CHAPTER 22

Cisco IOS SSL VPN

Cisco IOS SSL VPN は、Web ブラウザとそのネイティブの SSL 暗号化機能だけを使用して、インターネットに接続可能なほぼすべての場所からの Secure Socket Layer（SSL）VPN によるリモートアクセス接続を提供します。企業は、Cisco IOS WebVPN によってインターネットに接続できる場所ならどこからでも企業リソースにリモートアクセス接続できるようにすることで、安全に企業ネットワークをすべての許可ユーザに拡張することができます。

また、Cisco IOS SSL VPN を使用すれば、ホーム コンピュータ、インターネット キオスク、ワイヤレス ホットスポットなどの、IT 部門が IPsec VPN 接続に必要な VPN クライアント ソフトウェアを展開および管理することが難しい、自社所有でないマシンからもアクセスが可能になります。

SSL VPN アクセスには、クライアントレス、シンクライアント、およびフルトンネル クライアントの 3 つのモードがあります。Cisco Router and Security Device Manager（Cisco CP）はこれら 3 つのモードをすべてサポートしています。各モードについて、以下に示します。

- **クライアントレス SSL VPN —** クライアントレス モードは、プライベート Web リソースへの安全なアクセスを提供し、Web コンテンツにアクセスできます。このモードは、イントラネット アクセスなど、Web ブラウザ内での使用を想定している大部分のコンテンツと、Web インターフェイスを使用しているオンライン ツールにアクセスする場合に便利です。
- **シン クライアント SSL VPN**（ポート転送 Java アプレット）**—** シン クライアント モードは、POP3、SMTP、IMAP、Telnet、SSH などの TCP ベースのアプリケーションにリモート アクセスできるように、Web ブラウザの暗号関数の機能を拡張しています。

- **フル トンネル クライアント SSL VPN —** フル トンネル クライアント モードは、動的にダウンロードされる Cisco IOS SSL VPN 用の SSL VPN クライアント ソフトウェアを通じて、広範なアプリケーションをサポートします。Cisco IOS SSL VPN のフル トンネル クライアントでは、中央から設定する軽量でサポートしやすい SSL VPN トンネリング クライアントが提供され、これによりあらゆるアプリケーションへのネットワーク レイヤー接続アクセスが可能となります。

Cisco IOS SSL VPN 設定コンポーネントが連携して動作する方法については、「Cisco IOS SSL VPN コンテキスト、ゲートウェイ、およびポリシー」で説明します。

Cisco IOS SSL VPN ドキュメントへのリンクについては、「Cisco.com の Cisco IOS SSL VPN リンク」を参照してください。

この章の内容は、次のとおりです。

- Cisco.com の Cisco IOS SSL VPN リンク
- SSL VPN 接続の作成
- SSL VPN 接続の編集
- その他のヘルプ トピック

Cisco.com の Cisco IOS SSL VPN リンク

このヘルプ トピックでは、Cisco IOS SSL VPN に関して最も役立つ情報が記載されている最新リンクを示します。

次のリンクから、Cisco IOS SSL VPN に関するドキュメントにアクセスできます。ときどきこのリンクをクリックして、最新情報を確認してください。

www.cisco.com/go/iosSSLVPN

次のリンクでは、Cisco IOS SSL VPN に対して RADIUS プロトコルを使用して AAA サーバを設定する方法を説明しています。

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

SSL VPN 接続の作成

SSL VPN 接続を作成するには、次のタスクを実行します。

ステップ 1　Cisco CP の機能バーで、[設定]>[セキュリティ]>[VPN]の順にクリックします。

ステップ 2　［VPN］ツリーで、［SSL VPN］>［SSL VPN マネージャ］の順に選択します。

ステップ 3　［SSL VPN の作成］タブで、タスクのリンクをクリックして、表示された推奨タスクをすべて完了します。Cisco CP によってタスクが自動的に完了するか、または設定に必要な設定画面が表示されます。

ステップ 4　完了するタスクを選択します。最初の SSL VPN 接続を作成する場合は、［新しい SSL VPN を作成］を選択します。

ステップ 5　［選択したタスクを実行する］をクリックして、接続の設定を開始します。

ステップ 6　ウィザード画面で設定を行います。［次へ］をクリックして、現在の画面から次の画面に移動します。［戻る］をクリックして、前の画面に戻ります。

ステップ 7　設定を完了すると、Cisco CP に要約画面が表示されます。設定を確認します。変更が必要な場合は、［戻る］をクリックして該当画面に戻り、変更を加えてから要約画面に戻ります。

ステップ 8　［設定の編集］画面で［コマンドをルータに配信する前にプレビューする］を選択している場合は、送信する Cisco IOS CLI コマンドが表示されます。ルータに設定を送信する場合は［OK］を、この設定を破棄する場合は［キャンセル］をクリックします。この設定が行われていない場合、[完了]をクリックするとルータに設定が送信されます。

「SSL VPN 接続の作成のリファレンス」では、このタスクを完了するために使用する画面について説明しています。

SSL VPN 接続の作成のリファレンス

この章の各トピックでは、SSL VPN の作成画面について説明します。

- SSL VPN の作成
- 永続的な自己署名証明書
- ようこそ
- SSL VPN ゲートウェイ
- ユーザ認証
- イントラネット Web サイトの設定
- URL の追加 / 編集
- SSL VPN ポータルページのカスタマイズ
- SSL VPN パススルー設定
- ユーザ ポリシー
- SSL VPN グループ ポリシーの詳細：ポリシー名
- SSL VPN ユーザ グループの選択
- ［拡張ファイアウォール］の選択
- シン クライアント（ポート転送）
- サーバの追加 / 編集
- フル トンネル
- Cisco CP 用のインストール バンドルの検索
- Cisco Secure Desktop の有効化
- Common Internet File System
- クライアントレス Citrix を有効にする
- 要約

SSL VPN の作成

Cisco IOS SSL VPN ウィザードを使用すると、新しい Cisco IOS SSL VPN を作成したり、既存の Cisco IOS SSL VPN に新しいポリシーや機能を追加することができます。

Cisco CP でサポートする機能の概要については、「Cisco IOS SSL VPN」を参照してください。Cisco IOS SSL VPN 設定コンポーネントが連携して動作する方法については、「Cisco IOS SSL VPN コンテキスト、ゲートウェイ、およびポリシー」で説明します。

Cisco IOS SSL VPN ドキュメントへのリンクについては、「Cisco.com の Cisco IOS SSL VPN リンク」を参照してください。

必須タスク

ルータ上で AAA と 証明書を設定しておかなければ、Cisco IOS SSL VPN の設定を行うことはできません。AAA と 証明書のいずれかまたは両方の設定を行っていない場合、ウィンドウ上のこのエリアにその通知と未設定項目へのリンクが表示されるので、そのリンク先で設定していない項目を設定できます。すべての必須設定が完了したら、このウィンドウに戻って Cisco IOS SSL VPN の設定を開始できます。

ユーザが何も入力しなくても、Cisco CP により AAA は有効になります。Cisco CP を使用すると、ルータのパブリック キーとプライベート キーを生成し、それらのキーを認証機関に登録してデジタル証明書を取得できます。詳細については、「パブリック キー インフラストラクチャ」を参照してください。また、CA による承認を必要としない永続的な自己署名証明書も設定できます。永続的な自己署名証明書機能の詳細については、次のリンク先を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

この URL 全部が完全にブラウザのリンク フィールドに指定されていることを確認してください。

新しい SSL VPN を作成

新しい Cisco IOS SSL VPN 設定を作成する場合に選択します。このウィザードでは、1 つのユーザ ポリシーと限定された機能セットを持つ Cisco IOS SSL VPN を作成できます。このウィザードを終了したら、別のウィザードを使用すれば、その Cisco IOS SSL VPN の追加ポリシーと機能を設定できます。このウィザードに戻ると、別の Cisco IOS SSL VPN 設定を作成できます。

Cisco CP を使用してルータ上に最初の Cisco IOS SSL VPN 設定を作成したら、Cisco IOS SSL VPN コンテキストの作成、ゲートウェイの設定、およびグループ ポリシーの作成を行います。ウィザードを終了したら、［SSL VPN の編集］をクリックして設定を表示し、Cisco IOS SSL VPN コンポーネントがどのように連携して動作するか理解してください。表示される設定内容については、「Cisco IOS SSL VPN コンテキスト、ゲートウェイ、およびポリシー」を参照してください。

ユーザの新しいグループ用に、既存の SSL VPN に新しいポリシーを追加します

ユーザの新しいグループ用に、既存の Cisco IOS SSL VPN 設定に新しいポリシーを追加する場合に選択します。複数のポリシーを使用すると、異なるユーザ グループに対して別々の機能を定義することができます。たとえば、「エンジニアリング」に定義したポリシーとは別のポリシーを「セールス」に定義できます。

既存の SSL VPN の詳細機能を設定する

既存の Cisco IOS SSL VPN ポリシーに追加機能を設定する場合に選択します。この WebVPN ポリシーが設定されているコンテキストを指定する必要があります。

選択したタスクを実行するボタン

選択した設定を開始する場合にクリックします。選択したタスクを実行できない場合、警告メッセージが表示されます。実行しなければならない必須タスクがある場合は、その必須タスクと実行方法が表示されます。

永続的な自己署名証明書

このダイアログ ボックスでは、永続的な自己署名証明書の情報を指定できます。ここで指定した情報を使用して、SSL ハンドシェイクで使用する証明書が HTTPS サーバによって生成されます。永続的な自己署名証明書はルータがリロードされた場合でも設定に残っているので、SSL ハンドシェイク プロセス中は存在しています。ルータがリロードされた場合、新規ユーザはこの証明書を手動で受け入れる必要がありますが、すでに受け入れているユーザはその必要はありません。

永続的な自己署名証明書機能の詳細については、次のリンク先を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

この URL 全部が完全にブラウザのリンク フィールドに指定されていることを確認してください。

名前

このフィールドには、Router_Certificate という名前が表示されています。必要に応じて、この名前を変更できます。この名前は、証明書要求で使用される件名に対応しています。

RSA キーの長さ

このフィールドには、値 512 が表示されています。必要に応じて、より長いキー（1024 など）を指定できます。キーの長さは 64 の倍数でなければなりません。

件名

件名エリア内のフィールドの情報を指定します。これらのフィールドの詳細については、「その他の件名属性」を参照してください。

生成ボタン

このウィンドウに情報を指定したら、［生成］をクリックして、ルータで永続的な自己署名証明書を作成します。

ようこそ

各ウィザードの［ようこそ］ウィンドウには、そのウィザードで実行できるタスクが表示されます。この情報を見て、正しいウィザードを使用していることを確認してください。間違ったウィザードを開いているときは、［キャンセル］をクリックして［SSL VPN の作成］ウィンドウに戻り、使用したいウィザードを選択します。

ウィザードですべての情報を指定すると、指定した情報が［要約］ウィンドウに表示されます。ルータに配信している Cisco IOS CLI コマンドを確認するときは、［キャンセル］をクリックしてウィザードを終了し、［編集］>［設定］を順にクリックし、［コマンドをルータに配信する前にプレビューする］チェック ボックスを選択します。次に、ウィザードを再起動して、必要な情報を指定します。ルータに設定を配信するときは、別のウィンドウが表示され、配信する Cisco IOS CLI コマンドをこのウィンドウで確認できます。

