IOS および PIX 6.3 デバイスでのリモートアクセス VPN の管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

Cisco IOS ソフトウェアまたは PIX 6.3 を実行するデバイスのリモートアクセス IPsec、および IOS 12.4(6)T 以上のデバイス（PIX デバイスではありません）の SSL VPN を設定および管理できます。サポート対象の特定のデバイスモデルの詳細については、各リモート アクセス VPN テクノロジーでサポートされるデバイスについてを参照してください。

これらのリモートアクセス VPN の設定は、これらのデバイスタイプで同じです。ASA および PIX 7.0 以降のデバイスは、リモートアクセス VPN に異なる設定を使用します（ASA および PIX 7.0+ デバイスでのリモートアクセス VPN の管理を参照）。

この章のトピックでは、IOS および PIX 6.3 デバイスに固有のポリシーを設定する方法を説明します。リモート アクセス VPN の詳細については、次のトピックを参照してください。

- リモート アクセス VPN について
- 各リモート アクセス VPN テクノロジーでサポートされるデバイスについて
- リモート アクセス VPN ポリシーの検出
- Remote Access VPN Configuration ウィザードの使用
  - Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス）
  - Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）

この章は次のトピックで構成されています。

IOS および PIX 6.3 デバイスのリモート アクセス VPN ポリシーの概要

（注）　バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

IOS または PIX 6.3 デバイスでリモート アクセス VPN を設定する場合、設定する VPN のタイプに基づいて、次のポリシーを使用します。PIX 6.3 デバイスでは SSL VPN を設定できないことに注意してください。

- **IPsec および SSL リモート アクセス VPN の両方で使用されるポリシー**：
  - **グローバル設定**：リモートアクセス VPN のすべてのデバイスに適用されるグローバル設定を定義できます。グローバル設定には、Internet Key Exchange（IKE; インターネット キー交換）、IPsec、NAT、フラグメンテーションの定義などがあります。グローバル設定には、通常、ほとんどの状況に適用できるデフォルトが設定されています。そのため、グローバル設定ポリシーの設定はオプションです。デフォルト以外の動作が必要な場合だけ設定してください。詳細については、VPN グローバル設定を参照してください。
  - **Public Key Infrastructure**：Public Key Infrastructure（PKI）ポリシーを作成して、CA 証明書および RSA キーの登録要求を生成し、キーや証明書を管理できます。Certification Authority（CA; 認証局）サーバは、これらの証明書要求を管理し、IPsec または SSL リモート アクセス VPN に接続するユーザに対して証明書を発行するために使用されます。詳細については、Public Key Infrastructure ポリシーについておよびリモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定を参照してください。
- **リモート アクセス IPsec VPN だけで使用されるポリシー**：
  - **IKE プロポーザル**：インターネット キー エクスチェンジ（IKE）は、ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーションプロトコルです。IKE は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動確立に使用されます。IKE プロポーザル ポリシーは、IKE ネゴシエーションのフェーズ 1 の要件を定義するときに使用します。詳細については、IKE プロポーザルの設定を参照してください。

- **IPsec プロポーザル（IOS/PIX 6.x）**：IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。このポリシーは、IKE フェーズ 2 ネゴシエーションに使用されます。詳細については、リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス） （3 ページ）を参照してください。
- **高可用性**：Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを提供する 2 つ以上のハブデバイスで構成された HA グループを作成することで、高可用性（HA）がサポートされます。詳細については、リモートアクセス VPN での高可用性の設定（IOS） （14 ページ）を参照してください。
- **ユーザーグループ（IOS/PIX 6.x）**：ユーザーグループポリシーには、VPN へのユーザーアクセスおよびVPNの使用を決定する属性を指定します。詳細については、ユーザ グループ ポリシーの設定 （16 ページ）を参照してください。

- **リモート アクセス SSL VPN だけで使用されるポリシー**：
  - **SSL VPN**：SSL VPN ポリシーテーブルには、SSL VPN の仮想設定を定義するすべてのコンテキストが一覧表示されます。各コンテキストには、ゲートウェイ、ドメインまたは仮想ホスト名、およびユーザ グループ ポリシーが含まれます。詳細については、SSL VPN ポリシーの設定（IOS） （18 ページ）を参照してください。

リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、サーバーが Cisco IOS Software または PIX リリース 6.3 を使用している場合の、リモートアクセス VPN サーバーの IPsec プロポーザルを作成または編集する方法について説明します。

IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプトマップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。

IPsec プロポーザルを設定する場合は、リモート アクセス クライアントがサーバに接続する外部インターフェイス、および VPN トンネル内のデータを保護する暗号化と認証のアルゴリズムを定義する必要があります。また、（ローカル サーバまたは外部 AAA サーバで）グループ

ポリシーの検索順序を定義するグループ認可（グループ ポリシー ルックアップ）方式、およびユーザ アカウントの検索順序を定義するユーザ認証（Xauth）方式も選択できます。

IPsec トンネルの概念の詳細については、IPsec プロポーザルについてを参照してください。

IPsec プロポーザルを作成または編集する場合は、次を設定することもできます。

- Catalyst 6500/7600 デバイス上の VPN Services Module（VPNSM; VPN サービス モジュール）インターフェイス IPsec VPN Shared Port Adapter（VPN SPA; VPN 共有ポート アダプタ）（[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス（8 ページ）を参照）
- 7600 デバイスを除く、Cisco IOS ソフトウェアバージョン 12.4(2)T 以降を実行している IOS ルータ上の動的仮想インターフェイス。詳細については、 リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス） （10 ページ）を参照してください。
- ルータまたは Catalyst 6500/7600 デバイスの VRF 対応 IPsec（ リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス） （10 ページ）を参照）。

関連項目

- VRF 対応 IPsec について
- [VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス（8 ページ）
- テーブル カラムおよびカラム見出しの機能

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（IOS/PIX 6.x）（IPsec Proposal (IOS/PIX 6.x)）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（IOS/PIX 6.x）（IPsec Proposal (IOS/PIX 6.x)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[IPsec Proposal] ページが開き、VPN エンドポイント、IPsec トランスフォーム セット、および逆ルート注入がプロポーザルで設定されているかどうかなど、設定されているプロポーザルが一覧表示されます。デフォルトの表示に他の列を追加して、AAA、VRF、および dVTI の設定を表示できます。

