CHAPTER 15

Enhanced Easy VPN

次の各セクションで、Enhanced Easy VPN に関する Cisco Configuration Professional の設定画面について説明します。

インターフェイスと認証

このウィンドウでは、仮想テンプレート インターフェイスをアンナンバードに設定するルータ インターフェイスと、認証に使用する方式を指定します。

フィールド リファレンス

表 15-1　インターフェイスと認証

項目	説明
インターフェイス	IP アドレスを取得するには、仮想テンプレート インターフェイスをルータ インターフェイスに対してアンナンバードとする必要があります。 最大限の柔軟性を確保するために、仮想テンプレート インターフェイスは、ループバック アドレスに対してアンナンバードにすることをお勧めします。これを実行するには、［新しいアンナンバード ループバック インターフェイス］をクリックし、ループバック インターフェイスの IP アドレスおよびサブネット マスクを入力します。たとえば、127.0.0.1、255.255.255.0 などのループバック IP アドレスおよびサブネット マスクを入力します。 別のインターフェイスに対して仮想テンプレート インターフェイスをアンナンバードにするには、［アンナンバード］をクリックして、インターフェイスを選択します。選択するインターフェイスは、ルータ上でトンネルを終端するものであることが必要です。選択するインターフェイスの IP アドレス、認証、ポリシーなどの情報を確認するには、［詳細］をクリックします。
認証	Easy VPN クライアントがルータに設定された Easy VPN サーバに対して自身の認証に使用する方式を選択します。事前共有キーを使用する場合は、そのキーを Easy VPN クライアントの管理者に通知する必要があります。デジタル証明書についてはこの通知は必要ありませんが、各クライアントは、登録を行ってデジタル証明書を取得する必要があります。

RADIUS サーバ

［RADIUS サーバ］ウィンドウでは、ルータが認証とグループ ポリシー検索に使用する RADIUS サーバ、および RADIUS サーバに設定されている VPN グループを指定します。

フィールド リファレンス

表 15-2　RADIUS サーバのフィールド

項目	説明
RADIUS クライアント ソース	RADIUS のソースを設定すると、RADIUS サーバにバインドされたパケットで送信されるように、送信元 IP アドレスを指定できます。IP アドレスおよびインターフェイスに関するその他の情報を確認するには、インターフェイスを選択して［詳細］ボタンをクリックします。このオプションには、次のいずれかの値を指定できます。 • ［ルータが送信元を選択します］— RADIUS パケットの送信元 IP アドレスを RADIUS パケットがルータから送り出されるときに通過するインターフェイスのアドレスにするには、［ルータが送信元を選択します］を選択します。 • ［インターフェイス名］— 特定のルータ インターフェイスを選択すると、RADIUS パケットの送信元 IP アドレスは、そのインターフェイスのアドレスになります。 Cisco Access Control Server（ACS）バージョン 3.3 以降では、ルータから送信される RADIUS パケットの送信元 IP アドレスを NAD IP アドレスとして設定する必要があります。 **（注）** Cisco IOS ソフトウェアを使用すると、単一 RADIUS ソースのインターフェイスはルータ上で設定できます。ルータには設定された RADIUS ソースがあるため、別のソースを選択する場合、RADIUS サーバに送信されるパケットにある送信元 IP アドレスは、新しいソースの IP アドレスに変わり、Cisco ACS で設定された NAD IP アドレスと一致しない場合があります。

表 15-2　RADIUS サーバのフィールド（続き）

項目	説明
RADIUS サーバ リスト	
サーバ IP	［サーバ IP］カラムには、設定されている各サーバの IP アドレスが表示されます（192.168.108.14 など）。
パラメータ	［パラメータ］カラムには、各サーバの許可ポートおよびアカウンティング ポートが表示されます。たとえば、カラムには RADIUS サーバの次のエントリが表示されます。 `Authorization Port 1645; Accounting Port 1646`
選択	［選択］カラムには、設定されているサーバごとにチェック ボックスが表示されます。使用するサーバの横にあるチェック ボックスを選択します。横のボックスが選択されていない RADIUS サーバには、ルータはアクセスしません。
追加	RADIUS サーバのエントリを作成するには、［追加］をクリックします。
編集	サーバのエントリを選択して［編集］をクリックすると、ルータに設定されているそのサーバの情報を変更できます。
Ping	ルータと RADIUS サーバ間の接続をテストするには、サーバのエントリを選択して［Ping］をクリックします。
RADIUS サーバにある VPN グループ	RADIUS サーバに設定されている VPN グループのうち、この接続でアクセスを許可するグループを入力します。各エントリはカンマを使用して区切ります。次にエントリの入力例を示します。 `WGP-1, WGP-2, ACCTG, CSVC` これらの名前は、RADIUS サーバに設定されているグループ名と一致している必要があります。管理を容易にするために、Easy VPN クライアントに設定するグループ名とも一致させる必要があります。