SSL VPN ゲートウェイ

Cisco IOS SSL VPN ゲートウェイは、ゲートウェイを使用する SSL VPN コンテキストの IP アドレスとデジタル証明書を提供します。このウィンドウではゲートウェイの情報と、ユーザをポータルにアクセスできるようにする情報を指定できます。

IP アドレス フィールドと名前フィールド

これらのフィールドでは、ユーザが Cisco IOS SSL VPN ポータルにアクセスするときに入力する URL を作成します。IP アドレス リストには、設定済みのルータインターフェイスすべての IP アドレスと、既存の Cisco IOS SSL VPN ゲートウェイすべての IP アドレスが含まれます。ルータ インターフェイスの IP アドレスが目的のクライアントが到達可能なパブリック アドレスである場合は、その IP アドレスを使用し、そうでない場合は、そのクライアントが到達可能な別のパブリック IP アドレスを使用することができます。

ゲートウェイで使用されたことがない IP アドレスを使用する場合は、新しいゲートウェイを作成します。

*IP アドレス*を介した、セキュリティ保護された Cisco CP アクセスの有効化チェック ボックス

この IP アドレスから引き続き Cisco CP にアクセスする場合に、このチェック ボックスを選択します。Cisco CP へのアクセスに現在使用している IP アドレスを入力すると、このチェック ボックスが表示されます。

（注）　このチェック ボックスを選択すると、設定をルータに配信した後で Cisco CP へのアクセスに使用する必要がある URL が変更されます。ウィンドウ下部の情報エリアを調べて、使用する URL を確認してください。PC のデスクトップ上にこの URL へのショートカットが表示されるので、今後はこのショートカットを使用して Cisco CP にアクセスできます。

デジタル証明書

新しいゲートウェイを作成する場合、ゲートウェイへのログオン時にルータからクライアントに提示するデジタル証明書を選択します。既存のゲートウェイの IP アドレスを選択した場合は、ルータではそのゲートウェイに設定されているデジタル証明書を使用するので、このフィールドは無効になります。

情報エリア

［IP アドレス］フィールドと［名前］フィールドに情報を指定すると、このエリアにユーザが入力する URL が表示されます。この URL を、この Cisco IOS SSL VPN の作成対象であるユーザに提供する必要があります。

［**IP アドレス**を介した、セキュリティ保護された Cisco CP アクセスの有効化］チェック ボックスを選択した場合、今後 Cisco CP へのアクセスに使用する必要がある URL がこのエリアに表示されます。Cisco IOS SSL VPN 設定をルータに配信すると、PC のデスクトップ上にこの URL へのショートカットが表示されます。

ユーザ認証

このウィンドウでは、ルータでユーザ認証を実行する方法を指定します。ルータでは Cisco IOS SSL VPN ユーザをローカルに認証したり、リモート AAA サーバに認証リクエストを送信したりすることができます。

外部 AAA サーバ ボタン

ルータで AAA サーバを使用して Cisco IOS SSL VPN ユーザを認証する場合にクリックします。ルータは、このウィンドウに表示されている AAA サーバを使用します。設定されている AAA サーバがない場合は、このウィンドウで設定できます。このオプションを使用するには、少なくとも 1 つの AAA サーバをルータに設定しておく必要があります。

このルータ上でローカルにボタン

ルータ自身でユーザを認証する場合にクリックします。ルータではこのウィンドウに表示される各ユーザを認証します。ルータにユーザが設定されていない場合は、このウィンドウでユーザを追加できます。

最初は外部 AAA サーバ、次にこのルータ上でローカルにボタン

最初はルータで AAA サーバを使用して認証を行い、その認証が失敗したら、ローカル認証を行う場合にクリックします。そのユーザが設定済み AAA サーバに設定されていないか、またはルータ上でローカルに設定されていない場合は、そのユーザの認証は失敗します。

AAA 認証方式リストの使用ボタン

ルータで認証用の方式リストを使用する場合にクリックします。方式リストには、使用する認証方式が含まれています。ルータはこのリスト内の最初の認証方式を試みます。認証に失敗したら、このリスト内の次の方式を試みます。ユーザが認証されるか、またはリストの最後に達するまでこれを繰り返します。

このルータに対して設定されている AAA サーバ リスト

このリストには、ルータがユーザの認証に使用する AAA サーバが含まれています。AAA サーバを使用したユーザ認証を選択する場合、少なくとも 1 つのサーバの名前または IP アドレスがこのリストに含まれている必要があります。新しいサーバの情報を追加するには、［追加］ボタンを使用します。ルータ上の AAA 設定を管理するには、ウィザードを終了して［追加タスク］をクリックし、［追加タスク］ツリーの AAA ノードをクリックします。［このルータ上でローカルに］を選択している場合は、このリストは表示されません。

ユーザ アカウントをこのルータでローカルに作成します

このリストには、ルータで認証を行うユーザを入力します。［追加］ボタンと［編集］ボタンを使用して、ルータ上のユーザを管理します。［外部 AAA サーバ］を選択した場合は、このリストは表示されません。

イントラネット Web サイトの設定

ユーザがアクセスするイントラネット Web サイトのグループをこのウィンドウで設定します。これらのリンクは、Cisco IOS SSL VPN ユーザのログイン時に表示されるポータルに表示されます。

アクション カラムと URL リスト カラム

既存の Cisco IOS SSL VPN コンテキストにポリシーを追加する場合、表示されているテーブルに URL リストが含まれている場合があります。表示されている URL リストをポリシーで使用する場合は、［選択］を選択します。

新しいリストを作成するときは、［追加］をクリックして、表示されるダイアログに必要な情報を入力します。このテーブル内の URL リストを変更するときは［編集］キーを、削除するときは［削除］キーを使用します。

URL の追加 / 編集

このウィンドウでは、Cisco IOS SSL VPN リンクの情報を追加または編集します。

ラベル

ラベルは、ユーザが Cisco IOS SSL VPN にログインすると表示されるポータルに表示されます。たとえば、有給休暇と給料日を表示するカレンダーへのリンクを指定しているときは、ラベル「給与カレンダー」が使用されます。

URL リンク

ユーザにアクセスを許可する企業イントラネット Web サイトへの URL を入力または編集します。

SSL VPN ポータルページのカスタマイズ

この画面で行う設定によって、ユーザに対するポータルの外観が決まります。リストに挙げられている定義済みのテーマから選択して、そのテーマを使用した場合のポータルの表示をプレビューすることができます。

テーマ

定義済みのテーマの名前を選択します。

プレビュー

このエリアには、選択したテーマが反映されたポータルが表示されます。いくつかのテーマをプレビューして、使用するテーマを決定してください。

SSL VPN パススルー設定

ユーザをイントラネットにアクセスできるようにするには、アクセス コントロール エントリ（ACE）をファイアウォールとネットワーク アクセス コントロール（NAC）設定に追加して、SSL トラフィックがイントラネットに到達できるようにする必要があります。Cisco CP にこれらの ACE の設定を任せることもできますが、［セキュリティ］>［ファイアウォールと ACL］>［ファイアウォール ポリシー/ACL の編集］を選択して必要な編集を行えば、ユーザ自身で設定することもできます。

Cisco IOS SSL VPN ウィザード実行中に Cisco CP で ACE を設定する場合は、［NAC およびファイアウォールで作業するために SSL VPN を許可］をクリックします。Cisco CP によって作成された ACE を表示するには、［詳細の表示］をクリックします。Cisco CP が追加するエントリは、次の例のようになります。

```
permit tcp any host 172.16.5.5 eq 443
```

Cisco IOS SSL VPN コンテキストを編集しているときには、影響を受けるインターフェイスとそのインターフェイスに適用される ACL が表示されます。Cisco CP で ACL にエントリを追加し、SSL トラフィックがファイアウォールを通過できるようにするには、［変更］をクリックします。Cisco CP で追加したエントリを表示するには、［詳細］をクリックします。このエントリは、上記の例と同様のエントリになります。

ユーザ ポリシー

このウィンドウでは、既存の Cisco IOS SSL VPN を選択して、それに新しいポリシーを追加することができます。たとえば、Corporate という名前で作成されている Cisco IOS SSL VPN に、Engineering という名前の新しいユーザ グループに対するイントラネット アクセスを定義することができます。

既存の SSL VPN の選択

ユーザの新しいグループを作成する Cisco IOS SSL VPN を選択します。すでにその Cisco IOS SSL VPN に設定されているポリシーが、リストの下のボックスに表示されます。いずれかのポリシーをクリックすると、その詳細を表示できます。詳細については、「SSL VPN グループ ポリシーの詳細：ポリシー名」を参照してください。

新規ポリシーの名前

ユーザの新しいグループに付ける名前を入力します。このフィールドの下のエリアに、この Cisco IOS SSL VPN に設定されているグループ ポリシーが表示されます。

SSL VPN グループ ポリシーの詳細：ポリシー名

このウィンドウには、既存の Cisco IOS SSL VPN ポリシーの詳細が表示されます。

サービス

このエリアには、URL の細分化、Cisco Secure Desktop など、このポリシーが設定されているサービスが表示されます。

ユーザに表示される URL

このエリアには、このポリシーで制御されるユーザに表示されるイントラネット URL が表示されます。

ユーザに表示されるサーバ

このエリアには、このポリシーで使用するよう設定されているポート転送サーバの IP アドレスが表示されます。

WINS サーバ

このエリアには、このポリシーで使用するよう設定されている WINS サーバの IP アドレスが表示されます。

SSL VPN ユーザ グループの選択

詳細サービスを設定する Cisco IOS SSL VPN およびそれに関連付けられているユーザ グループをこのウィンドウで選択します。

SSL VPN

このリストから、ユーザ グループが関連付けられている Cisco IOS SSL VPN を選択します。

ユーザ グループ

詳細機能を設定するユーザ グループを選択します。このリストの内容は、選択した Cisco IOS SSL VPN によって異なります。

［拡張ファイアウォール］の選択

このウィンドウでは、設定する機能を選択します。選択した機能を設定できるウィンドウが、ウィザードに表示されます。

たとえば、［シン クライアント（ポート転送）］、［Cisco Secure Desktop］、および［Common Internet File System（CIFS）］をクリックすると、それらの機能の設定ウィンドウがウィザードに表示されます。

少なくとも 1 つの設定する機能を選択する必要があります。

シン クライアント（ポート転送）

リモート ワークステーションでは、イントラネット サーバと通信するために、クライアント アプリケーションを実行しなければならないことがあります。たとえば、Internet Mail Access Protocol（IMAP）サーバや Simple Mail Transfer Protocol（SMTP）サーバでは、電子メールを送受信するために、ワークステーションでクライアント アプリケーションを実行する必要があります。シン クライアント機能（ポート転送とも呼ばれる）を使用すると、ポータルと同時に小さなアプレットをダウンロードして、リモート ワークステーションがイントラネット サーバと通信できるようになります。

このウィンドウには、イントラネット用に設定されているサーバとポート番号のリストが表示されます。サーバの IP アドレスとポート番号を追加するには、［追加］ボタンを使用します。このリストの情報を変更するときは［編集］ボタンを、サーバの情報を削除するときは［削除］ボタンを使用します。

作成したリストは、クライアントのログイン時に表示されるポータルに表示されます。

サーバの追加 / 編集

このウィンドウでは、サーバ情報を追加または編集します。

サーバの IP アドレス

サーバの IP アドレスまたはホスト名を入力します。

サービスがリッスンするサーバ ポート

このサービスに対してサーバがリッスンするポートの番号を入力します。サービスの標準ポート番号（Telnet の場合はポート番号 23 など）、または Port-to-Application Mapping（PAM）が作成されている非標準ポート番号を指定できます。たとえば、サーバ上の Telnet ポート番号を 2323 に変更し、そのサーバ上のそのポート番号に PAM エントリを作成した場合は、このウィンドウに 2323 を入力します。