ステップ 2 次のいずれかを実行します。

- 新しい IPsec プロポーザルを追加するには、[行の追加（Add Row）]（+）ボタンをクリックして、[IPsec Proposal Editor] ダイアログボックスに入力します。使用可能なオプションの詳細については、 IPsec Proposal Editor（IOS、PIX 6.3 デバイス） （5 ページ）を参照してください。
- 既存のプロポーザルを編集するには、プロポーザルを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

- プロポーザルを削除するには、そのプロポーザルを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

IPsec Proposal Editor（IOS、PIX 6.3 デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

[IPsec Proposal Editor] を使用して、Catalyst 6500/7600 など、リモート アクセス VPN の IOS または PIX 6.3 デバイスの IPsec プロポーザルを作成または編集します。エディタには、[全般（General）] と [動的VTI/VRF対応IPsec（Dynamic VTI/VRF Aware IPsec）] の 2 つのタブがあります。このトピックでは、[全般（General）] タブの基本設定について説明します。[Dynamic VTI/VRF Aware IPsec] 設定の説明については、リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス） （10 ページ）を参照してください。

このダイアログボックスの要素は、選択したデバイスによって異なります。次の表に、Cisco IOS ルータ、Catalyst 6500/7600、または PIX 6.3 デバイスを選択したときの [IPsec Proposal Editor] ダイアログボックス内の [General] タブの要素を示します。

（注） PIX 7.0+ または ASA デバイスを選択したときのダイアログボックス内の要素の詳細については、[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（IOS/PIX 6.x）（IPsec Proposal (IOS/PIX 6.x)）]** を選択します。[Add Row]（+）または [Edit Row]（鉛筆）ボタンをクリックします。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（IOS/PIX 6.x）（IPsec Proposal (IOS/PIX 6.x)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。[Add Row]（+）または [Edit Row]（鉛筆）ボタンをクリックします。

関連項目

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（3 ページ）
- IPsec プロポーザルについて
- インターフェイス ロール オブジェクトの作成

- AAA サーバ グループ オブジェクトの作成

フィールド リファレンス

表 *1 : [IPsec Proposal Editor]* の *[General]* タブ（*IOS* および *PIX 6.3* デバイス）

要素	説明
外部インターフェイス	（注） 選択したデバイスが IOS ルータの場合にかぎり使用できます。 リモート アクセス クライアントがサーバへの接続に使用する外部インターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックして選択するか、または新しいオブジェクトを作成します。
Inside VLAN	（注） 選択したデバイスが Catalyst 6500/7600 ルータの場合にだけ使用可能です。 VPN Services Module（VPNSM; VPN サービス モジュール）または VPN SPA または VSPA への Inside インターフェイスとして機能する内部 VLAN。[選択（Select）] をクリックし、[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス （8 ページ）の説明に従って内部 VLAN を設定します。
IKEv1 トランスフォーム セット	トンネル ポリシーで使用するトランスフォーム セット。トランスフォーム セットは、トンネル内のトラフィックの確立に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。最大 9 個のトランスフォーム セットを選択できます。詳細については、トランスフォーム セットの概要を参照してください。 選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォーム セットが使用されます。 [選択（Select）] をクリックして、トポロジで使用する IPsec トランスフォーム セット ポリシー オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクト リストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定を参照してください。

要素	説明
リバース ルート インジェクション（Reverse Route Injection）	リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。詳細については、逆ルート注入についてを参照してください。 次のいずれかのオプションを選択して、クリプト マップで RRI を設定します。 • [なし（None]）：クリプトマップで RRI の設定を無効にします。 • [標準（Standard）]：クリプトマップのアクセス制御リスト（ACL）で定義されている宛先情報に基づいて、ルートが作成されます。これがデフォルトのオプションです。 • [リモートピア（Remote Peer）]：リモートエンドポイント用に 1 つ、クリプトマップが適用されるインターフェイス経由でのリモートエンドポイントへのルート再帰用に 1 つ、合計 2 つのルートを作成します。 • [リモートピアIP（Remote Peer IP）]：アドレスをリモート VPN デバイスへの明示的なネクストホップとして指定します。IP アドレス、またはアドレスを指定するネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）]をクリックして、リストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） ネットワークまたはホストオブジェクトを使用する場合は、オブジェクトで [デバイスごとの値のオーバーライドを許可（Allow Value Override per Device）] オプションを選択し、必要に応じて、このオブジェクトを使用する特定のデバイスの IP アドレスをオーバーライドできます。
Group Policy Lookup/AAA Authorization Method	グループ ポリシーを検索する順序を定義するために使用される AAA 認可方式リスト。グループ ポリシーは、ローカル サーバまたは外部 AAA サーバ上に設定できます。リモート ユーザはグループ化され、リモート クライアントから VPN サーバに接続が正常に確立されたときに、その特定のユーザ グループのグループ ポリシーがユーザ グループに属するすべてのクライアントにプッシュされます。 [選択（Select）]をクリックすると、使用可能なすべての AAA グループサーバーを表示したダイアログボックスが開き、そこで、AAA グループ サーバー オブジェクトを作成できます。該当する項目をすべて選択し、上矢印ボタンと下矢印ボタンを使用してプライオリティ順に並べ替えます。

要素	説明
User Authentication (Xauth)/AAA Authentication Method	ユーザ アカウントの検索順序を定義する AAA または Xauth ユーザ認証方式。 Xauth では、すべての Cisco IOS ソフトウェア AAA 認証方式で、IKE 認証フェーズ 1 の交換後に別のフェーズでユーザ認証を実行できます。 [選択（Select）] をクリックすると、使用可能なすべての AAA グループサーバーを表示したダイアログボックスが開き、そこで、AAA グループ サーバー オブジェクトを作成できます。該当する項目をすべて選択し、上矢印ボタンと下矢印ボタンを使用してプライオリティ順に並べ替えます。

[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス

（注） このダイアログボックスは、選択したデバイスが Catalyst 6500/7600 の場合にだけ使用可能です。

[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックスを使用して、Catalyst 6500/7600 デバイスで VPN Services Module（VPNSM; VPN サービスモジュール）、VPN Shared Port Adapter（VPN; 共有ポートアダプタ）、または Cisco VPN Service Port Adapter（VSPA; VPN サービスポートアダプタ）を構成するための設定を指定します。

注記

- 設定を定義する前に、Catalyst 6500/7600 デバイスを Cisco Security Manager インベントリにインポートし、そのインターフェイスを検出する必要があります。詳細については、VPNSM または VPN SPA/VSPA エンドポイントの設定を参照してください。
- デバイスで VRF 対応 IPsec を使用して VPNSM または VPN SPA を設定する前に、VRF 対応 IPsec を使用する IPsec プロポーザルと、VRF 対応 IPsec を使用しない IPsec プロポーザルがデバイスで設定されていないことを確認してください。

