CHAPTER 28

一般的な VPN 設定

バーチャル プライベート ネットワーク（VPN）とは、インターネットなどのパブリック ネットワーク経由でプライベート トラフィックを伝送する仮想回線のネットワークのことです。VPN は、2 か所以上の LAN、またはリモート ユーザと LAN を接続できます。VPN は、すべてのユーザに認証を義務付け、すべてのデータ トラフィックを暗号化することにより、プライバシーとセキュリティを確保します。

この項では、一般的な VPN 設定アトリビュートについて説明します。次の項目を取り上げます。

- Client Update
- Default Tunnel Gateway
- Group Policy
- Browse Time Range
- ACL Manager
- Tunnel Group
- VPN System Options
- Zone Labs Integrity Server
- Easy VPN Remote
- Advanced Easy VPN Properties

Client Update

Configuration > VPN > General > Client Update

Client Update ウィンドウを使用して、中央にいる管理者は次のアクションを実行できます。

- アップデートをイネーブルにする。アップデートを適用するクライアントのタイプとリビジョン番号を指定する
- アップデートを取得する URL または IP アドレスを提供する
- Windows クライアントの場合に、オプションで VPN クライアント バージョンをアップデートする必要があることをユーザに通知する

（注）　Configuration > VPN > General > Client Update よりアクセスするクライアント アップデート機能は、Windows クライアント と VPN 3002 ハードウェア クライアントにだけ適用されます。

Windows クライアントの場合は、アップデートを実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアントのユーザの場合、アップデートは通知せずに自動的に行われます。クライアント アップデートは、IPSec リモートアクセス トンネルグループのタイプだけに適用できます。

（注）　IPSec LAN-to-LAN トンネル グループまたは WebVPN トンネル グループを対象にクライアント アップデートを実行しようとしても、エラー メッセージは受信されず、アップデート通知やクライアント アップデートはそれらのトンネル グループに届きません。

特定のクライアント タイプのすべてのクライアントに対してクライアント アップデートをグローバルにイネーブルにするには、このウィンドウを使用します。また、このウィンドウから、アップグレードが必要であることをすべての Windows クライアントに通知し、すべての VPN 3002 ハードウェア クライアントのアップグレードを開始することもできます。アップデートの適用先クライアント リビジョンと、アップデートのダウンロード元 URL または IP アドレスを設定するには、Edit をクリックします。

特定のトンネル グループのクライアント アップデート リビジョンとソフトウェア アップデート ソースを設定するには、Configuration > VPN > General > Tunnel Group > Add/Edit > IPSec タブ > Client VPN Software Update テーブルを参照してください。

フィールド

- Enable Client Update : すべてのトンネル グループと特定のトンネル グループの両方を対象にクライアント アップデートをイネーブルまたはディセーブルにします。クライアント アップデートをイネーブルにしてから、クライアント アップデート通知を Windows VPN クライアントに送信、またはハードウェア クライアントの自動アップデートを開始します。
- Client Type : アップグレードするクライアント（ソフトウェアまたはハードウェア）を一覧表示します。ソフトウェア クライアントの場合には、すべての Windows クライアントまたはサブセットを表示します。All Windows Based をクリックした場合には、Windows 95、98 または ME と Windows NT、2000 または XP を個別に指定しません。ハードウェア クライアントは、ASA 5505 ソフトウェアまたは VPN 3002 ハードウェア クライアントのリリースと一緒にアップデートされます。

- VPN Client Revisions：このクライアントに合ったソフトウェア イメージ リビジョンのカンマ区切りリストを格納しています。ユーザのクライアント リビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合には、クライアントを更新する必要はありません。Windows ベースのクライアントの場合には、アップデート通知を受信しません。次の警告が適用されます。
  - リビジョン リストには、このアップデートのソフトウェア バージョンが記載されている必要があります。
  - 自分のエントリが、VPN クライアントの場合には URL と、ハードウェア クライアントの場合には TFTP サーバと正確に一致する必要があります。
  - ハードウェア クライアント イメージを配布するための TFTP サーバは堅牢である必要があります。
  - VPN クライアント ユーザは、一覧表示されている URL から適切なソフトウェア バージョンをダウンロードする必要があります。
  - VPN 3002 ハードウェア クライアント ソフトウェアは、ユーザに通知することなく、自動的に TFTP 経由でアップデートされます。
- Image URL：ソフトウェア イメージのダウンロード元 URL または IP アドレスを格納しています。必ず、このクライアントに適したファイルのある URL を指定してください。Windows ベースのクライアントの場合、URL は http:// または https:// という形式にする必要があります。ハードウェア クライアントの場合、URL は tftp:// という形式にする必要があります。
  - Windows ベースの VPN クライアントの場合：VPN クライアント通知で Launch ボタンをアクティブにするには、URL に、HTTP または HTTPS というプロトコル情報と、アップデートを格納するサイトのサーバ アドレスが記載されている必要があります。URL の形式は、http(s):// サーバ _ アドレス：ポート / ディレクトリ / ファイル名です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。次の例を参考にしてください。

    http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe

    ディレクトリはオプションです。ポート番号は、80 以外の HTTP ポート、443 以外の HTTPS ポートを使用する場合にだけ必要です。
  - ハードウェア クライアントの場合、URL の形式は、tftp:// サーバ _ アドレス / ディレクトリ / ファイル名です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。次の例を参考にしてください。

    tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin
- Edit：Edit Client Update Entry ダイアログボックスを開きます。このボックスを使用して、クライアント アップデート パラメータを設定または変更できます。「Edit Client Update Entry」を参照してください。
- Live Client Update：現在接続中のすべての VPN クライアント、または選択したトンネル グループにアップグレード通知メッセージを送信します。
  - Tunnel Group：すべてまたは特定のトンネル グループをアップデートの対象として選択します。
  - Update Now：アップグレード通知をただちに送信します。この通知には、選択したトンネル グループまたは接続中のすべてのトンネル グループ内で現在接続中の Windows VPN クライアントを対象とするアップデート済みソフトウェアの取得場所を指定する URL が記載されています。メッセージには、ソフトウェアの新バージョンをダウンロードする場所が記載されています。その VPN クライアントの管理者は、新しいソフトウェア バージョンを取得し、VPN クライアント ソフトウェアをアップデートできます。

    VPN 3002 ハードウェア クライアントの場合、アップグレードは通知せずに自動的に行われます。

    アップグレードを実行するには、ウィンドウ内の Enable Client Update を選択する必要があります。接続していないクライアントは、アップグレード通知を受信するか、次回ログオンしたときに自動的にアップグレードされます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit Client Update Entry

Configuration > VPN > General > Client Update > Edit Client Update Entry

Edit Client Update ダイアログボックスを使用して、表示されたクライアント タイプの VPN クライアント リビジョンと URL に関する情報を変更できます。クライアントは、表示されたクライアント タイプ用として指定されているいずれかのリビジョンを実行している必要があります。該当するリビジョンを実行していないと、そのクライアントは、アップグレードが必要であると通知されます。

フィールド

- Client Type：（表示のみ）編集対象として選択したクライアント タイプを表示します。
- VPN Client Revisions：このクライアントに合ったソフトウェアまたはファームウェア イメージのカンマ区切りリストを入力できます。ユーザのクライアント リビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合は、クライアントを更新する必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していなくても、更新は正しく実行されます。Windows ベースの VPN クライアントのユーザは、一覧表示されている URL から適切なソフトウェア バージョンをダウンロードする必要があります。VPN 3002 ハードウェア クライアント ソフトウェアは、自動的に TFTP 経由でアップデートされます。
- Image URL：ソフトウェアまたはファームウェア イメージの URL を指定できます。必ず、このクライアントに適したファイルのある URL を指定してください。
  - Windows ベースの VPN クライアントの場合は、URL に、HTTP または HTTPS というプロトコル情報と、アップデートを格納するサイトのサーバ アドレスが記載されている必要があります。URL の形式は、http(s):// サーバ _ アドレス : ポート / ディレクトリ / ファイル名です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。次の例を参考にしてください。

    ```
    http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
    ```

    ディレクトリはオプションです。ポート番号は、80 以外の HTTP ポート、443 以外の HTTPS ポートを使用する場合にだけ必要です。
  - ハードウェア クライアントの場合、URL の形式は、tftp:// サーバ _ アドレス / ディレクトリ / ファイル名です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。次の例を参考にしてください。

    tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin

    ディレクトリはオプションです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Default Tunnel Gateway

Configuration > VPN > General > Default Tunnel Gateway

デフォルトのトンネル ゲートウェイを設定するには、このウィンドウにある Static Route リンクをクリックします。Configuration > Routing > Routing > Static Route ウィンドウが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Group Policy

Configuration > VPN > General > Group Policy

Group Policy ウィンドウを使用して、VPN グループ ポリシーを管理できます。VPN グループ ポリシーは、デバイスの内部（ローカル）または外部の RADIUS または LDAP サーバに格納されているユーザ指向のアトリビュートと値のペアのセットです。VPN グループ ポリシーを設定することによって、個別のグループまたはユーザ名レベルで設定しなかったアトリビュートをユーザが継承するようにできます。デフォルトでは、VPN ユーザにグループ ポリシー アソシエーションはありません。グループ ポリシー情報は、VPN トンネル グループおよびユーザ アカウントで使用されます。

「子」のウィンドウ、タブ、およびダイアログボックスを使用して、デフォルト グループ パラメータを設定できます。これらのパラメータは、すべてのグループおよびユーザに共通であると考えられ、これによって設定タスクが効率化されます。グループはデフォルト グループからパラメータを「継承」でき、ユーザはグループまたはデフォルト グループからパラメータを「継承」できます。これらのパラメータは、グループおよびユーザを設定するときに上書きできます。

Add ダイアログボックスをクリックすると、新しい内部グループ ポリシーを作成するか、外部の RADIUS または LDAP サーバに格納される外部グループ ポリシーを作成するかを選択できる小さなメニューが表示されます。Add Internal Group Policy ウィンドウと Edit Group Policy ウィンドウのどちらにも、6 つのタブ付きセクションがあります。WebVPN タブをクリックすると、6 つの追加タブが表示されます。それぞれのタブをクリックすると、パラメータが表示されます。タブ間を移動するとき、セキュリティ アプライアンスは新しい設定を保持します。すべてのタブ付きセクションでパラメータの設定を完了したら、OK または Cancel をクリックします。

これらのダイアログボックスで、次の種類のパラメータを設定します。

- 全般的なパラメータ：プロトコル、フィルタリング、接続設定、サーバ
- IPSec パラメータ : IP セキュリティ トンネリング プロトコルのパラメータおよびクライアント アクセス ルール
- クライアント設定パラメータ：バナー、パスワード保管、スプリットトンネリング ポリシー、デフォルト ドメイン名、IPSec over UDP、バックアップ サーバ
- クライアント ファイアウォール パラメータ : VPN クライアント パーソナル ファイアウォールの要件
- ハードウェア クライアント パラメータ：インタラクティブ ハードウェア クライアントおよび個別のユーザ認証、ネットワーク拡張モード
- WebVPN パラメータ：SSL VPN アクセス

これらのパラメータを設定する前に、次の項目を設定する必要があります。

- アクセス時間
- ルールとフィルタ
- IPSec セキュリティ アソシエーション
- フィルタリングおよびスプリット トンネリング用のネットワーク リスト
- ユーザ認証サーバ（特に、内部認証サーバ）

フィールド

- Group Policy：現在設定されているグループ ポリシーが一覧表示されているテーブルと、VPN グループ ポリシーを管理するための Add、Edit、および Delete ボタンがあります。
  - Name：現在設定されているグループ ポリシーの名前を一覧表示します。
  - Type：現在設定されている各グループ ポリシーのタイプを一覧表示します。
  - Tunneling Protocol : 現在設定されている各グループ ポリシーが使用するトンネリング プロトコルを一覧表示します。

- AAA Server Group：現在設定されている各グループ ポリシーが属する AAA サーバ グループが存在すれば、一覧表示します。
- Add：Add Group Policy ダイアログボックスを表示します。このボックスを使用して、新しい AAA グループ ポリシーをリストに追加できます。この画面には、7 つのタブ付きセクションがあります。それぞれのタブをクリックすると、パラメータが表示されます。タブ間を移動するとき、ASDM は新しい設定を保持します。すべてのタブ付きセクションでパラメータの設定を完了したら、Apply または Cancel をクリックします。
- Edit：Edit Group Policy ダイアログボックスを表示します。このボックスを使用して、既存の AAA グループ ポリシーを修正できます。
- Delete：AAA グループ ポリシーをリストから削除します。確認されず、やり直しもできません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit External Group Policy

Configuration > VPN > General > Group Policy > Add > External Group Policy > Add or Edit External Group Policy

Add or Edit External Group Policy ダイアログボックスを使用して、外部グループ ポリシーを設定できます。

フィールド

- Name：追加または変更するグループ ポリシーを特定します。Edit External Group Policy の場合、このフィールドは表示のみです。
- Server Group：このポリシーの適用先として利用できるサーバ グループを一覧表示します。
- Password：このサーバ グループ ポリシーのパスワードを指定します。
- New：新しい RADIUS サーバ グループまたは新しい LDAP サーバ グループを作成するかどうかを選択できるダイアログボックスを開きます。どちらの場合も Add AAA Server Group ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add AAA Server Group

Configuration > VPN > General > Group Policy > Add/Edit > External Group Policy > New > RADIUS Server Group/New LDAP Server Group > Add AAA Server Group

Add AAA Server Group ダイアログボックスを使用して、新しい AAA サーバ グループを設定できます。Accounting Mode アトリビュートは、RADIUS および TACACS+ プロトコルにのみ適用されます。

フィールド

- Server Group：サーバ グループの名前を指定します。
- Protocol：（表示のみ）RADIUS サーバ グループか、LDAP サーバ グループかを示します。
- Accounting Mode : 同時アカウンティング モードか単一アカウンティング モードかを示します。単一モードでは、セキュリティ アプライアンスはアカウンティング データを 1 つのサーバにのみ送信します。同時モードでは、セキュリティ アプライアンスはアカウンティング データをグループ内のすべてのサーバに送信します。Accounting Mode アトリビュートは、RADIUS および TACACS+ プロトコルにのみ適用されます。
- Reactivation Mode：障害が発生したサーバを再アクティブ化する方法を Depletion または Timed 再アクティブ化モードから指定します。Depletion モードでは、障害が発生したサーバは、グループ内のサーバのすべてが非アクティブになった場合にだけ再アクティブ化されます。Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。
- Dead Time : Depletion モードで、グループの最後のサーバがディセーブルになってから、すべてのサーバを次に再度イネーブルにするまでの経過時間を分単位（0 ～ 1440）で指定します。デフォルト値は 10 分です。このフィールドは、Timed モードでは使用できません。
- Max Failed Attempts : 応答しないサーバが非アクティブであると宣言するまでの失敗接続試行回数を指定します（1 ～ 5 の整数）。デフォルト値は 3 回です。

Add/Edit Internal Group Policy > General タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > General タブ

Add or Edit Group Policy ウィンドウの General タブを使用して、追加または修正するグループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。このウィンドウの各フィールドで、Inherit チェックボックスを選択すると、対応する設定の値をデフォルト グループ ポリシーから取得できます。

フィールド

- Inherit：（複数のインスタンス）対応する設定の値をデフォルト グループ ポリシーから取得できます。このタブのアトリビュートすべてのデフォルト値です。
- Tunneling Protocols : このグループが使用できるトンネリング プロトコルを指定します。ユーザは、選択されているプロトコルのみを使用できます。選択肢は次のとおりです。
  - IPSec : IP セキュリティ プロトコル。IPSec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。IPSec は、LAN 間（ピアツーピア）接続と、クライアントと LAN の接続の両方で使用できます。
  - WebVPN : SSL/TLS を利用する VPN。Web ブラウザを使用して、セキュリティ アプライアンスへのセキュアなリモートアクセス トンネルを確立します。ソフトウェア クライアントもハードウェア クライアントも不要です。WebVPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。

- L2TP over IPSec：いくつかの一般的な PC およびモバイル PC オペレーティング システムに付属する VPN クライアントを使用して、パブリック IP ネットワークを介して、セキュリティ アプライアンスおよびプライベート企業ネットワークへのセキュアな接続を確立できるようにします。L2TP は、PPP over UDP（ポート 1701）を使用して、データをトンネリングします。セキュリティ アプライアンスは、IPSec 転送モード用に設定する必要があります。

（注）　プロトコルを選択しなかった場合、エラー メッセージが表示されます。

- Filter : 使用するフィルタを指定するか、グループ ポリシーから値を継承するかどうかを指定します。フィルタは、セキュリティ アプライアンスを経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。　フィルタとルールを設定する場合は、Configuration > Features > VPN > VPN General > Group Policy ウィンドウを参照してください。
- Manage : アクセス コントロール リスト（ACL）と拡張アクセス コントロール リスト（ACE）を追加、編集、および削除できる ACL Manager ウィンドウを表示します。ACL Manager の詳細については、そのウィンドウのオンライン ヘルプを参照してください。
- Connection Settings：接続設定パラメータを指定します。
  - Access Hours : Inherit チェックボックスがオフである場合、このユーザに適用される既存のアクセス時間ポリシーが存在する場合にはその名前を選択でき、存在しない場合には、新しいアクセス時間ポリシーを作成できます。デフォルト値は Inherit ですが、Inherit チェックボックスがオフである場合のデフォルト値は --Unrestricted-- です。
  - Manage : Browse Time Range ダイアログボックスを開きます。このダイアログボックスでは、時間範囲を追加、編集、または削除できます。
  - Simultaneous Logins : Inherit チェックボックスがオフである場合、このパラメータは、このユーザに許可される同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合は、ログインをディセーブルにし、ユーザ アクセスを阻止します。

（注）　最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼす恐れがあります。

  - Maximum Connect Time : Inherit チェックボックスがオフである場合、このパラメータは、ユーザの最大接続時間を分単位で指定します。この時間が終了すると、接続が終了します。最小時間は 1 分で、最大時間は 35791394 分（4000 年以上）です。接続時間を無制限にするには、Unlimited を選択します（デフォルト）。
  - Idle Timeout：Inherit チェックボックスがオフである場合、このパラメータは、ユーザのアイドル タイムアウト時間を分単位で指定します。その期間中にユーザの接続上で通信アクティビティがなかった場合、接続が終了します。最小時間は 1 分で、最大時間は 10080 分です。デフォルトは 30 分です。接続時間を無制限にするには、Unlimited を選択します。この値は、WebVPN ユーザには適用されません。
- Servers：DNS、WINS サーバ、および DHCP スコープを設定します。
  - DNS Servers : 使用する DNS サーバを指定します。Inherit を選択解除した場合には、それぞれのボックスで、プライマリおよびセカンダリ DNS サーバを指定できます。
  - WINS Servers : 使用する WINS サーバを指定します。Inherit を選択解除した場合には、それぞれのボックスで、プライマリおよびセカンダリ WINS サーバを指定できます。
  - DHCP Scope : DHCP スコープを指定します。これは、このグループ ポリシーのユーザにアドレスを割り当てるときにセキュリティ アプライアンス DHCP サーバが使用する IP アドレスの範囲です。Inherit を選択解除した場合には、このボックスでスコープを入力できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse Time Range

このパネルに移動するパスは数種類あります。

Browse Time Range ダイアログボックスを使用して、時間範囲を追加、編集、または削除します。時間範囲とは、グループ ポリシーに適用できる開始および終了時刻を定義する、再利用可能なコンポーネントのことです。時間範囲を定義した後、その時間範囲を選択し、スケジューリングが必要な各種オプションに適用できます。たとえば、アクセスリストを時間範囲に添付して、セキュリティ アプライアンスへのアクセスを制限できます。時間範囲は、開始時刻、終了時刻、およびオプションの繰り返し（つまり定期的な）エントリで構成されます。時間範囲の詳細については、Add or Edit Time Range ダイアログボックスのオンライン ヘルプを参照してください。

