L2TP over IPsec

この章では、ASA での L2TP over IPsec/IKEv1 の設定方法について説明します。

L2TP over IPsec/IKEv1 VPN について

Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）は、リモート クライアントがパブリック IP ネットワークを使用して、企業のプライベート ネットワーク サーバと安全に通信できるようにする VPN トンネリング プロトコルです。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。

L2TP プロトコルは、クライアント/サーバ モデルを基本にしています。機能は L2TP ネットワーク サーバ（LNS）と L2TP アクセス コンセントレータ（LAC）に分かれています。LNS は、通常、ルータなどのネットワーク ゲートウェイで実行されます。一方、LAC は、ダイヤルアップの Network Access Server（NAS; ネットワーク アクセス サーバ）や、Microsoft Windows、Apple iPhone、または Android などの L2TP クライアントが搭載されたエンドポイント デバイスで実行されます。

リモート アクセスのシナリオで、IPsec/IKEv1 を使用する L2TP を設定する最大の利点は、リモート ユーザがゲートウェイや専用回線を使わずにパブリック IP ネットワークを介して VPN にアクセスできることです。これにより、実質的にどの場所からでも POTS を使用してリモート アクセスが可能になります。この他に、Cisco VPN Client ソフトウェアなどの追加のクライアント ソフトウェアが必要ないという利点もあります。

（注） L2TP over IPsec は、IKEv1 だけをサポートしています。IKEv2 はサポートされていません。

IPsec/IKEv1 を使用する L2TP の設定では、事前共有キーまたは RSA シグニチャ方式を使用する証明書、および（スタティックではなく）ダイナミック クリプト マップの使用がサポートされます。ただし、ここで説明する概要手順では、IKEv1、および事前共有キーまたは RSA 署名の設定が完了していることを前提にしています。事前共有キー、RSA、およびダイナミック クリプト マップの設定手順については、一般的操作用コンフィギュレーション ガイドの第 41 章「Digital Certificates」を参照してください。

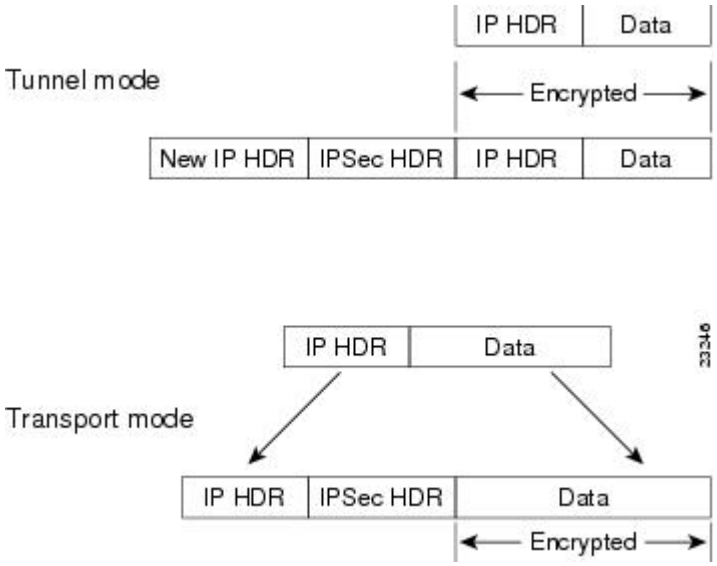
（注） ASA で IPsec を使用する L2TP を設定すると、Windows、MAC OS X、Android および Cisco IOS などのオペレーティング システムに統合されたネイティブ VPN クライアントと LNS が相互運用できるようになります。IPsec を使用する L2TP だけをサポートしています。ネイティブ L2TP は、ASA では対応していません。Windows クライアントがサポートしている IPsec セキュリティ アソシエーションの最短ライフタイムは、300 秒です。ASA でライフタイムを 300 秒未満に設定している場合、Windows クライアントはこの設定を無視して、300 秒のライフタイムに置き換えます。

IPsec の転送モードとトンネル モード

ASA は、デフォルトで IPsec トンネル モードを使用します。このモードでは、元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネル モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から保護することもできます。トンネル モードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

ただし、Windows の L2TP/IPsec クライアントは、IPsec 転送モードを使用します。このモードでは IP ペイロードだけが暗号化され、元の IP ヘッダーは暗号化されません。このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。次の図に、IPsec のトンネル モードと転送モードの違いを示します。

図 *1 : IPsec* のトンネル モードと転送モード



Windows の L2TP および IPsec クライアントから ASA に接続するには、**crypto ipsec transform-set trans_name mode transport** コマンドを使用してトランスフォーム セット用に IPsec 転送モードを設定する必要があります。このコマンドは、設定手順で使用されます。.

