CHAPTER 69

L2TP over IPsec の設定

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。この章では、次の事項について説明します。

- 「L2TP over IPsec/IKEv1 に関する情報」（P.69-1）
- 「L2TP over IPsec のライセンス要件」（P.69-3）
- 「注意事項と制限事項」（P.69-9）
- 「L2TP over IPsec の設定」（P.69-11）
- 「L2TP over IPsec の機能履歴」（P.69-21）

L2TP over IPsec/IKEv1 に関する情報

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 Network Server（LNS; L2TP ネットワーク サーバ）と L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）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、第 41 章「デジタル証明書の設定」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。サポートされているのは、IPsec を使用する L2TP だけで、ネイティブの L2TP そのものは、ASA ではサポートされていません。
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

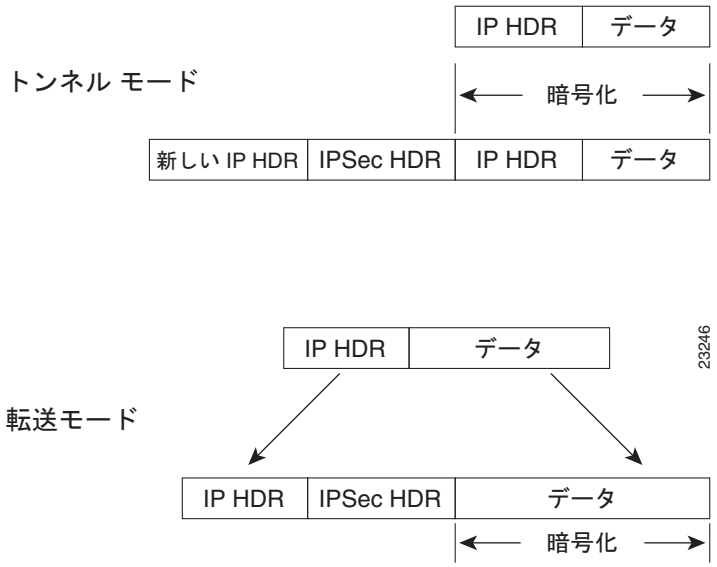
ASA は、デフォルトで IPsec トンネル モードを使用します。このモードでは、元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネル モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から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。図 69-1 に、IPsec のトンネル モードと転送モードの違いを示します。

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。

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。

図 69-1　IPsec のトンネル モードと転送モード



L2TP over IPsec のライセンス要件

次の表に、この機能のライセンス要件を示します。

（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。

モデル	ライセンス要件[1]
ASA 5505	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10 または 25 セッション。* *共有ライセンスはサポートされていません。*[2] – AnyConnect Essentials ライセンス[3]：25 セッション。 • 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 サイトツーサイト VPN： – 基本ライセンス：10 セッション。 – Security Plus ライセンス：25 セッション。
ASA 5510	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス*[2]*：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • 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 サイトツーサイト VPN： 基本ライセンスと Security Plus ライセンス：250 セッション。
ASA 5520	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス*[2]*：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：750 セッション。

モデル	ライセンス要件[1]
ASA 5540	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：2500 セッション。
ASA 5550	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：5000 セッション。
ASA 5580	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：10000 セッション。

モデル	ライセンス要件[1]
ASA 5512-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：250 セッション。
ASA 5515-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：250 セッション。
ASA 5525-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：750 セッション。

モデル	ライセンス要件[1]
ASA 5545-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：2500 セッション。
ASA 5555-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：5000 セッション。
ASA 5585-X（SSP-10）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：5000 セッション。

モデル	ライセンス要件[1]
ASA 5585-X（SSP-20、-40、および -60）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：10000 セッション。
ASASM	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • 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 サイトツーサイト VPN： 基本ライセンス：10000 セッション。

1. すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を越えることはできません。ASA 5505 では、組み合わせセッションの最大数は 10（基本ライセンスの場合）または 25（Security Plus ライセンスの場合）です。
2. 共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

3. AnyConnect Essentials ライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。

   （注）AnyConnect Essentials ライセンスの場合、VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントのダウンロードと起動（WebLaunch）を実行できます。

   このライセンスと AnyConnect Premium SSL VPN ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアントソフトウェアには同じクライアント機能のセットが装備されています。

   特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。

   デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、このライセンスをディセーブルにして他のライセンスを使用するには **no anyconnect-essentials** コマンドを使用します。

   AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

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。

- 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。
- 「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。

注意事項と制限事項

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。マルチ コンテキスト モードはサポートされていません。

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。

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 の L2TP over IPsec 接続は表 69-1 に示す PPP 認証タイプだけをサポートします。

表 69-1　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 69-1　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。
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。

表 69-1　PPP 認証タイプの特性 （続き）

キーワード	認証タイプ	特性
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。

L2TP over IPsec の設定

この項では、ASA IKEv1（ISAKMP）ポリシーの設定について説明します。これは、エンドポイント上のオペレーティング システムと統合されたネイティブ VPN クライアントが、L2TP over IPsec プロトコルを使用して ASA への VPN 接続を行う場合に必要です。

