ASA およびネイティブ L2TP IPSec Android クライアントの設定例

目次

概要

レイヤ 2 トンネリング プロトコル（L2TP）over IPSec により、単一のプラットフォームで、IPSec VPN およびファイアウォール サービスとともに L2TP VPN ソリューションを導入し、管理することが可能になります。 リモート アクセスのシナリオでの L2TP over IPSec の設定の主な利点は、リモート ユーザが、ゲートウェイや専用線を使用せずに、パブリック IP ネットワークから VPN にアクセスできることです。これにより、事実上、一般電話サービス（POTS）のあらゆる場所からリモート アクセスが可能になります。 この他に、VPN にアクセスするクライアントは Windows で Microsoft ダイヤルアップ ネットワーク（DUN）を使用するだけでよいという利点もあります。 Cisco VPN Client ソフトウェアなどの、追加のクライアント ソフトウェアは必要ありません。

このドキュメントでは、ネイティブ L2TP/IPSec Android クライアントの設定例を紹介します。Cisco 適応型セキュリティ アプライアンス（ASA）に必要なすべてのコマンドと、Android デバイス自体で実行する手順を詳しく説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Android L2TP/IPSec には、Cisco ASA ソフトウェア バージョン 8.2.5 以降、バージョン 8.3.2.12 以降、またはバージョン 8.4.1 以降が必要です。
- ASA では、L2TP/IPSec プロトコルを使用する場合の Microsoft Windows 7 および Android ネイティブ VPN クライアント用の Secure Hash Algorithm 2（SHA2）証明書署名がサポートされます。
- 『CLI 8.4 および 8.6 を使用した Cisco ASA 5500 シリーズ設定ガイド： L2TP over IPsec の設定： L2TP over IPsec のライセンス要件』（英語）を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

このセクションでは、このドキュメントで説明する機能の設定に必要な情報を説明しています。

Android での L2TP/IPSec 接続の設定

この手順では、Android での L2TP/IPSec 接続の設定方法について説明します。

1. メニューを開き、[Settings] を選択します。
2. [Wireless and Network] または [Wireless Controls] を選択します。 使用できるオプションは、Android のバージョンによって異なります。
3. [VPN Settings] を選択します。
4. [Add VPN] を選択します。
5. [Add L2TP/IPsec PSK VPN] を選択します。
6. [VPN Name] を選択し、分かりやすい名前を入力します。
7. [VPN Server] を選択し、分かりやすい名前を入力します。
8. [Set IPSec pre-shared key] を選択します。
9. [Enable L2TP secret] をオフにします。
10. （オプション）ASA トンネル グループ名として IPsec ID を設定します。 設定しないと、ASA で DefaultRAGroup に該当するという意味になります。
11. メニューを開き、[Save] を選択します。

ASA での L2TP/IPSec 接続の設定

次に示すのは、必要な ASA Internet Key Exchange バージョン 1（IKEv1）（Internet Security Association and Key Management Protocol（ISAKMP））ポリシーの設定です。この設定により、L2TP over IPSec 使用時に、エンドポイントのオペレーティング システムに統合されているネイティブ VPN クライアントは、ASA への VPN 接続が可能になります。

- IKEv1 フェーズ 1：SHA1 ハッシュ方式による Triple Data Encryption Standard（3DES）暗号化
- IPSec フェーズ 2：Message Digest 5（MD5）または SHA ハッシュ方式による 3DES または高度暗号化規格（AES）暗号化
- PPP 認証：パスワード認証プロトコル（PAP）、マイクロソフト チャレンジ ハンドシェイク認証プロトコル バージョン 1（MS-CHAPv1）、または MS-CHAPv2（推奨）
- 事前共有鍵

  注: ASA が、ローカル データベースでサポートするのは、PPP 認証の PAP と MS-CHAP（バージョン 1 および 2）だけです。 Extensible Authentication Protocol（EAP）と CHAP は、プロキシ認証サーバで実行されます。 したがって、**authentication eap-proxy** または **authentication chap** コマンドで設定されているトンネル グループにリモート ユーザが属しており、ASA がローカル データベースを使用するように設定されていると、そのユーザは接続できません。

  さらに、Android は PAP をサポートしていません。また、Lightweight Directory Access Protocol（LDAP）が MS-CHAP をサポートしていないために、LDAP は実行可能な認証メカニズムではありません。 唯一の回避策は、RADIUS を使用することです。 MS-CHAP と LDAP での問題の詳細については、Cisco Bug ID CSCtw58945、「LDAP 承認と mschapv2 を使用した L2TP over IPSec 接続が失敗する」を参照してください。

