CHAPTER 28

L2TP over IPSec の設定

セキュリティ アプライアンスこの章では、に L2TP over IPSec を設定する方法について説明します。次の項で構成されています。

L2TP の概要

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 2000 などの L2TP クライアントが搭載された PC で実行されます。

リモート アクセスのシナリオで、IPSec 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、VPN にアクセスするクライアントは Windows 2000 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。

L2TP over IPSec を設定するには、まず、IPSec の転送モードを設定して、IPSec で L2TP を使用できるようにします。次に、L2TP に Virtual Private Dial-up Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）グループを設定します。

IPSec 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、IKE、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 39 章「証明書の設定」を参照してください。

（注）　セキュリティ アプライアンスで IPSec を使用する L2TP を設定すると、LNS が Windows 2000 L2TP クライアントと相互運用できるようになります。現時点では、シスコや他のベンダーの LAC との相互運用はサポートされていません。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、セキュリティ アプライアンスではサポートされていません。
Windows 2000 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。セキュリティ アプライアンスでライフタイムを 300 秒未満に設定している場合、Windows 2000 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

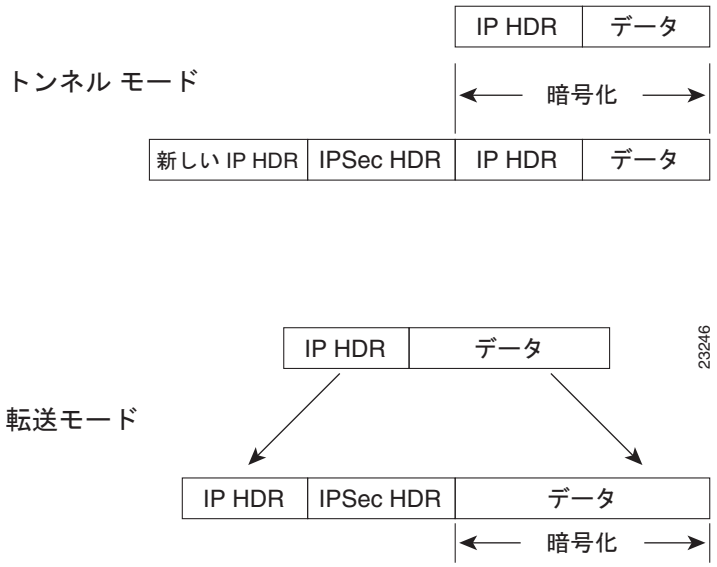
セキュリティ アプライアンスは、デフォルトで IPSec トンネル モードを使用します。このモードでは、元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。このモードでは、ルータなどのネットワーク デバイスが IPSec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPSec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネル モードの大きな利点は、エンド システムを変更しなくても IPSec を利用できるということです。また、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 2000 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 28-1 に、IPSec のトンネル モードと転送モードの違いを示します。

このように、Windows 2000 の L2TP/IPSec クライアントからセキュリティ アプライアンスに接続するには、**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。このコマンドの設定手順については、「L2TP over IPSec 接続の設定」（P.28-3）を参照してください。

この機能（転送）を設定することにより、IP ヘッダーの情報に基づいて、中間ネットワークで特別な処理（QoS など）を実行できるようになります。ただし、レイヤ 4 ヘッダーは暗号化されるので、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ため、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 28-1　IPSec のトンネル モードと転送モード



L2TP over IPSec 接続の設定

セキュリティ アプライアンスが L2TP over IPSec 接続を受け入れるように設定するには、次の手順を実行します。

（注）　Cisco VPN Client バージョン 3.x または Cisco VPN 3000 Client バージョン 2.5 のいずれかがインストールされている場合、セキュリティ アプライアンスは Windows 2000 で L2TP/IPSec トンネルを確立しません。Windows 2000 の [Services] パネル（[Start] > [Programs] > [Administrative Tools] > [Services] の順にクリック）で、Cisco VPN Client バージョン 3.x の *Cisco VPN Service*、または Cisco VPN 3000 Client バージョン 2.5 の *ANetIKE Service* をディセーブルにします。次に、[Services] パネルで IPSec Policy Agent Service を再起動してから、マシンを再起動します。

