設定の開始

この章では、VPN 3000 コンセントレータの クイック コンフィギュレーション プログラムの概要を示し、対応する機能を ASDM のどこで設定するかを説明します。また、設定タスクの概要に続いて、サイトツーサイトおよびリモート アクセスのトンネルを設定するための VPN ウィザードの実行に必要な情報のリストも提供します。

クイック コンフィギュレーションのタスクと対応する ASDM の機能

表 3-1 に、次の設定タスクと、ASDM でこれらを実行する場所を示します。

- IP インターフェイスの設定
- システム情報の設定
- トンネリング プロトコルとオプションの設定
- アドレス管理方式の設定
- 認証の設定
- 内部サーバのユーザ データベースの設定
- IPSec グループの設定
- 管理者パスワードの設定

表 3-1　最初のタスク

VPN 3000 クイック コンフィギュレーションのタスク	ASA の対応する機能
IP インターフェイスの設定 プライベート イーサネット接続およびパブリック イーサネット接続のアドレスとサブネット マスクを入力します。オプションとして、外部インターフェイスのアドレスを入力します。 • イネーブル / ディセーブル • DHCP クライアント / システムの名前 • 固定 IP アドレッシング（IP アドレス / サブネット マスク） • インターフェイスのタイプ（パブリックまたはプライベート） • MAC アドレス • フィルタ • 速度 • 二重化 • MTU	**Configuration > Interfaces** に移動します。 • 次の項目を追加 / 編集します。 　– ハードウェア ポートの選択 　– インターフェイスのイネーブル化 • 次の項目を入力します。 　– VLAN ID 　– サブインターフェイス ID 　– インターフェイス名 　– セキュリティ レベル 　– IP アドレスの送信元：固定 IP または DHCP 　– IP アドレス 　– サブネット マスク 　– MTU • **Configure Hardware Properties...** をクリックします。 　– 二重化タイプを選択：全二重、半二重、自動 　– 速度を選択：10、100、自動 • オプションとして、同一のセキュリティ レベルが設定された 2 つ以上のインターフェイス間のトラフィックをイネーブルにできます。
システム情報の設定 • システムのホスト名 • 日時 • DNS サーバ情報（IP アドレス、インターネット ドメイン名、デフォルト ゲートウェイ）	**Configuration > Properties > Device Administration > Device** に移動します。 • ホスト名とドメイン名を入力します。 • **Configuration > Properties >Device Administration > Clock** に移動して、日時を入力します。 • **Configuration > Properties > DNS Client** に移動します。 　– サーバを追加します（上限は 6）。 　– タイムアウトを秒で入力します。 　– リトライ回数を入力します。 　– インターフェイスの DNS ルックアップをイネーブルにします。
トンネリング プロトコルとオプションの設定 • PPTP：暗号化オプション • L2TP：暗号化オプション • IPSec（リモート アクセスのみを許可します。QC を介したサイトツーサイトでは実行できません）。	トンネル グループを定義するには、**Configuration > VPN > General > Tunnel Group** に移動します。 IPSec には次の 2 つのデフォルト トンネル グループがあります。 • LAN 間用の DefaultL2LGroup • リモート アクセス用の DefaultRAGroup