フィールド

- Add：Add Time Range ダイアログボックスを開きます。このダイアログボックスでは、新しい時間範囲を作成できます。

（注） 時間範囲を作成しても、デバイスへのアクセスは制限されません。

- Edit：Edit Time Range ダイアログボックスを開きます。このダイアログボックスでは、既存の時間範囲を修正できます。このボタンは、Browse Time Range テーブルから既存の時間範囲を選択した場合にだけアクティブになります。
- Delete：選択した時間範囲を Browse Time Range テーブルから削除します。この処理は、確認されず、やり直しもできません。
- Name：時間範囲の名前を指定します。
- Start Time：時間範囲の始まる時期を指定します。
- End Time：時間範囲が終了する時期を指定します。
- Recurring Entries：指定した開始時刻と停止時刻の範囲内でアクティブな時間の追加制限を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Time Range

このパネルに移動するパスは数種類あります。

Add or Edit Time Range ダイアログボックスを使用して、新しい時間範囲を設定できます。

フィールド

- Time Range Name：この時間範囲に割り当てる名前を指定します。
- Start Time：時間範囲を開始する時刻を定義します。
  - Start now：時間範囲がただちに開始されるように指定します。
  - Start at：時間範囲を開始する月、日、年、時間、および分を選択します。
- End Time：時間範囲を終了する時刻を定義します。
  - Never end：時間範囲でエンド ポイントを定義しないように指定します。
  - End at (inclusive)：時間範囲を終了する月、日、年、時間、および分を選択します。
- Recurring Time Ranges：時間範囲がアクティブである場合に、開始時刻から終了時刻までの範囲内でアクティブな時間を制限します。たとえば、開始時刻が Start now で終了時刻が Never end であり、月曜日から金曜日までの毎日 8:00 AM ～ 5:00 PM を有効な時間範囲とする場合には、繰り返し時間範囲を、平日の 08:00 ～ 17:00 までアクティブになるように設定します。
- Add：Add Recurring Time Range ダイアログボックスを開きます。このダイアログボックスで、繰り返し時間範囲を設定できます。
- Edit：Edit Recurring Time Range ダイアログボックスを開きます。このダイアログボックスで、繰り返し時間範囲を修正できます。
- Delete：選択した繰り返し時間範囲を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Recurring Time Range

このパネルに移動するパスは数種類あります。

Add or Edit Recurring Time Range ダイアログボックス を使用して、繰り返し時間範囲を設定または修正できます。

フィールド

- Specify days of the week and times on which this recurring range will be active：Days of week 領域のオプションを使用可能にします。たとえば、時間範囲を毎週月曜日から木曜日の 08:00 ～ 16:59 の間のみアクティブにする場合にこのオプションを使用します。
  - Days of week：この繰り返し時間範囲に含める曜日を選択します。 可能なオプションは、Every day、Weekdays、Weekends、および On these days of week です。On these days of week については、範囲に入れる曜日ごとにチェックボックスをオンにします。
  - Daily Start Time：選択した各曜日に繰り返し時間範囲をアクティブにする場合に、時間と分を 24 時間形式で指定します。
  - Daily End Time (inclusive)：選択した各曜日に繰り返し時間範囲をアクティブにする場合に、時間と分を 24 時間形式で指定します。

- Specify a weekly interval when this recurring range will be active：Weekly Interval 領域のオプションを使用可能にします。範囲は終了時刻まで拡張されます。この領域の時間は、すべて 24 時間形式です。たとえば、時間範囲を月曜日から金曜日の 8:00 AM ～ 4:30 PM の間で連続的にアクティブにする場合にこのオプションを使用します。
  - From：毎週の時間範囲を開始する日、時間、および分を選択します。
  - Through：毎週の時間範囲を終了する日、時間、および分を選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ACL Manager

このパネルに移動するパスは数種類あります。

ACL Manager ダイアログボックスを使用してアクセス コントロール リスト（ACL）を定義することにより、特定のホストまたはネットワークから別のホストまたはネットワークへのアクセス（使用できるプロトコルやポートなど）を制御できます。

ユーザ セッションに適用する ACL（アクセス コントロール リスト）を設定できます。ACL は、特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザ アクセスを許可または拒否するフィルタです。

- フィルタを定義しない場合は、すべての接続が許可されます。
- セキュリティ アプライアンスは、インターフェイスのインバウンド ACL のみをサポートします。
- 各 ACL の最後には、許可されないすべてのトラフィックを拒否する、表記されない暗黙のルールが含まれます。トラフィックがアクセス コントロール エントリ（ACE）によって明示的に許可されていない場合には、セキュリティ アプライアンスがそのトラフィックを拒否します。このトピックでは、ACE をルールと呼びます。

Standard ACL タブ

このペインには、標準 ACL に関する要約情報が表示され、このペインを使用して、ACL と ACE を追加または削除できます。

フィールド

- Add : 新しい ACL を追加できます。既存の ACL を選択すると、その ACL 用に新しい ACE を追加できます。
- Edit：Edit ACE ダイアログボックスを開きます。このダイアログボックスでは、既存のアクセス コントロール リスト ルールを変更できます。
- Delete：ACL または ACE を削除します。確認されず、やり直しもできません。
- Move Up/Move Down：ACL Manager テーブルでのルールの位置を変更します。
- Cut：ACL Manager テーブルから選択内容を削除し、クリップボードに保存します。
- Copy：選択内容のコピーをクリップボードに保存します。
- Paste：Paste ACE ダイアログボックスを開きます。このダイアログボックスでは、既存のルールから新しい ACL ルールを作成できます。
- No : ルールの評価順序を示します。暗黙のルールには番号が付けられず、ハイフンで表されます。
- Address : ACE が適用されるアプリケーションまたはサービスの IP アドレスまたは URL を表示します。
- Action：このフィルタがトラフィック フローを許可するか拒否するかを指定します。
- Description：ルールを追加したときに入力した説明が表示されます。　　暗黙のルールには、「Implicit outbound rule.」という説明が付けられます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Extended ACL タブ

このペインには、拡張 ACL に関する要約情報が表示され、このペインを使用して、ACL と ACE を追加または削除できます。

フィールド

- Add : 新しい ACL を追加できます。既存の ACL を選択すると、その ACL について新しい ACE を追加できます。
- Edit : Opens Edit ACE ダイアログボックスを開きます。このダイアログボックスでは、既存のアクセス コントロール リスト ルールを変更できます。
- Delete：ACL または ACE を削除します。確認されず、やり直しもできません。
- Move Up/Move Down：ACL Manager テーブルでのルールの位置を変更します。
- Cut：ACL Manager テーブルから選択内容を削除し、クリップボードに保存します。
- Copy：選択内容のコピーをクリップボードに保存します。
- Paste：Paste ACE ダイアログボックスを開きます。このダイアログボックスでは、既存のルールから新しい ACL ルールを作成できます。
- No：ルールの評価順序を示します。暗黙のルールには番号が付けられず、ハイフンで表されます。
- Enabled：ルールをイネーブルまたはディセーブルにします。暗黙のルールはディセーブルにできません。
- Source：Destination カラムにリストされている IP アドレスへのトラフィックの送信を許可または拒否する IP アドレス（ホストまたはネットワーク）を指定します。詳細モード（Show Detail オプション ボタンを参照）では、アドレス カラムに、単語 any が付いたインターフェイス名が含まれることがあります（inside: any など）。これは、内部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。
- Destination：Source カラムにリストされている IP アドレスへのトラフィックの送信を許可または拒否する IP アドレス（ホストまたはネットワーク）を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が含まれることがあります（outside: any など）。これは、外部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。アドレス カラムには、IP アドレスが含まれることもあります（209.165.201.1-209.165.201.30 など）。これらのアドレスは、変換済みアドレスです。内部ホストが外部ホストへの接続を作成すると、ファイアウォールは内部ホストのアドレスをプールのアドレスにマッピングします。ホストがアウトバウンド接続を作成した後、ファイアウォールはこのアドレス マッピングを維持します。アドレス マッピング構造は xlate と呼ばれ、一定の時間、メモリに保持されます。ACL で許可されていれば、この時間内に、外部ホストはプールの変換済みアドレスを使用して、内部ホストへの接続を開始できます。通常、内部ホストは常に同じ IP アドレスを使用するため、外部から内部への接続にはスタティック トランスレーションが必要です。
- Service：ルールで指定されるサービスとプロトコルの名前。
- Action：このフィルタがトラフィック フローを許可するか拒否するかを指定します。

- Logging：ログレベルと、ログ メッセージ間の間隔（秒単位）が表示されます（ACL のロギングをイネーブルにした場合）。ロギング オプション（ロギングのイネーブル化とディセーブル化を含む）を設定するには、このカラムを右クリックして、Edit Log Option を選択します。Log Options ウィンドウが表示されます。
- Time：このルールで適用される時間範囲の名前を指定します。
- Description：ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule.」という説明が付けられます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit/Paste ACE

ACL Manager > Add/Edit/Paste Extended ACE

Add/Edit/Paste ACE ダイアログボックスを使用して、新しい拡張アクセスリスト ルールの作成、または既存のルールの修正ができます。Paste オプションは、ルールを切り取りまたはコピーするときにだけ利用できるようになります。

フィールド

- Action：新しいルールのアクション タイプを決めます。permit または deny を選択します。
  - Permit：すべての一致したトラフィックを許可します。
  - Deny：すべての一致したトラフィックを拒否します。
- Source/Destination：送信元または宛先タイプを指定し、そのタイプに応じて、送信元または宛先ホストまたはネットワーク IP アドレスが記載されているその他の該当パラメータを指定します。使用できる値は、any、IP address、Network Object Group、および Interface IP です。その後のフィールドは、Type フィールドの値によって異なります。
  - any：その送信元または宛先ホストまたはネットワークがどのタイプでも可能であることを指定します。Type フィールドのこの値については、Source または Destination 領域にその他のフィールドがありません。
  - IP Address：送信元または宛先ホストまたはネットワークの IP アドレスを指定します。このフィールドを選択すると、IP Address、省略符号ボタン、および Netmask フィールドが利用できるようになります。Select IP アドレスまたはホスト名を IP Address フィールドのドロップダウン リストから選択するか、省略符号（...）ボタンをクリックして、IP アドレスまたは名前を参照します。ネットワーク マスクをドロップダウン リストから選択します。
  - Network Object Group：ネットワーク オブジェクト グループの名前を指定します。ドロップダウン リストから名前を選択するか、省略符号（...）ボタンをクリックして、ネットワーク オブジェクト グループ名を参照します。
  - Interface IP：ホストまたはネットワークが存在するインターフェイスを指定します。インターフェイスをドロップダウン リストから選択します。デフォルト値は、inside と outside です。参照機能はありません。
- Protocol and Service：この ACE フィルタが適用されるプロトコルとサービスを指定します。サービス グループを使用して、ACL と一致させる複数の連続していないポート番号を識別できます。たとえば、ポート番号 5、8、9 で HTTP および FTP をフィルタリングする場合は、これらのすべてのポートを含むサービス グループを定義します。サービス グループを使用しない場合は、ポートごとに個別のルールを作成する必要があります。

TCP、UDP、TCP-UDP、ICMP、およびその他の IP プロトコル用にサービス グループを作成できます。TCP-UDP プロトコルを使用するサービス グループには、TCP または UDP プロトコルを使用するサービス、ポート、および範囲が含まれます。

- Protocol：このルールが適用されるプロトコルを選択します。使用できる値は、ip、tcp、udp、icmp などです。Protocol and Service 領域のその他のフィールドは、選択するプロトコルによって異なります。次の項目で、各選択内容の結果について説明します。
- Protocol: TCP and UDP：そのルールの TCP/UDP プロトコルを選択します。Source Port 領域と Destination Port 領域で、ACL がパケットを照合するために使用するポートを指定できます。
- Source Port/Destination Port：（*TCP* および *UDP* プロトコルの場合のみ使用可能）演算子、ポート番号、ポート範囲、またはサービスのリストにあるウェルノウン サービス名（HTTP や FTP など）を指定します。演算子リストで、ACL がポートを照合する方法を指定します。次のいずれかの演算子を選択します。=（ポート番号と等しい）、not =（ポート番号と等しくない）、>（ポート番号より大きい）、<（ポート番号より小さい）、range（範囲内のポート番号のいずれかと等しい）。
- Group：（*TCP* と *UDP* プロトコルの場合のみ使用可能）送信元ポート サービス グループを選択します。Browse (...) ボタンをクリックすると、Browse Source Port または Browse Destination Port ダイアログボックスが開きます。
- Protocol: ICMP：定義済みリストから ICMP タイプまたは ICMP グループを選択するか、browse （...）をクリックして、ICMP グループを選択できます。Browse ボタンをクリックすると、Browse ICMP ダイアログボックスが表示されます。
- Protocol: IP：IP プロトコル ボックスで、そのルールの IP プロトコルを指定します。このフィールドを選択した場合、他のフィールドは表示されません。
- Protocol: Other：ドロップダウン リストからプロトコルまたはプロトコル グループを選択、またはプロトコル グループを参照できます。Browse (...) ボタンをクリックすると、Browse Other ダイアログボックスが表示されます。

- Rule Flow Diagram：（表示のみ）設定済みのルール フローをグラフィカルに表示します。この表示を明示的に閉じない限り、ACL Manager ダイアログボックスに同じ図が表示されます。
- Options：ロギング パラメータ、時間範囲、説明など、このルールのオプション機能を設定します。
  - Logging：ロギングをイネーブルまたはディセーブルにします。または、デフォルト ロギング設定を使用するように指定します。ロギングをイネーブルにすると、Syslog Level および Log Interval フィールドが使用可能になります。
  - Syslog Level：ロギング アクティビティのレベルを選択します。デフォルトは Informational です。
  - Log Interval：許可および拒否のロギング間隔を指定します。デフォルトは 300 秒です。範囲は 1 ～ 6000 秒です。
  - Time Range：このルールを使用する時間範囲の名前を選択します。デフォルトは (any) です。Browse (...) ボタンをクリックして Browse Time Range ダイアログボックスを開き、時間範囲を選択または追加します。
  - Description：（オプション）このルールの簡単な説明を示します。説明行の長さは最大 100 文字ですが、説明を改行して複数行にすることができます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse Source/Destination Address

ACL Manager > Add/Edit Extended Access List Rule > Source or Destination > Browse ボタン

Browse Source or Destination Address ダイアログボックスを使用して、このルールの送信元または宛先として使用するオブジェクトを選択できます。

フィールド

- Type：このルールの送信元または宛先として使用するオブジェクトのタイプを決めます。選択肢は、IP Address Objects、IP Names、Network Object Groups、および All です。このフィールドに続くテーブルの内容は、選択内容によって変わります。
- Source/Destination Object Table : 送信元または宛先オブジェクトの選択元オブジェクトを表示します。type フィールドで All を選択すると、各カテゴリのオブジェクトが、それぞれの見出しの下に表示されます。テーブルの見出しは次のとおりです。
  - Name：各オブジェクトのネットワーク名（IP アドレスの場合もあります）を表示します。
  - IP address：各オブジェクトの IP アドレスを表示します。
  - Netmask：各オブジェクトで使用するネットワーク マスクを表示します。
  - Description：Add/Edit/Paste Extended Access List Rule ダイアログボックスに入力された説明を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse Source/Destination Port

ACL Manager > Add/Edit Extended Access List Rule > Protocol and Service > Protocol: tcp or udp >Source or Destination Port > Group オプション > Browse ボタン

Browse Source or Destination Port ダイアログボックスを使用して、このルールのこのプロトコルの送信元または宛先ポートを選択できます。

フィールド

- Add：Add TCP Service Group ダイアログボックスを開きます。このダイアログボックスで、新しい TCP サービス グループを設定できます。
- Find：Filter フィールドを開きます。
- Filter/Clear : Name リストの項目を検索するために使用できるフィルタ規準を指定します。その規準に一致する項目だけが表示されます。Filter フィールドに入力すると、Filter ボタンがアクティブになります。Filter ボタンをクリックすると、検索が実行されます。検索を実行した後は、Filter ボタンがグレー表示になり、Clear ボタンがアクティブになります。Clear ボタンをクリックすると、filter フィールドがクリアされ、Clear ボタンがグレー表示になります。
- Type：このルールの送信元または宛先として使用するオブジェクトのタイプを決めます。選択肢は、IP Address Objects、IP Names、Network Object Groups、および All です。このフィールドに続くテーブルの内容は、選択肢によって変わります。
- Name：選択したタイプの定義済みプロトコルとサービス グループを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add TCP Service Group

ACL Manager > Add/Edit Extended Access List Rule > Protocol and Service > Protocol: tcp or udp >Source or Destination Port > Group オプション > Browse ボタン > Browse Source or Destination Port > Add ボタン

Add TCP Service Group ダイアログボックスを使用して、新しい TCP サービス グループまたはポートを設定し、このルールでこのプロトコルに使用する参照可能な送信元または宛先ポート リストに追加できます。Members not in Group リストまたは Members in Group リストのメンバーを選択すると、Add と Remove ボタンがアクティブになります。

フィールド

- Group Name：新しい TCP サービス グループの名前を指定します。
- Description：（オプション）このグループの簡単な説明を示します。
- Members not in Group：Members in Group リストに追加するサービスまたはサービス グループ、あるいはポート番号を選択するためのオプションを表示します。
- Service/Service Group：Members in Group リストに追加する TCP サービスまたはサービス グループの名前を選択するためのオプションを選択します。
- Port # : Members in Group リストに追加するポート番号の範囲を指定するためのオプションを選択します。
- Add：選択した項目を Members not in Group リストから Members in Group リストに移動します。
- Remove：選択した項目を Members in Group リストから Members not in Group リストに移動します。
- Members in Group：すでにこのサービス グループで設定されているメンバーを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse ICMP

ACL Manager > Add/Edit Extended Access List Rule > Protocol and Service > Protocol: icmp >ICMP > Group オプション > Browse ボタン

Browse ICMP ダイアログボックスを使用して、このルールの ICMP グループを選択します。

フィールド

- Add：Add ICMP Group ダイアログボックスを開きます。このダイアログボックスで、新しい TCP サービス グループを設定できます。
- Find：Filter フィールドを開きます。
- Filter/Clear：Name リストの項目を検索するために使用できるフィルタ基準を指定します。その基準に一致する項目だけが表示されます。Filter フィールドに入力すると、Filter ボタンがアクティブになります。Filter ボタンをクリックすると、検索が実行されます。検索を実行した後は、Filter ボタンがグレー表示になり、Clear ボタンがアクティブになります。Clear ボタンをクリックすると、filter フィールドがクリアされ、Clear ボタンがグレー表示になります。
- Type：このルールの ICMP グループとして使用するオブジェクトのタイプを決めます。選択肢は、IP Address Objects、IP Names、Network Object Groups、および All です。このフィールドに続くテーブルの内容は、選択肢によって変わります。
- Name：選択したタイプを対象とする定義済みの ICMP グループを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add ICMP Group

ACL Manager > Add/Edit Extended Access List Rule > Protocol and Service > Protocol: icmp >ICMP > Group オプション > Browse ボタン > Browse ICMP > Add ボタン

Add ICMP Group ダイアログボックスを使用して、新しい ICMP グループの名前または番号を設定して、このルールでのプロトコルに使用する参照可能な ICMP リストに追加できます。Members not in Group リストまたは Members in Group リストのメンバーを選択すると、Add と Remove ボタンがアクティブになります。

フィールド

- Group Name：新しい TCP サービス グループの名前を指定します。
- Description：（オプション）このグループの簡単な説明を示します。
- Members not in Group：Members in Group リストに追加する ICMP タイプ /ICMP グループまたは ICMP 番号を選択するためのオプションを表示します。
- ICMP Type/ICMP Group：Members in Group リストに追加する ICMP グループの名前を選択するためのオプションを選択します。
- ICMP #：Members in Group リストに追加する ICMP メンバーを番号で指定するためのオプションを選択します。
- Add：選択した項目を Members not in Group リストから Members in Group リストに移動します。
- Remove：選択した項目を Members in Group リストから Members not in Group リストに移動します。