ナビゲーション パス

[IPsecプロポーザルエディタ（IPsec Proposal Editor）] ダイアログボックス（Catalyst 6500/7600 デバイスの場合）の [全般（General）] タブで、[内部VLAN（Inside VLAN）] フィールドの横にある [選択（Select）] をクリックします。IPsec プロポーザルエディタを開く方法の詳細については、IPsec Proposal Editor（IOS、PIX 6.3 デバイス） （5 ページ）を参照してください。

関連項目

- インターフェイス ロール オブジェクトの作成

フィールド リファレンス

表 *2 : [VPNSM/VPN SPA/VSPA*設定（*VPNSM/VPN SPA/VSPA Settings*）*]* ダイアログボックス

要素	説明
Inside VLAN	必要なクリプト マップが適用される、VPNSM、VPN SPA または VSPA への Inside インターフェイスとして機能する内部 VLAN。[VLAN ID] を入力します。あるいは、[選択（Select）] をクリックして VLAN を選択するか、または新しいインターフェイス ロール オブジェクトを作成して VLAN を識別します。
スロット サブスロット	VPNSM または VPNSPA/VSPA のスロット位置を指定する番号です。VPNSPA/VSPA を設定する場合は、サブスロット番号も必要です。 （注） VPNSM を設定している場合は、0 を選択します。
External Port	内部 VLAN に接続する外部ポートまたは VLAN。VLAN またはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択します。内部 VLAN に選択したものとは異なるインターフェイスまたはインターフェイス ロールを選択する必要があります。 （注） VRF 対応 IPsec がデバイスに設定されている場合は、外部ポートまたは VLAN に IP アドレスが必要です。VRF 対応 IPsec が設定されていない場合は、外部ポートまたは VLAN に IP アドレスを含めないでください。
Enable Failover Blade	シャーシ内のハイ アベイラビリティを確保するために、フェールオーバー VPNSM または VPNSPA/VSPA ブレードを設定するかどうかを指定します。 （注） 同じデバイスで VPNSM ブレードと VPNSPA/VSPA ブレードをプライマリ ブレードおよびフェールオーバー ブレードとして使用することはできません。 次のように、フェールオーバー ブレードを指定します。 • [スロット（Slot）] : VPNSM ブレードまたは VPNSPA/VSPA ブレードの位置を特定するスロット番号です。 • [サブスロット（Subslot）] : VPNSPA/VSPA を設定している場合は、フェールオーバー VPN SPA ブレードがインストールされているサブスロットの番号を選択します。 （注） VPNSM を設定している場合は、0 を選択します。

リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス）

（注） [Dynamic VTI/VRF Aware IPsec] タブは、選択したデバイスが Cisco IOS ルータまたは Catalyst 6500/7600 の場合にかぎり使用可能です。

[IPsec Proposal Editor] の [Dynamic VTI/VRF Aware IPsec] タブを使用して、（Cisco IOS ルータまたは Catalyst 6500/7600 デバイスで）リモート アクセス VPN の [VRF Aware IPsec]、または（Cisco IOS ルータで）ダイナミック仮想インターフェイス、あるいはその両方を設定します。

IOS デバイスでは、ダイナミック Virtual Template Interface（VTI; 仮想テンプレート インターフェイス）を使用できます。このインターフェイスは、リモート アクセス VPN に非常に安全でスケーラブルな接続を提供し、ダイナミック クリプト マップおよびダイナミック ハブアンドスポーク方式に代わってトンネルを確立します。ダイナミック VTI は、サーバ設定とリモート設定の両方に使用できます。トンネルにより、各 VPN セッションに対して、仮想アクセス インターフェイスがオンデマンドで個別に提供されます。仮想アクセスインターフェイスの設定は、仮想テンプレート設定から複製されます。仮想テンプレート設定には、IPsec 設定および仮想テンプレート インターフェイスに設定されたすべての機能が含まれています。ダイナミック VTI によって IP アドレスの使用が効率的になり、セキュアな接続が提供されます。それらによって、動的にダウンロード可能な、グループごとおよびユーザーごとのポリシーを RADIUS サーバー上で設定できます。VRF がインターフェイスに設定されるため、VRF 対応 IPsec の展開はダイナミック VTI によって簡素化されます。

この機能をイネーブルにすると、リモート アクセス VPN 内の選択デバイスの仮想テンプレート インターフェイスが Security Manager によって暗黙的に作成されます。必要となる作業は、仮想テンプレート インターフェイスとして使用されるサーバの IP アドレスの指定、または既存のループバック インターフェイスの使用だけです。仮想テンプレートインターフェイスは、リモートクライアントで IP アドレスなしで作成されます。

注記

- ダイナミック VTI を設定できるのは、Cisco IOS Release 12.4(2)T 以降が稼働しているルータだけです（7600 デバイスを除く）。
- ダイナミック VTI は、VRF 対応 IPsec が設定されているかどうかにかかわらず設定できます。VRF 対応 IPsec の詳細については、VRF 対応 IPsec についてを参照してください。
- また、ダイナミック VTI は、サイト間 Easy VPN トポロジでも設定できます。詳細については、Easy VPN とダイナミック仮想トンネル インターフェイスを参照してください。

ナビゲーション パス

[IPsecプロポーザルエディタ（IPsec Proposal Editor）] ダイアログボックス（IOS ルータおよび Catalyst 6500/7600 デバイス）で、[ダイナミック VTI/VRF 対応 IPsec（Dynamic VTI/VRF Aware

IPsec）] タブをクリックします。詳細については、 IPsec Proposal Editor（IOS、PIX 6.3 デバイス） （5 ページ）を参照してください。

関連項目

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（3 ページ）
- インターフェイス ロール オブジェクトの作成

フィールド リファレンス

表 *3 : IPsec* プロポーザルエディタの *[ダイナミック VTI/VRF* 対応 *IPsec*（*Dynamic VTI/VRF Aware IPsec*）*]* タブ

