IPsec トンネル ピアの Real-Time Resolution

リモート IP セキュリティ（IPsec）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、証明書などのインターネット キー交換（IKE）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 セキュリティ アソシエーション（SA）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キー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 ルックアップを開始します。DNS ルックアップが完了すると、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

セキュア DNS による Real-Time Resolution

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、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、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

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 ルックアップ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。

始める前に

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 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、クリプト 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。
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 ルックアップ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順（最高のプライオリティのものが最初）に列挙します。

トラブルシューティングのヒント

暗号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

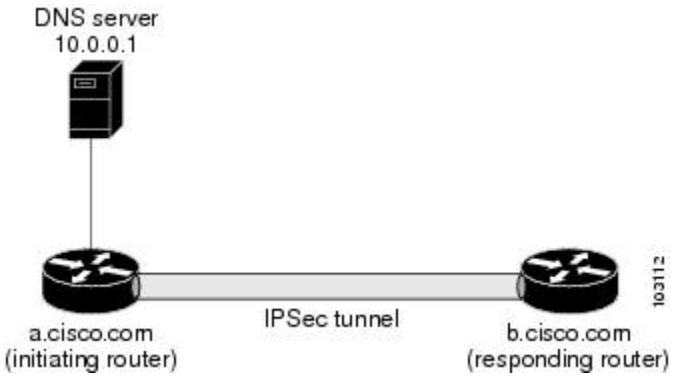
IPSec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。インターフェイスにクリプト マップ セットを適用すると、ルータには、接続中にクリプトマップセットに対してすべてのインターフェイスのトラフィックを評価し、暗号で保護するトラフィックのために、指定されたポリシーまたは SA のネゴシエーションを使用するように指示されます。

Real-Time Resolution の設定例

IPsec ピアの Real-Time Resolution の設定例

次の図および例を使って、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 ルックアップで DNS 解決するように設定する暗号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 10.10.0.1
  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 10.10.0.1
  set transform-set
```

```
interface serial0/1
  ip address 10.0.0.1
  crypto map secure_a
access-list 150 ...
! DNS server configuration
b.cisco.com 10.0.0.1       # the address of serial0/1 of b.cisco.com
```

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
クリプト マップ	『*Security for VPNs with IPsec Configuration Guide*』の「Configuring Security for VPNs with IPsec」モジュール
ISAKMP ポリシー	『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
IPsec および IKE のコンフィギュレーション コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	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 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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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/techsupport

IPsec トンネル ピアの Real-Time Resolution 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 : IPsec* トンネル ピアの *Real-Time Resolution* の機能情報

機能名	リリース	機能情報
IPsec トンネル ピアの Real-Time Resolution	Cisco IOS XE Release 2.1	リモート IP セキュリティ（IPsec）ピアにホスト名（IP アドレスではない）を指定した後、この機能を使用すると、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。 次のコマンドが導入または変更されました。**set peer (IPsec)**。

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。