クライアント PC 上のポート

このフィールドには、Cisco CP によって 番号 3000 から始まる値が入力されます。エントリを追加するたびに、値が 1 ずつ増加します。このフィールドに入力されているエントリを使用します。

説明

エントリの説明を入力します。たとえば、ユーザがサーバに 10.10.11.2 で telnet 接続できるようにするエントリを追加する場合は、「Telnet to 10.10.11.2」と入力します。入力した説明はポータルに表示されます。

詳細

詳細な情報を表示する場合にこのリンクをクリックします。「ポート転送サーバについての理解を深める」をクリックすると、サーバに関する情報を表示できます。

フル トンネル

フル トンネル クライアントは、フル トンネル ソフトウェアをダウンロードして、ルータから IP アドレスを取得する必要があります。このウィンドウでは、フル トンネル クライアントがログオン時に取り出す IP アドレスが含まれている IP アドレス プールを設定し、フル トンネル インストール バンドルの場所を指定します。

（注） ソフトウェア インストール バンドルがインストールされていない場合は、このウィザード終了後にこのバンドルをインストールするための十分なメモリがルータのフラッシュになければなりません。

フル トンネルの有効化チェック ボックス

このチェック ボックスを選択すると、ルータがユーザの PC にフル トンネル クライアント ソフトウェアをダウンロードできるようになり、このウィンドウの他のフィールドが有効になります。

IP アドレス プール

フル トンネル クライアントが取り出す IP アドレスが含まれている IP アドレス プールを指定します。このフィールドに既存のプールの名前を入力したり、フィールドの右側にあるボタンをクリックして［既存の IP プールを選択］を選択し、プールのリストを参照して選択することができます。［新しいプールの作成］を選択して表示されるダイアログ ボックスに入力すれば、新しいプールを作成することもできます。選択または作成するアドレス プールには、企業イントラネットのアドレスが含まれている必要があります。

クライアント PC にインストールされているフル トンネル クライアント ソフトウェアの維持チェック ボックス

ログオフしても、クライアント PC 上にフル トンネル ソフトウェアを残しておく場合は、このチェック ボックスを選択します。このチェック ボックスを選択しない場合は、クライアントがゲートウェイと通信を確立するたびに、このソフトウェアをダウンロードします。

フル トンネル クライアントのインストール チェック ボックス

ここでフル トンネル クライアント ソフトウェアをインストールするときに、このチェック ボックスを選択します。クライアント ソフトウェアは、Cisco IOS SSL VPN の編集時にインストールすることもできます。

フル トンネル クライアント ソフトウェアは、クライアントがダウンロードしてフルトンネル接続を確立できるように、ルータにインストールされている必要があります。フル トンネル ソフトウェアが Cisco CP とともにインストールされた場合は、このソフトウェアへのパスが［場所］フィールドに自動的に表示されます。その一例を例 22-1 に示します。

例 22-1　ルータにインストールされるフル トンネル パッケージ

```
flash:sslclient-win-1.0.2.127.pkg
```

例 22-1 では、フル トンネル インストール バンドルはルータのフラッシュ メモリにロードされています。ルータのプライマリ デバイスがディスクまたはスロットの場合は、表示されるパスは *diskn* または *slotn* から始まります。

このフィールドが空白の場合は、インストール バンドルの場所を指定して Cisco CP がルータのプライマリ デバイスにインストール バンドルをロードできるようにするか、または、このウィンドウの下部にある最新版をダウンロードするリンクをクリックして、Cisco.com からソフトウェア インストール バンドルをダウンロードする必要があります。このリンクをクリックすると、次の Web ページにアクセスします。

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

（注）　Cisco ソフトウェア ダウンロード サイトからソフトウェアをダウンロードするには、CCO ユーザ名とパスワードが必要となる場合があります。これらのクレデンシャルを取得するには、いずれかの Cisco.com Web ページの上部の［ユーザ登録］をクリックして、必要な情報を入力してください。ユーザ ID とパスワードは電子メールで送信されてきます。

フル トンネル ソフトウェア インストール バンドルの検索方法と、Cisco CP で使用するバンドルへのパスの指定方法については、「Cisco CP 用のインストール バンドルの検索」を参照してください。

詳細ボタン

スプリット トンネリング、スプリット DNS、クライアントの Microsoft Internet Explorer の設定など、詳細オプションを設定するときにクリックします。

Cisco CP 用のインストール バンドルの検索

Cisco CP が Cisco IOS SSL VPN 設定で使用できるようにソフトウェア インストール バンドルの場所を検索するには、次の手順を使用します。あるいは、必要に応じて、ルータ上にこのソフトウェアをロードすることもできます。

（注）　Cisco ソフトウェア ダウンロード サイトからソフトウェアをダウンロードするには、CCO ユーザ名とパスワードが必要となる場合があります。これらのクレデンシャルを取得するには、いずれかの Cisco.com Web ページの上部の［ユーザ登録］をクリックして、必要な情報を入力してください。ユーザ ID とパスワードは電子メールで送信されてきます。

ステップ 1　［場所］フィールドを確認します。インストール　バンドルへのパスが［場所］フィールドに表示されているときは、これ以上何も行う必要はありません。Cisco CP により、その場所からソフトウェアをダウンロードするようルータが設定されます。例 22-2 は、ソフトウェア インストール バンドルへのパスを示しています。

例 22-2　ルータにインストールされるフル トンネル パッケージ

```
flash:sslclient-win-1.0.2.127.pkg
```

ステップ 2　［場所］フィールドが空白の場合は、このフィールドの右にある［...］ボタンをクリックして、ソフトウェアの場所を指定します。

ステップ 3　ルータにソフトウェアがインストールされている場合は、［ルータ ファイル システム］を選択して、そのファイルを検索します。

使用している PC にソフトウェアがインストールされている場合は、［マイ コンピュータ］を選択してそのファイルを検索します。

指定したルータ ファイル システムまたは PC パスが、［場所］フィールドに表示されます。

ステップ 4　ルータまたは使用している PC にソフトウェアがインストールされていない場合は、ソフトウェアを PC にダウンロードして、このフィールドにそのファイルへのパスを指定する必要があります。

a. ウィンドウの最新版をダウンロードするリンクをクリックします。必要なソフトウェアのダウンロード ページに接続されます。

b. 表示される Web ページでは、Cisco IOS プラットフォームおよびその他のプラットフォームで使用できるソフトウェア パッケージが提供されている場合があります。Cisco IOS プラットフォームにダウンロードするソフトウェアの最新バージョンをダブルクリックし、CCO のユーザ名とパスワードの入力を求められたら指定します。

c. PC にソフトウェア パッケージをダウンロードします。

d. Cisco IOS SSL VPN ウィザードで、［場所］フィールドの右にある［...］ボタンをクリックし、表示された場所を選択するウィンドウの［マイ コンピュータ］を選択して、ファイルをダウンロードしたディレクトリに移動します。

e. インストール　バンドル　ファイルを選択し、場所を選択するウィンドウの［OK］をクリックします。［場所］フィールドにそのパスが表示されます。次の例では、PC のデスクトップに置かれているインストール バンドル ファイルを示しています。

例 22-3　ルータにインストールされているフル トンネル パッケージ

```
C:\Documents and Settings\username\Desktop\sslclient-win-1.1.0.154.pkg
```

［完了］をクリックすると、この設定をルータに配信したときに、指定した PC のディレクトリからルータ上にソフトウェアがインストールされます。

Cisco Secure Desktop の有効化

ユーザが Cisco IOS SSL VPN にログオンすると、ルータはユーザの PC 上に Cisco Secure Desktop をインストールできます。Web トランザクションでは、ユーザのログアウト後も、cookie、ブラウザの履歴ファイル、電子メールの添付ファイル、およびその他のファイルが PC 上にそのまま残ることがあります。Cisco Secure Desktop は、デスクトップ上に安全なパーティションを作成し、セッション終了後に米国国防総省のアルゴリズムを使用してファイルを削除します。

Cisco Secure Desktop のインストール

クライアントは、ルータから Cisco Secure Desktop ソフトウェア インストール バンドルをダウンロードする必要があります。このソフトウェアが Cisco CP とともにインストールされた場合は、例 22-4 に示すように、このソフトウェアへのパスが［場所］フィールドに自動的に表示されます。

例 22-4　ルータにインストールされている Cisco Secure Desktop パッケージ

```
flash:/securedesktop-ios-3.1.0.29-k9.pkg
```

例 22-4 では、Cisco Secure Desktop インストール バンドルはルータのフラッシュ メモリにロードされています。ルータのプライマリ デバイスがディスクまたはスロットの場合は、表示されるパスは `diskn` または `slotn` から始まります。

このフィールドが空白の場合は、インストール バンドルの場所を指定して Cisco CP がルータのプライマリ デバイスにインストール バンドルをロードできるようにするか、または、このウィンドウの下部にある最新版をダウンロードするリンクをクリックして、Cisco.com からソフトウェア インストール バンドルをダウンロードする必要があります。このリンクをクリックすると、次の Web ページにアクセスします。

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

（注） Cisco ソフトウェア ダウンロード サイトからソフトウェアをダウンロードするには、CCO ユーザ名とパスワードが必要となる場合があります。これらのクレデンシャルを取得するには、いずれかの Cisco.com Web ページの上部の［ユーザ登録］をクリックして、必要な情報を入力してください。ユーザ ID とパスワードは電子メールで送信されてきます。

Cisco Secure Desktop ソフトウェア インストール バンドルの検索方法と、Cisco CP で使用するバンドルへのパスの指定方法については、「Cisco CP 用のインストール バンドルの検索」を参照してください。

Common Internet File System

Common Internet File System（CIFS）を使用すると、クライアントは Web ブラウザ インターフェイスを使用して、Microsoft Windows ベースのファイル サーバ上のファイルをリモートで参照、アクセス、および作成することができます。

WINS サーバ

Microsoft Windows Internet Naming Service（WINS）サーバでは、クライアント IP アドレスを、対応する NetBIOS 名にマップするデータベースを保持しています。使用しているネットワークの WINS サーバの IP アドレスをこのボックスに入力します。複数のアドレスはセミコロン（;）で区切ります。

たとえば、IP アドレス 10.0.0.18 と 10.10.10.2 を入力するときは、このボックスに 10.0.0.18;10.10.10.2 と入力します。

権限

ユーザに許可する権限を指定します。

クライアントレス Citrix を有効にする

クライアントレス Citrix を使用すると、ユーザは、PC 上にクライアント ソフトウェアをインストールする必要なしに、リモート サーバ上の Microsoft Word、Excel などのアプリケーションを、ローカルで実行するときと同じように実行できます。ルータがアクセスできるネットワーク上の 1 つ以上のサーバに Citrix ソフトウェアをインストールしておく必要があります。

Citrix サーバ

新しいリストを作成するときは、［追加］をクリックして、表示されるダイアログに必要な情報を入力します。このテーブル内の URL リストを変更するときは［編集］キーを、削除するときは［削除］キーを使用します。

要約

このウィンドウには、作成した Cisco IOS SSL VPN 設定の要約が表示されます。ルータに設定を配信するときは［完了］をクリックし、ウィザード ウィンドウに戻って変更を行うときは［戻る］をクリックします。