（注） ASA は、スプリットトンネル アクセスリストで 28 を超える ACE をプッシュすることはできません。

このような転送が可能になると、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。転送モードでは、IP ヘッダーがクリア テキストで送信されると、攻撃者に何らかのトラフィック分析を許すことになります。

L2TP over IPsec のライセンス要件

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

IKEv2 を使用した IPsec リモート アクセス VPN には、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイト間 VPN では、基本ライセンスに付属の Other VPN ライセンスが使用されます。モデルごとの最大値については、「Cisco ASA Series Feature Licenses」を参照してください。

L2TP over IPsec を設定するための前提条件

L2TP over IPsec の設定については、次の前提条件があります。

- グループ ポリシー：デフォルト グループ ポリシー（DfltGrpPolicy）またはユーザ定義グループ ポリシーを L2TP/IPsec 接続に対して設定できます。どちらの場合も、L2TP/IPsec トンネリング プロトコルを使用するには、グループ ポリシーを設定する必要があります。L2TP/IPsec トンネリング プロトコルがユーザ定義グループ ポリシーに対して設定されていない場合は、DfltGrpPolicy を L2TP/IPsec トンネリング プロトコルに対して設定し、ユーザ定義グループ ポリシーにこの属性を継承させます。
- 接続プロファイル：「事前共有キー」認証を実行する場合は、デフォルトの接続プロファイル（トンネル グループ）、DefaultRAGroup を設定する必要があります。証明書ベースの認証を実行する場合は、証明書 ID に基づいて選択できるユーザ定義接続プロファイルを使用できます。
- IP 接続性をピア間で確立する必要があります。接続性をテストするには、エンドポイントから ASA への IP アドレスの ping と、ASA からエンドポイントへの IP アドレスの ping を実行します。
- 接続パス上のどの場所でも、UDP ポート 1701 がブロックされていないことを確認してください。
- Windows 7 のエンドポイント デバイスが、SHA のシグニチャ タイプを指定する証明書を使用して認証を実行する場合、シグニチャ タイプは、ASA のシグニチャ タイプと SHA1 または SHA2 のいずれかが一致している必要があります。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント モードはサポートされていません。

フェールオーバーのガイドライン

L2TP over IPsec セッションはステートフル フェールオーバーではサポートされていません。

IPv6 のガイドライン

L2TP over IPsec に対してネイティブの IPv6 トンネル セットアップのサポートはありません。

すべてのプラットフォームでのソフトウェアの制限

現時点では、IPsec トンネルを介した 4096 L2TP のみをサポートしています。

認証のガイドライン

ローカル データベースの場合、ASA は、PPP 認証方式として PAP および Microsoft CHAP のバージョン 1 と 2 だけをサポートします。EAP と CHAP は、プロキシ認証サーバによって実行されます。そのため、リモート ユーザが **authentication eap-proxy** または **authentication chap** コマンドで設定したトンネル グループに所属している場合、ASA でローカル データベースを使用するように設定すると、このユーザは接続できなくなります。

サポートされている PPP 認証タイプ

ASA 上の L2TP over IPsec 接続は、次の図に示す PPP 認証タイプだけをサポートします。

表 *1 : AAA* サーバ サポートと *PPP* 認証タイプ

AAA サーバ タイプ	サポートされている **PPP** 認証タイプ
LOCAL	PAP、MSCHAPv1、MSCHAPv2
RADIUS	PAP、CHAP、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACACS+	PAP、CHAP、MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

表 *2 : PPP* 認証タイプの特性

キーワード	認証タイプ	特性
chap	CHAP	サーバのチャレンジに対する応答で、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。このプロトコルは、PAP より安全ですが、データは暗号化されません。

キーワード	認証タイプ	特性
eap-proxy	EAP	EAP をイネーブルにします。これによってセキュリティ アプライアンスは、PPP 認証プロセスを外部の RADIUS 認証サーバにプロキシします。
ms-chap-v1 **ms-chap-v2**	Microsoft CHAP、バージョン 1 Microsoft CHAP、バージョン 2	CHAP と似ていますが、サーバは、CHAP のようなクリアテキストのパスワードではなく、暗号化されたパスワードだけを保存および比較するのでよりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。
pap	PAP	認証中にクリアテキストのユーザ名とパスワードを渡すので、セキュアではありません。

CLI での L2TP over Eclipse の設定

ネイティブ VPN クライアントが L2TP over Eclipse プロトコルを使用して ASA に VPN 接続できるように IKEv1（ISAKMP）ポリシーを設定する必要があります。