要素	説明
Enable Dynamic VTI	選択すると、Security Manager は IOS ルータ上にダイナミック仮想テンプレート インターフェイスを暗黙的に作成できます。 （注） ダイナミック VTI は、Cisco IOS Release 12.4(2)T 以降を実行している IOS ルータ（7600 デバイスを除く）でだけ設定できます。デバイスがダイナミック VTI をサポートしていない場合、オプションはグレー表示されます。
Enable VRF Settings	選択すると、選択済みのハブアンドスポーク トポロジに対してデバイスで VRF を設定できます。 （注） VPN トポロジにすでに定義されている VRF 設定を削除するには、このチェックボックスをオフにします。
ユーザー グループ	リモート アクセス VPN サーバを設定する場合、リモート クライアントがデバイスに接続できるように、リモートクライアントのグループ名を、VPN サーバで設定されているユーザ グループ オブジェクトと同じにする必要があります。 デバイスに関連付けられているユーザー グループ ポリシー オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからユーザー グループ ポリシー オブジェクトを選択します。また、新しいオブジェクトを作成したり、選択リストから既存のオブジェクトを編集したりすることもできます。
CA Server	デバイスの証明書要求の管理に使用する Certification Authority（CA; 証明局）サーバを選択します。[選択（Select）] をクリックして CA サーバーを定義する PKI 登録ポリシーオブジェクトを選択するか、または新規オブジェクトを作成します。詳細については、[PKI Enrollment] ダイアログボックスを参照してください。 CA サーバを使用する IPsec 設定の詳細については、Public Key Infrastructure ポリシーについてを参照してください。

要素	説明
Virtual Template IP Type	[ダイナミック VTI の有効化（Enable Dynamic VTI）] を選択した場合に使用可能になります。 使用する仮想テンプレート インターフェイスを指定します。 • [IP]：仮想テンプレート インターフェイスとして IP アドレスを使用します。プライベート IP アドレスを指定します。 • [ループバック インターフェイスを使用（Use Loopback Interface）]：仮想テンプレート インターフェイスとして既存のループバック インターフェイスから取得した IP アドレスを使用します。[選択（Select）] をクリックしてインターフェイスまたはインターフェイス ロール オブジェクトを選択するか、あるいはループバック インターフェイスを識別する新規オブジェクトを作成します。
VRF Solution	[VRF 設定の有効化（Enable VRF Settings）] を選択した場合に使用可能になります。 VRF ソリューションを選択します。 • [1 ボックス（1-Box）]（IPsec Aggregator + MPLS PE）：1 つのデバイスが、カスタマーエッジ（CE）デバイスから IPsec 暗号化および復号化を実行する以外に、パケットの MPLS タギングも実行するプロバイダー エッジ（PE）ルータとして機能します。詳細については、VRF 対応 IPsec 1 ボックス ソリューションを参照してください。 • [2 ボックス（2-Box）]（IPsec Aggregator だけ）：PE デバイスは MPLS タギングだけを実行し、IPsec Aggregator デバイスが CE から IPsec 暗号化および復号化を実行します。詳細については、VRF 対応 IPsec 2 ボックス ソリューションを参照してください。
[VRF名（VRF Name）]	IPsec Aggregator の VRF ルーティング テーブルの名前。VRF 名では、大文字と小文字が区別されます。
ルート識別子	IPsec Aggregator の VRF ルーティング テーブルの固有識別情報。この一意のルート識別子によって、他の PE ルータへの MPLS コアにわたって各 VPN のルーティング分離を保持します。識別情報は次のいずれかの形式です。 • *IP address:X*（*X* は 0 ～ 999999999） • *N:X*（*N* は 0 ～ 65535、X は 0 ～ 999999999） （注） VRF 設定をデバイスに展開したあとは RD 識別子を上書きできません。展開後に RD 識別子を変更するには、デバイス CLI を介してその RD 識別子を手動で削除してから、再び展開する必要があります。

要素	説明
Interface Towards Provider Edge	2 ボックス VRF でのみ使用可能。 IPsec Aggregator 上の、PE デバイスに向けた VRF 転送インターフェイス。[選択（Select）] をクリックしてインターフェイスまたはインターフェイス ロール オブジェクトを選択するか、あるいはインターフェイスを識別する新規オブジェクトを作成します。 （注） IPsec Aggregator（ハブ）が Catalyst VPN サービス モジュールの場合は、VLAN を指定する必要があります。
ルーティング プロトコル（Routing Protocol）	2 ボックス VRF でのみ使用可能。 IPsec Aggregator と PE の間に使用するルーティング プロトコルを選択します。オプションは、[BGP]、[EIGRP]、[OSPF]、[RIPv2]、または [Static route] です。 保護された IGP 用のルーティング プロトコルが、IPsec Aggregator と PE の間のルーティング プロトコルとは異なる場合、ルーティングを保護された IGP に再配布するためのルーティング プロトコルを選択します。
AS 番号（AS Number）	BGP または EIGRP ルーティングによる 2 ボックス VRF でのみ使用可能。 IPsec Aggregator と PE の間の自律システム（AS）を識別するために使用する番号。AS 番号は 1 ～ 65535 の範囲にしてください。 保護された IGP 用のルーティング プロトコルが、IPsec Aggregator と PE の間のルーティング プロトコルと異なる場合、IPsec Aggregator と PE からルーティングを再配布する宛先の保護された IGP を識別する AS 番号を入力します。これは、GRE または DMVPN が適用される場合だけに関連します。
Process Number	OSPF ルーティングによる 2 ボックス VRF でのみ使用可能。 IPsec Aggregator と PE の間のルーティングを設定するために使用するルーティング プロセス ID 番号。プロセス番号は、1 ～ 65535 の範囲にしてください。
OSPF Area ID	OSPF ルーティングによる 2 ボックス VRF でのみ使用可能。 パケットが属する領域の ID 番号。0 ～ 4294967295 の範囲で任意の番号を入力できます。 （注） すべての OSPF パケットは単一の領域に関連付けられるため、すべてのデバイスに同じ領域 ID 番号が必要です。

要素	説明
Redistribute Static Route	スタティック ルート以外の任意のルーティング プロトコルによる 2 ボックス VRF でのみ使用可能。 選択すると、スタティック ルートを、PE デバイス方向の IPsec Aggregator で設定されているルーティング プロトコルでアドバタイズできます。 （注） このチェックボックスがオフになっており、かつ、IPsec プロポーザルに対して [Enable Reverse Route Injection] がイネーブルになっている場合（デフォルト）も、スタティック ルートは IPsec Aggregator のルーティング プロトコルでアドバタイズされます。
Next Hop IP Address	スタティック ルーティングによる 2 ボックス VRF でのみ使用可能。 プロバイダー エッジ デバイス（または IPsec Aggregator に接続されているインターフェイス）の IP アドレス。