ステップ 1　**crypto ipsec transform-set** コマンドに **mode** キーワードを指定して使用し、トンネル モードではなく転送モードを使用するように IPSec を指定します。

```
hostname(config)# crypto ipsec transform-set trans_name mode transport
```

ステップ 2　（任意）トンネル グループ一般属性モードで **address-pool** コマンドを次のように使用して、クライアントに IP アドレスを割り当てるのに使用するローカル アドレス プールを指定します。

```
hostname(config)# tunnel-group name general-attributes
hostname(config-tunnel-general)# address-pool pool_name
```

ステップ 3　（任意）グループ ポリシー コンフィギュレーション モードで **dns value** コマンドを次のように使用して、セキュリティ アプライアンスが DNS サーバの IP アドレスをクライアントに送信するように指示します。

```
hostname(config)# group-policy group_policy_name attributes
hostname(config-group-policy)# dns value [none | IP_primary [IP_secondary]]
```

ステップ 4　（任意）グループ ポリシー コンフィギュレーション モードで **wins-server** コマンドを次のように使用して、セキュリティ アプライアンスが WINS サーバの IP アドレスをクライアントに送信するように指示します。

```
hostname(config-group-policy)# wins-server value [none | IP_primary [IP_secondary]]
```

ステップ 5　（任意）トンネル グループ一般属性モードで、**accounting-server-group** コマンドを次のように使用して、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。

```
hostname(config)# tunnel-group name general-attributes
hostname(config-tunnel-general)# accounting-server-group aaa_server_group
```

ステップ 6　**vpn-tunnel-protocol l2tp-ipsec command** コマンドを次のように使用して、グループまたはユーザ用の有効な VPN トンネリング プロトコルとして L2TP over IPSec を設定します。

グループの場合、次のようにグループ ポリシー属性モードに入ります。

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

ユーザの場合、次のようにユーザ名属性モードに入ります。

```
hostname(config)# username user_name attributes
hostname(config-username)# vpn-tunnel-protocol l2tp-ipsec
```

ステップ 7　**tunnel-group** コマンドを使用してトンネル グループを作成し、トンネル グループ一般属性モードで **default-group-policy** コマンドを次のように使用して、グループ ポリシーの名前をトンネル グループにリンクします。

```
hostname(config)# tunnel-group name type ipsec-ra
hostname(config)# tunnel-group name general-attributes
hostname(config-tunnel-general)# group-policy group_policy_name
```

ステップ 8　トンネル グループ ppp 属性モードで **authentication** *type* コマンドを使用して、PPP 認証プロトコルを設定します。表 28-1 に、PPP 認証タイプとその特性を示します。

```
hostname(config)# tunnel-group name ppp-attributes
hostname(config-ppp)# authentication pap
```

表 28-1　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。
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。

ステップ 9　L2TP over IPSec 接続を試行するユーザの認証方式を指定します。トンネル グループ一般属性モードで **authentication-server-group** コマンドを使用して、認証サーバまたは独自のローカル データベースを使用するようにセキュリティ アプライアンスを設定します。

認証サーバを使用する場合

認証サーバを使用するには、**authentication server group** キーワードを使用します。

```
hostname(config)# tunnel-group name general-attributes
hostname(config-tunnel-general)# authentication-server-group auth_server_group
```

ローカル データベースを使用する場合

ローカル データベースを使用するには、**LOCAL** キーワードを入力します。

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

（注）　ローカル データベースの場合、セキュリティ アプライアンスは、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、セキュリティ アプライアンスでローカル 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。

ステップ 10　グローバル コンフィギュレーション モードで **username** コマンドを入力して、ローカル データベースにユーザを作成します。

ユーザが Microsoft CHAP バージョン 1 または 2 を使用している L2TP クライアントで、セキュリティ アプライアンスがローカル データベースに対して認証を行うように設定されている場合は、必ず **mschap** キーワードを付けてください。例：

```
hostname(config)# username t_wmith password eu5d93h mschap
```

ステップ 11　グローバル コンフィギュレーション モードで **l2tp tunnel hello** コマンドを次のように使用して、hello メッセージの間隔を秒単位で設定します。

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

ステップ 12　（任意）NAT デバイスの背後にセキュリティ 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 をイネーブルにして、ESP パケットが 1 台または複数の NAT デバイスを通過できるよう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。次に例を示します。

```
hostname(config)# crypto isakmp enable
hostname(config)# crypto isakmp nat-traversal 30
```