- IKEv1 フェーズ 1：SHA1 ハッシュ方式を使用する 3DES 暗号化
- Eclipse フェーズ 2：MD5 または SHA ハッシュ方式を使用する 3DES または AES 暗号化
- PPP 認証：PAP、MS-CHAPv1、または MSCHAPv2（推奨）
- 事前共有キー（iPhone の場合に限る）

手順

ステップ 1 特定の ESP 暗号化タイプおよび認証タイプで、トランスフォーム セットを作成します。

crypto ipsec ike_version transform-set *transform_name ESP_Encryption_Type ESP_Authentication_Type*

例：

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-des esp-sha-hmac
```

ステップ 2 Eclipse 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。

crypto ipsec ike_version transform-set *trans_name* **mode transport**

例：

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
```

ステップ 3 L2TP/Eclipse を vpn トンネリングプロトコルとして指定します。

vpn-tunnel-protocol *tunneling_protocol*

例：

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec
```

ステップ 4 （任意） 適応型セキュリティ アプライアンスに DNS サーバ IP アドレスをグループ ポリシーのクライアントに送信するように指示します。

dns value [**none** | *IP_Primary* | *IP_Secondary*]

例：

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2
```

ステップ 5 （任意） 適応型セキュリティ アプライアンスに WINS サーバ IP アドレスをグループ ポリシーのクライアントに送信するように指示します。

wins-server value [**none** | *IP_primary* [*IP_secondary*]]

例：

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4
```

ステップ 6 （任意） IP アドレス プールを作成します。

ip local pool *pool_name starting_address-ending_address* **mask** *subnet_mask*

例：

```
hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0
```

ステップ 7 （任意） IP アドレス プールを接続プロファイル（トンネル グループ）と関連付けます。

address-pool *pool_name*

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# address-pool sales_addresses
```

ステップ 8 グループ ポリシーの名前を接続プロファイル（トンネル グループ）にリンクします。

default-group-policy name

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
```

ステップ 9 L2TP over IPSec 接続を試行するユーザを確認する認証サーバを指定します。サーバが使用できない場合に認証をローカル認証にフォールバックする場合は、コマンドの末尾に LOCAL を追加します。

authentication-server-group *server_group* [**local**]

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL
```

ステップ 10 L2TP over Eclipse 接続を試行するユーザの認証方式を、接続プロファイル（トンネルグループ）に対して指定します。ローカル認証の実行に ASA を使用していない場合や、ローカル認証にフォールバックする場合は、コマンドの末尾に LOCAL を追加します。

authentication *auth_type*

例：

```
hostname(config)# tunnel-group DefaultRAGroup ppp-attributes
hostname(config-ppp)# authentication ms-chap-v1
```

ステップ 11 接続プロファイル（トンネル グループ）の事前共有キーを設定します。

tunnel-group *tunnel group name* **ipsec-attributes**

例：

```
hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
```

ステップ 12 （任意） 接続プロファイル（トンネル グループ）に対して、L2TP セッション用に AAA アカウンティングの開始レコードと終了レコードを生成します。

accounting-server-group *aaa_server_group*

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# accounting-server-group sales_aaa_server
```

ステップ 13 hello メッセージの間隔を（秒単位で）設定します。範囲は 10 ～ 300 秒です。デフォルト インターバルは 60 秒です。

l2tp tunnel hello *seconds*

例：

```
hostname(config)# l2tp tunnel hello 100
```

ステップ 14 （任意） ESP パケットが 1 つ以上の NAT デバイスを通過できるように、NAT-Traversal をイネーブルにします。

NAT デバイスの背後に適応型セキュリティアプライアンスへの L2TP over Eclipse 接続を試行する L2TP クライアントが複数あると予想される場合、NAT-Traversal をイネーブルにする必要があります。

crypto isakmp nat-traversal *seconds*

NAT トラバーサルをグローバルにイネーブルにするには、ISAKMP がグローバル コンフィギュレーション モードでイネーブルになっていることを確認し（**crypto isakmp enable** コマンドでイネーブルにできます）、次に **crypto isakmp nat-traversal** コマンドを使用します。

例：

```
hostname(config)# crypto ikev1 enable
hostname(config)# crypto isakmp nat-traversal 1500
```

ステップ 15 （任意）トンネル グループのスイッチングを設定します。トンネル グループのスイッチングにより、ユーザがプロキシ認証サーバを使用して認証する場合に、VPN接続の確立が容易になります。トンネル グループは、接続プロファイルと同義語です。

strip-group

strip-realm

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
```