SSL VPN 接続の編集

SSL VPN 接続を編集するには、次のタスクを実行します。

ステップ 1　Cisco CP 機能バーで、［設定］>［セキュリティ］>［VPN］の順にクリックします。

ステップ 2　［VPN］ツリーで、［SSL VPN］>［SSL VPN マネージャ］の順に選択します。

ステップ 3　［SSL VPN の編集］をクリックします。

ステップ 4　編集する SSL VPN 接続を選択します。

ステップ 5　［編集］をクリックします。次に、表示されたダイアログで設定を変更します。

ステップ 6　［OK］をクリックしてこのダイアログ　ボックスを閉じ、変更をルータに送信します。

「SSL VPN 接続の編集のリファレンス」で、設定画面について説明します。

SSL VPN 接続の編集のリファレンス

この章の各トピックでは、SSL VPN の編集画面について説明します。

- SSL VPN の編集
- SSL VPN コンテキスト
- 内部および外部インターフェイスの指定
- ゲートウェイの選択
- コンテキスト：グループ ポリシー
- グループ ポリシー：全般タブ
- グループ ポリシー：クライアントレス タブ
- グループ ポリシー：シン クライアント タブ
- グループ ポリシー：SSL VPN クライアント（フル トンネル）タブ
- 詳細トンネル オプション
- DNS および WINS サーバ
- コンテキスト：HTML 設定
- 色の選択
- コンテキスト：NetBIOS 名サーバ リスト
- NBNS サーバ リストの追加 / 編集
- NBNS サーバの追加 / 編集
- コンテキスト：ポート転送リスト
- ポート転送リストの追加 / 編集
- コンテキスト：URL リスト
- URL リストの追加 / 編集
- コンテキスト：Cisco Secure Desktop
- SSL VPN ゲートウェイ
- SSL VPN ゲートウェイの追加 / 編集
- パッケージ
- インストール パッケージ

SSL VPN の編集

［SSL VPN の編集］ウィンドウでは、Cisco IOS SSL VPN 設定を変更または作成できます。タブの上部に、設定されている Cisco IOS SSL VPN コンテキストのリストが表示されています。下部には、そのコンテキストの詳細が表示されています。

Cisco CP でサポートする Cisco IOS SSL VPN 機能の概要については、「Cisco IOS SSL VPN」を参照してください。

Cisco IOS SSL VPN ドキュメントへのリンクについては、「Cisco.com の Cisco IOS SSL VPN リンク」を参照してください。

Cisco IOS SSL VPN 設定コンポーネントが連携して動作する方法については、「Cisco IOS SSL VPN コンテキスト、ゲートウェイ、およびポリシー」を参照してください。

SSL VPN コンテキスト

このエリアには、ルータに設定されている Cisco IOS SSL VPN コンテキストが表示されます。このエリアのコンテキストをクリックすると、ウィンドウの下部にそのコンテキストの詳細情報が表示されます。新しいコンテキストを追加するときは、［追加］をクリックして、表示されるダイアログ ボックスに情報を入力します。コンテキストを編集するときは、コンテキストを選択し、［編集］をクリックします。コンテキストとそれが関連付けられているグループ ポリシーを削除するときは、コンテキストを選択して［削除］をクリックします。

サービスを停止しているコンテキストを有効にするときは、そのコンテキストを選択して［有効］をクリックします。コンテキストのサービスを停止するときは、そのコンテキストを選択して［無効］をクリックします。

各コンテキストには、次の情報が表示されます。

名前

Cisco IOS SSL VPN コンテキストの名前です。Cisco IOS SSL VPN ウィザードでコンテキストを作成した場合、コンテキスト名は［IP アドレスおよび名前］ウィンドウに入力した文字列になります。

ゲートウェイ

コンテキストで使用されるゲートウェイには、Cisco IOS SSL VPN コンテキストが使用する IP アドレスとデジタル証明書が含まれています。

ドメイン

コンテキストでドメインが設定されているときは、そのドメインがこのカラムに表示されます。ドメインが設定されている場合、ユーザはポータルにアクセスするために Web ブラウザにそのドメインを入力する必要があります。

ステータス

すばやくステータスを識別するためのアイコンが含まれています。

管理ステータス

ステータスの説明文です。

- サービス提供中 — コンテキストはサービスを提供しています。コンテキストで設定されているポリシーに指定されているユーザは、その Cisco IOS SSL VPN ポータルにアクセスできます。
- サービス停止中 — コンテキストはサービスを停止しています。コンテキストで設定されているポリシーに指定されているユーザは、その Cisco IOS SSL VPN ポータルにアクセスできません。

サンプル表示

次の表は、サンプルの Cisco IOS SSL VPN コンテキスト表示を示しています。

名前	ゲートウェイ	ドメイン	ステータス	管理ステータス
WorldTravel	Gateway1	wtravel.net		サービス提供中
A+Insurance	Gateway2	aplus.com		サービス停止中

SSL VPN コンテキストの詳細：*名前*

このエリアには、ウィンドウの上部で選択した、名前 < *名前* > を持つコンテキストの詳細が表示されます。ウィンドウの上部の［編集］をクリックすると、表示されている設定を変更できます。

SSL VPN コンテキスト

このウィンドウでは、Cisco IOS SSL VPN コンテキストを追加または編集します。

フィールドのリファレンス

表 22-1　SSL VPN コンテキストのフィールド

項目	説明
名前	新しいコンテキストの名前を入力するか、既存のコンテキストの名前を選択してそれを編集します。
関連付けられたゲートウェイ	既存のゲートウェイを選択するか、または［ゲートウェイの作成］をクリックして、そのコンテキスト用の新しいゲートウェイを作成します。ゲートウェイには、このコンテキストで使用される IP アドレスとデジタル証明書が含まれています。各ゲートウェイには一意のパブリック IP アドレスが必要です。
ドメイン	このコンテキスト用のドメインがある場合、このフィールドに入力します。Cisco IOS SSL VPN ユーザは、ポータルにアクセスするときに、IP アドレスの代わりにこのドメイン名を使用することができます。mycompany.com がその一例です。
認証リスト	このコンテキストに対するユーザの認証に使用する AAA 方式リストを選択します。
認証ドメイン	認証のために送信される前に、ユーザ名に追加するドメイン名を入力します。このドメインは、このコンテキストに対してユーザを認証するための AAA サーバ上で使用されるドメインと一致していなければなりません。

表 22-1　SSL VPN コンテキストのフィールド（続き）

項目	説明
コンテキストの有効化	設定したコンテキストを有効にする場合は、［コンテキストの有効化］チェック ボックスを選択します。ここでコンテキストを有効にした場合、コンテキストを無効にするときに、このウィンドウに戻る必要はありません。［SSL VPN の編集］タブで、個々のコンテキストの有効化と無効化の切り替えを行うことができます。
最大ユーザ数	一度にこのコンテキストの使用を許可する最大ユーザ数を入力します。
VRF 名	このコンテキストの VPN ルーティング / 転送（VRF）名を入力します。この VRF 名は、ルータで設定しておく必要があります。
デフォルトの グループ ポリシー	デフォルトのグループ ポリシーとして使用するポリシーを選択します。AAA サーバに設定されているポリシーに含まれていないユーザに対して、デフォルトのグループ ポリシーが使用されます。
RADIUS アカウンティングの 有効化	編集しているコンテキストで RADIUS アカウンティングの機能を有効にするには、［RADIUS アカウンティングの有効化］チェック ボックスを選択します。このチェック ボックスを選択していない場合は、コンテキストに対して選択した AAA 認証リストに、設定済みの AAA サーバは含まれません。別の認証リストを選択するか、新規の認証リストを設定する必要があります。 ルータ設定に AAA の情報を追加するには、［VPN コンポーネント］>［AAA］>［AAA サーバ］>［追加］の順にクリックします。表示されたダイアログ ボックスに、IP アドレスなどの必要な情報を入力します。これで、入力した AAA サーバ情報が認証リストで使用できるようになります。

内部および外部インターフェイスの指定

Cisco IOS SSL VPN 接続が設定されているインターフェイスに ACL が適用されていると、SSL トラフィックがブロックされることがあります。このトラフィックがファイアウォールを通過できるように、Cisco CP では自動的に ACL を変更することができます。ただし、Cisco CP に対して、どのインターフェイスが内部（信頼できる）インターフェイスであり、どのインターフェイスが外部（信頼で

きない）インターフェイスであるかを指定して、適切なトラフィックにファイアウォールの通過を許可するアクセス コントロール エントリ（ACE）を作成する必要があります。

表示されているインターフェイスが信頼できるインターフェイスである場合は［内部］チェック ボックスを選択し、信頼できないインターフェイスである場合は［外部］チェック ボックスを選択します。

ゲートウェイの選択

このウィンドウから既存のゲートウェイを選択します。このウィンドウでは、ゲートウェイを選択するときに必要な情報が提供されます。このウィンドウには、すべてのゲートウェイの名前と IP アドレス、各ゲートウェイが関連付けられているコンテキスト数、およびゲートウェイが有効になっているかどうかが表示されます。

コンテキスト：グループ ポリシー

このウィンドウには、選択した Cisco IOS SSL VPN コンテキストに対して設定されているグループ ポリシーが表示されます。グループ ポリシーを管理するには、［追加］、［編集］、および［削除］ボタンを使用します。

このウィンドウには、各ポリシーのポリシー名と、そのポリシーがデフォルトのグループ ポリシーであるかどうかが表示されます。デフォルトのグループ ポリシーは、他のポリシーに含まれていないユーザに割り当てられるポリシーです。［コンテキスト］ウィンドウに戻り、別のポリシーをデフォルトとして選択すれば、グループ ポリシーを変更できます。

リスト内のポリシーをクリックすると、ウィンドウの下部にそのポリシーの詳細が表示されます。これらの詳細情報の説明については、以下のリンクをクリックしてください。

グループ ポリシー：全般タブ

グループ ポリシー：クライアントレス タブ

グループ ポリシー：シン クライアント タブ

グループ ポリシー：SSL VPN クライアント（フル トンネル）タブ

詳細についてはここをクリック

重要な情報については、ウィンドウ内のこのリンクをクリックしてください。このヘルプ ページからグループ ポリシーの情報を表示するときは、「グループ ポリシーについての理解を深める」をクリックします。

グループ ポリシー：全般タブ

新しいグループ ポリシーを作成する場合、［全般］タブの各フィールドに情報を入力します。

フィールドのリファレンス

表 22-2　［全般］タブのフィールド

項目	説明
名前	グループ ポリシーの名前を入力します（たとえば、Engineering、Human Resources、Marketing など）。
これをコンテキストのデフォルトのグループ ポリシーにします	このグループ ポリシーをデフォルトのグループ ポリシーにする場合に選択します。デフォルトのグループ ポリシーは、他のポリシーに含まれていないユーザに割り当てられるポリシーです。このチェック ボックスを選択すると、このポリシーが［グループ ポリシー］ウィンドウのデフォルトのポリシーとして表示されます。
タイムアウト	
アイドル タイムアウト	クライアントがアイドル状態になってからセッションが終了するまでの秒数を入力します。
セッション タイムアウト	セッションのアクティビティに関係なく、セッションの最大秒数を入力します。