トンネル グループのスイッチング

トンネル グループのスイッチングを使用すると、セキュリティ アプライアンスで、L2TP over IPSec 接続を確立する異なるユーザを別々のトンネル グループに関連付けることができます。トンネル グループごとに独自の AAA サーバ グループと IP アドレス プールがあるため、ユーザは自分のトンネル グループに固有の方式で認証を受けることができます。

この機能を使用する場合、ユーザは、ユーザ名だけではなく、ユーザ名とグループ名を *username@group_name 形式で送信します。「@」は、設定可能な区切り文字で、group_name は、セキュリティ アプライアンスに設定されているトンネル グループの名前です。*

トンネル グループのスイッチングをイネーブルにするには、トンネル グループ一般属性モードで **strip-group** コマンドを使用して、グループの除去処理をイネーブルにする必要があります。イネーブルにすると、セキュリティ アプライアンスが VPN クライアントによって提示されるユーザ名からグループ名を取得してユーザ接続のトンネル グループを選択します。次に、セキュリティ アプライアンスは許可および認証のために、ユーザ名のユーザの部分だけを送信します。それ以外の場合（ディセーブルになっている場合）、セキュリティ アプライアンスは領域を含むユーザ名全体を送信します。次の例では、*telecommuters* というトンネル グループのグループ除去処理をイネーブルにしています。

```
asa1(config)# tunnel-group telecommuters general-attributes
asa1(config-tunnel-general)# strip-group
```

L2TP over IPSec 接続情報の表示

show vpn-sessiondb コマンドには、L2TP over IPSec 接続に関する詳細な情報を表示するために使用できるプロトコル フィルタが含まれています。グローバル コンフィギュレーション モードから、**show vpn-sessoindb detailed remote filter protocol l2tpOverIpsec** とフル コマンドを入力します。

次の例では、1 つの L2TP over IPSec 接続に関する詳細情報を表示します。

```
hostname# show vpn-sessiondb detail remote filter protocol L2TPOverIPSec

Session Type: Remote Detailed

Username     : b_smith
Index        : 1
Assigned IP  : 90.208.1.200           Public IP    : 70.208.1.212
Protocol     : L2TPOverIPSec          Encryption   : 3DES
Hashing      : SHA1
Bytes Tx     : 418464                 Bytes Rx     : 424440
Client Type  :                        Client Ver   :
Group Policy : DfltGrpPolicy
Tunnel Group : DefaultRAGroup
Login Time   : 13:24:48 UTC Thu Mar 30 2006
Duration     : 1h:09m:18s
Filter Name  : #ACSACL#-IP-ACL4Clients-440fa5aa
NAC Result   : N/A
Posture Token:

IKE Sessions: 1
IPSec Sessions: 1
L2TPOverIPSec Sessions: 1


IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
  Encryption   : 3DES                   Hashing      : SHA1
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 24643 Seconds
  D/H Group    : 2

IPSec:
  Session ID   : 2
  Local Addr   : 80.208.1.2/255.255.255.255/17/1701
  Remote Addr  : 70.208.1.212/255.255.255.255/17/1701
  Encryption   : 3DES                   Hashing      : SHA1
```

```
  Encapsulation: Transport
  Rekey Int (T): 3600 Seconds           Rekey Left(T): 2856 Seconds
  Rekey Int (D): 95000 K-Bytes          Rekey Left(D): 95000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Bytes Tx     : 419064                 Bytes Rx     : 425040
  Pkts Tx      : 4201                   Pkts Rx      : 4227


L2TPOverIPSec:
  Session ID   : 3
  Username     : l2tp
  Assigned IP  : 90.208.1.200
  Encryption   : none                   Auth Mode    : PAP
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Bytes Tx     : 301386                 Bytes Rx     : 306480
  Pkts Tx      : 4198                   Pkts Rx      : 4224
```

