CHAPTER 17

VPN グローバル設定

このヘルプ トピックでは、VPN グローバル設定のウィンドウについて説明します。

VPN グローバル設定

このウィンドウには、ルータの VPN グローバル設定が表示されます。

フィールド リファレンス

表 17-1 に、この画面のフィールドの説明を示します。

表 17-1　VPN グローバル設定のフィールド

項目	説明
編集ボタン	［編集］ボタンをクリックすると、VPN グローバル設定の追加または変更ができます。
IKE の有効化	IKE を有効にする場合は値を True にし、無効にする場合は False にします。 **（注）** IKE が無効の場合、VPN 設定は機能しません。［編集］をクリックして、［VPN グローバル設定］画面の［IKE］タブで IKE を有効化できます。

表 17-1　VPN グローバル設定のフィールド（続き）

項目	説明
アグレッシブ モードの有効化	アグレッシブ モードを有効にする場合は値を True にし、無効にする場合は False にします。アグレッシブ モード機能を使用すると、IPSec ピアの RADIUS トンネル属性を指定し、その属性で IKE アグレッシブ モード ネゴシエーションを初期化できます。
XAuth タイムアウト	システムが XAuth チャレンジに応答するのをルータが待つ秒数です。
IKE ID	ルータが IKE ネゴシエーションで自身の識別に使用する、ルータのホスト名または IP アドレスを入力します。
デッド ピア検知	デッド ピア検知（DPD）を使用すると、ルータでデッド ピアを検出できます。検出された場合は、そのピアとの IPSec および IKE セキュリティ アソシエーションが削除されます。DPD が有効な場合、次の追加情報が表示されます。 • ［IKE キープアライブ（秒）］— IKE キープアライブ パケットの送信ごとにルータが待機する秒数です。 • ［IKE 再試行（秒）］— リモート ピアとの IKE 接続試行ごとにルータが待機する秒数です。デフォルトでは 2 秒と表示されます。 • ［DPD タイプ］—［必要時］または［定期的］です。［必要時］に設定した場合は、トラフィック パターンに基づいて DPD メッセージが送信されます。たとえば、ルータは、アウトバウンド トラフィックを送信する場合にピアの活動状態に問題があると、DPD メッセージを送信してピアのステータスを問い合わせます。送信するトラフィックがルータにない場合、DPD メッセージは送信されません。 ［定期的］に設定した場合は、IKE キープアライブの値で指定した間隔で DPD メッセージが送信されます。
IPSec SA ライフタイム（秒）	IPSec セキュリティ アソシエーション（SA）の有効期限が切れるまでの時間です。この後 SA が再生成されます。デフォルトは 3,600 秒（1 時間）です。

表 17-1　VPN グローバル設定のフィールド（続き）

項目	説明
IPSec SA ライフタイム（キロバイト）	IPSec SA の有効期限が切れるまでにルータが VPN 接続を介して送信できるキロバイト数です。SA は最短のライフタイムに達すると更新されます。
Easy 接続のシスログ メッセージ	このフィールドには、次のいずれかの値を指定できます。 • ［有効］— シスログ（Syslog）メッセージはすべての Easy VPN 接続に対して有効です。 • ［次のグループの syslog メッセージを有効にする］— シスログ（Syslog）メッセージはリストされたグループに対して有効です。 • ［無効］— シスログ（Syslog）メッセージは無効です。

VPN グローバル設定：IKE

このウィンドウでは、IKE および IPSEC のグローバル設定を行うことができます。

IKE の有効化

VPN を使用する場合はこのチェック ボックスを選択したままにします。

注意　IKE が無効の場合、VPN 設定は機能しません。

アグレッシブ モードの有効化

アグレッシブ モード機能を使用すると、IPSec ピアの RADIUS トンネル属性を指定し、その属性で IKE アグレッシブ モード ネゴシエーションを初期化できます。

ID（このルータ）

このフィールドでは、ルータが自身を識別する方法を指定します。［IP アドレス］または［ホスト名］を選択します。

XAuth タイムアウト

XAuth 認証を要求するシステムからの応答をルータが待つ秒数です。

デッド ピア検知（DPD）を有効にする

デッド ピア検知（DPD）を使用すると、ルータでデッド ピアを検出できます。検出された場合は、そのピアとの IPSec および IKE セキュリティ アソシエーションが削除されます。