- Members in Group : すでにこのサービス グループで設定されているメンバーを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse Other

ACL Manager > Add/Edit Extended Access List Rule > Protocol and Service > Protocol: other >Other > Group オプション > Browse ボタン

Browse Other ダイアログボックスを使用して、このルールのプロトコル グループを選択します。

フィールド

- Add：Add Protocol Group ダイアログボックスを開きます。このダイアログボックスで、新しいサービス グループを設定できます。
- Find：Filter フィールドを開きます。
- Filter/Clear : Name リストの項目を検索するために使用できるフィルタ基準を指定します。その基準に一致する項目だけが表示されます。Filter フィールドに入力すると、Filter ボタンがアクティブになります。Filter ボタンをクリックすると、検索が実行されます。検索を実行した後は、Filter ボタンがグレー表示になり、Clear ボタンがアクティブになります。Clear ボタンをクリックすると、filter フィールドがクリアされ、Clear ボタンがグレー表示になります。
- Type：このルールのプロトコル グループとして使用するオブジェクトのタイプを決めます。選択肢は、IP Address Objects、IP Names、Network Object Groups、および All です。このフィールドに続くテーブルの内容は、選択内容によって変わります。
- Name：選択したタイプを対象とする定義済みのプロトコル グループを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add Protocol Group

ACL Manager > Add/Edit Extended Access List Rule > Protocol and Service > Protocol: other > Group オプション > Browse ボタン > Browse Other > Add ボタン

Add Protocol Group ダイアログボックスを使用して、新しいプロトコル グループの名前または番号を設定して、このルールでのプロトコルに使用する参照可能なプロトコル リストに追加できます。Members not in Group リストまたは Members in Group リストのメンバーを選択すると、Add と Remove ボタンがアクティブになります。

フィールド

- Group Name：新しい TCP サービス グループの名前を指定します。
- Description：（オプション）このグループの簡単な説明を示します。
- Members not in Group：Members in Group リストに追加するプロトコル / プロトコル グループまたはプロトコル番号を選択するためのオプションを表示します。
- Protocol/Protocol Group：Members in Group リストに追加するプロトコルまたはプロトコル グループの名前を選択するためのオプションを選択します。
- Protocol #：Members in Group リストに追加するプロトコルを番号で指定するためのオプションを選択します。
- Add：選択した項目を Members not in Group リストから Members in Group リストに移動します。
- Remove：選択した項目を Members in Group リストから Members not in Group リストに移動します。
- Members in Group：すでにこのサービス グループで設定されているメンバーを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Internal Group Policy > IPSec タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > IPSec タブ

Add or Edit Group Policy ウィンドウの IPSec タブを使用して、追加または修正するグループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。

フィールド

- Inherit：（複数のインスタンス）対応する設定の値をデフォルト グループ ポリシーから取得できます。このタブのアトリビュートすべてのデフォルト オプションです。
- Re-Authentication on IKE Re-key：Inherit チェックボックスがオフである場合に、IKE キーの再生成が行われたときの再認証をイネーブルまたはディセーブルにします。
- IP Compression：Inherit チェックボックスがオフである場合に、IP Compression をイネーブルまたはディセーブルにします。
- Perfect Forward Secrecy：Inherit チェックボックスがオフである場合に、完全転送秘密（PFS）をイネーブルまたはディセーブルにします。PFS は、特定の IPSec SA のキーが他のシークレット（他のキーなど）から導出されたものでないことを保証します。つまり、PFS では、攻撃者があるキーを突破しても、そこから他のキーを導出することはできないことが保証されます。PFS がイネーブルになっていない場合は、IKE SA の秘密鍵が突破されると、その攻撃者は、IPSec のすべての保護データをコピーし、IKE SA のシークレットの知識を使用して、その IKE SA によって設定された IPSec SA のセキュリティを侵すことができると推測されます。PFS を使用すると、攻撃者が IKE を突破しても、直接 IPSec にアクセスすることはできません。その場合、攻撃者は各 IPSec SA を個別に突破する必要があります。
- Tunnel Group Lock：Inherit チェックボックスまたは値 None が選択されていない場合に、リストから選択したトンネル グループのロックをイネーブルにします。
- Client Access Rules：最大 25 のクライアント アクセス ルールを設定できます。Inherit チェックボックスを選択解除すると、Add、Edit、および Delete ボタンがアクティブになり、次のカラム見出しがテーブルに表示されます。

- Priority：このルールの優先順位が表示されます。
- Action：このルールがアクセスを許可するか拒否するかを指定します。
- Client Type：このルールを適用する VPN クライアントのタイプ（ソフトウェアまたはハードウェア）を指定します。ソフトウェア クライアントの場合は、すべての Windows クライアントかサブセットかを指定します。
- VPN Client Version：このルールを適用する VPN クライアントのバージョンを指定します（複数可）。このボックスには、このクライアントに適用されるソフトウェアまたはファームウェア イメージのカンマ区切りリストが含まれます。

- Add：IPSec グループ ポリシーの新しいルールを追加します。このボタンは、Inherit チェックボックスが選択解除されている場合にだけアクティブになります。
- Edit：IPSec グループ ポリシーの既存のルールを修正します。このボタンは、Inherit チェックボックスが選択解除されている場合にだけアクティブになります。
- Delete：IPSec グループ ポリシーの既存のルールを削除します。このボタンは、Inherit チェックボックスが選択解除されている場合にだけアクティブになります。確認されず、やり直しもできません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Client Access Rule

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > IPSec > Add or Edit Client Access Rule

Add or Edit Client Access Rule ウィンドウは、Add or Edit Group Policy ウィンドウの IPSec タブから生成され、このウィンドウで、IPSec グループ ポリシーの新しいクライアント アクセス ルールを追加するか、既存のルールを修正します。

フィールド

- Priority：このルールの優先順位が表示されます。
- Action：このルールがアクセスを許可するか拒否するかを指定します。
- VPN Client Type：このルールを適用する VPN クライアントのタイプ（ソフトウェアまたはハードウェア）を指定します。ソフトウェア クライアントの場合は、すべての Windows クライアントかサブセットかを指定します。VPN クライアント タイプの共通値としては、VPN 3002、PIX、Linux、*（すべてのクライアント タイプと一致）、Win9x（Windows 95、Windows 98、および Windows ME）、および WinNT（Windows NT、Windows 2000、および Windows XP）があります。* を選択した場合は、Windows NT など、個々の Windows のタイプを設定しません。
- VPN Client Version：このルールを適用する VPN クライアントのバージョンを指定します（複数可）。このボックスには、このクライアントに適用されるソフトウェアまたはファームウェア イメージのカンマ区切りリストが含まれます。次の警告が適用されます。
  - このクライアントのソフトウェア バージョンを指定する必要があります。* を指定して、任意のバージョンと一致させることができます。
  - 自分のエントリが、VPN クライアントの場合には URL と、VPN 3002 の場合には TFTP サーバと正確に一致する必要があります。

- ハードウェア クライアント イメージを配布するための TFTP サーバは堅牢である必要があります。
- クライアントがリストにあるソフトウェア バージョンをすでに実行している場合、ソフトウェアをアップデートする必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していなくても、更新は正しく実行されます。
- VPN クライアント ユーザは、一覧表示されている URL から適切なソフトウェア バージョンをダウンロードする必要があります。
- VPN 3002 ハードウェア クライアント ソフトウェアは、自動的に TFTP 経由でアップデートされます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Internal Group Policy > Client Configuration タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Client Configuration タブ

Add or Edit Group Policy ウィンドウの Client Configuration タブには、全般的なクライアント パラメータ、Cisco クライアント パラメータ、および Microsoft クライアント パラメータを設定する 3 つのタブがあります。

個々のタブの詳細については、次のリンクを参照してください。

- Add/Edit Internal Group Policy > Client Configuration タブ > General Client Parameters タブ
- Add/Edit Internal Group Policy > Client Configuration タブ > Cisco Client Parameters タブ
- Add/Edit Internal Group Policy > Client Configuration タブ > Microsoft Client Parameters タブ

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Internal Group Policy > Client Configuration タブ > General Client Parameters タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Client Configuration タブ >General Client Parameters タブ

このタブでは、バナー テキスト、デフォルト ドメイン、スプリット トンネル パラメータ、アドレス プールなど、Cisco クライアントと Microsoft クライアントに共通のクライアント アトリビュートを設定します。

フィールド

- Inherit：（複数のインスタンス）対応する設定の値をデフォルト グループ ポリシーから取得できます。Inherit チェックボックスを選択解除すると、パラメータのその他のオプションが使用できるようになります。このタブのアトリビュートすべてのデフォルト オプションです。
- Banner：デフォルト グループ ポリシーからバナーを継承するか、新しいバナー テキストを入力するかを指定します。詳細については、「View/Config Banner」を参照してください。
- Edit Banner：View/Config Banner ダイアログボックスが表示され、500 文字までのバナー テキストを入力できます。
- Default Domain：デフォルト グループ ポリシーからデフォルト ドメインを継承するか、このフィールドで指定する新しいデフォルト ドメインを使用するかを指定します。
- Split Tunnel DNS Names (space delimited)：デフォルト グループ ポリシーからスプリット トンネル DNS 名を継承するか、このフィールドで新しい名前または名前のリストを指定するかを指定します。
- Split Tunnel Policy：デフォルト グループ ポリシーからスプリット トンネル ポリシーを継承するか、メニューからポリシーを選択するかを指定します。メニュー オプションは、すべてのネットワークをトンネリングする、下のネットワーク リストに含まれるネットワークをトンネリングする、または下のネットワーク リストに含まれるネットワークを除外するです。
- Split Tunnel Network List：デフォルト グループ ポリシーからスプリットトンネル ネットワーク リストを継承するか、ドロップダウン リストから選択するかを指定します。
- Manage：ACL Manager ダイアログボックスを開き、標準および拡張アクセス コントロール リストを管理できます。
- Address Pools：このグループ ポリシーを通じて使用できるアドレス プールを設定します。
  - Available Pools：リモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定します。Inherit チェックボックスが選択解除され、Assigned Pools リストにアドレス プールがない場合、アドレス プールは設定されず、グループ ポリシーの他のソースから継承されません。
  - Add：アドレス プールの名前を Available Pools リストから Assigned Pools リストに移動します。
  - Remove：アドレス プールの名前を Assigned Pools リストから Available Pools リストに移動します。
  - Assigned Pools (up to 6 entries)：割り当て済みプール リストに追加したアドレス プールをリストします。このテーブルのアドレス プール設定は、グループのローカル プール設定を上書きします。6 つまでのローカル アドレス プールのリストを指定し、ローカル アドレス割り当てに使用できます。プールを指定する順番が重要です。このコマンドにあるプールの順番に従って、セキュリティ アプライアンスがアドレスを割り当てます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

View/Config Banner

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Client Configuration > Edit Banner > View/Config Banner

View/Config Banner ダイアログボックスを使用して、指定されているクライアントのバナーとして表示する最大 500 文字のテキストをテキストボックスに入力します。

（注） Enter キーを押したときに作成される復帰または改行は 2 文字としてカウントされます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Internal Group Policy > Client Configuration タブ > Cisco Client Parameters タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Client Configuration タブ >Cisco Client Parameters タブ

このタブでは、パスワード保管など、IPSec over UDP のイネーブルまたはディセーブル化、UDP ポート番号の設定、IPSec バックアップ サーバの設定など、Cisco クライアントに固有のクライアント アトリビュートを設定します。

フィールド

- Store Password on Client System：クライアント システムでのパスワードの保管をイネーブルまたはディセーブルにします。

（注） パスワードをクライアント システムで保管すると、潜在的なセキュリティ リスクが発生します。

- IPSec over UDP：IPSec over UDP の使用をイネーブルまたはディセーブルにします。
- IPSec over UDP Port：IPSec over UDP で使用する UDP ポートを指定します。
- IPSec Backup Servers：Server Configuration フィールドと Server IP Addresses フィールドをアクティブにします。これによって、これらの値が継承されない場合に使用する UDP バックアップ サーバを指定できます。
- Server Configuration：IPSec バックアップ サーバとして使用するサーバ設定オプションを一覧表示します。使用できるオプションは、Keep Client Configuration（デフォルト）、Use Backup Servers Below、および Clear Client Configuration です。
- Server Addresses （space delimited）：IPSec バックアップ サーバの IP アドレスを指定します。このフィールドは、Server Configuration で選択した値が Use Backup Servers Below である場合にだけ使用できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Internal Group Policy > Client Configuration タブ > Microsoft Client Parameters タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Client Configuration タブ >Microsoft Client Parameters タブ

このタブでは、Microsoft クライアントに固有のクライアント アトリビュート（特に、Microsoft Internet Explorer 用のプロキシ サーバ パラメータ）を設定します。

フィールド

- Proxy Server Policy：クライアント PC の Microsoft Internet Explorer ブラウザのプロキシ アクション（「メソッド」）を設定します。
  - Do not modify client proxy settings：このクライアント PC の Internet Explorer の HTTP ブラウザ プロキシ サーバ設定を変更しません。
  - Do not use proxy：クライアント PC の Internet Explorer の HTTP プロキシ設定をディセーブルにします。
  - Auto-detect proxy：クライアント PC で、Internet Explorer の自動プロキシ サーバ検出の使用をイネーブルにします。
  - Use proxy server settings specified below：Proxy Server Name or IP Address フィールドで設定された値を使用するように、Internet Explorer の HTTP プロキシ サーバ設定値を設定します。
- Proxy Server Settings：Microsoft Internet Explorer を使用して、Microsoft クライアントのプロキシ サーバ パラメータを設定します。
  - Proxy Server Name or IP Address：このクライアント PC に適用する Microsoft Internet Explorer サーバの IP アドレスまたは名前を指定します。

（注） ASDM を使用して、プロキシ サーバ名または IP アドレスを設定できます。サーバのほかに使用するオプションのポートを設定するには、group-policy　設定モードで **msie-proxy server** コマンドを使用する必要があります。

  - Bypass Proxy Server for Local Addresses：クライアント PC の Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定値を設定します。Yes を選択するとローカル バイパスがイネーブルになり、No を選択するとローカル バイパスがディセーブルになります。
  - Proxy Server Exception List：クライアント PC のローカル バイパス用 Microsoft Internet Explorer ブラウザ プロキシ例外リスト設定値を設定します。プロキシ サーバ経由のアクセスを行わないアドレスのリストを入力します。このリストは、Internet Explorer の Proxy Settings ダイアログボックスにある Exceptions ボックスに相当します。
  - Name or IP Address (use * as a wildcard)：このクライアント PC に適用する MSIE サーバの IP アドレスまたは名前を指定します。
  - Add：指定した名前または IP アドレスを Proxy Server Exceptions 例外リストに追加します。
  - Delete：指定した名前または IP アドレスを Proxy Server Exceptions リストから削除します。

- Proxy Server Exceptions：プロキシ サーバ アクセスから除外するサーバ名および IP アドレスをリストします。このリストは、Internet Explorer の Proxy Settings ダイアログボックスにある Exceptions ボックスに相当します。

- DHCP Intercept : DHCP 代行受信をイネーブルまたはディセーブルにします。DHCP 代行受信を使用すると、Microsoft XP クライアントがセキュリティ アプライアンスでスプリットトンネリングを使用できるようになります。セキュリティ アプライアンスは、DHCP 情報のメッセージを Microsoft Windows XP クライアントに直接返信します。このメッセージには、トンネルの IP アドレスのサブネット マスク、ドメイン名、クラスのないスタティック ルートが含まれます。XP 以前の Windows クライアントでは、DHCP 代行受信はドメイン名とサブネット マスクを提供します。これは、DHCP サーバを使用するのに利点が少ない環境で便利です。

（注） Microsoft Windows XP では、スプリット トンネル オプションが 255 バイトを超えると、ドメイン名が壊れます。この問題を回避するために、セキュリティ アプライアンスは、送信するルート数を 27 ～ 40 ルートに制限します。このルート数は、ルートのクラスによって異なります。

  - Intercept DHCP Configure Message：グループ ポリシーから DHCP 代行受信ポリシーを継承するか、DHCP ポリシーをイネーブル（Yes）またはディセーブル（No）にするかを指定します。
  - Subnet Mask (optional)：ドロップダウン リストからサブネット マスクを選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Standard Access List Rule

ACL Manager > Add or Edit Standard Access List Rule

Add/Edit Standard Access List Rule ダイアログボックスを使用して、新しいルールの作成、または既存のルールの修正ができます。

フィールド

- Action：新しいルールのアクション タイプを決めます。permit または deny を選択します。
  - Permit：すべての一致したトラフィックを許可します。
  - Deny：すべての一致したトラフィックを拒否します。
- Host/Network IP Address：IP アドレスによってネットワークを識別します。
  - IP address：ホストまたはネットワークの IP アドレス。
  - Mask：ホストまたはネットワークのサブネット マスク。
- Description：（オプション）アクセス ルールの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Internal Group Policy > Client Firewall タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Client Firewall タブ

Add or Edit Group Policy ウィンドウの Client Firewall タブでは、追加または変更するグループ ポリシーに対して VPN クライアントのファイアウォール設定を指定できます。

（注） これらのファイアウォール機能を使用できるのは、Microsoft Windows を実行する VPN クライアントだけです。現在、ハードウェア クライアントまたは他の（Windows 以外の）ソフトウェア クライアントでは、これらの機能は使用できません。

ファイアウォールは、インバウンドおよびアウトバウンドの各データ パケットを検査し、許可するかドロップするかを判断することによって、コンピュータをインターネットから隔離し、保護します。ファイアウォールは、グループのリモート ユーザがスプリット トンネリングを設定してある場合、セキュリティの向上をもたらします。この場合、ファイアウォールは、インターネットまたはユーザのローカル LAN を経由する侵入からユーザの PC を保護することで、企業ネットワークを保護します。VPN クライアントを使用してセキュリティ アプライアンスに接続しているリモート ユーザは、適切なファイアウォール オプションを選択できます。

最初のシナリオでは、リモート ユーザの PC 上にパーソナル ファイアウォールがインストールされています。VPN クライアントは、ローカル ファイアウォールで定義されているファイアウォール ポリシーを適用し、そのファイアウォールが実行されていることを確認するために監視します。ファイアウォールの実行が停止すると、VPN クライアントはセキュリティ アプライアンスへの通信をドロップします（このファイアウール適用メカニズムは、*Are You There*（*AYT*）と呼ばれます。VPN クライアントが、定期的に「are you there?」メッセージを送信することによってファイアウォールを監視するからです。応答が返されない場合、VPN クライアントは、ファイアウォールがダウンしてセキュリティ アプライアンスへの接続が終了したことを認識します）。ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合もありますが、この方法を使用すれば、ユーザは各自の設定をカスタマイズできます。

第 2 のシナリオでは、VPN クライアント PC のパーソナル ファイアウォールに中央集中型ファイアウォール ポリシーを適用することが選択されることがあります。一般的な例としては、スプリット トンネリングを使用してグループのリモート PC へのインターネット トラフィックをブロックすることがあげられます。この方法は、トンネルが確立されている間、インターネット経由の侵入から PC を保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、プッシュ ポリシーまたは *Central Protection Policy*（*CPP*）と呼ばれます。セキュリティ アプライアンスでは、VPN クライアントに適用するトラフィック管理規則のセットを作成し、これらの規則をフィルタに関連付けて、そのフィルタをファイアウォール ポリシーに指定します。セキュリティ アプライアンスは、このポリシーを VPN クライアントまで配信します。その後、VPN クライアントはポリシーをローカル ファイアウォールに渡し、そこでポリシーが適用されます。