- IKEv1 フェーズ 1：SHA1 ハッシュ方式を使用する 3DES 暗号化
- IPsec 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）

詳細な CLI の設定手順

	コマンド	目的
ステップ 1	**crypto ipsec transform-set** *transform_name ESP_Encryption_Type ESP_Authentication_Type* **例：** `hostname(config)# crypto ipsec transform-set my-transform-set esp-des esp-sha-hmac`	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。
ステップ 2	**crypto ipsec transform-set** *trans_name* **mode transport** **例：** `hostname(config)# crypto ipsec transform-set my-transform-set mode transport`	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。
ステップ 3	**vpn-tunnel-protocol** *tunneling_protocol* **例：** `hostname(config)# group-policy DfltGrpPolicy attributes` `hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec`	L2TP/IPsec を vpn トンネリング プロトコルとして指定します。

	コマンド	目的
ステップ 4	**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	（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。
ステップ 5	**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	（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。
ステップ 6	**tunnel-group** *name* **type remote-access** **例：** hostname(config)# tunnel-group sales-tunnel type remote-access	接続プロファイル（トンネル グループ）を作成します。
ステップ 7	**default-group-policy** *name* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy	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。
ステップ 8	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	（任意）IP アドレス プールを作成します。
ステップ 9	**address-pool** *pool_name* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# address-pool sales_addresses	（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。
ステップ 10	**authentication-server-group** *server_group* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL	L2TP over IPsec 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。
ステップ 11	**authentication** *auth_type* **例：** hostname(config)# tunnel-group name ppp-attributes hostname(config-ppp)# authentication ms-chap-v1	トンネル グループに対して PPP 認証プロトコルを指定します。PPP 認証のタイプとその特性については、表 69-1 を参照してください。

	コマンド	目的
ステップ 12	**tunnel-group** *tunnel group name* **ipsec-attributes** **例：** `hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes` `hostname(config-tunnel-ipsec)# pre-shared-key cisco123`	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。
ステップ 13	**accounting-server-group** *aaa_server_group* **例：** `hostname(config)# tunnel-group sales_tunnel general-attributes` `hostname(config-tunnel-general)# accounting-server-group sales_aaa_server`	（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。
ステップ 14	**l2tp tunnel hello** *seconds* **例：** `hostname(config)# l2tp tunnel hello 100`	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。デフォルトは 60 秒です。
ステップ 15	**crypto isakmp nat-traversal** *seconds* **例：** `hostname(config)# crypto isakmp enable` `hostname(config)# crypto isakmp nat-traversal 1500`	（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 IPsec 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。 グローバルに NAT-Traversal をイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP がイネーブルになっていることをチェックし（**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。
ステップ 16	`strip-group` `strip-realm` **例：** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# strip-group` `hostname(config-tunnel-general)# strip-realm`	（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。

	コマンド	目的
ステップ 17	**username** *name* **password** *password* **mschap** **例：** `hostname(config)# username jdoe password j!doe1 mschap`	次に、ユーザ名 `jdoe`、パスワード `j!doe1` でユーザを作成する例を示します。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。
ステップ 18	**crypto isakmp policy** *priority* **例：** `hostname(config)# crypto isakmp policy 5`	crypto isakmp policy コマンドは、フェーズ 1 の IKE ポリシーを作成し、番号を割り当てます。IKE ポリシーの設定可能なパラメータは数種類あります。 ASA が IKE ネゴシエーションを完了するためには、isakamp ポリシーが必要です。 Windows 7 のネイティブ VPN クライアントの設定例については、「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」（P.69-15）を参照してください。

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。

	コマンド	目的
ステップ 1	「詳細な CLI の設定手順」（P.69-11）	詳細な CLI の設定手順 の手順に従ってください（ステップ 18 まで）。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、この表の追加の手順を実行します。
ステップ 2	**show run crypto isakmp** **例：** `hostname(config)# show run crypto isakmp`	既存の IKE ポリシーの属性と番号をすべて表示します。
ステップ 3	**crypto isakmp policy** number **例：** `hostname(config)# crypto isakmp policy` *number* `hostname(config-isakmp-policy)#`	IKE ポリシーを設定できます。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 isakmp` コマンドの出力で表示されたものです。
ステップ 4	**authentication** **例：** `hostname(config-isakmp-policy)# authentication pre-share`	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。
ステップ 5	**encryption** *type* **例：** `hostname(config-isakmp-policy)# encryption {3des|aes|aes-256}`	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**、**aes**（128 ビット AES の場合）、または **aes-256** を選択します。
ステップ 6	**hash** **例：** `hostname(config-isakmp-policy)# hash sha`	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。
ステップ 7	**group** **例：** `hostname(config-isakmp-policy)# group 5`	Diffie-Hellman グループ識別番号を選択します。Windows 7 の場合は、1536 ビット Diffie-Hellman グループを表す 5 を指定します。
ステップ 8	**lifetime** **例：** `hostname(config-isakmp-policy)# lifetime 86400`	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。