表 22-2　［全般］タブのフィールド（続き）

項目	説明
アプリケーション ACL	
アプリケーション ACL	SSLVPN では、アプリケーション ACL を使用して、グループで許可する URL および拒否する URL を指定します。このグループ向けに設定済みのアプリケーション ACL を選択します。 アプリケーション ACL を設定するには、SSL VPN コンテキストのツリーに移動し、［アプリケーション ACL］をクリックして、［アクセス コントロール リスト］ウィンドウを表示します。次に、［追加］をクリックします。
表示	選択したアプリケーション ACL の詳細を表示するには、［表示］をクリックします。

グループ ポリシー：クライアントレス タブ

クライアントレス Citrix を使用すると、ユーザは、アプリケーションを使用してリモート システムにクライアント ソフトウェアをインストールする必要なしに、リモート サーバ上のアプリケーションを、ローカルで実行するときと同じように実行できます。ルータがアクセスできるネットワーク上の 1 つ以上のサーバに Citrix ソフトウェアをインストールしておく必要があります。

Cisco IOS SSL VPN クライアントでクライアントレス Citrix を使用できるようにする場合に、情報を入力します。

フィールドのリファレンス

表 22-3　［クライアントレス］タブのフィールド

項目	説明
クライアントレス Web 参照	
アクション URL リスト	このグループのユーザに表示されるポータルに表示する 1 つ以上の URL リストを選択します。指定したリスト内の URL がポータルに表示されます。

表 22-3　［クライアントレス］タブのフィールド（続き）

項目	説明
表示	URL リストを確認する場合は、リストから名前を選択して［表示］をクリックします。
追加	URL リストまたは Citrix サーバ リストを追加するには、［追加］をクリックして、必要なオプションを選択します。
ポータル ページの URL バー非表示	ユーザのアクセスをリスト内の URL に制限する場合、およびユーザが他の URL を入力できないようにする場合は、［ポータル ページの URL バー非表示］をクリックします。
URL の難読化	グループ ポリシーで URL の難読化の機能を有効にするには、［URL の難読化］をクリックします。URL の難読化を有効にすると、Web サーバや Web ページ内のその他の内部リソースへのパスが、それらを使用しているエンド ユーザには表示されなくなります。代わりに、ネットワークに関する情報を把握できない難読化されたパスが表示されます。
Citrix の有効化	グループ ポリシーでクライアントレス Citrix を有効にするには、［Citrix の有効化］をクリックします。Citrix を使用すると、ユーザは、PC 上にクライアント ソフトウェアをインストールする必要なしに、リモート サーバ上の Microsoft Word、Excel などのアプリケーションを、ローカルで実行するときと同じように実行できます。ルータがアクセスできるネットワーク上の 1 つ以上のサーバに Citrix ソフトウェアをインストールしておく必要があります。
CIFS の有効化	
企業ネットワーク内の MS Windows サーバにあるファイルをグループ メンバが閲覧できるようにする場合は、［CIFS の有効化］を選択します。CIFS を有効にすると、以下のオプションが有効になります。	
読み取り	グループ メンバにファイルの読み取りを許可するときは、［読み取り］をクリックします。
書き込み	グループ メンバにファイルの変更を許可するときは、［書き込み］をクリックします。

表 22-3　［クライアントレス］タブのフィールド（続き）

項目	説明
NBNS サーバ リスト	対象とするユーザに適切なファイルを表示できるようにする NBNS サーバ リストを指定する必要があります。このグループに使用する NBNS サーバ リストを選択します。リストを設定するには、SSL VPN コンテキスト ツリーで［NetBIOS 名サーバ リスト］をクリックし、［追加］をクリックしてリストを設定します。
表示	WINS サーバ リストの内容を確認するには、そのリストを選択して［表示］をクリックします。

グループ ポリシー：シン クライアント タブ

このグループのメンバに対してシン クライアント（ポート転送とも呼ばれる）を設定する場合に、このタブで設定を行います。

フィールドのリファレンス

表 22-4　［シン クライアント］タブのフィールド

項目	説明
シン クライアントの有効化	［シン クライアントの有効化（ポート転送）］をクリックし、ポート転送リストを指定してこの機能を有効にします。このグループ ポリシーを設定した Cisco IOS SSL VPN コンテキストに対して、少なくとも 1 つのポート転送リストを設定する必要があります。
表示	選択したポート転送リストを確認するときは、［表示］をクリックします。
アプレットの自動ダウンロード	［アプレットの自動ダウンロード］オプションを使用すると、クライアントがログオンしたときに、シン クライアント アプレットが自動的にクライアントにダウンロードされます。このオプションはデフォルトで選択されています。

グループ ポリシー：SSL VPN クライアント（フル トンネル）タブ

グループ メンバがフルトンネル クライアント ソフトウェアをダウンロードして使用できるようにする場合に、このタブで設定を行います。

（注）　［SSL VPN］ツリーの［パッケージ］をクリックし、インストール バンドルの場所を指定してから、［インストール］をクリックして、フル トンネル クライアント ソフトウェアの場所を指定する必要があります。

リストから［有効］をクリックして、フル トンネル接続を有効にします。フル トンネル接続を必要とする場合は、［必須］をクリックします。［必須］を選択すると、Cisco IOS SSL VPN クライアント ソフトウェアがクライアント PC に正常にインストールされているときだけ、クライアントレス通信とシン クライアント通信が動作します。

クライアントが IP アドレスを割り当てられる IP アドレス プール

フル トンネル接続を確立するクライアントは、ルータから IP アドレスを割り当てられます。プールの名前を指定するか、または［...］ボタンをクリックして、ルータが割り当てることができる IP アドレスが格納される新しいプールを作成します。

クライアント PC にインストールされているフル トンネル クライアント ソフトウェアの維持チェック ボックス

ログオフしても、クライアント PC 上にフル トンネル ソフトウェアを残しておく場合は、このチェック ボックスを選択します。このチェック ボックスを選択しない場合は、クライアントがゲートウェイと通信を確立するたびに、このソフトウェアをダウンロードします。

再ネゴシエート キー フィールド

トンネルが停止してから、新しい SSL キーをネゴシエートしてトンネルが再確立できるようになるまでの秒数を入力します。

このグループのユーザによる企業リソースへのアクセスを制限する ACL

企業ネットワーク上で、グループ メンバが利用できるリソースを指定するアクセス リスト（ACL）を選択または作成できます。

フルトンネル ソフトウェアがインストールされた状態で Web ブラウザを開くと、ホーム ページ クライアントが表示されます

このグループのフル トンネル クライアントに表示されるホームページの URL を入力します。

デッド ピア検知タイムアウト

デッド ピア検知（DPD）を使用すると、応答していないピアを検出できます。ルータが検出の際に使用するタイムアウトを、応答していないクライアントと応答していないサーバについて別々に設定できます。いずれのタイムアウト範囲も 0 ～ 3,600 秒です。

DNS および WINS サーバの設定ボタン

クリックすると、［DNS および WINS サーバ］ダイアログが表示され、クライアントがイントラネットのホストとサービスにアクセスするときに使用する、企業イントラネット上の DNS サーバと WINS サーバの IP アドレスを指定できます。

詳細トンネル オプションの設定ボタン

クリックすると、［詳細トンネル オプション］ダイアログが表示され、スプリット トンネリングのトンネル設定、スプリット DNS、およびクライアントのプロキシ サーバ設定を Microsoft Internet Explorer を使用して行うことができます。

詳細トンネル オプション

このダイアログ ボックスでは、暗号化されたトラフィックの制御、企業イントラネット上の DNS サーバの指定、およびクライアントのブラウザに送信されるプロキシ サーバ設定を行うことができます。

スプリット トンネリング

すべてのトンネルのトラフィックを暗号化すると、大量のシステムのリソースを消費してしまうことがあります。スプリット トンネリングを使用すると、トラフィックを暗号化するネットワークを指定して、それ以外のネットワーク宛てのトラフィックは暗号化しないようにすることができます。暗号化するトンネル トラフィックを指定することも、暗号化*しない*トラフィックを指定して、それ以外のトンネル トラフィックをすべてルータで暗号化するように指定することもできます。作成できるリストは 1 つのみで、そのリストに含まれるトラフィックと除外されるトラフィックは相互排他になります。

［トラフィックを含む］をクリックし、［追加］、［編集］、および［削除］キーを使用して、トラフィックを暗号化する宛先ネットワークのリストを作成します。あるいは、［トラフィックを含まない］をクリックして、トラフィックを暗号化*しない*宛先ネットワークのリストを作成します。

ルータが接続されている LAN に送信される暗号化クライアント トラフィックから明示的に除外するときは、［ローカル LAN を含まない］をクリックします。ルータが接続されている LAN にネットワーク プリンタが接続されている場合は、このオプションを使用する必要があります。

「スプリット トンネリングについての理解を深める」には、このトピックに関する詳細情報があります。

スプリット DNS

Cisco IOS SSL VPN クライアントが特定のドメインを解決するときにだけ企業ネットワークの DNS サーバを使用する場合は、このエリアにそのドメインを入力できます。入力するドメインは、企業イントラネット内のドメインでなければなりません。各エントリはセミコロンで区切り、キャリッジ リターンは使用しないでください。エントリのサンプル リストを示します。

yourcompany.com;dev-lab.net;extranet.net

それ以外のすべてのドメインを解決するときは、クライアントは自分の ISP から提供されている DNS サーバを使用する必要があります。

ブラウザ プロキシ設定

このエリアの設定は、フル トンネル接続が設定されているクライアントの Microsoft Internet Explorer ブラウザに送信されます。クライアントで別のブラウザを使用している場合は、これらの設定は使用されません。

プロキシ サーバを使用しない

Cisco IOS SSL VPN クライアント ブラウザにプロキシ サーバを使用しないよう指示する場合にクリックします。

プロキシ設定の自動検出

Cisco IOS SSL VPN クライアント ブラウザにプロキシ サーバ設定を自動検出するよう指示する場合にクリックします。

ローカル アドレスのプロキシ設定をバイパスする

ローカル アドレスに接続しているクライアントが通常のプロキシ設定をバイパスできるようにする場合にクリックします。

プロキシ サーバ

プロキシ サーバの IP アドレスと、プロキシ サーバが提供するサービスで使用するポート番号を、これらのフィールドに入力します。たとえば、プロキシ サーバが FTP 要求をサポートしている場合は、プロキシ サーバの IP アドレスとポート番号 21 を入力します。

次のアドレスで始まるプロキシ サーバを使用しない

特定の IP アドレスまたはネットワークにトラフィックを送信する際に、クライアントでプロキシ サーバを使用しないようにする場合は、その IP アドレスまたはネットワークをここに入力します。各エントリはセミコロンを使用して区切ります。たとえば、10.10.0.0 または 10.11.0.0 ネットワークのサーバに接続するときに、クライアントでプロキシ サーバを使用しないようにする場合は、「10.10;10.11」と入力します。ネットワークはいくつでも入力できます。

DNS および WINS サーバ

企業ネットワークの DNS サーバおよび WINS サーバの、Cisco IOS SSL VPN クライアントに送信する IP アドレスを入力します。Cisco IOS SSL VPN クライアントはこれらのサーバを使用して、企業イントラネット上のホストとサービスにアクセスします。

プライマリとセカンダリ両方の DNS サーバおよび WINS サーバの IP アドレスを指定します。

DNS および WINS サーバ

企業ネットワークの DNS サーバおよび WINS サーバの、Cisco IOS SSL VPN クライアントに送信する IP アドレスを入力します。Cisco IOS SSL VPN クライアントはこれらのサーバを使用して、企業イントラネット上のホストとサービスにアクセスします。