この手順では、ASA での L2TP/IPSec 接続の設定方法について説明します。

1. ローカル アドレス プールを定義するか、適応型セキュリティ アプライアンスに DHCP サーバを使用して、グループ ポリシーの各クライアントに IP アドレスを割り当てます。
2. 内部グループ ポリシーを作成します。 L2TP/IPSec になるトンネル プロトコルを定義します。クライアントが使用するドメイン ネーム サーバ（DNS）を設定します。
3. 新しいトンネル グループを作成するか、既存の DefaultRAGroup の属性を変更します。（電話でグループ名として IPsec ID が設定されている場合は、新しいトンネル グループを使用できます。 電話設定については、ステップ 10 を参照してください。）
4. 使用するトンネル グループの一般属性を定義します。 このトンネル グループに、定義済みグループ ポリシーをマッピングします。このトンネル グループが使用する定義済みアドレス プールをマッピングします。LOCAL 以外を使用する場合は、認証サーバ グループを変更します。
5. 使用するトンネル グループの IPSec 属性の下で事前共有キーを定義します。
6. chap、ms-chap-v1、ms-chap-v2 だけが使用されるように、使用するトンネル グループの PPP の属性を変更します。
7. 特定の Encapsulating Security Payload（ESP）暗号化タイプと認証タイプを含むトランスフォーム セットを作成します。
8. IPsec に、トンネル モードではなく、転送モードを使用するように指示します。
9. SHA1 ハッシュ方式の 3DES 暗号化を使用して ISAKMP/IKEv1 ポリシーを定義します。
10. ダイナミック クリプト マップを作成し、クリプト マップにマッピングします。
11. インターフェイスにクリプトマップを適用します。
12. そのインターフェイスで ISAKMP を有効にします。

ASA 互換性のコンフィギュレーション ファイル コマンド

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

この例は、あらゆるオペレーティング システムでネイティブ VPN クライアントとの ASA 互換性を確保するコンフィギュレーション ファイル コマンドを示します。

ASA 8.2.5 以降の設定例

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_address
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 65535 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

ASA 8.3.2.12 以降の設定例

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_addresses
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set my-transform-set-ikev1
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
           authentication pre-share
```

```
encryption 3des
hash sha
group 2
lifetime 86400
```

確認

ここでは、設定が正常に動作していることを確認します。

この手順では、接続の確立方法を説明します。

1. メニューを開き、[Settings] を選択します。
2. [Wireless and Network] または [Wireless Controls] を選択します（使用できるオプションは、Android のバージョンによって異なります）。
3. リストから、VPN 設定を選択します。
4. ユーザ名とパスワードを入力します。
5. [Remember username] を選択します。
6. [Connect] を選択します。

この手順では、接続の切断方法を説明します。

1. メニューを開き、[Settings] を選択します。
2. [Wireless and Network] または [Wireless Controls] を選択します（使用できるオプションは、Android のバージョンによって異なります）。
3. リストから、VPN 設定を選択します。
4. [Disconnect] を選択します。

接続が正常に機能していることを確認するには、次のコマンドを使用します。

- **show run crypto isakmp**：ASA バージョン 8.2.5 の場合
- **show run crypto ikev1**：ASA バージョン 8.3.2.12 以降の場合
- **show vpn-sessiondb ra-ikev1-ipsec**：ASA バージョン 8.3.2.12 以降の場合
- **show vpn-sessiondb remote**：ASA バージョン 8.2.5 の場合

> **注:** 特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

既知の警告

- Cisco bug ID CSCtq21535、「Android L2TP/IPsec クライアントとの接続時の ASA トレースバック」
- Cisco bug ID CSCtj57256、「Android から ASA55xx への L2TP/IPSec 接続が確立されない」
- Cisco bug ID CSCtw58945、「ldap 認証と mschapv2 を使用した L2TP over IPSec 接続が失敗する」

関連情報

- CLI を使用した Cisco ASA 5500 シリーズ設定ガイド、8.4 および 8.6： L2TP over IPsec の

設定

- Cisco ASA 5500 シリーズ、バージョン 8.4(x) のリリース ノート
- CLI 8.3 を使用した Cisco ASA 5500 シリーズ設定ガイド： NAT に関する情報
- ASA 8.3 より前のバージョンから 8.3 までの NAT の設定例
- テクニカルサポートとドキュメント - Cisco Systems