表 3-1　最初のタスク

VPN 3000 クイック コンフィギュレーションのタスク	ASA の対応する機能
アドレス管理方式の設定 • クライアントが独自に IP アドレスを指定します。 • ユーザごとに IP アドレスを割り当てます（認証サーバを使用）。 • DHCP を使用します（サーバ アドレスまたはサーバ名を指定）。 • プールを設定します（開始 / 終了の範囲）。	**Configuration > VPN > IP Address Management > Assignment** に移動します。 いずれかを選択します。 • 認証サーバから付与されたアドレスを使用します。 • DHCP を使用します。 • 内部アドレス プールを使用します。 • **Configuration > VPN > IP Address Management > IP Pools** で IP アドレス プールを設定します。
認証の設定 • サーバ タイプを選択します：内部、RADIUS、NTDomain、SDI、Kerberos/Active Directory。 • 選択した認証サーバの情報を入力します。それぞれ独自の画面が用意されています。	**Configuration > Properties > AAA Setup** に移動します。 • サーバ グループを追加します。 • サーバ グループにサーバを追加します。 • 認証プロンプトを設定します。
内部サーバのユーザ データベースの設定 次のユーザ情報を入力します。 • ユーザ名 • パスワード • パスワードの確認 • IP アドレス（ユーザごとにアドレスが割り当てられている場合） • サブネット マスク	**Configuration > Properties > Device Administration > User Accounts** に移動します。 ユーザ アカウントを追加し、次の情報を入力します。 • Identity の項目： ユーザ名 パスワード パスワードの確認 特権レベル • VPN Policy の項目（指定するか、またはグループ ポリシーから継承する場合は選択する）： グループ ポリシー（以前に定義済み） トンネリング プロトコル フィルタ トンネル グループ ロック クライアント システムにパスワードを保存 接続の設定 専用の IP アドレス（オプション）
IPSec グループの設定 • グループ名 • パスワード • 確認	**Configuration > VPN > General > Tunnel Group** に移動します。 IPSec タイプのトンネル グループを追加します。
管理者パスワードの設定	**Configuration > Properties > Device Administration > Password** に移動します。
VPN 接続手順のテスト	

VPN ウィザードを使用した VPN トンネルの設定

VPN ウィザードを使用すると、ASA から別の VPN デバイスまたはリモート クライアント ユーザのいずれかへの VPN トンネルを設定できます。この VPN トンネルは、サイトツーサイト アクセスまたはリモート アクセスに使用します。このウィザードは、新しい VPN 設定を定義する場合にだけ使用できます。このウィザードを使用して設定した VPN トンネルについては、ASDM 機能を使用して（特に **Configuration > Features > VPN** セクションで使用して）編集できます。

情報の収集

VPN ウィザードを起動する前に、VPN トンネルの設定に必要な情報を収集します。設定するトンネル タイプの項を参照してください。

- サイトツーサイト VPN トンネル
- ローカルに保存されたユーザ アカウントを使用したリモート アクセス
- クライアント認証に AAA サーバ グループを使用したリモート アクセス

サイトツーサイト VPN トンネル

VPN ウィザードを使用してサイトツーサイト VPN トンネルを設定する場合は、事前に次の情報を収集する必要があります。

（注）　これらの値を記録する場合は、関連付けられている番号をメモしてください。これらの値は、このデータを収集した後で実行する VPN ウィザードに表示されるステップ番号に対応しています。

1. VPN トンネル タイプ

   サイトツーサイト VPN トンネル用のインターフェイス（たとえば、「inside」や「outside」）。VPN トンネルを設定する前に、セキュリティ アプライアンスにインターフェイスを設定します。トンネルを設定する場合は、設定する VPN トンネルに関連付けるインターフェイスを選択します。

2. リモート サイト ピア

   トンネルのもう一方の終端にあるピア デバイスの IP アドレス。

   トンネル グループのオプション名（ピアの IP アドレスのデフォルト）。

   認証タイプ（事前共有鍵またはデジタル証明書）。次のいずれかも必要です。

   - 事前共有鍵の場合は、鍵の名前。
   - デジタル証明書の場合は、証明書署名アルゴリズム（RSA または DSA）、およびトラストポイントの名前。

     RSA アルゴリズムと DSA アルゴリズムの違いについては、「鍵ペア」を参照してください。

     トラストポイントは、CA または ID ペアを示します。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、および 1 つの登録済み ID 証明書とのアソシエーションが含まれています。

     （注）　デジタル証明書認証タイプを選択する場合は、VPN ウィザードを実行する前に、トラストポイントを設定します（P.4-4 の「トラストポイントの作成」を参照してください）。