表 15-2　RADIUS サーバのフィールド（続き）

項目	説明
PKI ベースのユーザごとのポリシーのダウンロード	モード設定時に Easy VPN サーバが RADIUS サーバからユーザ固有属性をダウンロードしてクライアントにプッシュするように設定するには、[PKI ベースのユーザごとのポリシーのダウンロード] を選択します。Easy VPN サーバはクライアントのデジタル証明書からユーザ名を取得します。 このオプションは、次の場合に表示されます。 • ルータが Cisco IOS 12.4(4)T 以降のイメージを実行している場合。 • IKE ポリシー設定でデジタル証明書認証を選択した場合。 • RADIUS または RADIUS およびローカル グループ許可を選択した場合。

グループ許可およびユーザ グループ ポリシー

独自の IP アドレス プール、クライアント アップデート設定、スプリット トンネリング設定などのカスタム設定を持つユーザ グループを作成できます。これらのグループの属性は、そのグループが Easy VPN サーバに接続したときに、グループ内のクライアントにダウンロードされます。正しいグループ属性がダウンロードされるように、グループのメンバであるクライアント上に同じグループ名を設定する必要があります。

フィールド リファレンス

表 15-3　グループ許可およびユーザ グループ ポリシー

項目	説明
グループ ポリシー	グループ ポリシーがすでに設定されている場合は、このウィンドウにそれらのポリシーが一覧表示されます。グループ名の左側にある［選択］チェック ボックスを選択すれば、この接続に使用するポリシーを選択できます。 リストには、設定されている各グループのグループ名、IP アドレス プール名、DNS サーバ名、WINS サーバ名、およびドメイン名が表示されます。［追加］をクリックして新しいグループを設定したり、［編集］をクリックして設定を変更したりした場合は、その変更がこのリストに表示されます。既存のグループの設定を基に新しいグループを設定するには、既存のグループを選択して、［複製］をクリックします。［追加］、［編集］、および［複製］ボタンをクリックすると、グループ設定を指定できるダイアログが表示されます。
アイドル タイマの設定	アイドル状態のクライアントの接続を維持する時間を［アイドル タイマ］フィールドに指定する場合は、［アイドル タイマの設定］を選択します。時間の値は HH:MM:SS の形式で入力します。たとえば、3 時間 20 分 32 秒と指定するには、次のようにフィールドに値を入力します。 `03:20:32` タイムアウト値は、この接続に設定されているすべてのグループに適用されます。

Easy VPN サーバの追加または編集：全般タブ

このダイアログには、Easy VPN サーバ接続の全般的な情報を入力します。

フィールド リファレンス

表 15-4　Easy VPN サーバの追加または編集：全般タブ

項目	説明
この接続の名前	この接続を識別するための名前を入力します。入力した名前は、［Easy VPN サーバの編集］ウィンドウに表示されます。
仮想トンネル インターフェイスの IP アドレス	仮想トンネルの IP アドレスに関するフィールドの説明については、「インターフェイスと認証」を参照してください。
トンネル モード	［トンネル モード］フィールドでは［IPSec-IPV4］を選択します。［IPSec-IPV4］オプションを選択すると、IP バージョン 4 の IPSec トンネルを作成できます。
説明	ここには、ネットワーク管理者にとって、ネットワークの設定変更やトラブルシューティングに役立つ情報を入力できます。

Easy VPN サーバの追加または編集：IKE タブ

Easy VPN サーバの追加に関するダイアログの［IKE］ダイアログでは、この接続の IKE プロファイルを作成できます。

フィールド リファレンス

表 15-5　Easy VPN サーバ接続の追加 / 編集：IKE タブ

項目	説明
ID タイプの一致	IKE プロファイルには、IKE 接続パラメータの適用先の送受信接続をルータが識別できるようにするための、一致条件が含まれています。ここで、一致条件を VPN グループに適用することができます。グループは、［ID タイプの一致］フィールドで自動的に選択されます。