フィールド

- Inherit: グループ ポリシーがデフォルト グループ ポリシーからクライアントのファイアウォール設定を取得するかどうかを決めます。このオプションはデフォルト設定です。設定すると、このタブにある残りのアトリビュートがその設定によって上書きされ、名前がグレー表示になります。
- Client Firewall Attributes : 実装されているファイアウォールのタイプ（実装されている場合）やそのファイアウォールのポリシーなど、クライアント ファイアウォール アトリビュートを指定します。
- Firewall Setting : ファイアウォールが存在するかどうかを一覧表示します。存在する場合には、そのファイアウォールが必須かオプションかを一覧表示します。No Firewall（デフォルト）を選択すると、このウィンドウにある残りのフィールドは、いずれもアクティブになりません。このグループのユーザをファイアウォールで保護する場合は、Firewall Required または Firewall Optional 設定を選択します。

  Firewall Required を選択した場合は、このグループのユーザ全員が、指定されたファイアウォールを使用する必要があります。セキュリティ アプライアンスは、指定された、サポートされているファイアウォールがインストールおよび実行されていない状態で接続を試行したセッションをドロップします。この場合、セキュリティ アプライアンスは、ファイアウォール設定が一致しないことを VPN クライアントに通知します。

（注）　グループでファイアウォールを必須にする場合には、そのグループに Windows VPN クライアント以外のクライアントが存在しないことを確認してください。Windows VPN クライアント以外のクライアント（クライアント モードの ASA 5505 と VPN 3002 ハードウェア クライアントを含む）は接続できません。

  このグループに、まだファイアウォールに対応していないリモート ユーザがいる場合は、Firewall Optional を選択します。Firewall Optional 設定を使用すると、グループ内のすべてのユーザが接続できるようになります。ファイアウォールに対応しているユーザは、ファイアウォールを使用できます。ファイアウォールなしで接続するユーザには、警告メッセージが表示されます。この設定は、一部のユーザがファイアウォールをサポートしており、他のユーザがサポートしていないグループを作成するときに役立ちます。たとえば、移行途中のグループでは、一部のメンバはファイアウォール機能を設定し、別のユーザはまだ設定していないことがあります。

- Firewall Type : Cisco を含む複数のベンダーのファイアウォールを一覧表示します。 Custom Firewall を選択すると、Custom Firewall の下のフィールドがアクティブになります。指定したファイアウォールが、使用できるファイアウォール ポリシーと相関している必要があります。設定したファイアウォールにより、サポートされるファイアウォール ポリシー オプションが決まります。
- Custom Firewall : カスタム ファイアウォールのベンダー ID、製品 ID、および説明を指定します。
  - Vendor ID : このグループ ポリシーのカスタム ファイアウォールのベンダーを指定します。
  - Product ID : このグループ ポリシー用に設定されるカスタム ファイアウォールの製品またはモデル名を指定します。
  - Description :（オプション）カスタム ファイアウォールについて説明します。
- Firewall Policy : カスタム ファイアウォール ポリシーのタイプと送信元を指定します。
  - Policy defined by remote firewall (AYT) : ファイアウォール ポリシーがリモート ファイアウォールによって定義されるように指定します（Are You There）。Policy defined by remote firewall（AYT）は、このグループのリモート ユーザのファイアウォールが、各自の PC に存在することを意味しています。このローカル ファイアウォールが、VPN クライアントにファイアウォール ポリシーを適用します。セキュリティ アプライアンスは、指定されたファイアウォールがインストールされ、実行中である場合にだけ、このグループの VPN クライアントが接続できるようにします。指定されたファイアウォールが実行されていない場合、接続は失敗します。接続が確立すると、VPN クライアントがファイアウォールを 30 秒ごとにポーリングして、そのファイアウォールが実行されていることを確認します。ファイアウォールの実行が停止すると、VPN クライアントはセッションを終了します。

- Policy pushed (CPP) : ポリシーがピアからプッシュされるように指定します。このオプションを選択する場合は、Inbound Traffic Policy および Outbound Traffic Policy リストと Manage ボタンがアクティブになります。セキュリティ アプライアンスは、Policy Pushed (CPP) ドロップダウン メニューで選択されたフィルタによって定義されるトラフィック管理ルールをこのグループの VPN クライアントに適用します。メニューで使用できる選択肢は、このセキュリティ アプライアンスで定義されているフィルタで、デフォルト フィルタも含まれます。セキュリティ アプライアンスがこれらのルールを VPN クライアントにプッシュすることに注意してください。セキュリティ アプライアンスではなく VPN クライアントから見たルールを作成し、定義する必要があります。たとえば、「in」と「out」はそれぞれ、VPN クライアントに着信するトラフィックと、VPN クライアントから発信されるトラフィックです。VPN クライアントにローカル ファイアウォールもある場合、セキュリティ アプライアンスからプッシュされたポリシーは、ローカル ファイアウォールのポリシーと同時に機能します。いずれかのファイアウォールのルールでブロックされたすべてのパケットがドロップされます。
- Inbound Traffic Policy : 着信トラフィックに対して使用できるプッシュ ポリシーを一覧表示します。
- Outbound Traffic Policy：発信トラフィックに対して使用できるプッシュ ポリシーを一覧表示します。
- Manage : ACL Manager ウィンドウを表示します。このウィンドウで、アクセス コントロール リスト（ACL）を設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Internal Group Policy > Hardware Client タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Hardware Client タブ

Add or Edit Group Policy ウィンドウの Hardware Client タブでは、追加または変更するグループ ポリシーに対して VPN 3002 ハードウェア クライアントの設定を指定できます。Hardware Client タブのパラメータは、クライアント モードの ASA 5505 とは無関係です。

フィールド

- Inherit :（複数インスタンス）対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。このタブのアトリビュートすべてのデフォルト設定です。
- Require Interactive Client Authentication : インタラクティブ クライアント認証の要求をイネーブルまたはディセーブルにします。このパラメータはデフォルトでディセーブルになっています。インタラクティブ ハードウェア クライアント認証は、VPN 3002 がトンネルを開始するたびに、手動で入力したユーザ名とパスワードで認証を行うように VPN 3002 に要求することによって、追加のセキュリティを提供します。この機能をイネーブルにすると、VPN 3002 はユーザ名とパスワードを保存しません。ユーザ名とパスワードを入力すると、VPN 3002 は接続するセキュリティ アプライアンスにクレデンシャルを送信します。セキュリティ アプライアンスは、内部または外部認証サーバを利用して認証を行います。ユーザ名とパスワードが有効な場合、トンネルが確立されます。

グループのインタラクティブ ハードウェア クライアント認証をイネーブルにすると、セキュリティ アプライアンスがグループ内の VPN 3002 にポリシーをプッシュします。以前、VPN 3002 でユーザおよびパスワードを設定していた場合、ソフトウェアによってコンフィギュレーション ファイルから削除されます。接続しようとすると、ソフトウェアによって、ユーザ名とパスワードを要求するプロンプトが表示されます。

後で、セキュリティ アプライアンスでグループのインタラクティブ ハードウェア認証をディセーブルにすると、VPN 3002 でローカルにイネーブルにされ、ユーザ名とパスワードを要求するプロンプトが表示され続けます。これによって、保存されたユーザ名およびパスワードがなく、セキュリティ アプライアンスでインタラクティブ ハードウェア クライアント認証がディセーブルにされても、VPN 3002 は接続できます。後で、ユーザ名とパスワードを設定し、機能をディセーブルにすると、プロンプトは表示されなくなります。VPN 3002 は、保存されたユーザ名とパスワードを使用して、セキュリティ アプライアンスに接続します。

- Require Individual User Authentication：クライアント モードの ASA 5505 またはグループ内の VPN 3002 ハードウェア クライアントの後ろにいるユーザに対する個々のユーザ認証の要求をイネーブルまたはディセーブルにします。グループ内のハードウェア クライアントにバナーを表示するには、個別ユーザ認証をイネーブルにする必要があります。このパラメータはデフォルトでディセーブルになっています。

  個別ユーザ認証は、VPN 3002 のプライベート ネットワークの許可されないユーザが中央サイトにアクセスできないように保護します。個別ユーザ認証をイネーブルにした場合、ハードウェア クライアントを介して接続する各ユーザは、トンネルがすでに存在していても、Web ブラウザを開いて手動で有効なユーザ名とパスワードを入力し、セキュリティ アプライアンスの後ろにあるネットワークにアクセスする必要があります。

（注）　ユーザ認証をイネーブルにした場合、コマンドライン インターフェイスを使用してログインすることはできません。ブラウザを使用する必要があります。

  セキュリティ アプライアンスの後ろにあるリモート ネットワークがデフォルト ホームページの場合、または、セキュリティ アプライアンスの後ろにあるリモート ネットワークの Web サイトをブラウザで開く場合、ハードウェア クライアントは、ユーザ ログイン用の適切なページをブラウザで開きます。正常にログインすると、元々入力していたページがブラウザに表示されます。

  セキュリティ アプライアンスの後ろにあるネットワークにある Web ベースではないリソース（電子メールなど）にアクセスしようとすると、ブラウザを使用して認証を行うまで、接続に失敗します。

  認証を行うには、ブラウザの Location フィールドまたは Address フィールドに、ハードウェア クライアントのプライベート インターフェイスの IP アドレスを入力する必要があります。ブラウザに、ハードウェア クライアントのログイン画面が表示されます。認証するには、Connect/Login Status ボタンをクリックします。

  1 人のユーザは、同時に最大 4 セッションのログインを実行できます。個別のユーザは、グループに対して設定された認証サーバの順序に従って認証されます。

- User Authentication Idle Timeout：ユーザ タイムアウト期間を設定します。セキュリティ アプライアンスは、この期間にユーザ トラフィックを受信しないと、接続を終了します。タイムアウト期間は、具体的な分数または無期限です。
  - Unlimited：接続がタイムアウトにならないように指定します。このオプションは、デフォルト グループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
  - Minutes：タイムアウト期間を分単位で指定します。1 ～ 35791394 の整数を使用します。デフォルト値は、Unlimited です。
- Cisco IP Phone Bypass：Cisco IP Phone にインタラクティブ個別ユーザ認証プロセスをバイパスさせます。イネーブルにした場合、ハードウェア クライアント認証は有効のままです。デフォルトでは、Cisco IP Phone Bypass はディセーブルになっています。

（注）　IP Phone 接続にネットワーク拡張モードを使用するように、クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアントを設定する必要があります。

- LEAP Bypass：シスコの無線デバイスからの LEAP パケットに、個々のユーザ認証プロセスをバイパスさせます（イネーブルの場合）。LEAP Bypass を使用して、ハードウェア クライアントの後ろにあるデバイスからの LEAP パケットを、ユーザ認証の前に VPN トンネルを通過させることができます。これによって、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。その後、ユーザ単位で再度認証を実行できます（イネーブルの場合）。デフォルトでは、LEAP Bypass はディセーブルになっています。

（注）　この機能は、インタラクティブ ハードウェア クライアント認証がイネーブルの場合、意図されたとおりに機能しません。

IEEE 802.1X は、有線および無線ネットワークにおける認証規格です。この規格は、クライアントと認証サーバの間の強力な相互認証を無線 LAN に提供します。ユーザごと、セッションごとのダイナミック WEP（wireless encryption privacy）鍵を提供することで、スタティック WEP 鍵で発生する管理作業とセキュリティ上の問題を軽減します。

シスコシステムズでは、Cisco LEAP という 802.1X 無線認証タイプを開発しています。LEAP は、無線クライアントと RADIUS サーバの間の接続における相互認証を実装します。パスワードなど、認証に使用されるクレデンシャルは、無線メディア上で送信される前に必ず暗号化されます。

（注）　Cisco LEAP は、RADIUS サーバに対して無線クライアントを認証します。RADIUS アカウンティング サービスは提供されません。

ハードウェア クライアントの後ろにいる LEAP ユーザには、面倒な問題があります。トンネルで中央サイト デバイスの後ろにある RADIUS サーバにクレデンシャルを送信することができないため、LEAP 認証をネゴシエートできません。トンネル経由でクレデンシャルを送信できない理由は、無線ネットワークで認証されていないためです。この問題を解決するために、LEAP バイパスは、個別のユーザ認証の前に LEAP パケット（LEAP パケットだけ）をトンネルで転送し、RADIUS サーバへの無線接続を認証できるようにします。これによって、ユーザは、個別のユーザ認証に進むことができます。

LEAP バイパスは、次の条件下で、意図されたとおりに機能します。

- インタラクティブ ユニット認証機能（有線デバイス用）が、ディセーブルであること。インタラクティブ ユニット認証がイネーブルの場合、トンネルを使用して LEAP デバイスが接続できるようになる前に、非 LEAP（有線）デバイスがハードウェア クライアントを認証する必要があります。
- 個別のユーザ認証がイネーブルであること（イネーブルでない場合、LEAP バイパスを使用する必要はありません）。
- 無線環境のアクセス ポイントが Cisco Aironet Access Point であること。PC の NIC カードは、他のブランドの製品でもかまいません。
- Cisco Aironet Access Point で、Cisco Discovery Protocol（CDP）を実行していること。
- ASA 5505 または VPN 3002 が、クライアント モードまたはネットワーク拡張モードで動作していること（どちらでもかまいません）。
- LEAP パケットが、ポート 1645 または 1812 経由で RADIUS サーバへのトンネルに転送されること。

（注）　未認証のトラフィックがトンネルを通過するのを許可すると、セキュリティ リスクが発生する可能性があります。

- Allow Network Extension Mode : ハードウェア クライアントでのネットワーク拡張モードの使用を制限します。このオプションを選択すると、ハードウェア クライアントがネットワーク拡張モードを使用できるようになります。Call Manager は実際の IP アドレスでのみ通信できるため、ハードウェア クライアントが IP Phone 接続をサポートするには、ネットワーク拡張モードが必要です。

（注）　ネットワーク拡張モードをディセーブルにすると（デフォルト設定）、ハードウェア クライアントはこのセキュリティ アプライアンスに PAT モードでのみ接続できるようになります。ここでネットワーク拡張モードを禁止するときは、グループ内のすべてのハードウェア クライアントを PAT モード用に設定してください。ネットワーク拡張モードを使用するようにハードウェア クライアントが設定されていて、接続しようとするセキュリティ アプライアンスがネットワーク拡張モードをディセーブルにしている場合、ハードウェア クライアントは 4 秒ごとに接続を試行し、すべての試行が拒否されます。この場合、ハードウェア クライアントは、接続しようとするセキュリティ アプライアンスに不要な処理負荷をかけることになります。多数のハードウェア クライアントがこのように誤設定されている場合、セキュリティ アプライアンスのサービス提供能力が損なわれます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Internal Group Policy > NAC タブ

Configuration > VPN > General > Group Policy > Add/Edit Internal Group Policy > NAC タブ

Add or Edit Internal Group Policy ウィンドウの NAC タブを使用して、デフォルト グループ ポリシーまたは代替グループ ポリシーのネットワーク アドミッション コントロールの設定値を設定できます。

フィールド

- Inherit :（複数インスタンス）対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。このタブのアトリビュートすべてのデフォルト設定です。
- Enable NAC : リモート アクセスに対してポスチャ検証を要求します。リモート コンピュータのポスチャが正しいことが確認されると、ACS サーバがセキュリティ アプライアンスで使用するアクセス ポリシーをダウンロードします。デフォルト設定は Disable です。
- Status Query Timer : セキュリティ アプライアンスは、ポスチャ検証とステータス クエリーの応答が成功するたびに、このタイマーを開始します。このタイマーの有効期限が過ぎると、ホスト ポスチャの変化を問い合せるクエリー（ステータス クエリー）が発行されます。秒単位で、30 ～ 1800 の数値を入力します。デフォルト設定は 300 です。

- Revalidation Timer：セキュリティ アプライアンスは、ポスチャ検証が成功するたびに、このタイマーを開始します。このタイマーの期限が切れると、次の無条件のポスチャ確認を開始します。セキュリティ アプライアンスは、再検証の間、ポスチャ検証を維持します。ポスチャ確認または再確認中に Access Control Server が使用できなくなると、デフォルト グループ ポリシーが有効になります。ポスチャを確認する間隔を秒数で入力します。範囲は 300 ～ 86400 です。デフォルト設定は 36000 です。
- Default ACL：（オプション）ポスチャ検証が失敗した場合、セキュリティ アプライアンスは、選択された ACL に関連付けられているセキュリティ ポリシーを適用します。None を選択するか、リストの拡張 ACL を選択します。デフォルト設定は None です。設定が None のときにポスチャ検証に失敗した場合、セキュリティ アプライアンスはデフォルト グループ ポリシーを適用します。

  Manage ボタンを使用して、ドロップダウン リストを読み込み、リストに ACL の設定を表示します。
- Manage：ACL Manager ダイアログボックスを開きます。クリックして、標準 ACL および各 ACL の ACE を表示、イネーブル化、ディセーブル化、削除します。Default ACL アトリビュートの横のリストに ACL が表示されます。
- Posture Validation Exception List：ポスチャ検証からリモート コンピュータを除外する 1 つ以上のアトリビュートが表示されます。少なくとも、エントリごとにオペレーティング システムと Enabled 設定（Yes または No）が表示されます。オプションのフィルタによって、リモート コンピュータの追加のアトリビュートと一致する ACL を識別します。ポスチャ検証からリモート コンピュータを除外するには、オペレーティング システムで構成されたエントリとフィルタの両方に一致する必要があります。セキュリティ アプライアンスは、Enabled 設定が No に設定されているエントリを無視します。
- Add：エントリを Posture Validation Exception リストに追加します。
- Edit：Posture Validation Exception リストのエントリを修正します。
- Delete：エントリを Posture Validation Exception リストから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Posture Validation Exception

Configuration > VPN > General > Group Policy > Add/Edit Internal Group Policy > NAC タブ > Add/Edit

Add/Edit Posture Validation Exception ダイアログ ウィンドウを使用して、オペレーティング システム、およびフィルタに一致するオプションのアトリビュートに基づいてリモート コンピュータをポスチャ検証から除外できます。

- Operating System：リモート コンピュータのオペレーティング システムを選択します。コンピュータでこのオペレーティング システムが実行されている場合は、ポスチャ検証から除外されます。デフォルト設定は None です。
- Enable：Enabled をオンにした場合にだけ、セキュリティ アプライアンスは、このウィンドウに表示されるアトリビュート設定がリモート コンピュータに存在するかどうかをチェックします。オフにした場合は、アトリビュート設定が無視されます。デフォルト設定はオフです。
- Filter：Filter（オプション）は、コンピュータのオペレーティング システムが Operating System アトリビュートの値に一致する場合に、トラフィックに ACL を適用してフィルタリングします。

- Manage : ACL Manager ダイアログボックスを開きます。クリックして、標準 ACL および各 ACL の ACE を表示、イネーブル化、ディセーブル化、削除します。Default ACL アトリビュートの横のリストに ACL が表示されます。このボタンを使用して、Filter アトリビュートの横のリストに入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

WebVPN タブ > Functions タブ

このパネルに移動するパスは数種類あります。

WebVPN タブ > Functions タブを使用して、WebVPN ユーザが使用できる機能を設定できます。WebVPN ユーザに表示されるインターフェイスは、ここで設定した値によって異なります。イネーブルにした機能だけを含む、カスタマイズされたホームページがユーザに表示されます。

- Inherit : 対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。
- Enable URL entry : URL 入力ボックスをホームページに配置します。この機能がイネーブルの場合、ユーザは URL 入力ボックスに Web アドレスを入力し、WebVPN を使用してこれらの Web サイトにアクセスできます。

  WebVPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。WebVPN は、企業ネットワーク上のリモート ユーザの PC やワークステーションとセキュリティ アプライアンスとの間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

  WebVPN 接続では、セキュリティ アプライアンスは、エンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。WebVPN ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュアな接続を確立し、そのサーバの SSL 証明書を検証します。エンド ユーザのブラウザは提示された SSL 証明書を受信しないため、この証明書を検証することはできません。現在の WebVPN の実装では、有効期限が切れた証明書を提供するサイトとの通信は許可されません。また、セキュリティ アプライアンスは、信頼済み CA 証明書の検証も実行しません。そのため、WebVPN ユーザは、SSL 対応 Web サーバと通信する前に、提供される証明書を分析できません。