次の例では、1 つの L2TP over IPSec over NAT 接続に関する詳細情報を表示します。

```
hostname# show vpn-sessiondb detail remote filter protocol L2TPOverIPSecOverNAtT

Session Type: Remote Detailed

Username     : v_gonzalez
Index        : 2
Assigned IP  : 90.208.1.202           Public IP    : 70.208.1.2
Protocol     : L2TPOverIPSecOverNatT  Encryption   : 3DES
Hashing      : MD5
Bytes Tx     : 1009                   Bytes Rx     : 2241
Client Type  :                        Client Ver   :
Group Policy : DfltGrpPolicy
Tunnel Group : l2tpcert
Login Time   : 14:35:15 UTC Thu Mar 30 2006
Duration     : 0h:00m:07s
Filter Name  :
NAC Result   : N/A
Posture Token:

IKE Sessions: 1
IPSecOverNatT Sessions: 1
L2TPOverIPSecOverNatT Sessions: 1


IKE:
  Session ID   : 1
  UDP Src Port : 4500                   UDP Dst Port : 4500
  IKE Neg Mode : Main                   Auth Mode    : rsaCertificate
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 300 Seconds            Rekey Left(T): 294 Seconds
  D/H Group    : 2

IPSecOverNatT:
  Session ID   : 2
  Local Addr   : 80.208.1.2/255.255.255.255/17/1701
  Remote Addr  : 70.208.1.2/255.255.255.255/17/0
  Encryption   : 3DES                   Hashing      : MD5
  Encapsulation: Transport
  Rekey Int (T): 300 Seconds            Rekey Left(T): 293 Seconds
  Idle Time Out: 1 Minutes              Idle TO Left : 1 Minutes
  Bytes Tx     : 1209                   Bytes Rx     : 2793
  Pkts Tx      : 20                     Pkts Rx      : 32
```

```
L2TPOverIPSecOverNatT:
  Session ID   : 3
  Username     : v_gonzalez
  Assigned IP  : 90.208.1.202
  Encryption   : none                    Auth Mode    : PAP
  Idle Time Out: 1 Minutes               Idle TO Left : 1 Minutes
  Bytes Tx     : 584                     Bytes Rx     : 2224
  Pkts Tx      : 18                      Pkts Rx      : 30
====================
```

L2TP デバッグ コマンドの使用

特権 EXEC モードで **debug l2tp** コマンドを使用すると、L2TP のデバッグ情報を表示できます。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug l2tp {**data** | **error** | **event** | **packet**} *level*

data を指定すると、データ パケットのトレース情報が表示されます。

error を指定すると、エラー イベントが表示されます。

event を指定すると、L2TP 接続イベントが表示されます。

packet を指定すると、パケットのトレース情報が表示されます。

level は、表示するデバッグ メッセージ レベルを 1 ～ 255 の範囲で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

次に、接続イベントに関する L2TP デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、L2TP デバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug l2tp event 1
hostname# show debug
debug l2tp event enabled at level 1
hostname#
```

IPSec デバッグのイネーブル化

次のレジストリを追加することで、IPSec のデバッグ情報を Windows 2000 クライアントに追加できます。

ステップ 1　Windows 2000 のレジストリ エディタ REGEDIT を起動します。

ステップ 2　次のレジストリ エントリを検索します。

MyComputer\HKEY_LOCAL_MACHINE\CurrentControlSet\Services\PolicyAgent

ステップ 3　**oakley** を入力してキーを作成します。

ステップ 4　**EnableLogging** を入力して DWORD を作成します。

ステップ 5　「Enable Logging」値を「1」に設定します。

ステップ 6　IPSec Policy Agent を停止し、再起動します（[Start] > [Programs] > [Administrative Tools] > [Services] をクリック）。デバッグ ファイルは「%windir%\debug\oakley.log」にあります。

追加情報の入手

www.microsoft.com サイトには、さまざまな項目に関する追加情報があります。

http://support.microsoft.com/support/kb/articles/Q240/2/62.ASP

事前共有キー認証を使用して L2TP/IPSec 接続を設定する方法が説明されています。

http://support.microsoft.com/support/kb/articles/Q253/4/98.ASP

IP Security（IPSec; IP セキュリティ）で使用する証明書をインストールする方法が説明されています。

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/WINDOWS2000/en/server/help/sag_VPN_us26.htm

L2TP over IPSec VPN 接続用の Windows 2000 マシン証明書を使用する方法が説明されています。

http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp#heading3

カスタム MMC コンソールを作成してコンピュータの監査ポリシーをイネーブルにする方法が説明されています。

http://support.microsoft.com/support/kb/articles/Q259/3/35.ASP