プライマリとセカンダリ両方の DNS サーバおよび WINS サーバの IP アドレスを指定します。

コンテキスト：HTML 設定

このウィンドウで行う設定によって、選択した Cisco IOS SSL VPN コンテキストのポータルの外観が制御されます。

テーマの選択

ポータルで使用する色を 1 つずつ自分で選択する代わりに、あらかじめ定義されているテーマを選択してポータル ページの外観を指定できます。テーマを選択すると、そのテーマの設定が［カスタマイズ］ボタンに関連付けられているフィールドに表示されます。

カスタマイズ ボタン

ポータルで使用する色を 1 つずつ選択したり、ログイン メッセージとタイトルを指定する場合にクリックします。あらかじめ定義されているテーマを選択した場合は、そのテーマの値がこのセクションの各フィールドに表示されます。これ

らの値は変更可能であり、入力する値は選択されているコンテキストのポータルで使用されます。このウィンドウで行った変更は、作成しているポータルだけに反映されます。テーマのデフォルト値は変更されません。

ログイン メッセージ

ブラウザにポータルが表示されるときにクライアントに表示するログイン メッセージを入力します。例：

```
Welcome to the company-name network. Log off if you are not an
authorized user.
```

タイトル

ポータルに付けるタイトルを入力します。例：

```
Company-name network login page
```

タイトルの背景色

タイトルの背後に表示される背景色のデフォルト値は #9999CC です。この値を変更するには、[...] ボタンをクリックして別の色を選択します。

二次タイトルの背景色

二次タイトルの背後に表示される背景色のデフォルト値は #9729CC です。この値を変更するには、[...] ボタンをクリックして別の色を選択するか、別の色の 16 進数値を入力します。

テキストの色

テキストの色のデフォルト値は白です。この色を変更するには、下矢印をクリックして別の色を選択します。

テキストの二次色

テキストの二次色のデフォルト値は黒です。この色を変更するには、下矢印をクリックして別の色を選択します。

ロゴ ファイル

ポータルにロゴを表示する場合は、[...] ボタンをクリックして、PC 上に保存されているロゴ ファイルを参照します。[OK] をクリックすると、ロゴ ファイルはルータのフラッシュ メモリに保存され、ロゴがポータルの左上隅に表示されます。

プレビュー ボタン

定義済みのテーマを選択したポータルや、カスタム値を設定したポータルのプレビューを表示する場合にクリックします。

色の選択

定義済みの色を選択するときは [基本] をクリックし、カスタムの色を作成するときは [RGB] をクリックします。

基本

左側のパレットから使用する色を選択します。選択した色は、ダイアログ ボックスの右側の大きな四角形の中に表示されます。

RGB

赤、緑、青のスライダを組み合わせて使用し、カスタムの色を作成します。作成した色は、ダイアログ ボックスの右側の大きな四角形の中に表示されます。

コンテキスト：NetBIOS 名サーバ リスト

選択した Cisco IOS SSL VPN コンテキストに設定されているすべての NetBIOS 名サーバ リストがこのウィンドウに表示されます。CIFS は NetBIOS サーバを使用して、企業の Microsoft Windows ファイルシステムを Cisco IOS SSL VPN ユーザに表示します。

SSL VPN コンテキストに設定されている各 NetBIOS 名サーバ リストは、［NetBIOS 名サーバ リスト］エリアに表示されます。これらのリストを管理するには、［追加］、［編集］、および［削除］ボタンをクリックします。リスト名をクリックすると、リストの内容が［NetBIOS 名サーバの詳細］エリアに表示されます。

NBNS サーバ リストの追加 / 編集

このウィンドウでは、NBNS サーバ リストを作成または管理します。作成する各リストの名前を入力し、リスト内の各サーバの IP アドレス、タイムアウト、および再試行回数を指定します。各リストの 1 つのサーバをマスター サーバとして指定します。

リスト内の各サーバは、そのマスターのステータス、タイムアウト、および再試行値とともにこのダイアログ ボックスに表示されます。

NBNS サーバの追加 / 編集

各サーバの IP アドレス、ルータがサーバに再接続を試みるまで待機する秒数、およびルータがサーバに接続を試みる回数を入力します。

このサーバをリストの中でルータが最初に接続するサーバにする場合は、［これをマスタ サーバにします。］チェック ボックスを選択します。

コンテキスト：ポート転送リスト

このウィンドウでは、選択したコンテキストのポート転送リストを設定します。リストは、選択したコンテキストで設定されている任意のグループ ポリシーに関連付けることができます。ポート転送リストは、Cisco IOS SSL VPN クライアントに TCP アプリケーション サービスを示します。

ウィンドウの上部に、選択したコンテキストに設定されているポート転送リストが表示されます。リスト名をクリックすると、ウィンドウの下部にそのリストの詳細が表示されます。

このウィンドウには、IP アドレス、使用されるポート番号、クライアントで対応しているポート番号、および説明（入力されている場合）が表示されます。

ポート転送リストの追加 / 編集

このウィンドウでは、ポート転送リストを作成および管理します。各リストには名前を指定し、少なくとも 1 つのサーバのエントリが含まれている必要があります。このリストのエントリを作成、変更、または削除するには、［追加］、［編集］、または［削除］ボタンを使用します。

コンテキスト：URL リスト

URL リストでは、特定のグループのユーザに対してポータルに表示するリンクを指定します。コンテキストごとに 1 つ以上の URL リストを設定し、グループ ポリシー ウィンドウを使用してそれらのリストを特定のグループ ポリシーに関連付けます。

ウィンドウの上部に、そのコンテキストに設定されているすべての URL リストが表示されます。ウィンドウの下部には、選択したリストの内容が表示されます。リストごとに、URL リストの一番上に表示される見出しと、そのリストに含まれている各 URL が表示されます。

URL リストを作成および管理するには、［追加］、［編集］、または［削除］ボタンを使用します。

URL リストの追加 / 編集

各 URL リストの名前、URL リストの一番上に表示される見出し文を入力します。

見出し文は、リストに含まれているリンクの全体的な内容を説明するものでなければなりません。たとえば、URL リストが健康保険の Web ページと保険金の Web ページへのアクセスを提供している場合は、給付金という見出し文を使用します。

新しいエントリをリストに作成するときは［追加］ボタンを使用し、リストを管理するときは［編集］と［削除］ボタンを使用します。追加した各エントリはリスト エリアに表示されます。

コンテキスト：Cisco Secure Desktop

Cisco Secure Desktop は、暗号化しないとセキュリティ問題が発生する可能性のある cookie、ブラウザの履歴ファイル、一時ファイル、および電子メールの添付ファイルを暗号化します。Cisco IOS SSL VPN セッションが終了すると、Cisco Secure Desktop は米国国防総省のデータ消去アルゴリズムを使用してデータを削除します。

このコンテキストのユーザ全員に Cisco Secure Desktop のダウンロードと使用を許可するときは、［Cisco Secure Desktop の有効化］をクリックします。このソフトウェアのインストール バンドルがルータで見つからない場合、このウィンドウにメッセージが表示されます。

Cisco Secure Desktop のインストール バンドルをルータにロードするには、［Cisco IOS SSL VPN］ツリーの［パッケージ］をクリックして、ウィンドウに表示される指示に従って操作します。

SSL VPN ゲートウェイ

このウィンドウには、ルータに設定されている Cisco IOS SSL VPN ゲートウェイが表示されます。既存のゲートウェイの変更と新しいゲートウェイの設定を、このウィンドウで行うことができます。Cisco IOS SSL VPN ゲートウェイは、安全なネットワークへのユーザの入口です。

SSL VPN ゲートウェイ

このエリアには、ルータに設定されている Cisco IOS SSL VPN ゲートウェイのリストが表示されます。ゲートウェイの名前と IP アドレス、ゲートウェイを使用するよう設定されているコンテキストの数、およびゲートウェイのステータスが表示されます。


ゲートウェイは有効で、サービスを提供しています。


ゲートウェイは無効で、サービスを提供していません。

ゲートウェイをクリックすると、ウィンドウの下部にそのゲートウェイに関する詳細が表示されます。無効化されているゲートウェイを有効にするときは、そのゲートウェイを選択して［有効］をクリックします。有効化されているゲートウェイのサービスを停止するときは、そのゲートウェイを選択して［無効］をクリックします。ゲートウェイを編集するときは、そのゲートウェイを選択して［編集］ボタンをクリックします。ゲートウェイを削除するときは、そのゲートウェイを選択して［削除］ボタンをクリックします。

SSL VPN ゲートウェイの詳細

このエリアには、ウィンドウの上部で選択したゲートウェイに関する設定の詳細と、このゲートウェイで使用するよう設定されている Cisco IOS SSL VPN コンテキストの名前が表示されます。

ゲートウェイの設定の詳細については、「SSL VPN ゲートウェイの追加 / 編集」を参照してください。コンテキストの詳細については、「SSL VPN コンテキスト」を参照してください。

SSL VPN ゲートウェイの追加 / 編集

このウィンドウでは、Cisco IOS SSL VPN ゲートウェイを作成または編集します。

ゲートウェイ名

ゲートウェイ名は、ルータ上でこのゲートウェイを一意に識別し、Cisco IOS SSL VPN コンテキスト設定時にゲートウェイの参照に使用される名前です。

IP アドレス

ゲートウェイが使用する IP アドレスを選択または入力します。これはパブリック IP アドレスでなければならず、ルータ上のほかのゲートウェイが使用しているアドレスは指定できません。

デジタル証明書

SSL 認証のために Cisco IOS SSL VPN クライアントに送信される証明書を選択します。

HTTP リダイレクト チェック ボックス

HTTP リダイレクトを使用しない場合は、選択を解除します。HTTP リダイレクトは自動的に HTTP リクエストを、安全な Cisco IOS SSL VPN 通信に使用されるポート 443 にリダイレクトします。

ゲートウェイを有効にするチェック ボックス

ゲートウェイを有効にしない場合は、選択を解除します。ゲートウェイの有効化と無効化の切り替えは、［SSL VPN ゲートウェイ］ウィンドウから行うこともできます。

パッケージ

このウィンドウでは、Cisco IOS SSL VPN 機能をサポートするために Cisco IOS SSL VPN クライアントにダウンロードする必要があるソフトウェア インストール バンドルを取得し、それをルータにロードすることができます。また、このウィンドウを使用して、インストールされているインストール バンドルを削除することもできます。

このウィンドウに表示される手順に従って、Cisco.com から PC にインストール バンドルをダウンロードし、PC からルータにそのバンドルをコピーします。いずれかのインストール バンドルを取得する必要がある場合は、ダウンロード サイトへのリンクをクリックして、手順 1 から開始してください。

（注） ダウンロード サイトにアクセスするには、CCO のユーザ名とパスワードが必要です。CCO ユーザ名とパスワードがない場合は、いずれかの Cisco.com Web ページの上部の［ユーザ登録］をクリックして、表示されるフォームに入力すれば取得できます。ユーザ名とパスワードは電子メールで送信されてきます。

すでにインストール バンドルが PC またはルータ上にロードされている場合は、手順 2 と 3 を実行し、インストール バンドルの現在の保存場所を指定して、ルータのフラッシュ メモリにコピーします。

インストール バンドルの現在の保存場所を指定するときは、各セクションで［...］ボタンをクリックします。

インストール バンドルの現在の保存場所と、そのバンドルのコピー先となるルータのフラッシュ メモリのコピー場所を指定したら、［インストール］をクリックします。

バンドルをルータ上にロードすると、そのパッケージの名前、バージョン、およびビルド日付情報がウィンドウに表示されます。パッケージで管理ツールが使用できる場合は、管理ツールを実行できるようにするボタンが表示されます。