  WebVPN ユーザのインターネット アクセスを制限するには、Enable URL Entry フィールドを選択解除します。これによって、WebVPN ユーザは、WebVPN 接続中に Web サーフィンができなくなります。
- Enable file server access : HTTPS を介した Windows ファイル アクセス（SMB/CIFS ファイルのみ）をイネーブルにします。このボックスを選択すると、ユーザはネットワーク上の Windows ファイルにアクセスできるようになります。WebVPN ファイル共有用にこのパラメータだけをイネーブルにした場合、ユーザは Servers and URLs 領域で設定されたサーバにのみアクセスできます。ユーザがサーバに直接アクセスしたり、ネットワーク上のサーバを参照できるようにするには、Enable file server entry および Enable file server browsing アトリビュートの説明を参照してください。

  このボックスをオンにすると、ユーザはファイルのダウンロード、編集、削除、名前変更、移動ができるようになります。ファイルとフォルダの追加もできます。

適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、ファイルにアクセスする前に、ユーザの認証が必要になります。

ファイル アクセス、サーバ / ドメイン アクセス、および参照を行うには、WINS サーバまたはマスター ブラウザ（通常、セキュリティ アプライアンスと同じネットワーク、またはそのネットワークから到達可能なネットワークに存在）を設定する必要があります。WINS サーバまたはマスター ブラウザは、セキュリティ アプライアンスにネットワーク上のリソースのリストを提供します。代わりに DNS サーバを使用することはできません。

（注）　ダイナミック DNS を同時に使用している場合、Active Native Directory 環境でファイル アクセスはサポートされません。WINS サーバを同時に使用している場合にサポートされます。

- Enable file server entry：ファイル サーバ入力ボックスをポータル ページに配置します。ファイル サーバ アクセスがイネーブルになっている必要があります。

  このボックスをオンにすると、ユーザは Windows ファイルのパス名を直接入力できるようになります。ファイルのダウンロード、編集、削除、名前変更、移動ができます。ファイルとフォルダの追加もできます。ここでも、適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、ファイルにアクセスする前に、ユーザの認証が必要になります。

- Enable file server browsing：Windows ネットワークでのドメイン / ワークグループ、サーバ、および共有を参照できるようにします。ファイル サーバ アクセスがイネーブルになっている必要があります。

  このボックスをオンにすると、ユーザがドメインおよびワークグループを選択し、そのドメイン内のサーバおよび共有を参照できるようになります。適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、サーバにアクセスする前に、ユーザの認証が必要になります。

- Enable auto applet download：ユーザが WebVPN にログインしたときに、ポート転送 Java アプレットを自動的にダウンロードし、起動できるようにします。デフォルトではディセーブルになっています。この機能は、ポート転送、Outlook/Exchange プロキシ、または HTTP プロキシもイネーブルになっている場合にだけイネーブルにできます。自動アプレット ダウンロードは、デフォルト グループ ポリシー（DfltGrpPolicy）またはユーザ定義のグループ ポリシーでもイネーブルにできます。

- Enable port forwarding：WebVPN ポート転送を使用すると、グループ内のリモート ユーザが既知の固定 TCP/IP ポートで通信するクライアント / サーバ アプリケーションにアクセスできるようになります。リモート ユーザは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモート サーバに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP（FTP over SSH）、Perforce、Outlook Express、および Lotus Notes についてテストしています。その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、シスコではテストしていません。

（注）　ポート転送は、一部の SSL/TLS バージョンでは機能しません。

このボックスをオンにすると、ローカルおよびリモート システムの TCP ポートをマッピングすることによって、ユーザがクライアント / サーバ アプリケーションにアクセスできるようになります。

注意　Sun Microsystems Java™ Runtime Environment（JRE）1.5.x がリモート コンピュータにインストールされており、ポート転送（アプリケーション アクセス）とデジタル証明書をサポートしていることを確認します。JRE 1.4.x が実行されており、ユーザがデジタル証明書を使用して認証しても、JRE が Web ブラウザの証明書ストアにアクセスできないため、アプリケーションは起動しません。

- Enable Outlook/Exchange proxy : Microsoft Outlook/Exchange 電子メール プロキシの使用をイネーブルにします。
- Apply Web-type ACL：このグループのユーザに定義した WebVPN アクセス コントロール リストを適用します。
- Enable HTTP proxy：クライアントへの HTTP アプレット プロキシの転送をイネーブルにします。プロキシは、Java、ActiveX、Flash など、適切なコンテンツ トランスフォームと干渉する技術にとって役立ちます。セキュリティ アプライアンスの使用を継続しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ設定を自動的に修正し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、実質的にすべてのクライアント サイド技術をサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。
- Enable Citrix/MetaFrame : MetaFrame Application Server からクライアントへのターミナル サービスのサポートをイネーブルにします。このアトリビュートを使用すると、セキュアな Citrix 設定内でセキュリティ アプライアンスがセキュア ゲートウェイとして機能できるようになります。これらのサービスは、ユーザが MetaFrame アプリケーションに標準 Web ブラウザでアクセスできるようにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Group Policy > WebVPN タブ > Content Filtering タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > Content Filtering タブ

- Add or Edit Group Policy ウィンドウの WebVPN タブにある Content Filtering タブを使用して、Web サイトのうち Java または Active X を使用する部分、スクリプトを使用する部分、画像を表示する部分、およびクッキーを配信する部分をブロックまたは削除するように、セキュリティ アプライアンスを設定できます。デフォルトでは、これらのパラメータはディセーブルになっていて、フィルタリングは行われません。

フィールド

- Inherit：このグループ ポリシーがデフォルト グループ ポリシーからコンテンツ フィルタリングの値を継承するかどうかを決めます。このオプションはデフォルト設定です。このアトリビュートがチェックされている場合、残りのアトリビュートはグレー表示になり、設定はできません。
- Filter Java/ActiveX：<applet>、<embed>、および <object> タグを HTML から削除します。
- Filter scripts：<script> タグを HTML から削除します。
- Filter images：<img> タグを HTML から削除します。画像を削除すると、Web ページの配信が大幅に高速化されます。
- Filter cookies from images：画像で配信されるクッキーを削除します。広告主はクッキーを使用して訪問者を追跡するため、これによってユーザのプライバシーが保護されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Group Policy > WebVPN タブ > Homepage タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > Homepage タブ

Add Group Policy または Edit Group Policy ウィンドウの WebVPN タブにある Homepage タブを使用して、使用するホームページ（存在する場合）を設定し、そのページに適用するカスタマイゼーション（色やロゴなど）を指定できます。ホームページのカスタマイゼーションを定義するわけではありません。

フィールド

- Inherit：対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。これは、Webpage Customization および Custom Homepage の両アトリビュートのデフォルト設定です。
- Webpage Customization：デフォルト グループ ポリシーから Web ページのカスタマイゼーションを継承して、（リストから選択した）既存のカスタマイゼーションを適用するか、新しいカスタマイゼーションを作成するかを指定します。
- New：Add Customization Object ダイアログボックスを開きます。このダイアログボックスで、ユーザに表示される GUI ページに適用する新しいカスタマイゼーションを作成および設定します。
- Custom Homepage：デフォルト グループ ポリシーからホームページを継承して既存の URL をホームページとして使用するか、ホームページを使用しないかを指定します。
- Specify URL：後続のフィールドで、プロトコル（http または https）と、ホームページとして使用する Web ページの URL を指定することを示します。具体的な内容は次のとおりです。
  - Protocol：ホームページの接続プロトコルとして http または https のどちらを使用するかを示します。
  - :// field：ホームページとして使用する Web ページの URL を指定します。
- Use none：ホームページを設定しないように指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Group Policy > WebVPN タブ > Port Forwarding タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > Port Forwarding タブ

Add Group Policy または Edit Group Policy ウィンドウの WebVPN タブの Port Forwarding タブを使用して、ポート転送パラメータを設定できます。

フィールド

- Inherit：（複数のインスタンス）チェックした場合、このオプションは、関連付けられているアトリビュートの値がデフォルト グループ ポリシーによって設定されるように指定します。このオプションは、Port Forwarding List と Applet Name の両アトリビュートのデフォルト設定です。
- Port Forwarding List：ポート転送リストをデフォルト グループ ポリシーから継承するか、リストから選択するか、新しいポート転送リストを作成するかを指定します。
- New：Add Port Forwarding List ウィンドウを開きます。このウィンドウで、新しいポート転送リストを追加できます。Add Port Forwarding List ウィンドウの説明を参照してください。
- Applet Name：アプレット名を継承するか、このフィールドで指定した名前を使用するかを指定します。この名前を指定して、エンド ユーザに対してポート転送を識別します。設定した名前は、エンド ユーザ インターフェイスで、ホットリンクとして表示されます。ユーザがこのリンクをクリックすると、Java アプレットによって、設定されているポート転送アプリケーションのリストを表示してアクセスできるようにするウィンドウが開きます。デフォルトのアプレット名は Application Access です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Port Forwarding List

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > Port Forwarding タブ > New ボタン > Add or Edit Port Forwarding List

Add Port Forwarding List ダイアログボックスを使用して、ポート転送リストの名前の指定と、設定したポート転送エントリのリストの表示ができます。

フィールド

- List Name：追加するポート転送リストの名前を割り当てます。
- Local TCP Port：ポート転送リストの各エントリが使用するローカル TCP ポートを一覧表示します。
- Remote Server：ポート転送リストの各エントリが使用するリモート サーバを割り当てます。
- Remote TCP Port:ポート転送リストの各エントリが使用するリモート TCP ポートを一覧表示します。
- Description：（オプション）ポート転送リストの各エントリに関する最大 64 文字の説明を一覧表示します。
- Add：Add Port Forwarding Entry ダイアログボックスを開きます。このダイアログボックスで、新しいポート転送エントリを設定できます。

- Edit：Edit Port Forwarding Entry ダイアログボックスを開きます。このダイアログボックスで、既存のポート転送エントリを修正できます。
- Delete：選択したポート転送エントリをポート転送リストから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Port Forwarding Entry

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > Port Forwarding タブ > New ボタン > Add Port Forwarding List > Add or Edit

Add or Edit Port Forwarding Entry ダイアログボックスを使用して、ポート転送リストの名前の指定と、設定したポート転送エントリのリストの表示ができます。

フィールド

- Local TCP Port：このポート転送リストエントリのローカル TCP ポートを指定します。
- Remote Server：ポート転送リスト エントリのリモート サーバを指定します。
- Remote TCP Port：ポート転送リスト エントリのリモート TCP ポートを指定します。
- Description：（オプション）ポート転送リスト エントリに関する最大 64 文字の説明を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Group Policy > WebVPN タブ > Other タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > Other タブ

Add Group Policy または Edit Group Policy ウィンドウの WebVPN タブの Other タブを使用して、サーバと URL のリストおよび Web-type ACL ID を設定できます。

フィールド

- Inherit：（複数インスタンス）対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。
- Servers and URL Lists：サーバおよび URL のリストを継承するか、既存のリストを選択するか、新しいリストを作成するかを指定します。

- New：新しいサーバまたは URL をリストに追加できるダイアログボックスを表示します。
- Web-Type ACL ID：Web-type ACL ID を継承して既存の Web-Type ACL の識別名を選択するか、Web-type ACL を追加または修正するかを指定します。
- Manage：Web-type ACL を管理できる ACL Manager ダイアログボックスを開きます。
- SSO Server：シングルサインオン サーバ設定を継承して、リストから既存の SSO サーバを選択するか、新しい SSO サーバを追加するかを指定します。
- New：Add SSO Server ダイアログボックスを開きます。このダイアログボックスで、リストに新しいサーバを設定できます。
- HTTP Compression：HTTP Compression の設定をデフォルト グループから継承するか、明示的に HTTP 圧縮をイネーブルまたはディセーブルにするかを指定します。
- Keepalive Ignore：デフォルトのグループから最大トランザクション サイズを継承するか、無視する HTTP/HTTPS トラフィックのトランザクション当たりの上限を設定するかを指定します。範囲は 0 ～ 900 KB です。
- Deny Message：正常にログインできたが VPN 権限がないリモート ユーザに送信するメッセージを次のように継承、指定、または削除できます。
  - Inherit をオンにして、WebVPN には正常にログインできたが VPN 権限がないリモート ユーザに送信するメッセージをデフォルト グループから継承します。
  - オフにして、フィールドのテキストを消去して、WebVPN　には正常にログインできたが VPN 権限がないリモート ユーザにメッセージを送信しないようにします。
  - オフにして、このフィールドで、WebVPN には正常にログインできたが VPN 権限がないリモート ユーザに送信するメッセージ（最大 490 文字）を作成または修正します。デフォルトのメッセージは、「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Server and URL List

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > Other タブ > Add or Edit Server or URL List

Add or Edit Server and URL List ダイアログボックスを使用して、指定された URL リストで項目の追加、編集、および並べ替えができます。

フィールド

- List Name：追加するリストの名前を指定するか、修正または削除するリストの名前を選択します。
- URL Display Name：ユーザに表示する URL 名を指定します。
- URL：表示名に関連付けられている URL を指定します。
- Add：Add Server or URL ダイアログボックスを開きます。このダイアログボックスで、新しいサーバまたは URL と表示名を設定できます。

- Edit：Edit Server or URL ダイアログボックスを開きます。このダイアログボックスで、新しいサーバまたは URL と表示名を設定できます。
- Delete：選択した項目をサーバ と URL リストから削除します。確認されず、やり直しもできません。
- Move Up/Move Down：サーバと URL リストでの、選択した項目の位置を変更します。

Add/Edit Server or URL

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > Other タブ > Add or Edit Server and URL

Add or Edit Server and URL ダイアログボックスを使用して、指定された URL リストで項目の追加、編集、および並べ替えができます。

フィールド

- URL Display Name：ユーザに表示する URL 名を指定します。
- URL：表示名に関連付けられている URL を指定します。

Add/Edit Group Policy > WebVPN タブ > SSL VPN Client タブ

Configuration > VPN > General > Group Policy > Add/Edit > Internal Group Policy > Web VPN タブ > SSL VPN Client タブ

Add or Edit Group Policy ウィンドウの WebVPN タブの SSL VPN Client タブを使用して、SSL VPN クライアント（SVC）をリモート コンピュータにダウンロードするようにセキュリティ アプライアンスを設定できます。

SVC は、ネットワーク管理者が IPSec VPN クライアントをリモート コンピュータにインストールし、設定する必要なしに、リモート ユーザが IPSec VPN を利用できるようにする VPN トンネリング技術です。SVC は、すでにリモート コンピュータにある SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVC セッションを確立するには、リモート ユーザはセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスをブラウザに入力します。ブラウザはそのインターフェイスに接続して WebVPN のログイン画面を表示します。ユーザがログインと認証を終了し、セキュリティ アプライアンスがこのユーザを SVC が必要なユーザとして識別した場合、セキュリティ アプライアンスはリモート コンピュータに SVC をダウンロードします。セキュリティ アプライアンスがこのユーザを SVC がオプションで使用できるユーザとして識別した場合、セキュリティ アプライアンスは SVC のインストールをスキップするリンクをユーザ画面に表示して、リモート コンピュータに SVC をダウンロードします。

ダウンロードが完了すると、SVC は自身のインストールと設定を実行します。接続終了時に（設定に応じて）、SVC はリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

セキュリティ アプライアンスは、異なるリモート コンピュータのオペレーティング システム用に、複数の一意の SVC イメージをキャッシュ メモリに常駐させることができます。ユーザが接続しようとしたとき、セキュリティ アプライアンスは、イメージとオペレーティング システムが一致するまで、これらのイメージの一部を連続してダウンロードします。一致すると、SVC の全体をダウンロードします。接続のセットアップ時間を短縮するため、ダウンロードされる最初のイメージが、最もよく遭遇するリモート コンピュータのオペレーティング システムになるように SVC イメージの順序を指定できます。

フィールド

- Inherit：（複数インスタンス）対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。このタブのアトリビュートすべてのデフォルト設定です。
- Use SSL VPN Client：デフォルト グループ ポリシーからこのアトリビュートの値を継承するかどうか、または SSL VPN Client を使用する時期を、always、optionally、または never の中から選択します。
- Keep Installer on Client System：永続的な SVC インストールをイネーブルにするか（Yes）、SVC の自動アンインストール機能をディセーブルにします（No）。後続の SVC 接続では、SVC がリモート コンピュータにインストールされたままの状態になるため、リモート ユーザの SVC への接続時間が短縮されます。
- Compression：SVC 接続での圧縮をイネーブルまたはディセーブルにします。

  SVC 圧縮を行うと、転送されるパケットのサイズが減少するため、セキュリティ アプライアンスと SVC 間の通信パフォーマンスが向上します。
- Keepalive Messages：キープアライブ メッセージの頻度を、15 ～ 600 秒の範囲で調整します。

  プロキシ、ファイアウォール、NAT デバイスを通じた SVC 接続をオープンにしておくためのキープアライブ メッセージを送信する頻度を調整することができます。これは、接続のアイドル状態を維持できる時間がデバイスで制限される場合も有効です。頻度を調整することで、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベースのアプリケーションをアクティブに実行していない場合でも、SVC が切断して再接続をしないようにできます。
- Key Renegotiation Settings : セキュリティ アプライアンスと SVC が鍵の再生成を実行するとき、接続のセキュリティを高めるために、暗号鍵と初期ベクトルを再ネゴシエートします。
  - Renegotiation Interval：セッション開始からキーの再生成までの時間に 1 ～ 10080（1 週間）を分単位で指定します。
  - Renegotiation Method：SVC の鍵の再生成の際に SVC が新しいトンネルを確立するかどうか、確立する場合はその方法を指定します。none をオンにすると、SVC キーの再生成がディセーブルになります。SSL をオンにすると、SVC の鍵の再生成の際に、SSL の再ネゴシエーションが実行されます。New tunnel を選択すると、SVC キー再生成中に SVC が新しいトンネルを確立します。SSL をキー再生成方式として設定することをお勧めします。
- Dead Peer Detection：Dead Peer Detection（DPD）は、ピアが応答していないために失敗した接続をセキュリティ アプライアンス（ゲートウェイ）または SVC で迅速に検出できるようにします。
  - Gateway Side Detection：Gateway Side Detection は、セキュリティ アプライアンス（ゲートウェイ）による DPD 実行をイネーブルにし、セキュリティ アプライアンスが DPD を実行する頻度を 30 ～ 3600 秒の範囲で指定します。enable をオフにすると、セキュリティ アプライアンスによる DPD の実行がディセーブルになります。
  - Client Side Detection：Client Side Detection は、SVC（クライアント）による DPD 実行をイネーブルにし、SVC が DPD を実行する頻度を 30 ～ 3600 秒の範囲で指定します。enable をオフにすると、SVC による DPD の実行がディセーブルになります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Group Policy > WebVPN タブ > Auto Signon タブ

このパネルに移動するパスは数種類あります。

Auto Signon ウィンドウまたはタブを使用して、WebVPN ユーザの自動サインオンを設定または編集できます。自動サインオンは、内部ネットワークに SSO 方式をまだ展開していない場合に使用できる簡素化された単一サインオン方式です。特定の内部サーバに対して自動サインオンを設定すると、セキュリティ アプライアンスは、WebVPN ユーザがセキュリティ アプライアンスへのログインに使用したログイン クレデンシャルをこれらの内部サーバに渡します。特定の範囲のサーバの特定の認証方式に応答するように、セキュリティ アプライアンスを設定します。セキュリティ アプライアンスが応答するように設定できる認証方式は、NTLM 認証、HTTP 基本認証、またはこれらの両方です。

自動サインオンは、特定の内部サーバに SSO を設定する直接的な方法です。この項では、自動サインオンを行うように SSO をセットアップする手順について説明します。すでに Computer Associates の SiteMinder SSO サーバを使用して SSO を展開していて、このソリューションをサポートするようにセキュリティ アプライアンスを設定する場合は、「SSO Servers」を参照してください。HTTP Forms プロトコルを使う SSO を使用して、この方式をサポートするようにセキュリティ アプライアンスを設定でする場合は、「AAA のセットアップ」を参照してください。