ルータが使用している Cisco IOS イメージが DPD をサポートしていない場合、［デッド ピア検知（DPD）を有効にする］チェック ボックスは無効になります。

キープアライブ

ルータが、使用されていない接続を維持する秒数を指定します。

再試行

ルータが、ピアとの IKE 接続試行間に待機する秒数を指定します。デフォルト値は 2 秒です。

DPD タイプ

［必要時］または［定期的］を選択します。

［必要時］に設定した場合は、トラフィック パターンに基づいて DPD メッセージが送信されます。たとえば、ルータは、アウトバウンド トラフィックを送信する場合にピアの活動状態に問題があると、DPD メッセージを送信してピアのステータスを問い合わせます。送信するトラフィックがルータにない場合、DPD メッセージは送信されません。

［定期的］に設定した場合は、IKE キープアライブの値で指定した間隔で DPD メッセージが送信されます。

VPN グローバル設定：IPSec

このウィンドウでグローバル IPSec 設定を編集します。

新しいキーを認証および生成する間隔

このボックスを選択して、ルータが新しいキーを認証および生成する間隔を指定します。値を指定しない場合、ルータは 1 時間ごとに新しいキーを認証および生成します。

現在のキーが次のボリュームを暗号化したら新しいキーを生成する

このボックスを選択して、ルータが新しいキーを認証および生成する前に現在のキーで暗号化するキロバイト数を指定します。値を指定しない場合、ルータは、現在のキーで 4,608,000 キロバイトを暗号化した後、新しいキーを認証および生成します。

VPN グローバル設定：Easy VPN サーバ

この画面では、Easy VPN サーバ接続のグローバル設定を行います。

フィールド リファレンス

表 17-2 に、この画面のフィールドの説明を示します。

表 17-2　VPN グローバル設定：Easy VPN サーバのフィールド

項目	説明
共有プール	すべてのクライアントが使用する共有 IP アドレス プールを設定できます。専用のプールがないグループに属するクライアントには、この共有プールから IP アドレスが割り当てられます。 ［共有プールを選択］— このリストからプール名を選択します。プールが設定されていない場合は、［追加タスク］>［ローカル プール］>［追加］の順にクリックして、表示されたダイアログでプールを設定します。その後でこの画面に戻り、設定したプールを選択します。
シスログメッセージの有効化	クライアント接続に対してシスログ（Syslog）メッセージを有効にする場合は、［シスログメッセージの有効化］を選択します。このオプションの適用範囲は、次のように指定できます。 • ［すべてのクライアント接続のシスログ メッセージを有効にする。］— シスログ（Syslog）メッセージを Easy VPN サーバに接続するすべてのグループに対して有効にする場合は、このオプションを選択します。 • ［次のグループのシスログ メッセージを有効にする。］— シスログ（Ssyslog）メッセージを指定したグループに対して有効にする場合は、このオプションを選択します。次に、ボックスにグループ名を入力します（複数の場合はグループ名をカンマで区切ります）。次にエントリの入力例を示します。 `WGP-1, WGP-2, ACCTG, CSVC` 画面のこの部分を表示するには、ルータが Cisco IOS 12.4(4)T 以降を使用している必要があります。

VPN キー暗号化の設定

［VPN キー暗号化の設定］ウィンドウは、ルータの Cisco IOS イメージで Type 6 の暗号化技術がサポートされている場合に表示されます。これは、*VPN キー暗号化*とも呼ばれます。このウィンドウを使用して、事前共有キー、Easy VPN キー、XAuth キーなどの VPN キーを暗号化するときに使用するマスタ キーを指定できます。これらのキーは、暗号化されると、ルータのコンフィギュレーション ファイルを表示しても読めなくなります。

VPN キー暗号化の有効化

これらのキーの暗号化を有効にするときに選択します。

現在のマスタ キー

マスタ キーが設定されている場合、このフィールドにはアスタリスク（*）が表示されます。

新しいマスタ キー

このフィールドには新しいマスタ キーを入力します。マスタ キーは、8 ～ 128 文字にする必要があります。

マスタ キーの確認

確認のため、このフィールドにマスタ キーを再入力します。このフィールドの値と［新しいマスタ キー］フィールドの値が一致しない場合は、キーの再入力が求められます。