リモートアクセス VPN での高可用性の設定（IOS）

[High Availability] ページを使用して、リモート アクセス VPN の Cisco IOS ルータまたは Cisco Catalyst スイッチに対して High Availability（HA）ポリシーを設定します。

Security Manager では、Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを提供する 2 つ以上のハブデバイスで構成された HA グループを作成することで、高可用性（HA）がサポートされます。仮想 IP アドレスを共有することによって、HA グループのデバイスは、外観上は、リモートアクセスユーザーに対して単一の仮想デバイスまたはデフォルトゲートウェイになります。HA グループの 1 つのデバイスが常にアクティブになって仮想 IP アドレスを独占的に使用し、同時に他のデバイスはスタンバイデバイスになります。グループ内のデバイスは、アクティブデバイスおよびスタンバイデバイスから hello パケットが着信するのを待ちます。アクティブデバイスが何らかの理由で使用できなくなると、スタンバイ デバイスが仮想 IP アドレスの所有権を取得して、リモート アクセス VPN を引き継ぎます。この転送は、リモートアクセスユーザーに対してシームレスかつ透過的に実行されます。

HA グループ内の HSRP デバイス間で状態情報が確実に共有するために、ステートフル スイッチオーバー（SSO）が使用されます。デバイスで障害が発生した場合、共有されている状態情報により、スタンバイ デバイスは、トンネルの再確立またはセキュリティ アソシエーションの再ネゴシエートを行わずに、IPsec セッションを維持できます。

ヒント

- HA グループを設定している場合は、デバイスのインターフェイスのいずれか 1 つのサブネットと一致し、IPsec プロポーザルで設定される VPN 仮想 IP に加えて、デバイス上のインターフェイスのいずれか 1 つのサブネットと一致する内部仮想 IP を指定する必要があります。リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス） （3 ページ）を参照してください。

- HA が設定されたリモートアクセス VPN サーバデバイスは、リモートアクセス VPN サーバに使用されたインターフェイスと同じ外部インターフェイスを使用して HA が設定されたサイト間 VPN トポロジのハブとしては設定できません。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）IOS デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [IPSec VPN] > [高可用性（High Availability）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [IPSec VPN] > [高可用性（High Availability）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[高可用性（High Availability）] ページが表示されます。

ステップ 2 次の表で説明されているオプションを設定します。

表 4 : [High Availability] ページ、[Remote Access VPN]

要素	説明
Inside Virtual IP	HA グループ内のデバイスによって共有され、HA グループの Inside インターフェイスを表す IP アドレス。仮想 IP アドレスは、HA グループ内のデバイスの内部インターフェイスと同じサブネットにする必要がありますが、これらのインターフェイスのいずれかと同じ IP アドレスにすることはできません。 デバイスのインターフェイスのいずれか 1 つのサブネットと一致し、IPsec プロポーザルで設定される VPN 仮想 IP に加えて、デバイス上のインターフェイスのいずれか 1 つのサブネットと一致する内部仮想 IP を指定する必要があります。 （注） デバイスに既存のスタンバイ グループがある場合は、提供する IP アドレスがデバイスにすでに設定されている仮想 IP アドレスと異なることを確認します。
Inside Mask	内部仮想 IP アドレスのサブネット マスク。
VPN Virtual IP	HA グループ内のデバイスによって共有され、HA グループの VPN インターフェイスを表す IP アドレス。この IP アドレスは、VPN トンネルのエンドポイントとして機能します。 （注） デバイスに既存のスタンバイ グループがある場合は、提供する IP アドレスがデバイスにすでに設定されている仮想 IP アドレスと異なることを確認します。
VPN Mask	VPN 仮想 IP アドレスのサブネット マスク。
Hello 間隔（Hello Interval）	ステータスと優先度を示すためにデバイスがグループ内の別のデバイスにエコー hello メッセージを送信する秒単位の間隔（1 ～ 254）。デフォルトは 5 秒です。

要素	説明
保留時間（Hold Time）	デバイスがダウンしていると結論付ける前に、スタンバイ デバイスがアクティブなデバイスから hello メッセージの受信を待機する秒単位の期間（2 ～ 255）。デフォルトは 15 秒です。
Standby Group Number (Inside)	HA グループ内のデバイスの内部仮想 IP サブネットと一致する内部デバイス インターフェイスのスタンバイ番号。番号は 0 ～ 255 の範囲である必要があります。デフォルトは 1 です。
Standby Group Number (Outside)	HA グループ内のデバイスの外部仮想 IP サブネットと一致する外部デバイス インターフェイスのスタンバイ番号。番号は 0 ～ 255 の範囲である必要があります。デフォルトは 2 です。 （注） 外部スタンバイ グループ番号は、内部スタンバイ グループ番号と異なっている必要があります。
Failover Server	リモート ピア フェールオーバー サーバの内部インターフェイスを識別する IP アドレスまたはネットワーク/ホスト ポリシー オブジェクト。IP アドレスまたはネットワーク/ホストオブジェクト名を入力するか、[選択（Select）] をクリックして、オブジェクトを選択するか、新しいオブジェクトを作成します。
Enable Stateful Failover	ステートフル フェールオーバーに対して SSO をイネーブルにします。このオプションは常に選択されるため、リモート アクセス VPN に対して選択解除することはできません。

ユーザ グループ ポリシーの設定

ユーザーグループ（IOS/PIX 6.x）ポリシーを使用して、リモートアクセス IPSec VPN サーバーのユーザーグループを指定します。ユーザーグループは、Cisco IOS ルータ、PIX 6.3 ファイアウォール、または Catalyst 6500/7600 デバイスに設定できます。

リモートアクセス VPN サーバーを設定する場合は、リモートクライアントが属するユーザーグループを作成する必要があります。ユーザ グループ ポリシーには、VPN へのユーザ アクセスおよび VPN の使用を決定する属性を指定します。ユーザ グループによってシステム管理が簡素化され、多数のユーザの VPN アクセスを迅速に設定できます。

たとえば、一般的なリモート アクセス VPN では、財務グループにアクセスを許可するプライベート ネットワーク、カスタマー サポート グループに許可するネットワーク、および MIS グループに許可するネットワークがそれぞれ異なる場合があります。また、MIS に所属する特定のユーザには、他の MIS ユーザにはアクセスできないシステムにアクセスを許可する場合があります。ユーザ グループ ポリシーにより、このようなアクセスを安全に行うための柔軟性が提供されます。