フィールド

- Inherit：クリックしてオフにすると、WebVPN ログイン クレデンシャルを使用して特定の内部サーバにログインできるようになります。
- IP Address：表示のみ。次の Mask と組み合せて、認証されるサーバの IP アドレスの範囲を Add/Edit Auto Signon ダイアログボックスで設定されたとおりに表示します。サーバは、サーバの URI またはサーバの IP アドレスとマスクで指定できます。
- Mask：表示のみ。前の IP Address と組み合せて、Add/Edit Auto Signon ダイアログボックスで自動サインオンをサポートするように設定されたサーバの IP アドレスの範囲を表示します。
- URI：表示のみ。Add/Edit Auto Signon ダイアログボックスで設定されたサーバを識別する URI マスクを表示します。
- Authentication Type：表示のみ。認証タイプを Add/Edit Auto Signon ダイアログボックスで設定されたとおりに表示します（Basic HTTP、NTLM、または Basic and NTLM）。
- Add/Edit：自動サインオン命令を追加または編集する場合にクリックします。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。
- Delete：Auto Signon テーブルで選択した自動サインオン命令を削除する場合にクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

ACL

Configuration > VPN > Web VPN > ACLs

このウィンドウを使用して、WebVPN の ACL を設定できます。

フィールド

- View (Unlabeled)：選択したエントリが展開されている（マイナス記号）か閉じられている（プラス記号）かを示します。
- # カラム：ACE ID 番号を指定します。
- Enable：この ACL がイネーブルかディセーブルかを示します。このチェックボックスを使用して、ACL をイネーブルまたはディセーブルにできます。
- Action：この ACL がアクセスを許可するか拒否するかを指定します。
- Type：この ACL が URL または TCP アドレス / ポートに適用されるかどうかを指定します。
- Filter：適用されるフィルタのタイプを指定します。
- Syslog Level (Interval)：この ACL の syslog パラメータを指定します。
- Time Range：この ACL の時間範囲（存在する場合）の名前を指定します。時間範囲には、1 つの間隔または複数の定期的な範囲を設定できます。
- Description：ACL の説明（存在する場合）を指定します。
- Add ACL：Add Web Type ACL ダイアログボックスを表示します。このダイアログボックスで、ACL ID を指定できます。
- Add ACE：Add Web Type ACE ダイアログボックスを表示します。このダイアログボックスで、名前付き ACL のパラメータを指定します。このボタンは、Web Type ACL テーブルに 1 つ以上のエントリが存在する場合にだけアクティブになります。
- Edit ACE/Delete：選択されている ACL または ACE を編集または削除する場合にクリックします。ACL を削除すると、その ACE もすべて削除されます。警告は表示されず、復元もできません。
- Move Up/Move Down：ACL または ACE を選択してこれらのボタンをクリックすると、ACL および ACE の順序が変更されます。セキュリティ アプライアンスは、WebVPN ACL と ACE を、ACL リストボックスでの優先順位に応じて、一致するものが見つかるまでチェックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Tunnel Group

Configuration > VPN > General > Tunnel Group

Tunnel Group ウィンドウのパラメータを使用して、VPN トンネル グループを管理できます。VPN トンネル グループとは、IPSec および WebVPN 接続の場合の接続固有のレコードを表します。

IPSec グループは、IPSec トンネル グループ パラメータを使用してトンネルを作成します。IPSec トンネル グループは、リモートアクセスと LAN 間のどちらでも可能です。IPSec グループは、内部サーバまたは外部 RADIUS サーバ上で設定されます。クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアント パラメータ（インタラクティブ ハードウェア クライアント認証と個別ユーザ認証をイネーブルまたはディセーブルにする）の場合は、IPSec トンネル グループ パラメータが、ユーザとグループに対して設定されたパラメータよりも優先されます。

WebVPN トンネルグループ パラメータは、このトンネル グループに適用する WebVPN グループのパラメータです。WebVPN アクセスは、Configuration > WebVPN ウィンドウで設定します。

フィールド

- Tunnel Group：既存の VPN トンネル グループ用に設定されたパラメータを表示します。Tunnel Group テーブルには、次のカラムがあります。
  - Name：トンネル グループの名前または IP アドレスを指定します。
  - Type：トンネルのタイプを表します。たとえば、ipsec-l2l は、IPSec LAN 間トンネルを示します。その他のタイプとしては、ipsec-ra（IPSec リモート アクセス）と webvpn があります。
  - Group Policy：このトンネル グループのグループ ポリシーの名前を示します。
- Add：IPSec for Remote Access、IPSec for LAN-to-LAN Access、または WebVPN Access といったトンネル タイプを選択できるメニューを表示し、新しいトンネル グループを設定できるダイアログボックスを開きます。
- Edit：既存のトンネル グループを修正できるダイアログボックスを開きます。
- Delete：選択したトンネル グループをリストから削除します。
- Group Delimiter：トンネルがネゴシエートされているときにセキュリティ アプライアンスが受け取るユーザ名からトンネル グループ名を解析するときに使用するデリミタ文字を選択できます。デフォルトではデリミタが指定されておらず、グループ名解析をディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > General タブ > Basic タブ

このパネルに移動するパスは数種類あります。

Add or Edit ウィンドウの General タブの Basic タブを使用して、追加するトンネル グループの名前の指定、グループ ポリシーの選択、領域やグループをユーザ名から除去した上で AAA サーバに渡すかどうかの指定ができます。また、パスワード管理を設定することもできます。

Edit Tunnel Group ウィンドウの General タブには、選択されているトンネル グループの名前とタイプが表示されます。その他の機能は、Add Tunnel Group ウィンドウと同じです。

フィールド

- Name：このトンネル　グループに割り当てられる名前を指定します。 Edit　機能の場合、このフィールドは表示のみです。
- Type：追加または削除するトンネル グループのタイプを表示します。Edit の場合、このフィールドは表示のみで、その内容は、Add ウィンドウでの選択内容によって異なります。
- Group Policy：現在設定されているグループ ポリシーを一覧表示します。デフォルト値は、デフォルト グループ ポリシーである DfltGrpPolicy です。
- Strip the realm (administrative domain) from the username before passing it on to the AAA server：領域をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名の領域修飾子を削除するには、Strip Realm チェックボックスをオンにします。領域名は、AAA （認証、認可、アカウンティング）のユーザ名に追加できます。領域に対して有効なデリミタは @ だけで、JaneDoe@it.cisco.com のように、username@realm という形式を取ります。この Strip Realm チェックボックスをオンにすると、ユーザ名だけに基づいて認証が行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注）　領域とグループは、両方をユーザ名に追加できます。その場合、セキュリティ アプライアンスは、グループと AAA 機能用の領域に対して設定されたパラメータを使用します。このオプションのフォーマットは、*JaneDoe@it.cisco.com#VPNGroup*　のように、ユーザ名 [*@realm*][<# または !> グループ] という形式を取ります。@ が領域デリミタとしても使用されている場合には、セキュリティ アプライアンスが @ をグループ デリミタと解釈できないため、このオプションを選択した場合は、グループ デリミタとして # または ! 文字を使用する必要があります。

Kerberos 領域は特殊事例です。Kerberos 領域の命名規則として、Kerberos 領域と関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザが it.cisco.com ドメインに存在する場合には、Kerberos 領域を IT.CISCO.COM と表記します。

- Strip the group from the username before passing it on to the AAA server：グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、Strip Group チェックボックスをオンにします。このオプションは、Enable Group Lookup ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、セキュリティ アプライアンスは、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、ユーザ名 < デリミタ > グループの形式でグループをユーザ名に追加します。
- Password Management：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - Override account-disabled indication from AAA server：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override-account-disabled を許可すると、セキュリティ上のリスクが発生する可能性があります。

  - Enable notification upon password expiration to allow user to change password：このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。Enable notification prior to expiration チェックボックスをオンにしないと、ユーザは、パスワードの期限が切れた後で通知を受信します。

- Enable notification prior to expiration：このオプションをオンにすると、セキュリティ アプライアンスは、リモート ユーザのログイン時に、現在のパスワードの期限切れが迫っているか、期限が切れていることを通知し、パスワードを変更する機会をユーザに提供します。現在のパスワードの期限がまだ切れていない場合は、ユーザはこのパスワードで引き続きログインできます。このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS 認証または LDAP 認証が設定されていない場合、セキュリティ アプライアンスはこのコマンドを無視します。

  この処理によってパスワードの期限が切れるまでの日数が変わるわけではなく、通知がイネーブルになるということに注意してください。このチェックボックスをオンにしたら、日数も指定する必要があります。
- Notify...days prior to expiration：現在のパスワードの期限切れが迫っていることをユーザに通知する日を、期限切れになるまでの日数で指定します。範囲は 1 ～ 180 日です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > General タブ > Authentication タブ

このパネルに移動するパスは数種類あります。

このタブは、IPSec on Remote Access および LAN-to-LAN トンネル グループで使用できます。このタブの設定は、セキュリティ アプライアンス全体のトンネル グループにグローバルに適用されます。インターフェイスごとに認証サーバ グループを設定するには、Advanced タブをクリックします。Add or Edit Tunnel Group ウィンドウ > General タブ > Authentication タブを使用して、次の アトリビュートを設定できます。

- Authentication Server Group：LOCAL グループ（デフォルト）などの利用可能な認証サーバ グループを一覧表示します。None も選択可能です。None または Local 以外を選択すると、Use LOCAL if Server Group Fails チェックボックスが利用できるようになります インターフェイスごとに認証サーバ グループを設定するには、Advanced タブに移動します。
- Use LOCAL if Server Group fails：Authentication Server Group アトリビュートによって指定されたグループに障害が発生した場合の LOCAL データベースへのフォールバックをイネーブルまたはディセーブルにします。
- NAC Authentication Server Group：ポスチャ検証用に使用する認証サーバ グループを指定します。このフィールドは、セキュリティ アプライアンスで NAC を設定した場合にだけアクティブになります。NAC をサポートするように設定された、少なくとも 1 台のサーバで構成される ACS グループが必要です。このセキュリティ アプライアンスに設定され、リモート アクセス トンネルで利用できる RADIUS タイプのすべてのサーバ グループ名が一覧表示されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > General タブ > Authorization タブ

このパネルに移動するパスは数種類あります。

このタブは、IPSec on Remote Access および LAN-to-LAN トンネル グループで使用できます。このタブの設定は、セキュリティ アプライアンス全体のトンネル グループにグローバルに適用されます。このタブでは、次のアトリビュートを設定できます。

- Authorization Server Group：LOCAL グループを含む、利用可能な認可サーバ グループを一覧表示します。VPN 認可が LOCAL と定義されている場合には、デフォルト グループ ポリシー DfltGrpPolicy で設定されたアトリビュートが適用されます。None（デフォルト）も選択可能です。None 以外を選択すると、Users must exist in authorization database to connect チェックボックスが利用できるようになります。
- Users must exist in authorization database to connect：セキュリティ アプライアンスに対し、認可データベース内のユーザだけに接続を許可するように命令します。デフォルトでは、この機能はディセーブルになっています。認可サーバでこの機能を使用するように設定しておく必要があります。
- Interface-Specific Authorization Server Groups：（オプション）インターフェイスごとに認可サーバ グループを設定できます。インターフェイスに固有の認可サーバ グループは、グローバル サーバ グループよりも優先されます。インターフェイスに固有の認可を明示的に設定していない場合には、グループ レベルでのみ認可が実行されます。
  - Interface：認可を実行するインターフェイスを選択します。　標準のインターフェイスは、outside（デフォルト）、inside、および DMZ です。他のインターフェイスを設定した場合には、そのインターフェイスもリストに表示されます。
  - Server Group：LOCAL グループを含む、先に設定した利用可能な認可サーバ グループを選択します。サーバ グループは、複数のインターフェイスと関連付けることができます。
  - Add：Add をクリックすると、インターフェイスまたはサーバ グループ設定がテーブルに追加され、利用可能なリストからインターフェイスが削除されます。
  - Remove：Remove をクリックすると、インターフェイスまたはサーバ グループがテーブルから削除され、利用可能なリストにインターフェイスが戻ります。
- Authorization Settings：セキュリティ アプライアンスが認可のために認識するユーザ名の値を設定できるようにします。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 認証を必要とするユーザに適用されます。
  - Use entire DN as username：認定者名（DN）全体をユーザ名として使用することを許可します。
  - Specify individual DN fields as the username：個々の DN フィールドをユーザ名として使用することをイネーブルにします。
  - Primary DN Field：選択内容の DN フィールド識別子すべてを一覧表示します。

DN フィールド	内容
Country (C)	2 文字の国名略記。これらのコードは、ISO 3166 の国名略記に準拠しています。
Common Name (CN)	人やシステム、その他のエンティティの名前。識別階層の最も低い（最も具体的な）レベルです。
DN Qualifier (DNQ)	特定の DN アトリビュート。
E-mail Address (EA)	証明書を所有する人、システム、またはエンティティの電子メール アドレス。
Generational Qualifier (GENQ)	Jr.、Sr.、III などの世代修飾子。
Given Name (GN)	証明書所有者の名。
Initials (I)	証明書所有者の姓名の最初の文字。
Locality (L)	組織が所在する市または町。
Name (N)	証明書所有者の名。
Organization (O)	会社、施設、機関、協会、その他のエンティティの名前。
Organizational Unit (OU)	組織内のサブグループ。
Serial Number (SER)	証明書のシリアル番号。
Surname (SN)	証明書所有者の姓。
State/Province (S/P)	組織が所在する州や県。
Title (T)	博士など、証明書の所有者の肩書。
User ID (UID)	証明書の所有者の識別番号。
User Principal Name (UPN)	スマート カードによる証明書認証で使用。

- Secondary DN Field：選択内容の DN フィールド識別子のすべて（上記の表を参照）を一覧表示し、選択していない場合には None オプションを追加します。

Add/Edit Tunnel Group > General タブ > Accounting タブ

このパネルに移動するパスは数種類あります。

このタブは、IPSec on Remote Access および LAN-to-LAN トンネル グループで使用できます。このタブの設定は、セキュリティ アプライアンス全体のトンネル グループにグローバルに適用されます。Add or Edit Tunnel Group ウィンドウ > General タブ > Accounting タブを使用して、次のアトリビュートを設定できます。

- Accounting Server Group：利用可能なアカウンティング サーバ グループを一覧表示します。None（デフォルト）も選択可能です。LOCAL はオプションではありません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > General タブ > Client Address Assignment タブ

このパネルに移動するパスは数種類あります。

アドレス割り当てに DHCP またはアドレス プールを使用するかどうかを指定するには、Configuration > VPN > I P Address Management > Assignment にアクセスします。Add or Edit Tunnel Group ウィンドウ > General タブ > Client Address Assignment タブを使用して、次の Client Address Assignment アトリビュートを設定できます。

- DHCP Servers:使用する DHCP サーバを指定します。一度に最大 10 台のサーバを追加できます。
  - IP Address：DHCP サーバの IP アドレスを指定します。
  - Add:指定された DHCP サーバを、クライアント アドレス割り当て用のリストに追加します。
  - Delete：指定された DHCP サーバを、クライアント アドレス割り当て用のリストから削除します。確認されず、やり直しもできません。
- Address Pools：次のパラメータを使用して、最大 6 つのアドレス プールを指定できます。
  - Available Pools：選択可能な設定済みのアドレス プールを一覧表示します。
  - Add : 選択したアドレス プールをクライアント アドレス割り当て用のリストに追加します。
  - Remove：選択したアドレス プールを Assigned Pools リストから Available Pools リストに移動します。
  - Assigned Pools：アドレス割り当て用に選択したアドレス プールを一覧表示します。

（注） インターフェイスに固有のアドレス プールを設定するには、Advanced タブに移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > General タブ > Advanced タブ

このパネルに移動するパスは数種類あります。

Add or Edit Tunnel Group ウィンドウの General タブの Advanced タブを使用して、次に示す、インターフェイスに固有のアトリビュートを設定できます。

- Interface-Specific Authentication Server Groups：インターフェイスとサーバ グループを認証用に設定できます。
  - Interface：選択可能なインターフェイスを一覧表示します。
  - Server Group：このインターフェイスで利用可能な認証サーバ グループを一覧表示します。
  - Use LOCAL if server group fails：サーバ グループに障害が発生した場合の LOCAL データベースへのフォールバックをイネーブルまたはディセーブルにします。
  - Add：選択した利用可能なインターフェイスと認証サーバ グループ間のアソシエーションを、割り当てられたリストに追加します。
  - Remove：選択したインターフェイスと認証サーバ　グループのアソシエーションを、割り当てられたリストから利用可能なリストに移動します。

- Interface/Server Group/Use Fallback：割り当てられたリストに追加した選択内容を表示します。

- Interface-Specific Client IP Address Pools：インターフェイスとクライアントの IP アドレス プールを指定できます。最大 6 個のプールを指定できます。
  - Interface：追加可能なインターフェイスを一覧表示します。
  - Address Pool：このインターフェイスと関連付けできるアドレス プールを一覧表示します。
  - Add：選択した利用可能なインターフェイスとクライアントの IP アドレス プール間のアソシエーションを、割り当てられたリストに追加します。
  - Remove：選択したインターフェイスまたはアドレス　プールのアソシエーションを、割り当てられたリストから利用可能なリストに移動します。
  - Interface/Address Pool：割り当てられたリストに追加された選択内容を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > IPSec for Remote Access > IPSec タブ

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > IPSec for Remote Access > IPSec タブ

IPSec for Remote Access の Add or Edit Tunnel Group ウィンドウにある IPSec タブ を使用して、IPSec に固有のトンネル グループ パラメータを設定または編集できます。

フィールド

- Pre-shared Key：トンネル グループの事前共有キーの値を指定できます。事前共有キーの最大長は 128 文字です。
- Trustpoint Name：トラストポイントが設定されている場合には、トラストポイント名を選択します。トラストポイントとは、認証局を表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。
- Authentication Mode：認証モードを、none、xauth、または hybrid の中から指定します。
  - none：認証モードを指定しません。
  - xauth：IKE　拡張認証モードを使用するように指定します。この認証モードは、TACACS+ または RADIUS を使用する IKE 内のユーザを認証する機能を提供します。
  - hybrid：ハイブリッド モードを使用するように指定します。この認証モードでは、セキュリティ アプライアンス認証にデジタル認証を使用でき、リモート VPN ユーザ認証に別のレガシー方式（RADIUS、TACACS+、SecurID など）を使用できます。このモードでは、インターネット キー エクスチェンジ（IKE）のフェーズ 1 が次の手順に分かれています。これらを合せてハイブリッド認証と呼びます。

  1. セキュリティ アプライアンスでは、リモート VPN ユーザが標準公開鍵技術で認証されます。これによって、単方向に認証される IKE セキュリティ アソシエーションが確立されます。
  2. 次に、拡張認証（xauth）交換でリモート VPN ユーザが認証されます。このような拡張認証では、サポートされているレガシー認証方式の 1 つを使用できます。