Cisco IOS SSL VPN クライアント インストール バンドルは、次のリンクから入手できます。

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

Cisco Secure Desktop インストール バンドルは、次のリンクから入手できます。

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

インストール パッケージ

このウィンドウでインストール バンドルの現在の保存場所を参照して指定します。インストール バンドルがすでにルータに保存されている場合は、［ルータ］をクリックして、インストール バンドルを参照します。インストール バンドルが PC に保存されている場合は、［マイ コンピュータ］をクリックして、インストール バンドルを参照します。インストール バンドルの現在の保存場所を指定してある場合は、［OK］をクリックします。

保存場所は［パッケージ］ウィンドウに表示されます。

その他のヘルプ トピック

この章のヘルプ トピックでは、これまでに紹介していない背景情報や、手動で実行する際に必要な手順について説明します。

ここでは、次のトピックについて説明します。

- Cisco IOS SSL VPN コンテキスト、ゲートウェイ、およびポリシー
- ポート転送サーバについての理解を深める
- グループ ポリシーについての理解を深める
- スプリット トンネリングについての理解を深める
- Cisco IOS SSL VPN の動作を確認する方法
- ファイアウォールの設定後、Cisco IOS SSL VPN を設定する方法
- VRF インスタンスと Cisco IOS SSL VPN コンテキストを関連付ける方法

Cisco IOS SSL VPN コンテキスト、ゲートウェイ、およびポリシー

Cisco CP では、リモート ユーザが Cisco IOS SSL VPN 接続を設定するための簡単な方法を提供しています。ただし、この技術で使用されている用語がわかりにくい場合があります。このヘルプ トピックでは、Cisco CP 設定画面で使用されている Cisco IOS SSL VPN 用語、および Cisco IOS SSL VPN のコンポーネントどうしが連携して動作する仕組みについて説明します。Cisco IOS SSL VPN ウィザードの使用例と Cisco CP の編集画面についても記載しています。

個々のコンポーネントの説明に入る前に、以下の事項に注意しておくと役立ちます。

- 1 つの Cisco IOS SSL VPN コンテキストで、複数のグループ ポリシーをサポートできます。
- 各コンテキストには 1 つの関連ゲートウェイが設定されている必要があります。
- 1 つのゲートウェイで、複数のコンテキストをサポートできます。
- ルータ上に複数のグループ ポリシーが存在する場合は、認証に AAA サーバを使用する必要があります。

Cisco IOS SSL VPN コンテキスト

Cisco IOS SSL VPN コンテキストは、リモート クライアントと、企業またはプライベート イントラネット間の SSL VPN トンネルのサポートに必要なリソースを識別し、1 つ以上のグループ ポリシーをサポートします。Cisco IOS SSL VPN コンテキストでは次のリソースを提供します。

- クライアントが到達可能な IP アドレスを提供する関連 Cisco IOS SSL VPN ゲートウェイと、安全な接続の確立に使用される証明書。
- 認証方法。ローカルで、または AAA サーバを使用して、ユーザを認証することができます。
- ネットワーク リソースへのリンクを提供するポータルの HTML 表示設定。
- リモート クライアントでシン クライアント アプレットを使用できるようにする、ポート転送リスト。各リストを特定のグループ ポリシーで使用するよう設定する必要があります。
- 企業イントラネットのリソースへのリンクが含まれている URL リスト。各リストを特定のグループ ポリシーで使用するよう設定する必要があります。
- NetBIOS 名サーバ リスト。各リストを特定のグループ ポリシーで使用するよう設定する必要があります。

これらのリソースは、Cisco IOS SSL VPN グループ ポリシーを設定すると使用できます。

1 つの Cisco IOS SSL VPN コンテキストで、複数のグループ ポリシーをサポートできます。1 つの Cisco IOS SSL VPN コンテキストは、1 つのゲートウェイにのみ関連付けることができます。

Cisco IOS SSL VPN ゲートウェイ

Cisco IOS SSL VPN ゲートウェイは、1 つ以上の Cisco IOS SSL VPN コンテキストの到達可能な IP アドレスと証明書を提供します。ルータ上に設定されている各ゲートウェイにはそれ自身の IP アドレスが設定されている必要があります。IP アドレスはゲートウェイ間で共有できません。ルータ インターフェイスの IP アドレスを使用することができ、別の到達可能な IP アドレスが使用できる場合は、それも使用できます。デジタル証明書または自己署名証明書のいずれかを、使用するゲートウェイに対して設定する必要があります。ルータ上のゲートウェイはすべて同じ証明書を使用できます。

1 つのゲートウェイで複数の Cisco IOS SSL VPN コンテキストを提供できる場合であっても、リソースの制約事項と IP アドレスの到達可能性を考慮する必要があります。

Cisco IOS SSL VPN ポリシー

Cisco IOS SSL VPN グループ ポリシーを使用すると、さまざまなユーザ グループのニーズに対応できます。リモートで作業しているエンジニア グループは、現場で働く販売担当者よりも各種ネットワーク リソースにアクセスする必要があります。ビジネス パートナーと外部ベンダーには、共同作業に必要な情報にアクセスを許可する必要がありますが、自社の機密情報など、必要でないその他のリソースにはアクセスを禁止する必要があります。これらのグループについて個々に異なるポリシーを作成することで、リモート ユーザに必要な情報を提供して、他のリソースへのアクセスを防止することができます。

グループ ポリシーを設定する場合、ポリシーに関連するコンテキストに設定されている URL リスト、ポート転送リスト、NetBIOS 名サーバ リストなどのリソースを選択できます。

ルータに複数のグループ ポリシーが設定されている場合は、AAA サーバを使用してユーザを認証し、特定のユーザが属しているポリシー グループを特定するようルータを設定する必要があります。詳細については、「グループ ポリシーについての理解を深める」を参照してください。

例

この例では、ユーザは［新しい SSL VPN を作成］をクリックし、ウィザードを使用してルータに最初の Cisco IOS SSL VPN 設定を作成します。このウィザードに入力すれば、新しいコンテキスト、ゲートウェイ、およびグループ ポリシーが作成されます。次の表は、ユーザがウィザードの各ウィンドウで入力する情報と、その情報から作成される設定を示しています。

表 22-5　新しい SSL VPN の作成

Cisco IOS SSL VPN ウィザード ウィンドウ	構成
SSL VPN の作成ウィンドウ	
［必須タスク］エリアは、そのルータにデジタル証明書が設定されていないことを示します。 ［自己署名証明書］をクリックして、［永続的な自己署名証明書］ダイアログ ボックスで証明書を設定します。Cisco CP で指定されている名前 Router_Certificate は変更しません。 ［新しい SSL VPN を作成］をクリックします。	すべての Cisco IOS SSL VPN 設定で使用できる「Router_Certificate」という名前の自己署名証明書が設定されます。
IP アドレスおよび名前ウィンドウ	
次の情報を入力します。 IP アドレス：172.16.5.5 名前 :Asia ［192.168.1.1 を経由してセキュア アクセス］チェック ボックスを選択します。 証明書：**Router_Certificate**	「Asia」という名前のコンテキストが作成されます。 IP アドレス 172.16.5.5 と Router_Certificate を使用する、「gateway_1」というゲートウェイが作成されます。このゲートウェイは、別の Cisco IOS SSL VPN コンテキストに関連付けることができます。 「http://172.16.5.5/Asia」と入力して、Cisco IOS SSL VPN ポータルにアクセスします。このゲートウェイが他のコンテキストに関連付けられている場合は、同じ IP アドレスがそのコンテキストの URL にも使用されます。たとえば、コンテキスト Europe も gateway_1 を使用するよう設定されている場合は、「https://172.16.5.5/Europe」と入力してポータルにアクセスします。 設定がルータに配信された後、この IP アドレスを使用して Cisco CP を起動するには「http://172.16.5.5:4443」と入力する必要があります。 また、policy_1 という名前の最初のグループ ポリシーの設定も開始されます。

表 22-5　新しい SSL VPN の作成（続き）

Cisco IOS SSL VPN ウィザード ウィンドウ	構成
ユーザ認証ウィンドウ	
［このルータ上でローカルに］を選択します。既存のリストに 1 つのユーザ アカウントを追加します。	認証リスト「sdm_vpn_xauth_ml_1」が作成されます。このリストは、ウィザードの終了時に［Cisco IOS SSL VPN コンテキスト］ウィンドウに表示されます。 ［ユーザ認証］ウィンドウのリストに表示されているユーザは、この認証リストのメンバであり、policy_1 により管理されます。
イントラネット Web サイトの設定ウィンドウ	
URL リスト Ulist_1 を設定します。見出しは Taiwan です。	Taiwan という見出しがついた URL リストが、「sdm_vpn_xauth_ml_1」のユーザがログオンしたときのポータルに表示されます。 この URL リストは、コンテキスト「Asia」で設定されている他のグループ ポリシーの設定でも使用できます。
フル トンネルの有効化ウィンドウ	
［フル トンネルの有効化］をクリックし、定義済みアドレス プールを選択します。詳細オプションは設定されません。	クライアントが初めてログインするときにフル トンネル クライアント ソフトウェアがクライアント PC にダウンロードされ、ユーザがポータルにログインすると、PC とルータ間のフル トンネルが確立されます。
SSL VPN ポータルページのカスタマイズ ウィンドウ	
［オーシャン ブリーズ］を選択します。	このカラー スキームで HTTP 表示設定が行われます。policy_1 ユーザのログイン時に表示されるポータルでこの設定が使用されます。これらのポータル設定は、コンテキスト「Asia」で設定されているすべてのポリシーにも適用されます。ユーザはウィザード終了後、［SSL VPN の編集］ウィンドウで HTTP 表示設定をカスタマイズできます。

表 22-5　新しい SSL VPN の作成（続き）

Cisco IOS SSL VPN ウィザード ウィンドウ	構成
SSL VPN パススルー設定ウィンドウ	
［NAC およびファイアウォールで作業するために SSL VPN を許可］チェック ボックスを選択します。	以下のエントリで ACL が追加されます。 `permit tcp any host 172.16.5.5 eq 443`
要約ウィンドウ	

［要約］ウィンドウには、右の欄に示す情報が表示されます。その他の詳細情報は、［SSL VPN の編集］ウィンドウで表示できます。	`SSL VPN Policy Name: policy_1`
	`SSL VPN Gateway Name: gateway_1`
	
	`User Authentication Method List:  Local`
	
	`Full Tunnel Configuration`
	`  SVC Status: Yes`
	`  IP Address Pool: Pool_1`
	`  Split Tunneling: Disabled`
	`  Split DNS: Disabled`
	`  Install Full Tunnel Client: Enabled`

この設定が配信されると、ルータには Asia という Cisco IOS SSL VPN コンテキスト、gateway_1 というゲートウェイ、および policy_1 というグループ ポリシーがそれぞれ 1 つずつ設定されます。これは［SSL VPN の編集］ウィンドウでは次の表に示すように表示されます。

名前	ゲートウェイ	ドメイン	ステータス	管理ステータス
Asia	gateway_1	Asia		サービス提供中

SSL VPN コンテキスト Asia の詳細：

項目名	項目値
グループ ポリシー	
policy_1	
サービス	URL の細分化、フル トンネル
ユーザに表示される URL	http://172.16.5.5/pricelist
	http://172.16.5.5/catalog