リモート クライアントのグループ名は、VPN サーバに設定されたユーザ グループの名前と同じである必要があります。この場合、リモート クライアントがデバイスに接続できます。名前

が異なる場合は接続を確立できません。リモート クライアントが VPN サーバへの接続を確立すると、そのユーザ グループのグループ ポリシーが同じユーザ グループに属するすべてのクライアントにプッシュされます。ローカル リモート アクセス VPN サーバーまたは外部 AAA サーバー上でユーザーグループを設定できます。

注記

- Remote Access VPN Configuration ウィザードを使用してユーザ グループを指定することもできます。詳細については、Remote Access VPN Configuration ウィザードの使用を参照してください。
- IOS デバイスで SSL VPN のグループ ポリシーを指定するには、SSL VPN ポリシーの設定（IOS） （18 ページ）で説明されているように、SSL VPN ポリシーを使用します。

関連項目

- リモート アクセス IPSec VPN について

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）IOS ルータ、Catalyst 6500/7600、または PIX 6.3 デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [ユーザーグループ（IOS/PIX 6.x）（User Groups (IOS/PIX 6.x)）]**を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [ユーザーグループ（IOS/PIX6.x）（User Groups (IOS/PIX6.x)）]**を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[User Groups] ページが開きます。

このページには、リモート アクセス IPsec VPNS に設定されているすべての既存ユーザ グループ ポリシー オブジェクトのリストである [Available User Groups] と、デバイス上に設定されるすべてのユーザ グループ ポリシー オブジェクトのリストである [Selected User Groups] という、2 つのリストが含まれています。

ステップ 2 選択したユーザ グループのリストに、適切なユーザ グループ ポリシー オブジェクトが含まれていることを確認してください。

- 新しいユーザ グループ ポリシー オブジェクトを作成するには、使用可能なユーザ グループ リストの下にある [Create]（+）ボタンをクリックして、[Add User Group] ダイアログボックスを開きます。オブジェクトの作成方法については、[Add User Group]/[Edit User Group] ダイアログボックスを参照してください。

グループを作成すると、そのグループは使用可能なリストに追加されます。そのグループを使用する場合は、選択したリストに追加する必要があります。

- 選択したリストにユーザーグループを追加するには、利用可能なリストでユーザーグループを選択し、[>>] をクリックします。
- ユーザーグループを削除するには、選択したリストでそのユーザーグループを選択して [<<] をクリックします。グループがデバイスにすでに設定されている場合、次の展開時に削除されます。

- いずれかのリストでユーザー グループ オブジェクトを選択し、[編集（Edit）] ボタンをクリックすることで、ユーザー グループ オブジェクトのプロパティを編集できます。

SSL VPN ポリシーの設定（IOS）

SSL VPN ポリシーを使用して、IOS ルータの SSL VPN 接続ポリシーを設定します。このページから、SSL VPN ポリシーを作成、編集、または削除できます。

関連項目

- リモート アクセス SSL VPN について
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）
- テーブルのフィルタリング

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）IOS デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] > [SSL VPN ポリシー（IOS）（SSL VPN Policy (IOS)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[SSL VPN] ページが表示されます。

テーブルに、SSL VPN の仮想設定を定義するすべてのコンテキストが一覧表示されます。各コンテキストには、ゲートウェイ、ドメインまたは仮想ホスト名、およびユーザ グループ ポリシーが含まれます。また、コンテキストのステータス（[In Service] または [Out of Service]）も表示されます。

ステップ 2 次のいずれかを実行します。

- コンテキストを追加するには、[行の追加（Add Row）] ボタンをクリックして、[SSL VPN Context Editor] ダイアログボックス（IOS） （20 ページ）を開きます。
- コンテキストを編集するには、コンテキストを選択し、[行の編集（Edit Row）] ボタンをクリックします。

（注） コンテキストを削除するには、コンテキストを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 3 ポリシーについて、少なくとも次の一般的な設定を行います。その他のフィールドの詳細については、[General] タブ （21 ページ）を参照してください。

- [名前、ドメイン（Name, Domain）]：新しいポリシーの場合は、SSL VPN の仮想設定を定義するコンテキストの名前。多数のコンテキスト設定の管理を簡素化するには、コンテキスト名をドメインまたは仮想ホスト名と同じ名前にします。
- [ゲートウェイ（Gateway）]：インターフェイスおよびポート設定を含む、ユーザーが接続するゲートウェイデバイスを識別する SSL VPN ゲートウェイ ポリシー オブジェクト。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

オブジェクトを選択すると、[Portal Page URL] フィールドに、ユーザが接続する URL が表示されます。

- [認証サーバーグループ（Authentication Server Group）]：ユーザーの認証に使用する AAA サーバーを識別する AAA サーバー グループ オブジェクトのプライオリティ付きリスト。
- [ユーザーグループ（User Groups）]：SSL VPN ポリシーで使用されるユーザーグループ。ユーザ グループでは、SSL VPN ゲートウェイへの接続時にユーザが使用できるリソースを定義します。

ユーザーグループを追加するには、[行の追加（Add Row）] をクリックすると、既存のユーザー グループ ポリシー オブジェクトのリストが開き、グループを選択できます。目的のグループがまだ存在しない場合は、使用可能なグループリストの下にある [作成（Create）] ボタンをクリックして作成します。ユーザ グループ オブジェクトの詳細については、[Add User Group]/[Edit User Group] ダイアログボックスを参照してください。

ステップ 4 [ポータルページ（Portal Page）] タブをクリックして、ログインページのデザインをカスタマイズします。タイトル、ロゴのグラフィック、ログイン プロンプトの上に表示されるメッセージ、およびバックグラウンドとテキストの色をカスタマイズできます。

別のグラフィックを選択する場合は、最初に Security Manager サーバにそのグラフィックをコピーする必要があります。ワークステーションのハードドライブからはグラフィックを選択できません。

ステップ 5 [Secure Desktop] タブをクリックして、Cisco Secure Desktop（CSD）ソフトウェアを設定します。CSD ポリシーは、クライアント システムのエントリ要件を定義し、クライアント システム上のセッション アクティビティおよび削除に、単一のセキュアなロケーションを提供します。これにより、機密データは SSL VPN セッションの間だけ共有されるようになります。