（注）　認証タイプをハイブリッドに設定する前に、認証サーバを設定し、事前共有キーを作成する必要があります。

- IKE Peer ID Validation：IKE ピア ID 確認要求を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- Enable sending certificate chain：証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションでは、ルート証明書と下位のすべての CA 証明書が送信されます。
- ISAKMP Keep Alive：ISAKMP キープアライブ モニタリングをイネーブルにし、設定します。
  - Disable Keep Alives：ISAKMP キープアライブをイネーブルまたはディセーブルにします。
  - Monitor Keep Alives：ISAKMP キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、Confidence Interval フィールドと Retry Interval フィールドが利用できるようになります。
  - Confidence Interval：ISAKMP キープアライブの信頼間隔を指定します。これは、ピアがキープアライブ モニタリングを開始するまでにセキュリティ アプライアンスが許可するアイドル時間を表す秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 300 秒です。
  - Retry Interval：ISAKMP キープアライブの再試行間の待機秒数を指定します。デフォルトは、2 秒です。
  - Head end will never initiate keepalive monitoring：中央サイトのセキュリティ アプライアンスがキープアライブ モニタリングを開始しないように指定します。
- Interface-Specific Authentication Mode：認証モードをインターフェイスごとに指定します。
  - Interface：インターフェイス名を選択できます。デフォルトのインターフェイスは inside と outside ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
  - Authentication Mode：認証モードを、上記の none、xauth、または hybrid の中から選択できます。
  - Interface/Authentication Mode テーブル：インターフェイス名と、選択されている関連認証モードを表示します。
  - Add：選択したインターフェイスと認証モードのペアを Interface/Authentication Modes テーブルに追加します。
  - Remove：選択したインターフェイスと認証モードのペアを Interface/Authentication Modes テーブルから削除します。
- Client VPN Software Update Table：クライアント タイプ、VPN クライアントのリビジョン、およびインストールされている各クライアント VPN ソフトウェア パッケージのイメージ URL を一覧表示します。クライアント タイプごとに、許可されるクライアント ソフトウェア リビジョンと、必要に応じて、ソフトウェア アップグレードをダウンロードする URL または IP アドレスを指定できます。クライアント アップデート メカニズム（Client Update ウィンドウに詳細説明があります）は、この情報を使用して、各 VPN クライアントが適切なリビジョン レベルで実行されているかどうか、適切であれば、通知メッセージとアップデート メカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。
  - Client Type：VPN クライアント タイプを識別します。
  - VPN Client Revisions：許可される VPN クライアントのリビジョン レベルを指定します。
  - Image URL：適切な VPN クライアント ソフトウェア イメージをダウンロードできる URL または IP アドレスを指定します。Windows ベースの VPN クライアントの場合、URL は http:// または https:// という形式です。クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアントの場合、URL は tftp:// という形式です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > PPP タブ

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > PPP タブ

IPSec リモート アクセス トンネル グループの Add or Edit Tunnel Group ウィンドウにある PPP タブを使用して、PPP 接続で許可される認証プロトコルを設定または編集できます。このタブは、IPSec リモートアクセス トンネルグループにだけ適用されます。

フィールド

- CHAP：PPP 接続で CHAP プロトコルの使用をイネーブルにします。
- MS-CHAP-V1：PPP 接続で MS-CHAP-V1 プロトコルの使用をイネーブルにします。
- MS-CHAP-V2：PPP 接続で MA-CHAP-V2 プロトコルの使用をイネーブルにします。
- PAP：PPP 接続で PAP プロトコルの使用をイネーブルにします。
- EAP-PROXY：PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。EAP は、Extensible Authentication protocol（拡張認証プロトコル）を意味します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > IPSec for LAN to LAN Access > General タブ > Basic タブ

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > IPSec for LAN to LAN Access > General タブ > Basic タブ

LAN 間リモート アクセス時の Add or Edit Tunnel Group ウィンドウにある General タブの Basic タブで、追加するトンネル グループの名前を指定し（Add 機能のみ）、グループ ポリシーを選択できます。

Edit Tunnel Group ウィンドウの General タブには、修正するトンネル グループの名前とタイプが表示されます。

フィールド

- Name：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示のみです。
- Type：（表示のみ）追加または編集するトンネル グループのタイプを表示します。このフィールドの内容は、前のウィンドウでの選択内容によって異なります。
- Group Policy：現在設定されているグループ ポリシーを一覧表示します。デフォルト値は、デフォルト グループ ポリシーである DfltGrpPolicy です。

- Strip the realm (administrative domain) from the username before passing it on to the AAA server : 領域をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名の領域修飾子を削除するには、Strip Realm チェックボックスをオンにします。領域名は、AAA （認証、認可、アカウンティング）のユーザ名に追加できます。領域に対して有効なデリミタは @ だけで、JaneDoe@it.cisco.com のように、username@realm という形式を取ります。この Strip Realm チェックボックスをオンにすると、ユーザ名だけに基づいて認証が行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注）　領域とグループは、両方をユーザ名に追加できます。その場合、セキュリティ アプライアンスは、グループと AAA 機能用の領域に対して設定されたパラメータを使用します。このオプションのフォーマットは、*JaneDoe@it.cisco.com#VPNGroup*　のように、ユーザ名 *[@realm][<#* または *!> グループ]* という形式を取ります。@ が領域デリミタとしても使用されている場合には、セキュリティ アプライアンスが @ をグループ デリミタと解釈できないため、このオプションを選択した場合は、グループ デリミタとして # または ! 文字を使用する必要があります。

Kerberos 領域は特殊事例です。Kerberos 領域の命名規則として、Kerberos 領域と関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザが it.cisco.com ドメインに存在する場合には、Kerberos 領域を IT.CISCO.COM と表記します。

- Strip the group from the username before passing it on to the AAA server: グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、Strip Group チェックボックスをオンにします。このオプションは、Enable Group Lookup ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、セキュリティ アプライアンスは、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、ユーザ名 < デリミタ > グループの形式でグループをユーザ名に追加します。
- Password Management : AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - Override account-disabled indication from AAA server : AAA サーバからの account-disabled インジケータを上書きします。

（注）　override-account-disabled を許可すると、セキュリティ上のリスクが発生する可能性があります。

  - Enable notification upon password expiration to allow user to change password: このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。Enable notification prior to expiration チェックボックスをオンにしないと、ユーザは、パスワードの期限が切れた後で通知を受信します。
  - Enable notification prior to expiration : このオプションをオンにすると、セキュリティ アプライアンスは、リモート ユーザのログイン時に、現在のパスワードの期限切れが迫っているか、期限が切れていることを通知し、パスワードを変更する機会をユーザに提供します。現在のパスワードの期限がまだ切れていない場合は、ユーザはこのパスワードで引き続きログインできます。このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS 認証または LDAP 認証が設定されていない場合、セキュリティ アプライアンスはこのコマンドを無視します。

この処理によってパスワードの期限が切れるまでの日数が変わるわけではなく、通知がイネーブルになるということに注意してください。このチェックボックスをオンにしたら、日数も指定する必要があります。

- Notify...days prior to expiration：現在のパスワードの期限切れが迫っていることをユーザに通知する日を、期限切れになるまでの日数で指定します。範囲は 1 ～ 180 日です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > IPSec for LAN to LAN Access > IPSec タブ

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > IPSec for LAN to LAN Access > IPSec タブ

LAN 間アクセス用 IPSec の Add or Edit Tunnel Group ウィンドウにある IPSec タブ を使用して、IPSec LAN 間に固有のトンネル グループ パラメータを設定または編集できます。

フィールド

- Name：このトンネル　グループに割り当てられた名前を指定します。 Edit　機能の場合、このフィールドは表示のみです。
- Type：（表示のみ）追加または編集するトンネル グループのタイプを表示します。このフィールドの内容は、前のウィンドウでの選択内容によって異なります。
- Pre-shared Key：トンネル グループの事前共有キーの値を指定できます。事前共有キーの最大長は 128 文字です。
- Trustpoint Name：トラストポイントが設定されている場合には、トラストポイント名を選択します。トラストポイントとは、認証局を表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。
- Authentication Mode：認証モードを、none、xauth、または hybrid の中から指定します。
  - none：認証モードを指定しません。
  - xauth：IKE　拡張認証モードを使用するように指定します。この認証モードは、TACACS+ または RADIUS を使用する IKE 内のユーザを認証する機能を提供します。
  - hybrid：ハイブリッド モードを使用するように指定します。この認証モードでは、セキュリティ アプライアンス認証にデジタル認証を使用でき、リモート VPN ユーザ認証に別のレガシー方式（RADIUS、TACACS+、SecurID など）を使用できます。このモードでは、インターネット キー エクスチェンジ（IKE）のフェーズ 1 が次の手順に分かれています。これらを合せてハイブリッド認証と呼びます。

  1. セキュリティ アプライアンスでは、リモート VPN ユーザが標準公開鍵技術で認証されます。これによって、単方向に認証される IKE セキュリティ アソシエーションが確立されます。
  2. 次に、拡張認証（xauth）交換でリモート VPN ユーザが認証されます。このような拡張認証では、サポートされているレガシー認証方式の 1 つを使用できます。

（注） 認証タイプをハイブリッドに設定する前に、認証サーバを設定し、事前共有キーを作成する必要があります。

- IKE Peer ID Validation：IKE ピア ID 確認要求を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- Enable sending certificate chain：証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションでは、ルート証明書と下位のすべての CA 証明書が送信されます。
- ISAKMP Keep Alive：ISAKMP キープアライブ モニタリングをイネーブルにし、設定します。
  - Disable Keep Alives：ISAKMP キープアライブをイネーブルまたはディセーブルにします。
  - Monitor Keep Alives：ISAKMP キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、Confidence Interval フィールドと Retry Interval フィールドが利用できるようになります。
  - Confidence Interval：ISAKMP キープアライブの信頼間隔を指定します。これは、ピアがキープアライブ モニタリングを開始するまでにセキュリティ アプライアンスが許可するアイドル時間を表す秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 300 秒です。
  - Retry Interval：ISAKMP キープアライブの再試行間の待機秒数を指定します。デフォルトは、2 秒です。
  - Head end will never initiate keepalive monitoring：中央サイトのセキュリティ アプライアンスがキープアライブ モニタリングを開始しないように指定します。
- Interface-Specific Authentication Mode：認証モードをインターフェイスごとに指定します。
  - Interface：インターフェイス名を選択できます。デフォルトのインターフェイスは inside と outside ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
  - Authentication Mode：認証モードを、上記の none、xauth、または hybrid の中から選択できます。
  - Interface/Authentication Mode テーブル：インターフェイス名と、選択されている関連認証モードを表示します。
  - Add：選択したインターフェイスと認証モードのペアを Interface/Authentication Modes テーブルに追加します。
  - Remove：選択したインターフェイスと認証モードのペアを Interface/Authentication Modes テーブルから削除します。
- Client VPN Software Update Table：クライアント タイプ、VPN クライアントのリビジョン、およびインストールされている各クライアント VPN ソフトウェア パッケージのイメージ URL を一覧表示します。クライアント タイプごとに、許可されるクライアント ソフトウェア リビジョンと、必要に応じて、ソフトウェア アップグレードをダウンロードする URL または IP アドレスを指定できます。クライアント アップデート メカニズム（Client Update ウィンドウに詳細説明があります）は、この情報を使用して、各 VPN クライアントが適切なリビジョン レベルで実行されているかどうか、適切であれば、通知メッセージとアップデート メカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。
  - Client Type：VPN クライアント タイプを識別します。
  - VPN Client Revisions：許可される VPN クライアントのリビジョン レベルを指定します。
  - Image URL：適切な VPN クライアント ソフトウェア イメージをダウンロードできる URL または IP アドレスを指定します。Windows ベースの VPN クライアントの場合、URL は http:// または https:// という形式です。クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアントの場合、URL は tftp:// という形式です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > WebVPN Access > General タブ > Basic タブ

Configuration > VPN > General > Tunnel Group > Add/Edit> WebVPN Access > General タブ > Basic タブ

Add or Edit ペインの General タブの Basic タブを使用して、追加するトンネル グループの名前の指定、グループ ポリシーの選択、およびパスワード管理の設定ができます。

Edit Tunnel Group ウィンドウの General タブには、選択されているトンネル グループの名前とタイプが表示されます。その他の機能は、Add Tunnel Group ウィンドウと同じです。

フィールド

- Name：このトンネル　グループに割り当てられる名前を指定します。 Edit　機能の場合、このフィールドは表示のみです。
- Type：追加または削除するトンネル グループのタイプを表示します。Edit の場合、このフィールドは表示のみで、その内容は、Add ウィンドウでの選択内容によって異なります。
- Group Policy：現在設定されているグループ ポリシーを一覧表示します。デフォルト値は、デフォルト グループ ポリシーである DfltGrpPolicy です。
- Strip the realm：WebVPN では利用できません。
- Strip the group：WebVPN では利用できません。
- Password Management：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - Override account-disabled indication from AAA server：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override-account-disabled を許可すると、セキュリティ上のリスクが発生する可能性があります。

  - Enable notification upon password expiration to allow user to change password: このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。Enable notification prior to expiration チェックボックスをオンにしない場合には、パスワードの期限が切れた後で通知を受信します。
  - Enable notification prior to expiration : このオプションをオンにすると、セキュリティ アプライアンスは、リモート ユーザのログイン時に、現在のパスワードの期限切れが迫っているか、期限が切れていることを通知し、パスワードを変更する機会をユーザに提供します。現在のパスワードの期限がまだ切れていない場合は、ユーザはこのパスワードで引き続きログインできます。このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS 認証または LDAP 認証が設定されていない場合、セキュリティ アプライアンスはこのコマンドを無視します。

    この処理によってパスワードの期限が切れるまでの日数が変わるわけではなく、通知がイネーブルになるということに注意してください。このチェックボックスをオンにしたら、日数も指定する必要があります。
  - Notify...days prior to expiration：現在のパスワードの期限切れが迫っていることをユーザに通知する日を、期限切れになるまでの日数で指定します。範囲は 1 ～ 180 日です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > WebVPN タブ > Basic タブ

Configuration > VPN > General > Tunnel Group > Add/Edit> WebVPN Access > WebVPN タブ > Basic タブ

WebVPN の Add/Edit Tunnel Group General Tab タブのアトリビュートは、IPSec リモート アクセスの Add/Edit Tunnel Group General Tab タブのアトリビュートと同じです。次の説明は、WebVPN Tab タブに表示されるフィールドに適用されます。

フィールド

Basic タブを使用して、次の WebVPN アトリビュートを設定できます。

- Authentication：認証のタイプを、AAA、Certificate、または Both の中から指定します。デフォルト値は AAA です。
- DNS Group : WebVPN トンネルグループで使用する DNS サーバを指定します。デフォルト値は DefaultDNS です。
- CSD Failure group policy : このアトリビュートは、Cisco Secure Desktop がインストールされているセキュリティ アプライアンスでのみ有効です。Cisco Secure Desktop Manager を使用して VPN 機能ポリシーを次のいずれかのオプションに設定すると、セキュリティ アプライアンスがこのアトリビュートを使用して、アクセス権をリモート CSD クライアントに制限します。
  - 「Use Failure Group-Policy.」
  - 「Use Success Group-Policy, if criteria match」、および条件が一致しない。

  このアトリビュートは、適用する障害グループ ポリシーの名前を指定します。デフォルト グループ ポリシーと関連付けられているアクセス権とは別のアクセス権にするグループ ポリシーを選択します。デフォルト値は DfltGrpPolicy です。

（注） VPN 機能ポリシーを「Always use Success Group-Policy」に設定した場合、セキュリティ アプライアンスはこのアトリビュートを使用しません。

詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > WebVPN Access > WebVPN タブ > NetBIOS Servers タブ

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN Access > WebVPN タブ > NetBIOS Servers タブ

このタブのテーブルは、設定済みの NetBIOS サーバのアトリビュートを表します。WebVPN Access の Add or Edit Tunnel Group ウィンドウの NetBIOS タブを使用して、トンネル グループの NetBIOS アトリビュートを設定できます。WebVPN は、NetBIOS および Common Internet File System（共通インターネット ファイル システム）プロトコルを使用して、リモート システム上のファイルをアクセスまたは共有します。コンピュータ名を使用して Windows コンピュータへのファイル共有接続を試みる場合、指定するファイル サーバは、ネットワーク上のリソースを識別する特定の NetBIOS 名に対応します。

セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NetBIOS ネーム サーバにクエリーを行います。WebVPN は、リモート システム上のファイルをアクセスまたは共有することを NetBIOS に要求します。

NBNS 機能を正常に動作させるには、少なくとも 1 つの NetBIOS サーバ（ホスト）を設定する必要があります。冗長性を確保するため、最大 3 つの NBNS サーバを設定できます。セキュリティ アプライアンスは、リストにある最初のサーバを NetBIOS/CIFS の名前解決に使用します。クエリーが失敗すると、次のサーバを使用します。

フィールド

- IP Address：設定された NetBIOS サーバの IP アドレスを表示します。
- Master Browser：サーバが WINS サーバであるか、あるいは CIFS サーバ（つまりマスタ ブラウザ）にもなれるサーバであるかを表します。
- Timeout (seconds)：サーバが NBNS クエリーに対する応答を待つ最初の時間を秒単位で表示します。この時間を過ぎると、次のサーバにクエリーを送信します。
- Retries：設定されたサーバに対する NBNS クエリーの送信を順番にリトライする回数を表示します。言い換えれば、エラーを返すまでサーバのリストを巡回する回数ということです。最小リトライ数は 0、デフォルトのリトライ数は 2、最大リトライ数は 10 です。
- Add/Edit：NetBIOS サーバを追加します。Add or Edit NetBIOS Server ダイアログボックスが開きます。
- Delete：選択した NetBIOS 行をリストから削除します。
- Move Up/Move Down：セキュリティ アプライアンスが、このボックスに表示された順序で NetBIOS サーバに NBNS クエリーを送信します。このボックスを使用して、クエリーをリスト内で上下に動かすことにより、優先順位を変更します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > WebVPN Access > WebVPN タブ > NetBIOS Servers タブ > Add/Edit NetBIOS Server

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN Access > WebVPN タブ > NetBIOS Servers タブ > Add/Edit NetBIOS Server

このダイアログボックスを使用して、NetBIOS サーバ テーブルの新しいエントリを作成、または既存のエントリを修正できます。

フィールド

- IP Address：NetBIOS サーバの IP アドレスを指定します。
- Master browser：現在の NetBIOS サーバを、WINS サーバではなくマスタ ブラウザとして指定します。
- Timeout：サーバが NBNS クエリーに対する応答を待つ最初の時間を秒単位で指定します。この時間を過ぎると、次のサーバにクエリーを送信します。最小時間は 1 秒です。デフォルト時間は 2 秒です。最大時間は 30 秒です。この時間は、サーバのリストのリトライ サイクルごとに 2 倍になります。
- Retries：設定したサーバに対する NBNS クエリーの送信を順番にリトライする回数を指定します。言い換えれば、エラーを返すまでサーバのリストを巡回する回数ということです。最小リトライ数は 0、デフォルトのリトライ数は 2、最大リトライ数は 10 です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > WebVPN Access > WebVPN タブ > Group Aliases and URLs タブ

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN Access > WebVPN タブ > Group Aliases and URLs タブ

WebVPN Remote Access の Add or Edit Tunnel Group ウィンドウの Group Aliases and URLs タブを使用して、グループ（グループ エイリアス）の代替名と、そのグループの着信 URL を指定できます。

グループ エイリアスを指定すると、ユーザがトンネルグループを参照できる代替名が 1 つ以上作成されます。ここで指定するグループ エイリアスは、ログイン ページでドロップダウン リストに表示されます。各グループに複数のエイリアスを持たせることも、エイリアスを持たせないこともできます。トンネル グループの実名をこのリストに表示する場合は、実名をエイリアスとして指定します。この機能は、「Devtest」と「QA」のように、複数の通常名によって同じグループが認識される場合に便利です。

グループ URL を指定すると、ユーザはログイン時にグループを選択する必要がなくなります。ユーザがログインするとき、セキュリティ アプライアンスは、ユーザの着信 URL を tunnel-group-policy テーブルで探します。URL が検出され、この機能がイネーブルになっている場合、セキュリティ アプライアンスは、適切なサーバを自動的に選択して、ユーザ名フィールドとパスワード フィールドだけをログイン ウィンドウでユーザに提示します。URL がディセーブルになっている場合には、グループのドロップダウン リストも表示されるため、ユーザはグループを選択する必要があります。

グループに複数の URL を設定（あるいは URL を設定しないことも）できます。各 URL は、個別にイネーブルまたはディセーブルにすることができます。指定した URL ごとに別個の指定を使用する必要があります。URL またはアドレス全体を指定する必要があります。その場合には、http または https プロトコルのどちらも使用できます。