表 15-5　Easy VPN サーバ接続の追加 / 編集：IKE タブ（続き）

項目	説明
この IKE プロファイルに関連付ける VPN グループを追加します。	一致条件に追加するグループのリストを作成します。追加したグループが表示されます。 • ［追加］— 次のオプションを含むメニューを表示する場合は、［追加］をクリックします。 　– ［外部グループ名の追加］— ルータに設定されていないグループの名前を追加する場合は、［外部グループ名の追加］を選択して、表示されるダイアログにその名前を入力します。 　– ［ローカル グループから選択］— ルータに設定されているグループの名前を追加する場合は、［ローカル グループから選択］を選択します。表示されるダイアログで、追加するグループの横にあるチェック ボックスを選択します。すべてのローカル グループが他の IKE プロファイルで使用されている場合は、すべてのグループがすでに選択されていることを示すメッセージが表示されます。 • ［削除］— リストからグループを削除するには、そのグループを選択し、［削除］をクリックします。
モード設定	次のいずれかのオプションを選択して、Easy VPN サーバがモード設定要求を処理する方法を指定します。 • ［応答］— Easy VPN サーバを使用してモード設定要求に応答する場合は、［モード設定］フィールドの［応答］を選択します。 • ［開始］— Easy VPN サーバを使用してモード設定要求を開始する場合は、［開始］を選択します。 • ［両方］— モード設定要求の開始と応答の両方に、Easy VPN サーバを使用する場合は、［両方］を選択します。

表 15-5　Easy VPN サーバ接続の追加 / 編集：IKE タブ（続き）

項目	説明
グループ ポリシー検索許可ポリシー	AAA サーバ上のグループ ポリシー情報へのアクセスを制御する許可ポリシーを指定します。 • ［デフォルト］— グループ ポリシー検索情報へのアクセスを許可する場合は、［デフォルト］を選択します。 • ［ポリシー名］— ポリシーを指定する場合は、リストから既存のポリシーを選択します。 • ［追加］— 表示されたダイアログでポリシーを作成する場合は、［追加］をクリックします。
ユーザ認証ポリシー	XAuth ログインを許可する場合、または XAuth ログインに使用するユーザ認証を指定する場合は、［ユーザ認証ポリシー］を選択します。次のいずれかのオプションを選択します。 • ［デフォルト］— XAuth ログインを許可する場合は、［デフォルト］を選択します。 • ［ポリシー名］— ルータ上でポリシーが設定されている場合は、リストから使用するポリシーを選択できます。 表示されたダイアログでポリシーを作成し、この IKE ポリシーで使用する場合は、［追加］をクリックします。
デッド ピア検出	ルータからデッド ピア検知（DPD）メッセージを Easy VPN リモート クライアントに送信できるようにするには、［デッド ピア検出］をクリックします。クライアントが DPD メッセージに応答しないと、そのクライアントとの接続は解除されます。 • ［キープアライブ間隔］— DPD メッセージの間隔を秒単位で指定します。範囲は 10 ～ 3,600 秒です。 • ［リトライ間隔］— DPD メッセージの送信に失敗した場合の再試行間隔を秒単位で指定します。範囲は 2 ～ 60 秒です。 デッド ピア検出では、管理者の介入なしに接続を管理できますが、接続を維持するために両方のピアで処理する必要がある追加のパケットが生成されます。

表 15-5　Easy VPN サーバ接続の追加 / 編集：IKE タブ（続き）

項目	説明
PKI 証明書フィールドに基づいて、RADIUS サーバからユーザ属性をダウンロードします。	モード設定時に Easy VPN サーバが RADIUS サーバからユーザ固有属性をダウンロードし、クライアントに通知するように設定するには、このオプションを選択します。Easy VPN サーバはクライアントのデジタル証明書からユーザ名を取得します。 このオプションは、次の場合に表示されます。 • ルータが Cisco IOS 12.4(4)T 以降のイメージを実行している場合。 • IKE ポリシー設定でデジタル証明書認証を選択した場合。 • RADIUS または RADIUS およびローカル グループ許可を選択した場合。

Easy VPN サーバの追加または編集：IPSec タブ

このダイアログには、IPSec プロファイルを作成するための情報を入力します。IPSec プロファイルは、使用するトランスフォーム セット、セキュリティ アソシエーション（SA）ライフタイムの特定方法などの情報を指定します。