3. トンネルのネゴシエートに使用する IPSec フェーズ 1 Internet Key Exchange Security Association ポリシー。これは、次のもので構成されます。
   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）: MD5 または SHA。デフォルトは SHA です。

     Diffie Hellman グループ（両方のデバイスで同じである必要がある）：グループ 1、グループ 2、グループ 5、またはグループ 7。デフォルトはグループ 2 です。
4. VPN トンネルに適用する IPSec フェーズ 2 Encryption and Authentication ポリシー。パラメータとオプションは、次のとおりです。
   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）: MD5 または SHA。デフォルトは SHA です。
5. ローカル ホストとネットワーク：IP 接続のローカル サイトのホストとネットワーク。IP 接続のローカル サイトにおけるホストおよびネットワークを指定するには、次のオプションがあります。
   - IP アドレス。このオプションを選択する場合は、次の情報が必要です。

     インターフェイス名 : ホストの接続先のインターフェイス、たとえば「inside」や「outside」。

     IP アドレス : any、特定のローカル ホストのアドレス、またはサブネット。any を選択すると、IP アドレスとサブネット マスクが 0.0.0.0 になります。

     サブネット マスク：255.255.255.255 ～ 0.0.0.0 の値。
   - ASA コンフィギュレーションにすでに存在するホストの名前。
   - 保護対象のネットワークまたはホストのリストを含むグループ。このオプションを選択する場合は、次の情報が必要です。

     ASA コンフィギュレーションにすでに存在するホストの名前。

     ASA コンフィギュレーションにすでに存在するグループの名前。

（注）　ホストまたはネットワークのグループ名を設定するには、**Configuration > Global Objects > Hosts/Networks** に移動します。

6. リモート ホストとネットワーク：IP 接続のリモート サイトのホストとネットワーク。

   オプションは、ローカル ホストとネットワークのオプションと同じです。

この項で説明した情報を準備した後、「VPN ウィザードの実行」に進みます。

ローカルに保存されたユーザ アカウントを使用したリモート アクセス

リモート アクセス VPN トンネルで ASA コンフィギュレーションにログイン アカウントを保存する必要がある場合は、次の情報を収集します。

（注）　これらの値を記録する場合は、関連付けられている番号をメモしてください。これらの番号は、VPN ウィザードに表示されるステップ番号に対応しています。

1. VPN トンネル タイプ

   サイトツーサイト VPN トンネル用のインターフェイス（たとえば、「inside」や「outside」）。VPN トンネルを設定する前に、セキュリティ アプライアンスにインターフェイスを設定します。トンネルを設定する場合は、設定する VPN トンネルに関連付けるインターフェイスを選択します。

2. リモートアクセス クライアント

   デフォルト設定（Cisco VPN Client リリース 3.x 以上、または他の Easy VPN Remote 製品）を使用して、この ASA へのトンネルでサポートされる VPN クライアントのタイプを指定します。このリリースでは、他のオプションはサポートされていません。

3. VPN トンネル グループ名および認証方式

   リモート クライアントと ASA の両方に使用するトンネル グループの名前。このグループ名によって、次のステップで指定する共通の接続設定およびクライアント設定が決まります。

   認証タイプ（事前共有鍵またはデジタル証明書）。次のいずれかも必要です。

   - 事前共有鍵の場合は、鍵の名前。
   - デジタル証明書の場合は、証明書署名アルゴリズム（RSA または DSA）、およびトラストポイントの名前。

     RSA アルゴリズムと DSA アルゴリズムの違いについては、「鍵ペア」を参照してください。

     トラストポイントは、CA または ID ペアを示します。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、および 1 つの登録済み ID 証明書とのアソシエーションが含まれています。

   （注）　デジタル証明書認証タイプを選択する場合は、VPN ウィザードを実行する前に、トラストポイントを設定します（Configuration > Properties > Certificate > Trustpoint）。