CSD を使用する場合は、[Cisco Secure Desktopの有効化（Enable Cisco Secure Desktop）] を選択し、[選択（Select）] をクリックして、VPN アクセスおよびホストスキャンの制御に使用するルールが定義される Cisco Secure Desktop 設定ポリシーオブジェクトを選択します。選択リストから新しいオブジェクトを作成できます。これらのオブジェクトの設定の詳細については、Cisco Secure Desktop 設定オブジェクトの作成（23 ページ）を参照してください。

（注） 設定を機能させるには、デバイスに Secure Desktop Client ソフトウェアをインストールしてアクティブ化する必要があります。

ステップ 6 [詳細設定（Advanced）] タブをクリックし、コンテキストの最大同時ユーザー数を設定するか、VRF を使用している場合は、SSL VPN コンテキストに関連付けられた VRF インスタンスの名前を設定します。

ステップ 7 [OK] をクリックして変更を保存します。

[SSL VPN Context Editor] ダイアログボックス（IOS）

このダイアログボックスを使用して、SSL VPN の仮想設定を定義するコンテキストを作成または変更します。詳細については、SSL VPN ポリシーの設定（IOS） （18 ページ）を参照してください。

ナビゲーション パス

SSL VPN（IOS）ポリシーを開き、[行の追加（Add Row）]（+）をクリックするか、テーブル内のコンテキストを選択して [行の編集（Edit Row）] をクリックします。SSL VPN ポリシーを開く方法については、SSL VPN ポリシーの設定（IOS） （18 ページ）を参照してください。

フィールド リファレンス

表 5 : [SSL VPN Context Editor] ダイアログボックス

要素	説明
[一般（General）] タブ	SSL VPN ポリシーに必要な一般設定を定義します。一般設定には、ゲートウェイ、ドメイン、アカウンティングと認証用の AAA サーバ、およびユーザグループの指定が含まれます。このタブの各フィールドの説明については、[General] タブ （21 ページ）を参照してください。
[Portal Page] タブ	SSL VPN ポリシーのログイン ページの設計を定義します。タブの一番下にある表示ボックスが変わり、選択内容がどのように表示されるかが示されます。次のことを設定できます。 • [Title]：ページの一番上に表示されるテキスト。[Title Color] フィールドと [Text Color] フィールド内の [Primary] 設定を使用して色を制御します。 • [Logo]：タイトルの隣に表示されるグラフィック。[None]、[Default]、または [Custom] を選択します。カスタムグラフィックを設定するには、目的のグラフィックを Cisco Security Manager サーバーにコピーし、[参照（Browse）] をクリックしてファイルを選択する必要があります。サポートされるグラフィック タイプは、GIF、JPG、および PNG で、最大サイズは 100 KB です。 • [Login Message]：ログイン プロンプトのすぐ上に表示されるテキスト。[Title Color] フィールドと [Text Color] フィールド内の [Secondary] 設定を使用して色を制御します。

要素	説明
[Secure Desktop] タブ	ルータで Cisco Secure Desktop（CSD）ソフトウェアを設定します。CSD ポリシーは、クライアントシステムのエントリ要件を定義し、クライアントシステム上のセッション アクティビティおよび削除に、単一のセキュアなロケーションを提供します。これにより、機密データは SSL VPN セッションの間だけ共有されるようになります。 （注） 設定を機能させるには、デバイスに Secure Desktop Client ソフトウェアをインストールしてアクティブ化する必要があります。 CSD を使用する場合は、[Cisco Secure Desktopの有効化（Enable Cisco Secure Desktop）] を選択し、[選択（Select）] をクリックして、VPN アクセスおよびホストスキャンの制御に使用するルールが定義される Cisco Secure Desktop 設定ポリシーオブジェクトを選択します。選択リストから新しいオブジェクトを作成できます。これらのオブジェクトの設定の詳細については、Cisco Secure Desktop 設定オブジェクトの作成 （23 ページ）を参照してください。
[詳細設定（Advanced）] タブ	次の追加設定を行います。 • [Maximum Number of Users]：一度に許可される SSL VPN ユーザ セッションの最大数（1 ～ 1000）。 • [VRF Name]：デバイスで Virtual Routing Forwarding（VRF）が設定されている場合、SSL VPN コンテキストに関連付けられている VRF インスタンスの名前。VRF の詳細については、VRF 対応 IPsec についてを参照してください。

[General] タブ

[SSL VPN Context Editor] ダイアログボックスの [General] タブを使用して、SSL VPN ポリシーに必要な一般設定を定義または編集します。一般設定には、ゲートウェイ、ドメイン、アカウンティングと認証用の AAA サーバ、およびユーザ グループの指定が含まれます。

ナビゲーション パス

[SSL VPN Context Editor] ダイアログボックス（IOS） （20 ページ）を開き、[全般（General）] タブをクリックします。

関連項目

- SSL VPN ポリシーの設定（IOS） （18 ページ）
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス
- AAA サーバおよびサーバ グループ オブジェクトについて

フィールド リファレンス

表 *6 : [SSL VPN Context Editor] の [General] タブ（IOS）*

要素	説明
Enable SSL VPN	SSL VPN 接続をアクティブにして、「In Service」にするかどうかを指定します。
名前	SSL VPN の仮想設定を定義するコンテキストの名前。 （注） 多数のコンテキスト設定の管理を簡素化するには、コンテキスト名をドメインまたは仮想ホスト名と同じ名前にします。
ゲートウェイ	ユーザが VPN に入るときに接続するゲートウェイの特性を定義する SSL VPN ゲートウェイ ポリシー オブジェクトの名前。SSL VPN 接続のインターフェイスおよびポート設定を提供するゲートウェイ オブジェクト。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
ドメイン	SSL VPN 接続のドメインまたは仮想ホスト名。
Portal Page URL	SSL VPN の URL。ゲートウェイ オブジェクトを選択すると、自動的に入力されます。ユーザは、この URL に接続して VPN に入ります。
Authentication Server Group	認証サーバ グループ。リストは、プライオリティ順に表示されます。認証は最初のグループを使用して試行され、ユーザが認証または拒否されるまで、リスト内のグループが順に使用されます。ゲートウェイ自体でユーザが定義されている場合は、LOCAL グループを使用します。 AAA サーバ グループの名前を入力します。複数のエントリはカンマで区切ります。[選択（Select）] をクリックして、グループを選択するか、または新しいグループを作成します。
認証ドメイン（Authentication Domain）	SSL VPN リモート ユーザ認証のリストまたは方式。リストも方式も指定しない場合、ゲートウェイではリモートユーザ認証にグローバル AAA パラメータが使用されます。
Accounting Server Group	アカウンティング サーバ グループ。AAA サーバー グループ ポリシー オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。