詳細な CLI の設定手順

	コマンド	目的
ステップ 1	`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`	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。
ステップ 2	`crypto ipsec ike_version transform-set trans_name mode transport` **例：** `crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport`	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。
ステップ 3	**vpn-tunnel-protocol** *tunneling_protocol* **例：** `hostname(config)# group-policy DfltGrpPolicy attributes` `hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec`	L2TP/IPsec を vpn トンネリング プロトコルとして指定します。
ステップ 4	**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`	（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。
ステップ 5	**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`	（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。
ステップ 6	`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`	（任意）IP アドレス プールを作成します。
ステップ 7	**address-pool** *pool_name* **例：** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# address-pool sales_addresses`	（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。

	コマンド	目的
ステップ 8	**tunnel-group** *name* **type remote-access** **例：** hostname(config)# tunnel-group sales-tunnel type remote-access	接続プロファイル（トンネル グループ）を作成します。
ステップ 9	**default-group-policy** *name* **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy	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。
ステップ 10	**authentication-server-group** *server_group* [local] **例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL	L2TP over IPsec 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。
ステップ 11	**authentication** *auth_type* **例：** hostname(config)# tunnel-group *name* ppp-attributes hostname(config-ppp)# authentication ms-chap-v1	トンネル グループに対して PPP 認証プロトコルを指定します。PPP 認証のタイプとその特性については、表 69-1 を参照してください。
ステップ 12	**tunnel-group** *tunnel group name* **ipsec-attributes** **例：** hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes hostname(config-tunnel-ipsec)# ikev1 pre-shared-key *cisco123*	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。
ステップ 13	**accounting-server-group** *aaa_server_group* **例：** hostname(config)# tunnel-group sales_tunnel general-attributes hostname(config-tunnel-general)# accounting-server-group sales_aaa_server	（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。
ステップ 14	**l2tp tunnel hello** *seconds* **例：** hostname(config)# l2tp tunnel hello 100	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。

	コマンド	目的
ステップ 15	**crypto isakmp nat-traversal** *seconds* **例：** `hostname(config)# crypto isakmp enable` `hostname(config)# crypto isakmp nat-traversal 1500`	（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 IPsec 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。 グローバルに NAT-Traversal をイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP がイネーブルになっていることをチェックし（**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。
ステップ 16	`strip-group` `strip-realm` **例：** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# strip-group` `hostname(config-tunnel-general)# strip-realm`	（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。
ステップ 17	**username** *name* **password** *password* **mschap** **例：** `asa2(config)# username jdoe password j!doe1 mschap`	次に、ユーザ名 `jdoe`、パスワード `j!doe1` でユーザを作成する例を示します。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。
ステップ 18	`crypto ikev1 policy` *priority* **group** *Diffie-Hellman Group* **例：** `hostname(config)# crypto ikev1 policy 5` `hostname(config-ikev1-policy)# group 5`	crypto isakmp policy コマンドは、フェーズ 1 の IKE ポリシーを作成し、番号を割り当てます。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は、isakamp ポリシーが必要です。 Windows 7 のネイティブ VPN クライアントの設定例については、「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」（P.69-19）を参照してください。

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。

	コマンド	目的
ステップ 1	「詳細な CLI の設定手順」（P.69-16）	詳細な CLI の設定手順 の手順に従ってください（ステップ 18 まで）。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、この表の追加の手順を実行します。
ステップ 2	**show run crypto ikev1** **例：** `hostname(config)# show run crypto ikev1`	既存の IKE ポリシーの属性と番号をすべて表示します。
ステップ 3	**crypto ikev1 policy** number **例：** `hostname(config)# crypto ikev1 policy` *number* `hostname(config-ikev1-policy)#`	IKE ポリシーを設定できます。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。
ステップ 4	**authentication** **例：** `hostname(config-ikev1-policy)# authentication pre-share`	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。
ステップ 5	**encryption** *type* **例：** `hostname(config-ikev1-policy)# encryption {3des|aes|aes-256}`	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**、**aes**（128 ビット AES の場合）、または **aes-256** を選択します。
ステップ 6	**hash** **例：** `hostname(config-ikev1-policy)# hash sha`	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。
ステップ 7	**group** **例：** `hostname(config-ikev1-policy)# group 5`	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。2 は 3des 暗号化タイプだけに指定できます。
ステップ 8	**lifetime** **例：** `hostname(config-ikev1-policy)# lifetime 86400`	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。

ASA 8.2.5 を使用する 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 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 20 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 8.4.1 以降を使用する 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 my-transform-set-ikev1 esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 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

表 69-2 に、この機能のリリース履歴を示します。

表 69-2　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。