フィールド リファレンス

表 15-6　Easy VPN サーバの追加または編集：IPSec タブ

項目	説明
トランスフォーム セット カラム	ダイアログの上部にある 2 つのカラムを使用して、プロファイルに追加するトランスフォーム セットを指定します。左側のカラムには、ルータに設定されているトランスフォーム セットが表示されます。設定されているトランスフォーム セットをプロファイルに追加するには、そのセットを選択して、[>>] ボタンをクリックします。左側のカラムにトランスフォーム セットが表示されていない場合や、まだ作成されていないトランスフォーム セットが必要な場合は、[追加] をクリックして、表示されるダイアログでトランスフォーム セットを作成します。

表 15-6　Easy VPN サーバの追加または編集：IPSec タブ（続き）

項目	説明
時間ベースの IPSec SA ライフタイム	一定時間が経過したら新しい SA が確立されるようにする場合は、［時間ベースの IPSec SA ライフタイム］をクリックします。右側の［HH:MM:SS］フィールドに時間を入力します。範囲は 0:2:0（2 分）～ 24:0:0（24 時間）です。
トラフィック量ベースの IPSec SA ライフタイム	指定した量のトラフィックが IPSec トンネルを通過したら新しい SA が確立されるようにする場合は、［トラフィック量ベースの IPSec SA ライフタイム］をクリックします。既存の SA が解除されて新しい SA が確立するまでに、トンネルを通過するトラフィックのキロバイト数（KB）を入力します。範囲は 2,560 ～ 536,870,912KB です。
IPSec SA アイドル タイム	指定した期間ピアがアイドル状態だった場合に新しい SA が確立されるようにする場合は、［IPSec SA アイドル タイム］をクリックします。右側の［HH:MM:SS］フィールドにアイドル時間を入力します。範囲は 0:1:0（1 分）～ 24:0:0（24 時間）です。
完全転送秘密	IPSec がこの仮想テンプレート インターフェイスに新しいセキュリティ アソシエーションを要求する際に PFS（perfect forward secrecy; 完全転送秘密）を求める必要がある場合、またはピアから受信する要求に PFS が必要な場合は、［完全転送秘密］をクリックします。指定できる値は次のとおりです。 • グループ 1 — PFS 要求の暗号化に、768 ビットの Diffie-Hellman プライム モジュラス グループが使用されます。 • グループ 2 — PFS 要求の暗号化に、1,024 ビットの Diffie-Hellman プライム モジュラス グループが使用されます。 • グループ 5 — PFS 要求の暗号化に、1,536 ビットの Diffie-Hellman プライム モジュラス グループが使用されます。

仮想トンネル インターフェイスの作成

このダイアログには、仮想トンネル インターフェイスの情報を入力します。

フィールド リファレンス

表 15-7　仮想トンネル インターフェイスの作成

項目	説明
インターフェイス タイプ	インターフェイスのタイプとして、［デフォルト］または［トンネル］を選択します。仮想トンネル インターフェイスを編集する場合は、設定されている値が表示され、フィールドは読み取り専用です。
インターフェイスの IP アドレスの設定	仮想トンネル インターフェイスの IP アドレスを別のインターフェイスに対してアンナンバードにすることも、仮想トンネル インターフェイスに IP アドレスを指定しないことも選択できます。［IP アンナンバード］を選択して［アンナンバード］フィールドでインターフェイス名を選択するか、または［IP アドレスなし］を選択します。
トンネル モード	Cisco CP では、現在 IPSec-IPv4 トンネル モードがサポートされているため、このモードが選択されます。
ゾーンの選択	このフィールドは、ゾーンポリシー ベース ファイアウォール（ZPF）をサポートする Cisco IOS イメージがルータで実行されていて、ルータにゾーンが設定されている場合に表示されます。この仮想トンネル インターフェイスをゾーン メンバにする場合は、このフィールドの右側にあるボタンをクリックします。［ゾーンの選択］をクリックし、インターフェイスをメンバにするゾーンを選択します。または、［ゾーンの作成］をクリックして、このインターフェイスに新しいゾーンを作成します。 **（注）** 仮想トンネル インターフェイスは必ずしもゾーンのメンバである必要はありません。ただし、ルータは、ゾーンのメンバであるインターフェイスとゾーンのメンバでないインターフェイス間ではトラフィックを転送しません。