要素	説明
ユーザー グループ	SSL VPN ポリシー内で使用されるユーザ グループ。ユーザ グループでは、SSL VPN ゲートウェイへの接続時にユーザが使用できるリソースを定義します。テーブルに、グループに対してフル クライアント、CIFS ファイル アクセス、シン クライアントのいずれがイネーブルになっているかが示されます。 • ユーザーグループを追加する場合は、[行の追加（Add Row）] をクリックして、既存のユーザー グループ ポリシー オブジェクトのリストを開き、グループを選択できます。目的のグループがまだ存在しない場合は、使用可能なグループリストの下にある [作成（Create）] ボタンをクリックして作成します。ユーザ グループ オブジェクトの詳細については、[Add User Group]/[Edit User Group] ダイアログボックスを参照してください。 • ユーザーグループを編集するには、ユーザーグループを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ユーザーグループを削除するには、ユーザーグループを選択し、[行の削除（Delete Row）] ボタンをクリックします。この操作ではポリシーからグループが削除されるだけで、ユーザ グループ ポリシー オブジェクトが削除されることはありません。

Cisco Secure Desktop 設定オブジェクトの作成

Cisco Secure Desktop (CSD) 設定オブジェクトでは、IOS デバイスの SSL VPN ポリシーで Secure Desktop をイネーブルにする場合に使用する設定を定義します（SSL VPN ポリシーの設定（IOS） （18 ページ）を参照）。ASA デバイスの場合、この機能は Dynamic Access ポリシーの一部として設定されます（ダイナミック アクセス ポリシーについておよびASA デバイスでの Cisco Secure Desktop ポリシーの設定を参照）。

Cisco Secure Desktop（CSD）は、クライアント システム上のセッション アクティビティおよび削除に、単一のセキュアなロケーションを提供することによって、機密データのすべてのトレースを確実に除去する方法を提供します。CSD では、機密データが SSL VPN セッションの間だけ共有されるセッションベースのインターフェイスを使用できます。すべてのセッション情報が暗号化され、セッションが終了したときに（たとえ接続が突然終了した場合でも）、セッション データのすべてのトレースがリモート クライアントから削除されます。

Windows ロケーションについて

Windows ロケーションを使用すると、クライアントとバーチャル プライベート ネットワークとの接続方法を判断して適宜に保護できます。たとえば、NAT デバイスの背後にある 10.x.x.x ネットワークの職場 LAN 内から接続しているクライアントが、機密情報を公開するリスクはほとんどないと考えられます。これらのクライアントについては、10.x.x.x ネットワークの IP アドレスで指定される Work という名前の CSD Windows ロケーションを設定して、このロケーションの Cache Cleaner および Secure Desktop 機能を両方ともディセーブルにします。

一方、ユーザーのホーム PC は多目的で使用されるため、ウイルスに対するリスクが高いと見なされます。これらのクライアントについては、会社から提供される証明書で指定されたHomeという名前のロケーションを設定し、従業員はホームPCにこの証明書をインストールします。このロケーションでネットワークにフル アクセスするには、アンチウイルス ソフトウェア、およびサポートされている特定のオペレーティング システムがインストールされている必要がある場合があります。

または、インターネットカフェなどの信頼できないロケーションの場合は、一致基準を持たない「Insecure」という名前のロケーションを設定します（これが他のロケーションに一致しないクライアントのデフォルトになります）。このロケーションではすべての Secure Desktop 機能が必要で、不正なユーザによるアクセスを防止するためにタイムアウト期間が短く設定される場合があります。ロケーションを作成して基準を指定しない場合は、そのロケーションが [Locations] リストの最後のエントリであることを確認してください。

関連項目

- SDM を使用した IOS 上の Cisco Secure Desktop 設定例：http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa7b.shtml [英語]
- Microsoft Windows クライアント用の CSD の設定：http://www.cisco.com/en/US/docs/security/csd/csd311/csd_for_vpn3k_cat6k/configuration/guide/CSDwin.html [英語]
- ポリシー オブジェクトの作成

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Managerを参照）。

ステップ 2 オブジェクトタイプセレクタから [Cisco Secure Desktopの設定（Cisco Secure Desktop Configuration）] を選択します。

ステップ 3 作業領域を右クリックし、[新規オブジェクト（New Object）] を選択して[Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックスを開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 [Windowsロケーションの設定（Windows Location Settings）] を選択して、（Work、Home、または Insecure などの）ロケーションを作成し、CSD のロケーションベース設定（適応型ポリシーとも呼ばれる）を定義します。

a) 設定するロケーションごとに [追加するロケーション（Location to Add）] フィールドに名前を入力し、[追加（Add）] をクリックして [ロケーション（Locations）] フィールドにその名前を移動します。[Move Up] ボタンおよび [Move Down] ボタンを使用すると、ロケーションの順序を並べ替えることができます。ユーザが接続すると、これらのロケーションが順番に評価され、最初に一致したロケーションがそのユーザのポリシー定義に使用されます。

ロケーションを追加すると、そのロケーション用のフォルダがコンテンツテーブルに追加されます。フォルダおよびそのサブフォルダでは、ロケーションのポリシーを定義します。

b) Secure Desktop のインストール後に、開いているブラウザ ウィンドウをすべて閉じる場合は、該当するチェックボックスがオンになっていることを確認します。

c) インストールまたはロケーション照合が失敗した場合に Web ブラウジング、ファイル アクセス、ポート転送、およびフル トンネリングをイネーブルにする VPN Feature ポリシーを設定するには、必要なチェックボックスをオンにします。

ステップ 6 追加した Windows ロケーションのフォルダおよびサブフォルダを選択し、その設定を行います。これらの設定の詳細については、『*Setting Up CSD for Microsoft Windows Clients*』（http://www.cisco.com/en/US/docs/security/csd/csd311/csd_for_vpn3k_cat6k/configuration/guide/CSDwin.html [英語]）を参照してください。

ステップ 7 [Windows CE] を選択して、Microsoft Windows CE が動作しているリモートクライアントの Web ブラウジングおよびリモート サーバー ファイル アクセスをイネーブル化または制限するように、VPN 機能ポリシーを設定します。

ステップ 8 [MacおよびLinuxキャッシュクリーナ（Mac and Linux Cache Cleaner）] を選択して、該当するクライアントのキャッシュクリーナと、Web ブラウジング、リモート サーバー ファイル アクセス、およびポート転送のイネーブル化または制限などの VPN 機能ポリシーを設定します。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。