同じ URL を複数のグループに関連付けることはできません。セキュリティ アプライアンスは、トンネル グループの URL を受け入れる前に、URL が一意であることを確認します。

フィールド

- Group Aliases：次のエントリがあります。
  - Alias：トンネル グループの代替名を指定します。
  - Add/Remove:選択したグループ エイリアスをリストに追加、またはリストから削除します。
  - Enable：選択したエイリアスをイネーブルにします。ログオン時にドロップダウン リストに表示されます。このチェックボックスは、デフォルトでオンになっています。

（注） Alias/Status テーブルでディセーブルになっているエイリアスのステータスを、Enable をオンにし、OK をクリックした後に Apply をクリックするだけで変更することはできません。まず、ディセーブルになっているエイリアスを削除し、Enable チェックボックスをオンにした状態でそのエイリアスを再度追加する必要があります。

  - Alias/Status：選択した各エイリアスがイネーブルかディセーブルかを表示します。
- Group URLs：次のエントリがあります。
  - URL (http or https) : http://www .cisco .com など、リストに追加する URL を指定します。URL には、http:// または https:// プロトコルを入れる必要があります。
  - Add/Remove：選択したグループ URL をリストに追加、またはリストから削除します。
  - Enable：選択した URL をイネーブルにします。デフォルトでイネーブルになっています。

（注） URL/Status テーブルでディセーブルになっている URL のステータスを、Enable をオンにし、OK をクリックした後に Apply をクリックするだけで変更することはできません。まず、ディセーブルになっている URL を削除し、Enable チェックボックスをオンにした状態でそのエイリアスを再度追加する必要があります。

  - URL/Status：選択した各 URL がイネーブルかディセーブルかを表示します。

例

カスタマイゼーション プロファイルとトンネルグループの組み合せを使用して、さまざまなグループに異なるログイン 画面をセットアップできます。たとえば、salesgui と呼ばれるカスタマイゼーション プロファイルを作成したとすれば、次の例で示すように、そのカスタマイゼーション プロファイルを参照する sales という名前の WebVPN トンネル グループを作成できます。この例では、ユーザが WebVPN を使用してログインしたときに、デフォルトの Cisco ロゴではなく、企業のロゴが表示されます。

ステップ 1　salesgui という名前の WebVPN カスタマイゼーションを定義して、デフォルトのロゴを mycompanylogo.gif に変更します。あらかじめ mycompanylogo.gif をセキュリティ アプライアンスのフラッシュ メモリにロードしてコンフィギュレーションを保存しておく必要があります。

ステップ 2　ユーザ名をセットアップして、定義した WebVPN カスタマイゼーションと関連付けます。

ステップ 3　sales という名前の WebVPN トンネルグループを作成します。

ステップ 4　このトンネルグループに salesgui カスタマイゼーションを使用することを指定します。

ステップ 5　セキュリティ アプライアンスへのログイン時にユーザがブラウザに入力するアドレスに、グループ URL を設定します。たとえば、セキュリティ アプライアンスの IP アドレスが 192.168.3.3 の場合、グループ URL を https://192.168.3.3 に設定します。

セキュリティ アプライアンスは、この URL を sales トンネルグループにマップし、salesgui カスタマイゼーション プロファイルを、ユーザに表示されるログイン画面に適用します。

ステップ 6　設定をメモリに保存します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Tunnel Group > WebVPN Access > WebVPN タブ > Web Page タブ

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN Access > WebVPN タブ > Web Page タブ

このタブを使用して、カスタマイズした WebVPN エンドユーザ ログオン Web ページのルックアンドフィールを選択します。

フィールド

- Webpage Customization：以前に定義した Web ページのカスタマイゼーションを選択します。
- New：新しい Web ページ カスタマイゼーションを設定できるダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

参考資料

WebVPN エンド ユーザ設定

VPN System Options

Configuration > VPN > General > VPN System Options

VPN System Options ウィンドウを使用して、VPN セッションに固有の機能をセキュリティ アプライアンスで設定できます。

フィールド

- Enable inbound IPSec sessions to bypass interface access-lists. Group policy and per-user authorization access lists still apply to the traffic：セキュリティ アプライアンスは、VPN トラフィックがセキュリティ アプライアンス インターフェイスで終了することをデフォルトで許可しているため、IKE または ESP（またはその他のタイプの VPN パケット）をアクセス ルールで許可する必要はありません。このオプションをオンにしている場合は、復号化された VPN パケットのローカル IP アドレスに対するアクセス ルールは不要です。VPN トンネルが セキュリティ メカニズムを使用して正常に終了したため、この機能によって設定が簡素化され、セキュリティ上のリスクを伴うことなく、セキュリティ アプライアンスのパフォーマンスが最大化されます（グループ ポリシーとユーザごとの認可アクセスリストはトラフィックに適用されます）。

  このオプションをオフにすることにより、アクセス ルールをローカル IP アドレスに適用することを強制的に適用できます。アクセス ルールはローカル IP アドレスに適用され、VPN パケットが復号化される前に使用されていた元のクライアント IP アドレスには適用されません。
- Limit maximum number of active IPSec VPN sessions：アクティブな IPSec VPN セッションの最大数の制限をイネーブルまたはディセーブルにします。範囲は、ハードウェア プラットフォームとソフトウェア ライセンスによって異なります。
- Maximum Active IPSec VPN Sessions：アクティブな IPSec VPN セッションの最大許可数を指定します。このフィールドは、上記のチェックボックスをオンにして、アクティブな IPSec VPN セッションの最大数を制限した場合にだけアクティブになります。
- L2TP Tunnel Keep-alive Timeout：キープアライブ メッセージの頻度を秒単位で指定します。範囲は 10 ～ 300 秒です。デフォルトは、60 秒です。
- Compression Settings：圧縮をイネーブルにする機能を、WebVPN と SSL VPN Client の中から指定します。デフォルトでは、圧縮はイネーブルです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Zone Labs Integrity Server

Configuration > VPN > General > Zone Labs Integrity Server

Zone Labs Integrity Server パネルを使用して、セキュリティ アプライアンスが Zone Labs Integrity Server をサポートするように設定できます。このサーバは、プライベート ネットワークにアクセスするリモート クライアントでセキュリティ ポリシーを適用する目的で設計された Integrity System というシステムの一部です。本質的には、セキュリティ アプライアンスが、ファイアウォール サーバに対するクライアント PC のプロキシとして機能し、Integrity クライアントと Integrity サーバ間で必要なすべての Integrity 情報をリレーします。

（注）　現在のバージョンのセキュリティ アプライアンスは、ユーザ インターフェイスが最大 5 つのサーバの設定をサポートする場合でも、1 度に 1 つの Integrity サーバをサポートします。アクティブ サーバに障害が発生したら、セキュリティ アプライアンス上に別の Integrity サーバを設定し、クライアント VPN セッションを再度確立します。

フィールド

- Server IP address：Integrity Server の IP アドレスを入力します。ドット付き 10 進数を使用します。
- Add：新しいサーバ IP アドレスを Integrity Server のリストに追加します。このボタンは、Server IP アドレス フィールドにアドレスが入力されるとアクティブになります。
- Delete：選択したサーバを Integrity Server リストから削除します。
- Move Up：選択したサーバを Integrity Server のリスト内で上に移動します。このボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。
- Move Down：選択したサーバを Integrity Server のリスト内で下に移動します。このボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。
- Server Port：アクティブな Integrity サーバをリスンするセキュリティ アプライアンスのポート番号を入力します。このフィールドは、Integrity Server のリストにサーバが少なくとも 1 台以上存在する場合にだけ使用できます。デフォルトのポート番号は 5054 で、可能な範囲は 10 ～ 10000 です。このフィールドは、Integrity Server リストにサーバが存在する場合にだけ使用できます。
- Interface：アクティブな Integrity Server と通信するセキュリティ アプライアンス インターフェイスを選択します。このインターフェイス名メニューは、Integrity Server リスト内にサーバが存在する場合にだけ使用できます。
- Fail Timeout：セキュリティ アプライアンスが、アクティブな Integrity Server に到達不能であることを宣言するまでの待機秒数を入力します。デフォルトは 10 で、範囲は、5 ～ 20 です。
- Enable SSL Authentication：セキュリティ アプライアンスによるリモート クライアントの SSL 証明書の認証をイネーブルにする場合にオンにします。デフォルトでは、クライアント SSL 認証はディセーブルになっています。
- Close connection on timeout：タイムアウト時に、セキュリティ アプライアンスと Integrity Server 間の接続を終了する場合にオンにします。デフォルトでは、接続が維持されます。
- Apply：設定を実行しているセキュリティ アプライアンスに Integrity Server 設定を適用します。
- Reset：まだ適用されていない Integrity Server 設定の変更を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Easy VPN Remote

Configuration > VPN > Easy VPN Remote

Easy VPN Remote を使用して、ASA 5505 を Easy VPN クライアント デバイスとして動作させることができます。ASA 5505 は、Easy VPN サーバへの VPN トンネルを開始できます。Easy VPN サーバの種類としては、セキュリティ アプライアンス、Cisco VPN 3000 コンセントレータ、IOS ベースのルータ、または Easy VPN サーバとして動作するファイアウォールがあります。

Easy VPN クライアントは次の 2 つの操作モードのいずれかをサポートします。クライアント モードまたは Network Extension Mode（NEM; ネットワーク拡張モード）です。操作モードによって、Easy VPN クライアントの内部ホストがトンネルを経由して企業ネットワークからアクセスできるかどうかが決まります。Easy VPN クライアントにはデフォルト モードが設定されていないため、必ず操作モードを指定してから接続を確立します。

クライアント モードは、Port Address Translation（PAT; ポート アドレス変換）モードとも呼ばれ、Easy VPN クライアント プライベート ネットワーク上のすべてのデバイスを企業ネットワークの IP アドレスから分離します。Easy VPN クライアントは、内部ホストのすべての VPN トラフィックに対してポート アドレス変換（PAT）を実行します。Easy VPN クライアント内部インターフェイスまたは内部ホストには、IP アドレスの管理は必要ではありません。

NEM は、内部インターフェイスとすべての内部ホストをトンネルを介した企業ネットワーク上でルーティングできるようにします。内部ネットワーク上のホストは、スタティック IP アドレスによって事前設定され、（スタティックにまたは DHCP 経由で）アクセス可能なサブネットから IP アドレスを取得します。PAT は、NEM 内の VPN トラフィックには適用されません。このモードでは、各クライアントに VPN 設定を行う必要はありません。NEM モード用に設定された Cisco ASA 5505 は、自動トンネル イニシエーションをサポートしています。設定には、グループ名、ユーザ名、パスワードを保存する必要があります。自動トンネル起動は、セキュアなユニット認証がイネーブルの場合はディセーブルになります。

Easy VPN クライアントのプライベート側のネットワークとアドレスは非表示になっており、直接アクセスすることはできません。

フィールド

- Enable Easy VPN Remote：Easy VPN Remote 機能をイネーブルにし、このウィンドウの残りのフィールドを設定できるようにします。
- Mode：Client mode または Network extension mode のどちらかを選択します。
  - Client mode：Port Address Translation（PAT; ポート アドレス変換）モードを使用して、クライアントに関連する内部ホストのアドレスを企業ネットワークから分離します。
  - Network extension mode：このようなアドレスを企業ネットワークからアクセス可能にします。

  （注） Easy VPN Remote が NEM を使用し、セカンダリ サーバに接続されている場合は、各ヘッドエンドへの ASDM 接続を確立し、Enable Reverse Route Injection on Configuration > VPN > IPSec > IPSec Rules > Tunnel Policy (Crypto Map) - Advanced タブを開き、RRI を使用したリモート ネットワークのダイナミック アナウンスメントを設定します。

  - Auto connect：Network extension mode がローカルに設定され、かつ Easy VPN Remote にプッシュされたグループ ポリシーでスプリットトンネリングが設定されている場合を除き、Easy VPN Remote は、自動 IPSec データ トンネルを確立します。両方の条件を満たしている場合は、このアトリビュートをオンにすると、IPSec データ トンネルの確立が自動化されます。両方の条件を満たしていて、このアトリビュートをオフにした場合、このアトリビュートは無視されます。

- Group Settings：事前共有キーまたは X.509 証明書をユーザ認証に使用するかどうかを指定します。
  - Pre-shared key：認証に事前共有キーを使用することをイネーブルにし、このアトリビュートを指定すると、その後の、Group Name、Group Password、Confirm Password の各フィールドに、その鍵に含まれるグループ ポリシー名とパスワードを指定できるようになります。
  - Group Name：認証に使用するグループ ポリシーの名前を指定します。
  - Group Password：指定したグループ ポリシーで使用するパスワードを指定します。
  - Confirm Password：入力したグループ パスワードの確認を必須にします。
  - X.509 Certificate：認証用に、認証局から提供された X.509 デジタル証明書の使用を指定します。
  - Select Trustpoint：ドロップダウン リストからトラストポイントを選択できます。トラストポイントは、IP アドレスまたはホスト名前です。トラストポイントを定義するには、この領域の下部にある Trustpoint(s) configuration リンクをクリックします。
  - Send certificate chain：証明書自体だけでなく、証明書チェーンの送信もイネーブルにします。このアクションでは、ルート証明書と下位のすべての CA 証明書が送信されます。
- User Settings：ユーザ ログイン情報を設定します。
  - User Name：Easy VPN Remote 接続用の VPN ユーザ名を設定します。Xauth は、TACACS+ または RADIUS を使用する IKE 内のユーザを認証する機能を提供します。Xauth は、RADIUS または別のサポートされたユーザ認証プロトコルを使用して、ユーザを認証します（この場合、Easy VPN ハードウェア クライアントを使用）。セキュア ユニット認証がディセーブルになっており、サーバが Xauth クレデンシャルを要求する場合には、Xauth ユーザ名とパスワード パラメータが使用されます。セキュア ユニット認証がイネーブルになっている場合は、これらのパラメータが無視され、セキュリティ アプライアンスがユーザにユーザ名とパスワードを求めるプロンプトを表示します。
  - User Password：Easy VPN Remote 接続用の VPN ユーザ パスワードを設定します。
  - Confirm Password：入力したユーザ パスワードの確認を必須にします。
- Easy VPN Server To Be Added：Easy VPN サーバを追加または削除します。どの ASA または VPN 3000 コンセントレータ シリーズでも Easy VPN サーバとして動作できます。接続を確立するには、まずサーバを設定する必要があります。セキュリティ アプライアンスは、IPv4 アドレス、名前データベース、または DNS 名をサポートしており、この順序でアドレスを解決します。Easy VPN Server(s) リストの最初のサーバはプライマリ サーバです。プライマリ サーバに加え、最大 10 台のバックアップ サーバを指定できます。
  - Name or IP Address：リストに追加する Easy VPN サーバの名前または IP アドレス。
  - Add：指定したサーバを Easy VPN Server(s) リストに移動します。
  - Remove：Easy VPN Server(s) リストから選択したサーバを Name または IP Address ファイルに移動します。ただし、この作業を実行した場合には、Name または IP Address フィールドにそのアドレスを再入力しないと、同じアドレスを再度追加することができません。
  - Easy VPN Server(s)：設定した VPN サーバを優先順位に応じて一覧表示します。
  - Move Up/Move Down：Easy VPN Server(s) リスト内でのサーバの位置を変更します。これらのボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Advanced Easy VPN Properties

Configuration > VPN > Easy VPN Remote > Advanced

デバイス パススルー

Cisco IP Phone やプリンタなどのデバイスは、認証を実行できないため、個別ユニット認証に追加できません。これらのデバイスに対応するために、Individual User Authentication がイネーブルになっている場合には、MAC Exemption アトリビュートによってイネーブルにされるデバイス パススルー機能が、指定した MAC アドレスを持つデバイスの認証を免除します。

MAC アドレスの最初の 24 ビットは、その機器の製造元を示します。最後の 24 ビットは、16 進数形式で表したユニットのシリアル番号です。

管理トンネル

ASA モデル 5505 デバイスを NAT デバイスの後ろで稼働させるときに、Tunneled Management アトリビュートを使用して、デバイス管理の設定方法（クリアまたはトンネリング）を指定し、トンネル経由での Easy VPN Remote 接続の管理を許可するネットワークを指定できます。ASA 5505 のパブリック アドレスが NAT デバイスの後ろにある場合は、NAT デバイスで静的 NAT マッピングを追加しなければアクセスできません。

NAT デバイスの後ろで Cisco ASA 5505 を稼働させるときに、**vpnclient management** コマンドを使用して、デバイスの管理方法（暗号化の追加または暗号化なし）を指定し、管理アクセスを与えるホストまたはネットワークを指定します。ASA 5505 のパブリック アドレスが NAT デバイスの後ろにある場合は、NAT デバイスで静的 NAT マッピングを追加しなければアクセスできません。

フィールド

- MAC Exemption：Easy VPN Remote 接続のデバイス パススルーで使用する MAC アドレスとマスクを設定します。
  - MAC Address：指定した MAC アドレスを持つデバイスの認証を免除します。このフィールドで MAC アドレスを指定するための形式は 3 桁の 16 進数値で、45ab.ff36.9999 のようにピリオドで区切られます。
  - MAC Mask：このフィールドで MAC アドレスを指定するための形式は 3 桁の 16 進数値で、たとえば ffff.ffff.ffff という MAC マスクは、指定した MAC アドレスとだけ一致します。すべてが 0 の MAC マスクはどの MAC アドレスにも対応せず、ffff .ff00 .0000 という MAC マスクは、同一メーカーが製造したすべてのデバイスに対応します。
  - Add：指定した MAC アドレスとマスクのペアを MAC Address/Mask リストに追加します。
  - Remove：MAC Address/MAC リストから選択した MAC アドレスとマスクのペアを、個々の MAC Address および MAC Mask フィールドに移動します。
- Tunneled Management：デバイス管理のための IPSec の暗号化を設定し、トンネル経由での Easy VPN ハードウェア クライアント接続の管理を許可するネットワークを指定します。Clear Tunneled Management を選択しても、IPSec の暗号化レベルが削除されるだけで、SSH や https など、その接続に存在する他の暗号化には影響しません。
  - Enable Tunneled Management：すでに管理トンネルに存在する SSH または HTTPS 暗号化に IPSec 暗号化レイヤを追加します。
  - Clear Tunneled Management：暗号化を追加せず、すでに管理トンネルに存在する暗号化を使用します。
  - IP Address：VPN トンネル経由での Easy VPN ハードウェア クライアントへの管理アクセスを許可するホストまたはネットワークの IP アドレスを指定します。1 つ以上の IP アドレスと各ネットワーク マスクを個別に追加できます。
  - Mask：対応する IP アドレスのネットワーク マスクを指定します。
  - Add：指定した IP アドレスとマスクを IP Address/Mask リストに移動します。

- Remove：選択した IP アドレスとマスクのペアを、IP Address/Mask リストから、この領域にある個々の IP Address/Mask フィールドに移動します。
- IP Address/Mask：この領域の Enable または Clear 機能によって処理される、設定した IP アドレスとマスクのペアを一覧表示します。

• IPSec Over TCP：Easy VPN Remote 接続に TCP でカプセル化された IPSec を使用するように設定します。

- Enable：IPSec over TCP をイネーブルにします。

（注） Easy VPN Remote 接続で、TCP でカプセル化された IPSec を使用する場合は、Configuration > VPN > IPSec > Pre-Fragmentation を選択し、外部インターフェイスをダブルクリックし、DF Bit Setting Policy を Clear に設定します。Clear 設定を使用して、セキュリティ アプライアンスに大きいパケットを送信させることができます。

- Enter Port Number：IPSec over TCP 接続で使用するポート番号を指定します。

• Server Certificate：Easy VPN Remote 接続が、証明書マップが指定した特定の証明書を持つ Easy VPN サーバとの接続だけを許可するように設定します。このパラメータを使用して、Easy VPN サーバ証明書のフィルタリングをイネーブルにします。証明書マップを定義するには、Configuration > VPN > IKE > Certificate Group Matching > Rules にアクセスします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—