4. クライアント認証（次のいずれかのオプションを選択できる）

   - ローカル（内部）ユーザ データベースを使用した認証。

     このオプションでは、ASA コンフィギュレーションにユーザ アカウントを入力できます。
   - AAA サーバ グループを使用した認証。

     このオプションでは、クライアント認証を処理するための AAA サーバ グループを選択できます。このオプションを選択した場合は、次の項の同じステップに進みます。

5. ユーザ アカウント

   「Authenticate using the local (internal) user database」を選択した場合は、ローカル データベースに挿入するために、各ユーザのログイン名とそれぞれのパスワードをリストします。

6. アドレス プール

   ASA コンフィギュレーション内にすでに存在する IP アドレス プールの名前を選択することも、新しい IP アドレス プールを指定することもできます。新しい IP アドレス プールを指定する場合は、新しいプールの名前、関連付けられる IP アドレス範囲、およびサブネット マスク（オプション）が必要です。

7. （オプション）クライアントにプッシュするアトリビュート

   VPN クライアントの接続時に、VPN クライアントに次のアトリビュートをプッシュするよう選択できます。

   - プライマリおよびセカンダリ DNS サーバの IP アドレス。
   - プライマリおよびセカンダリ WINS サーバの IP アドレス。
   - デフォルト ドメイン名。

8. トンネルのネゴシエートに使用する IPSec フェーズ 1 Internet Key Exchange Security Association ポリシー。これは、次のもので構成されます。
   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）: MD5 または SHA。デフォルトは SHA です。

     Diffie Hellman グループ（両方のデバイスで同じである必要がある）：グループ 1、グループ 2、グループ 5、またはグループ 7。デフォルトはグループ 2 です。
9. VPN トンネルに適用する IPSec フェーズ 2 Encryption and Authentication ポリシー。パラメータとオプションは、次のとおりです。
   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）: MD5 または SHA。デフォルトは SHA です。
10. （オプション）アドレス変換免除およびスプリット トンネリング

    VPN の認証済みリモート ユーザに公開される、内部ネットワーク内のホストおよびネットワーク。none を指定してトンネル内の認証済みリモート ユーザに内部ネットワーク全体を公開するか、トンネル内の認証済みリモート ユーザに公開する内部アドレスを指定して、残りのアドレスがネットワーク アドレス変換によって隠蔽されたままになるようにします。IP 接続のローカル サイトにおけるホストおよびネットワークの内部アドレスを指定するには、次のオプションがあります。
    - IP アドレス。このオプションを選択する場合は、次の情報が必要です。

      インターフェイス名 : ホストの接続先のインターフェイス、たとえば「inside」や「outside」。

      IP アドレス : any、特定のローカル ホストのアドレス、またはサブネット。any を選択すると、IP アドレスとサブネット マスクが 0.0.0.0 になります。

      サブネット マスク：255.255.255.255 ～ 0.0.0.0 の値。
    - ASA コンフィギュレーションにすでに存在するホストの名前。
    - 保護対象のネットワークまたはホストのリストを含むグループ。このオプションを選択する場合は、次の情報が必要です。

      ASA コンフィギュレーションにすでに存在するホストの名前。

      ASA コンフィギュレーションにすでに存在するグループの名前。

（注）　ホストまたはネットワークのグループ名を設定するには、**Configuration > Global Objects > Hosts/Networks** に移動します。

スプリット トンネリング：イネーブルにして VPN ユーザによるインターネットへの暗号化されていないアクセスを可能にするか、またはディセーブルのままにします。

（注）　スプリット トンネリングをイネーブルにすると、上記で指定したホストがスプリット トンネル アクセス リストとしても機能します。

この項で説明した情報を準備した後、「VPN ウィザードの実行」に進みます。

クライアント認証に AAA サーバ グループを使用したリモート アクセス

AAA サーバ グループを使用したクライアント認証が必要なリモート アクセス VPN トンネルには、次の情報を収集します。

（注）　これらの値を記録する場合は、関連付けられている番号をメモしてください。これらの番号は、VPN ウィザードに表示されるステップ番号に対応しています。

1. VPN トンネル タイプ

   サイトツーサイト VPN トンネル用のインターフェイス（たとえば、「inside」や「outside」）。VPN トンネルを設定する前に、セキュリティ アプライアンスにインターフェイスを設定します。トンネルを設定する場合は、設定する VPN トンネルに関連付けるインターフェイスを選択します。