名前	ゲートウェイ	ドメイン	ステータス	管理ステータス
ユーザに表示されるサーバ		< なし >		
WINS サーバ		< なし >		

policy_1 では、URL の細分化の基本的な Cisco IOS SSL VPN サービスを提供し、クライアントとルータ間にフル トンネルを確立するよう指定しています。その他の機能は設定されていません。［既存の SSL VPN の詳細機能を設定する］を選択し、［Cisco IOS SSL VPN ユーザ グループの選択］ウィンドウで［Asia］と［policy_1］を選択してから、［詳細機能］ウィンドウで追加する機能を選択すると、シン クライアントや Common Internet File System などの機能を policy_1 に追加できます。このウィザードでは、追加 URL リストを設定することもできます。

［ユーザの新しいグループ用に、既存の SSL VPN に新しいポリシーを追加します。］を選択すると、コンテキスト「Asia」に新しいグループ ポリシーを作成できます。

コンテキスト リストから Asia を選択して［編集］をクリックすると、コンテキスト Asia の設定とそのコンテキストに設定されているポリシーをカスタマイズすることができます。［SSL VPN コンテキスト Asia の編集］ウィンドウに、このコンテキストの詳細リソースの設定と、追加ポリシーの編集と設定を行うことができるツリーが表示されます。SSL VPN ノードの［SSL VPN ゲートウェイ］をクリックして、gateway_1 を選択し、［編集］をクリックすると、gateway_1 の設定を編集できます。

ポート転送サーバについての理解を深める

ポート転送を使用すると、リモート Cisco IOS SSL VPN ユーザは、企業イントラネット上のプライベート IP アドレスを持つサーバ上のスタティック ポートに接続できます。たとえば、ルータ上にポート転送を設定すると、リモート ユーザに企業イントラネット上のサーバへの Telnet アクセスを提供できます。ポート転送を設定するには、次の情報が必要です。

- サーバの IP アドレス
- サーバ上のスタティック ポート番号
- クライアント PC のリモート ポート番号。安全に使用できるポート番号がダイアログに表示されます。

たとえば、ユーザが Telnet を使用して IP アドレス 10.0.0.100（ポート 23）のサーバに接続できるようにするには、次の情報を使用してポート マッピング エントリを作成します。

サーバの IP アドレス：10.0.0.100

ユーザが接続するサーバ ポート：23

クライアント PC 上のポート：Cisco CP による指定値。この例では、3001。

説明：server-a への SSL VPN Telnet アクセス。この説明はポータルに表示されます。

クライアントのブラウザからゲートウェイ ルータに接続すると、ポータルのアプレットがクライアント PC にダウンロードされます。このアプレットには、サーバの IP アドレスとスタティック ポート番号、そして、クライアント PC が使用するポート番号が含まれています。このアプレットは以下を実行します。

- クライアント PC 上でマッピングを作成します。この例では、IP アドレス 10.0.0.100、ポート 23 のトラフィックを PC のループバック IP アドレス 127.0.0.1、ポート 3001 にマップします。
- ポート 3001、IP アドレス 127.0.0.1 をリッスンします。

ユーザが IP アドレス 10.0.0.100 のポート 23 に接続するアプリケーションを実行すると、要求は IP アドレス 127.0.0.1 のポート 3001 に送信されます。そのポートおよび IP アドレス上でリッスンするポータルのアプレットがこの要求を取得し、Cisco IOS SSL VPN トンネルを介してゲートウェイに送信します。ゲートウェイ ルータがその要求を IP アドレス 10.0.0.100 のサーバに転送し、PC にリターン トラフィックを送り返します。

グループ ポリシーについての理解を深める

Cisco IOS SSL VPN グループ ポリシーでは、これらのポリシーに含まれるユーザのためのポータルとリンクを定義します。リモート ユーザが指定された Cisco IOS SSL VPN の URL を入力すると、ルータではそのユーザがメンバとして含まれているポリシーを特定し、そのポリシーで設定されているポータルがユーザに表示されるようにする必要があります。ルータに設定されている Cisco IOS SSL VPN ポリシーが 1 つだけの場合、ルータではユーザをローカルで認証するか、または AAA サーバを使用して認証し、ポータルを表示します。

しかし、複数のポリシーが設定されている場合、ルータは使用するポリシーを、リモート ユーザがログインを試みるたびに AAA サーバを使用して特定する必要があります。複数の Cisco IOS SSL VPN グループ ポリシーを設定した場合は、少なくとも 1 つの AAA サーバをルータに設定し、Cisco IOS SSL VPN ポリシーを作成したユーザ グループごとに、そのサーバに 1 つのポリシーを設定する必要があります。AAA サーバ上のポリシー名は、ルータに設定したグループ ポリシー名と同じでなければならず、そのグループのメンバであるユーザのクレデンシャルを使って設定しなければなりません。

たとえば、Bob Smith のローカル認証を使用してルータが設定され、Sales というグループ ポリシーのみ設定されている場合は、Bob Smith のログイン時に表示可能なポータルは 1 つだけです。しかし、Sales、Field、および Manufacturing という 3 つの Cisco IOS SSL VPN グループ ポリシーが設定されている場合は、ルータでは Bob Smith がどのポリシー グループに含まれているか自動的に特定できません。それらのポリシーに関して AAA サーバが正しい情報で設定されていれば、ルータはその AAA サーバに接続して、Bob Smith が Sales というグループのメンバであるという情報を受け取ります。その結果、ルータは Sales グループのポータルを正しく表示できます。

AAA サーバの設定方法については、次のリンク先に掲載されている『SSL VPN Enhancements』の「Configuring RADIUS Attribute Support for SSL VPN」を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

スプリット トンネリングについての理解を深める

リモート クライアントで Cisco IOS SSL VPN 接続が設定されている場合、企業イントラネット上にないトラフィックを含め、そのクライアントが送受信するトラフィックがすべて Cisco IOS SSL VPN トンネルを経由して転送されることがあります。これにより、ネットワーク パフォーマンスが低下する可能性があります。スプリット トンネリングを使用すると、Cisco IOS SSL VPN トンネル経由で転送するトラフィックを指定し、それ以外のトラフィックを保護せずに他のルータで処理することができます。

スプリット トンネリング エリアでは、Cisco IOS SSL VPN に*含める*トラフィックを指定して、それ以外のトラフィックをすべてデフォルトで除外するか、または、Cisco IOS SSL VPN から*除外する*トラフィックを指定して、それ以外のトラフィックをすべてデフォルトで含めることができます。

たとえば、組織で 10.11.55.0 ネットワークと 10.12.55.0 ネットワークのアドレスを使用しているとします。宛先ネットワーク リストにこれらのネットワーク アドレスを追加して、［トラフィックを含む］ラジオ ボタンをクリックします。Google や Yahoo 宛てのトラフィックなど、それ以外のインターネット トラフィックはすべてインターネットに直接送信されます。

または、Cisco IOS SSL VPN トンネルから特定のネットワークへのトラフィックを除外する方がより実用的な場合があります。この場合は、宛先ネットワーク リストにこれらのアドレスを追加して、［トラフィックを含まない］ラジオ ボタンをクリックします。宛先ネットワーク リスト内のネットワーク宛てのすべてのトラフィックがセキュリティ保護されていないルート経由で送信され、それ以外のトラフィックはすべて Cisco IOS SSL VPN トンネル経由で送信されます。

Cisco IOS SSL VPN に接続しているときに使用するローカル LAN 上にプリンタが接続されている場合は、スプリット トンネリング エリアで［ローカル LAN を含まない］をクリックする必要があります。

（注） スプリット　トンネリング　エリアの宛先ネットワーク　リストにすでにネットワーク アドレスが含まれている場合があります。スプリット トンネリング エリアで行うトラフィック設定は、リストに含まれるネットワーク対して以前行われた設定より優先されます。

Cisco IOS SSL VPN の動作を確認する方法

Cisco IOS SSL VPN コンテキストがユーザ用に設定したアクセスを提供することを確認する最良の方法は、自分自身をユーザとして設定し、コンテキストで提供するよう設定されているすべての Web サイトとサービスにアクセスしてみることです。このテストを設定する際には、次の手順を使用してください。

ステップ 1　使用できるクレデンシャルが AAA サーバのすべての適切なポリシーに含まれていることを確認します。

ステップ 2　ルータへの Cisco CP セッションを開くことができる場合はそのセッションを開き、作成する Cisco IOS SSL VPN トラフィックを監視できるようにします。Cisco IOS SSL VPN コンテキストのテストに使用する PC が Cisco CP にアクセスできるネットワークに含まれていない場合は、別の PC でこれを行う必要があります。［監視］>［VPN ステータス］>［SSL VPN］を選択します。

ステップ 3　この Cisco IOS SSL VPN コンテキストに設定する各 Web ポータルの URL をそれぞれ入力します。各ページが設定した外観で表示され、ポリシーの URL リストで指定したすべてのリンクがページに表示されていることを確認します。

ステップ 4　このポリシーに含まれているユーザが使用できなければならないリンクとサービスをすべてテストします。テストしているいずれかのポリシーで Cisco Secure Desktop またはフル トンネル クライアント ソフトウェアのダウンロードが提供されている場合は、そのポリシーの Web ポータルの URL を入力し、ソフトウェアのダウンロードを必要とするリンクをクリックします。ソフトウェアが正常にダウンロードされていることと、ユーザがアクセスできなければならないサービスにこれらのリンクからアクセスできることを確認します。

ステップ 5　テスト開始前に Cisco CP セッションを確立できた場合は、テストしているコンテキストのブランチをクリックし、Cisco IOS SSL VPN ウィンドウの Cisco IOS SSL VPN トラフィック統計情報を確認します。

ステップ 6　テスト結果に基づき、必要があれば Cisco CP に戻り、検出した設定上の問題を修正します。

ファイアウォールの設定後、Cisco IOS SSL VPN を設定する方法

すでにファイアウォールを設定してある場合は、Cisco CP の Cisco IOS SSL VPN ウィザードを使用して、Cisco IOS SSL VPN コンテキストとポリシーを作成できます。ルータ上の既存の設定に対して、生成された Cisco IOS SSL VPN CLI コマンドが Cisco CP により検証されます。Cisco IOS SSL VPN トラフィックが通過できるように変更しなければならない既存のファイアウォール設定が検出された場合は、それが通知されます。Cisco CP による自動処理で、適切な設定になるようにファイアウォールを変更できますが、ここではファイアウォールを変更せず、［設定］>［セキュリティ］>［ファイアウォールと ACL］>［ファイアウォール ポリシー /ACL の編集］を選択し、Cisco IOS SSL VPN トラフィックがファイアウォールを通過する上で必要な許可のステートメントを入力して、手動でファイアウォールを変更することもできます。

VRF インスタンスと Cisco IOS SSL VPN コンテキストを関連付ける方法

VPN ルーティングおよび転送（VRF）インスタンスは、VPN 用のルーティングテーブルと転送テーブルを管理します。［設定］>［セキュリティ］>［VPN］>［SSL VPN］>［SSL VPN マネージャ］から［SSL VPN の編集］タブを選択することで、VRF インスタンスまたは名前を Cisco IOS SSL VPN コンテキストに関連付けることができます。VRF インスタンスを関連付けるコンテキストを選択して、［編集］をクリックします。表示されるダイアログ ボックスで VRF インスタンスの名前を選択します。

（注） VRF インスタンスがすでにルータで設定されている必要があります。