）ピアにホスト名（IP アドレスではない）を指定した後、IPsec トンネル ピアの Real-Time Resolution 機能を使用すると、ルータが IPsec トンネルを確立する前にドメイン ネーム サーバ（DNS）でホスト名を名前解決できます。これにより、ピアの IP アドレスが変更されたかどうかをルータが直ちに検出できます。

IPsec トンネル ピアの Real-Time Resolution の機能履歴

リリース	変更点
12.3(4)T	この機能が追加されました。

プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明の場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

- 「IPsec トンネル ピアの Real-Time Resolution の制約事項」（P.2）
- 「IPsec トンネル ピアの Real-Time Resolution に関する情報」（P.2）
- 「Real-Time Resolution の設定方法」（P.2）
- 「Real-Time Resolution の設定例」（P.4）
- 「その他の参考資料」（P.5）
- 「コマンド リファレンス」（P.7）

IPsec トンネル ピアの Real-Time Resolution の制約事項

セキュア DNS の要件

この機能はセキュア DNS とだけ使用し、さらに、DNS の応答を認証できる場合に使用することを推奨します。それ以外の場合に使用すると、攻撃者が DNS の応答を偽装または強制し、証明書などの Internet Key Exchange（IKE; インターネット キー エクスチェンジ）認証データへのアクセス権を取得するおそれがあります。攻撃者は、発信側のホストによって信頼されている証明書を取得すると、フェーズ 1 の IKE Security Association（SA; セキュリティ アソシエーション）を確立したり、発信側と実際の応答側で共有されている事前共有鍵を推測しようとしたりします。

DNS 発信側

DNS によるリモート IPsec ピアの名前解決が機能するのは、ピアを発信側として使用する場合だけです。暗号化される最初のパケットが DNS lookup を開始します。DNS lookup が完了すると、これに続くパケットによって IKE が開始されます。

IPsec トンネル ピアの Real-Time Resolution に関する情報

IPsec ピアに対して Real-Time Resolution を設定するには、次の概念を理解しておく必要があります。

- 「セキュア DNS による Real-Time Resolution の利点」（P.2）

セキュア DNS による Real-Time Resolution の利点

リモート IPsec ピアのホスト名を **set peer** コマンドで指定する際、キーワード **dynamic** も発行できますが、このキーワードを使用すると IPsec トンネルが確立される直前まで、DNS によるホスト名の解決が遅れます。解決が遅れることで、Cisco IOS ソフトウェアはリモート IPsec ピアの IP アドレスが変更されたかどうかを検出できます。こうしてこのソフトウェアは、新しい IP アドレスでこのピアと通信できるようになります。

キーワード **dynamic** を発行しない場合は、ホスト名は指定後すぐに解決されます。このため、Cisco IOS ソフトウェアは IP アドレスの変更を検知できず、以前に解決した IP アドレスに対して接続を試みます。

DNS 解決によって、確立した IPsec トンネルがセキュアで、認証済みであることが保証されます。

Real-Time Resolution の設定方法

ここでは、次の手順について説明します。

- 「IPsec ピアの Real-Time Resolution の設定」（P.2）

IPsec ピアの Real-Time Resolution の設定

この作業で、DNS によるリモート IPsec ピアのリアルタイム DNS 決を実行するようにルータを設定します。これにより、DNS lookup によるピアのホスト名の解決は、ルータがピアと接続（IPsec トンネル）を確立する直前になります。

前提条件

クリプト マップを作成する前に、次の作業を実行してください。

- Internet Security Association Key Management Protocol（ISAKMP）ポリシーの定義。
- IPsec トランスフォーム セットの定義。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **match address** *access-list-id*
5. **set peer** {*host-name* [**dynamic**] | *ip-address*}
6. **set transform-set** *transform-set-name1* [*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。 • プロンプトが表示されたら、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 map** *map-name seq-num* **ipsec-isakmp** **例：** `Router(config)# crypto map secure_b 10 ipsec-isakmp`	作成または変更するクリプト マップ エントリを指定して、暗号マップ 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	**match address** *access-list-id* **例：** `Router(config-crypto-m)# match address 140`	拡張アクセス リストに名前を付けます。 このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要があるトラフィックと、IPsec で保護しないトラフィックを決定します。