ステップ 16 （任意）ユーザ名 **jdoe**、パスワード **j!doe1** でユーザを作成します。mschap オプションは、パスワードを入力した後に、そのパスワードが Unicode に変換され、MD4 を使用してハッシュされることを示します。

この手順が必要になるのは、ローカル ユーザ データベースを使用する場合だけです。

username *name* **password** *password* **mschap**

例：

```
asa2(config)# username jdoe password j!doe1 mschap
```

ステップ 17 フェーズ 1 の IKE ポリシーを作成し、番号を割り当てます。

crypto ikev1 policy *priority*

group *Diffie-Hellman Group*

IKE ポリシーの設定可能なパラメータは数種類あります。ポリシーの Diffie-Hellman グループも指定できます。ASA が IKE ネゴシエーションを完了するために、isakamp ポリシーが使用されます。

例：

```
hostname(config)#   crypto ikev1 policy 5
hostname(config-ikev1-policy)#
```

Windows 7 のプロポーザルに応答するための IKE ポリシーの作成

Windows 7 の L2TP/IPsec クライアントは、ASA との VPN 接続を確立するために、数種類の IKE ポリシーのプロポーザルを送信します。Windows 7 の VPN ネイティブ クライアントからの接続を容易にするために、次の IKE ポリシーのいずれかを定義します。

ASA の L2TP over IPsec を設定する手順に従います。Windows 7 のネイティブ VPN クライアントの IKE ポリシーを設定するには、このタスクに新しいステップを追加します。

手順

ステップ 1 既存の IKE ポリシーの属性と番号をすべて表示します。

例：

```
hostname(config)# show run crypto ikev1
```

ステップ 2 IKE ポリシーを設定します。number 引数には、設定する IKE ポリシーの番号を指定します。この番号は、**show run crypto ikev1** コマンドの出力で表示されたものです。

crypto ikev1 policy *number*

ステップ 3 各 IPsec ピアの ID を確立し、事前共有キーを使用するために、ASA が使用する認証方式を設定します。

例：

```
hostname(config-ikev1-policy)# authentication pre-share
```

ステップ 4 2 つの IPsec ピア間で伝送されるユーザデータを保護する対称暗号化方式を選択します。Windows 7 の場合は、**3des** または **aes aes-256**（128 ビット AES の場合）を選択します。

encryption{**3des**|**aes**|**aes-256**}

ステップ 5 データの整合性を保証するハッシュ アルゴリズムを選択します。Windows 7 の場合は、SHA-1 アルゴリズムに **sha** を指定します。

例：

```
hostname(config-ikev1-policy)# hash sha
```

ステップ 6 Diffie-Hellman グループ識別番号を選択します。aes、aes-256、または 3des 暗号化タイプには 5 を指定できます。3des 暗号化タイプには 2 のみを指定できます。

例：

```
hostname(config-ikev1-policy)#  group 5
```

ステップ 7 SA ライフタイム（秒）を指定します。Windows 7 の場合は、86400 秒（24 時間）を指定します。

例：

```
hostname(config-ikev1-policy)# lifetime 86400
```

L2TP over IPsec の設定例

次に、任意のオペレーティング システム上のネイティブ VPN クライアントと ASA との互換性を保持するコンフィギュレーション ファイルのコマンドの例を示します。

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
 wins-server value 209.165.201.3 209.165.201.4
 dns-server value 209.165.201.1 209.165.201.2
 vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
 default-group-policy sales_policy
 address-pool sales_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 trans esp-des esp-sha-hmac

crypto ipsec ikev1 transform-set trans mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set trans
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
```

L2TP over IPsec の機能履歴

機能名	リリース	機能情報
L2TP over IPsec	7.2(1)	L2TP over IPsec は、単一のプラットフォームで IPsec VPN サービスとファイアウォール サービスとともに L2TP VPN ソリューションを展開および管理する機能を提供します。 リモート アクセスのシナリオで、L2TP over IPsec を設定する最大の利点は、リモート ユーザがゲートウェイや専用回線を使わずにパブリック IP ネットワークを介して VPN にアクセスできることです。これにより、実質的にどの場所からでも POTS を使用してリモート 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 Dial-Up Networking（DUN; ダイヤル アップ ネットワーク）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、追加のクライアント ソフトウェアは必要ありません。 authentication eap-proxy、authentication ms-chap-v1、authentication ms-chap-v2、authentication pap、l2tp tunnel hello、および vpn-tunnel-protocol l2tp-ipsec コマンドが導入または変更されました。