2. リモートアクセス クライアント

   デフォルト設定（Cisco VPN Client リリース 3.x 以上、または他の Easy VPN Remote 製品）を使用して、この ASA へのトンネルでサポートされる VPN クライアントのタイプを指定します。このリリースでは、他のオプションはサポートされていません。

3. VPN トンネル グループ名および認証方式

   リモート クライアントと ASA の両方に使用するトンネル グループの名前。このグループ名によって、次のステップで指定する共通の接続設定およびクライアント設定が決まります。

   認証タイプ（事前共有鍵またはデジタル証明書）。次のいずれかも必要です。

   - 事前共有鍵の場合は、鍵の名前。
   - デジタル証明書の場合は、証明書署名アルゴリズム（RSA または DSA）、およびトラストポイントの名前。

     RSA アルゴリズムと DSA アルゴリズムの違いについては、「鍵ペア」を参照してください。

     トラストポイントは、CA または ID ペアを示します。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、および 1 つの登録済み ID 証明書とのアソシエーションが含まれています。

     （注）　デジタル証明書認証タイプを選択する場合は、VPN ウィザードを実行する前に、トラストポイントを設定します（Configuration > Properties > Certificate > Trustpoint）。

4. クライアント認証（次のいずれかのオプションを選択できる）

   - ローカル（内部）ユーザ データベースを使用した認証。

     このオプションでは、ASA コンフィギュレーションにユーザ アカウントを入力できます。このオプションを選択した場合は、前の項のステップ 5 から操作を続けます。

   - AAA サーバ グループを使用した認証。

     このオプションを選択した場合は、コンフィギュレーションに追加済みの AAA サーバ グループの名前を選択するか、または新しい名前を作成します。**Configuration** > **Properties** > **AAA Setup** パスでは、AAA サーバのコンフィギュレーションを確認および管理できます。これらの認証オプションを提供する VPN ウィザードの Client Authentication パネルには、AAA サーバ グループの作成に使用できる **New** ボタンもあります。このオプションを選択した場合は、グループ名の入力、認証プロトコルの選択（RADIUS、TACACS+、SDI、NT、Kerberos のいずれか）、サーバの IP アドレスの指定、インターフェイスの選択（「inside」または「outside」）、およびサーバの秘密鍵の指定を実行できるように準備しておいてください。

5. アドレス プール

ASA コンフィギュレーション内にすでに存在する IP アドレス プールの名前を選択することも、新しい IP アドレス プールを指定することもできます。新しい IP アドレス プールを指定する場合は、新しいプールの名前、関連付けられる IP アドレス範囲、およびサブネット マスク（オプション）が必要です。

6. （オプション）クライアントにプッシュするアトリビュート

VPN クライアントの接続時に、VPN クライアントに次のアトリビュートをプッシュするよう選択できます。

- プライマリおよびセカンダリ DNS サーバの IP アドレス。
- プライマリおよびセカンダリ WINS サーバの IP アドレス。
- デフォルト ドメイン名。

7. トンネルのネゴシエートに使用する IPSec フェーズ 1 Internet Key Exchange Security Association ポリシー。これは、次のもので構成されます。

- IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）: DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
- IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）: MD5 または SHA。デフォルトは SHA です。

  Diffie Hellman グループ（両方のデバイスで同じである必要がある）: グループ 1、グループ 2、グループ 5、またはグループ 7。デフォルトはグループ 2 です。

8. VPN トンネルに適用する IPSec フェーズ 2 Encryption and Authentication ポリシー。パラメータとオプションは、次のとおりです。

- IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）: DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
- IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）: MD5 または SHA。デフォルトは SHA です。

