



# CHAPTER 30

## SSL VPN Wizard

### SSL VPN 機能

クライアントレス ブラウザベース SSL VPN によって、ユーザは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リモート アクセス VPN トンネルを確立できます。認証後にポータル ページを開き、サポートされる特定の内部リソースにアクセスできます。ネットワーク管理者は、グループ単位でユーザごとにリソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースには直接アクセスできません。

Cisco AnyConnect VPN クライアントによって、リモートユーザは、企業リソースへの完全な VPN トンネリングを使用して、セキュリティ アプライアンスにセキュアな SSL 接続を実行できます。リモートユーザは、あらかじめインストール済みのクライアントがなくても、クライアントレス SSL VPN 接続を受け入れるように設定されたインターフェイスのブラウザに IP アドレスを入力します。セキュリティ アプライアンスは、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロード後に、クライアントはクライアント自体をインストールして設定し、セキュアな SSL 接続を確立して、接続の終了時には（セキュリティ アプライアンスの設定に応じて）インストールされたまま残るか、またはクライアント自体をアンインストールします。あらかじめインストール済みのクライアントの場合、ユーザが認証を行うと、セキュリティ アプライアンスはクライアントのリビジョンを調べ、必要に応じてクライアントをアップグレードします。

#### フィールド

- [Clientless SSL VPN Access] : サポートされる特定の内部リソースに対する、ポータル ページからのクライアントレス ブラウザベース接続をイネーブルにします。
- [Cisco SSL VPN Client (AnyConnect VPN Client)] : 完全なネットワーク アクセスを実現する SSL VPN クライアント接続をイネーブルにします。セキュリティ アプライアンスをイネーブルにして、AnyConnect クライアントをリモート ユーザにダウンロードします。

#### モード

次の表は、この機能を使用できるモードを示したものです。

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

## [SSL VPN Interface]

このウィンドウでは、接続名（以前のトンネルグループ）を指定し、SSL VPN 接続のインターフェイスをイネーブルにし、デジタル証明書情報を指定します。

### フィールド

- [Connection Name] : このコネクション型アトリビュートグループの接続名を指定します。
- [SSL VPN Interface] : SSL VPN 接続を許可するインターフェイスを指定します。
- [Digital Certificate] : セキュリティアプライアンスがリモート PC に送信する証明書が存在する場合は、その証明書を指定します。
  - [Certificate] : 証明書の名前を指定します。
- [Connection Group Settings] : セキュリティアプライアンスをイネーブルにして、この接続のグループエイリアスをログインページに表示できます。
  - [Connection Group Alias] : 接続のエイリアス名を指定します。
  - [Display Group Alias list at the login page] : グループエイリアスを表示する場合にイネーブルにします。
- [Information] : SSL VPN 接続と ASDM 接続を確立するためのリモートユーザが必要とする情報を表示します。

### モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	トランスペアレント	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

## [User Authentication]

この画面では、認証情報を指定します。

### フィールド

- [Authenticate using a AAA server group] : セキュリティアプライアンスがリモート AAA サーバグループにアクセスしてユーザを認証できるようにする場合にイネーブルにします。
- [AAA Server Group Name] : 事前設定されたグループのリストから AAA サーバグループを選択するか、または [New] をクリックして新しいグループを作成します。
- [Authenticate using the local user database] : セキュリティアプライアンスに保存されているローカルデータベースに新しいユーザを追加します。
  - [Username] : ユーザのユーザ名を作成します。
  - [Password] : ユーザのパスワードを作成します。
  - [Confirm Password] : 確認のために同じパスワードを再入力します。
  - [Add/Delete] : ローカルデータベースにユーザを追加またはデータベースから削除します。

**モード**

次の表は、この機能を使用できるモードを示したものです。

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

## [Group Policy]

グループ ポリシーによって、ユーザ グループの共通アトリビュートを設定します。新しいグループ ポリシーを作成するか、または既存のポリシーを選択して修正します。

**フィールド**

- [Create new group policy] : 新しいグループ ポリシーを作成する場合にイネーブルにします。新しいポリシーの名前を入力します。
- [Modify existing group policy] : 修正する既存のグループ ポリシーを選択します。

**モード**

次の表は、この機能を使用できるモードを示したものです。

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

## [Bookmark List]

ブックマーク リストは、クライアントレス ブラウザベース接続のポータル ページに表示されます。SSL VPN クライアント ユーザには、これらのブックマークは表示されません。このウィンドウでは、新しいブックマーク リストを作成します。

**フィールド**

- [Bookmark List] : 既存のリストを選択するか、または [Manage] をクリックして新しいリストを作成します。あるいは、ブックマーク リストをインポートまたはエクスポートします。

**モード**

次の表は、この機能を使用できるモードを示したものです。

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

## [IP Address Pools and Client Image]

このウィンドウでは、リモート SSL VPN ユーザに対する IP アドレス範囲を入力し、セキュリティ アプライアンスに対する SSL VPN クライアント イメージを指定します。

**フィールド**

- [IP Address Pool] : SSL VPN クライアントはセキュリティ アプライアンスに接続するときに新しい IP アドレスを受け取ります。クライアントレス接続では新しい IP アドレスは不要です。アドレス プールでは、リモート クライアントが受け取ることのできるアドレス範囲が定義されます。
- [IP Address Pool] : 既存の IP アドレス プールを選択するか、または [New] をクリックして新しい プールを作成します。
- [AnyConnect VPN Client Image Location] : フラッシュメモリ内の SSL VPN クライアント イメージであるセキュリティ アプライアンス ファイルに対して指定します。[Browse] をクリックして ローカル PC 上のイメージの場所を指定します。
  - [Location] : フラッシュ メモリに保存されている有効な SSL VPN クライアント イメージのパスおよびファイル名を入力します。
  - [Download Latest AnyConnect VPN Client form CCO] : 最新クライアント イメージのソフトウェア ダウンロード ページに移動するには、このリンクをクリックします。

**モード**

次の表は、この機能を使用できるモードを示したものです。

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

## [Summary]

これまでのウィザードのウィンドウで行った選択の要約を表示します。

### モード

次の表は、この機能を使用できるモードを示したものです。

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