	コマンドまたはアクション	目的
ステップ 5	**set peer** {*host-name* [**dynamic**] | *ip-address*} **例：** `Router(config-crypto-m)# set peer b.cisco.com dynamic`	リモート IPsec ピアを指定します。 このピアは、IPsec で保護されたトラフィックの転送先となるピアです。 • **dynamic**：ルータがリモート ピアとの間で IPsec トンネルを確立する直前に DNS lookup でホスト名を解決するようにします。このキーワードを指定しない場合、ホスト名は指定後すぐに解決されます。 複数のリモート ピアに対して、同じ作業を繰り返します。
ステップ 6	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*] **例：** `Router(config-crypto-m)# set transform-set myset`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。複数のトランスフォーム セットをプライオリティの順に表示します（最もプライオリティの高いものを先頭に表示）。

トラブルシューティングのヒント

クリプト マップの設定情報を表示するには、**show crypto map** コマンドを使用します。

次の作業

IPsec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。インターフェイスにクリプト マップ セットを適用すると、ルータには、接続中にクリプト マップ セットに対してすべてのインターフェイスのトラフィックを評価し、暗号で保護するトラフィックのために、指定されたポリシーまたは SA のネゴシエーションを使用するように指示されます。

Real-Time Resolution の設定例

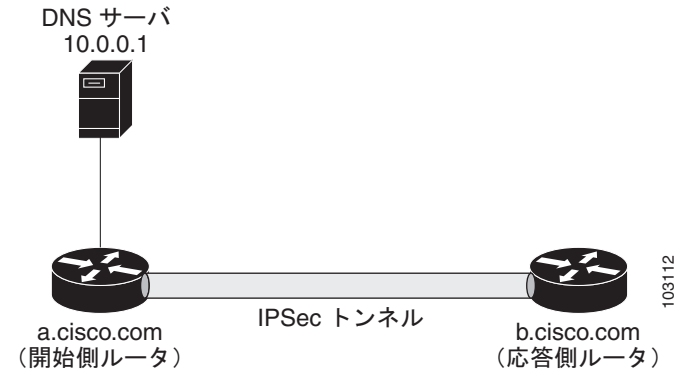
ここでは、次の設定例について説明します。

- 「IPsec ピアの Real-Time Resolution の設定：例」（P.4）

IPsec ピアの Real-Time Resolution の設定：例

図 1 および次の例を使って、Cisco IOS ソフトウェアがリモート IPsec ピアとの間で接続を確立しようとする直前に、そのピアのホスト名を DNS lookup で DNS 解決するように設定するクリプト マップの作成方法を説明します。

図 1　　Real-Time Resolution のサンプル トポロジ




```
! Configure the initiating router.
hostname a.cisco.com
ip domain name cisco.com
ip name server 10.0.0.1
!
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 30.0.0.1
  crypto map secure_b
access-list 140 permit ...
!
! Configure the responding router (the remote IPSec peer).
hostname b.cisco.com
!
crypto map secure_a 10 ipsec-isakmp
  match address 150
  set peer 30.0.0.1
  set transform-set
interface serial0/1
  ip address 40.0.0.1
  crypto map secure_a
access-list 150 ...

! DNS server configuration

b.cisco.com    40.0.0.1       # the address of serial0/1 of b.cisco.com
```

その他の参考資料

ここでは、IPsec トンネル ピアの Real-Time Resolution の関連資料について説明します。

関連資料

内容	参照先
クリプト マップ	「*Security for VPNs with IPsec*」
ISAKMP ポリシー	「*Configuring Internet Key Exchange for IPsec VPNs*」
IPsec および IKE の設定コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア 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	タイトル
なし	—

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

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。

- **set peer（IPsec）**

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。