9. （オプション）アドレス変換免除およびスプリット トンネリング

VPN の認証済みリモート ユーザに公開される、内部ネットワーク内のホストおよびネットワーク。none を指定してトンネル内の認証済みリモート ユーザに内部ネットワーク全体を公開するか、トンネル内の認証済みリモート ユーザに公開する内部アドレスを指定して、残りのアドレスがネットワーク アドレス変換によって隠蔽されたままになるようにします。IP 接続のローカル サイトにおけるホストおよびネットワークの内部アドレスを指定するには、次のオプションがあります。

- IP アドレス。このオプションを選択する場合は、次の情報が必要です。

  インターフェイス名 : ホストの接続先のインターフェイス、たとえば「inside」や「outside」。

  IP アドレス : any、特定のローカル ホストのアドレス、またはサブネット。any を選択すると、IP アドレスとサブネット マスクが 0.0.0.0 になります。

  サブネット マスク：255.255.255.255 ～ 0.0.0.0 の値。
- ASA コンフィギュレーションにすでに存在するホストの名前。
- 保護対象のネットワークまたはホストのリストを含むグループ。このオプションを選択する場合は、次の情報が必要です。

  ASA コンフィギュレーションにすでに存在するホストの名前。

  ASA コンフィギュレーションにすでに存在するグループの名前。

（注）　ホストまたはネットワークのグループ名を設定するには、**Configuration > Global Objects > Hosts/Networks** に移動します。

スプリット トンネリング：イネーブルにして VPN ユーザによるインターネットへの暗号化されていないアクセスを可能にするか、またはディセーブルのままにします。

（注）　スプリット トンネリングをイネーブルにすると、上記で指定したホストがスプリット トンネル アクセス リストとしても機能します。

この項で説明した情報を準備した後、「VPN ウィザードの実行」に進みます。

VPN ウィザードの実行

VPN ウィザードを実行するには、次の手順を実行します。

ステップ 1　**Wizards > VPN Wizard** に移動します。

ステップ 2　設定するトンネルのタイプとして、**Site to Site** または **Remote Access** を選択します。

ステップ 3　VPN Tunnel インターフェイスの横にある **Inside** または **Outside** を選択します。

ステップ 4　**Next** をクリックして、VPN ウィザードの指示に従います。詳細については、**Help** をクリックしてください。

コンフィギュレーションの保存

作業中は、次の手順を使用して、変更内容をフラッシュ メモリに保存して保持することを忘れないようにしてください。

- ASDM の場合：**File** > **Save Running Configuration to Flash** を選択します。
- CLI の場合：**write memory** コマンドを入力します。

コンフィギュレーションの表示

現在のコンフィギュレーション設定を表示するには、次のいずれかのコマンドを入力します。

- hostname# **show config**

  このコマンドを入力すると、フラッシュ メモリに保存されたスタートアップ コンフィギュレーションが表示されます。
- hostname# **show running-config**

  このコマンドを入力すると、オペレーティング コンフィギュレーションが表示されます。
- hostname# **show running config all**

  このコマンドを入力すると、デフォルト値を持つアトリビュートを含むオペレーティング コンフィギュレーションが表示されます。

（注）　最初の 2 つのコマンドは、実行したコンフィギュレーション変更を保存した場合は同じになります。

また、**show run ?** と入力すると、より詳細なリストを取得するために入力する show configuration コマンドの詳細なリストが表示されます。

ASDM の使用による CLI の学習

ASDM の **Options** > **Preferences** ウィンドウには、「Preview commands before sending to the device」オプションが表示されます。このオプションをイネーブルにすると、**Apply** をクリックするたびに、同等の CLI コマンドが Preview CLI Commands ウィンドウに表示されます。

コマンドを表示したら、**OK** をクリックし、次に確認ウィンドウで **Proceed** をクリックすると、実行コンフィギュレーションへの変更が保存されます。