VPN ウィザード

VPN の概要

ASA は、ユーザーがプライベート接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することにより、バーチャル プライベート ネットワークを構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。

セキュアな接続はトンネルと呼ばれ、ASA はトンネリング プロトコルを使用して、セキュリティパラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを介したパケットの送受信、パケットのカプセル化解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティアプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

VPN ウィザードを使用すると、基本的な LAN-to-LAN とリモート アクセス VPN 接続を設定して、事前共有キーまたはデジタル証明書を認証用に割り当てることができます。ASDM を使用して拡張機能を編集および設定してください。

ここでは、次の 4 つの VPN ウィザードについて説明します。

- セキュアクライアント VPN ウィザード （5 ページ）

  Cisco Secure Client AnyConnect VPN モジュールは、ASA へのセキュアな SSL 接続または IPsec（IKEv2）接続を提供し、これにより、リモートユーザーによる企業リソースへのフル VPN トンネリングが可能になります。事前にクライアントがインストールされていない場合、リモート ユーザーは、クライアントレス 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 IP アドレスをブラウザに入力します。ASA 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。ダウンロードが完了すると、クライアントが自動的にインストールされて設定され、セキュアな接続が確立されます。接続が終了すると、ASA の設定に応じて、クライアントはそのまま残るか、またはアンインストールされます。以前からインストールされているクライアントの場合は、ユーザーの認証時に、ASA によってクライアントのリビジョンが点検され、必要に応じてアップグレードされます。

セキュアクライアント VPN ウィザードは、ASA がマルチコンテキストモードのときにユーザーコンテキストのみで利用可能になります。必要なコンテキストのストレージとリソース クラスは、システム コンテキストから設定する必要があります。

Cisco セキュアクライアント パッケージとプロファイルファイルを使用するには、コンテキストごとのストレージが必要です。各コンテキストのライセンスの割り当てには、リソース クラスが必要です。使用するライセンスは、セキュアクライアント Premium です。

（注） このウィザードの残りの設定は、シングルコンテキストの場合と同じです。

- IPsec IKEv2 Remote Access Wizard （13 ページ）

  IKEv2 によって、他のベンダーの VPN クライアントが ASA に接続できます。これにより、セキュリティが強化されるとともに、国や地方自治体が規定している IPsec リモートアクセス要件を満たすことができます。

  IPSec IKEv2 リモート アクセス ウィザードは、ASA がマルチコンテキスト モードのときにユーザー コンテキストのみで利用可能になります。必要なコンテキストのリソース クラスは、ライセンス割り当て用のシステム コンテキストから設定する必要があります。使用するライセンスは、セキュアクライアント Premium です。

（注） このウィザードの残りの設定は、シングルコンテキストの場合と同じです。

- IPsec IKEv1 Remote Access Wizard （8 ページ）
- IPsec Site-to-Site VPN Wizard （3 ページ）

  LAN-to-LAN 接続で IPv4 と IPv6 の両方のアドレッシングが使用されている場合、ASA で VPN トンネルがサポートされるのは、両方のピアが ASA であり、かつ両方の内部ネットワークのアドレッシング方式が一致している（両方とも IPv4 または IPv6）ときです。これは、両方のピアの内部ネットワークが IPv6 で外部ネットワークが IPv6 の場合にも当てはまります。

IPsec Site-to-Site VPN Wizard

2 台の ASA デバイス間のトンネルは「サイトツーサイト トンネル」と呼ばれ、双方向です。サイトツーサイト VPN トンネルでは、IPsec プロトコルを使用してデータが保護されます。

Peer Device Identification

- [Peer IP Address]：他のサイト（ピア デバイス）の IP アドレスを設定します。
- [VPN Access Interface]：サイトツーサイト トンネルに使用するインターフェイスを選択します。
- [Crypto Map Type]：このピアに使用されるマップのタイプ（スタティックまたはダイナミック）を指定します。

Traffic to Protects

このステップでは、ローカル ネットワークおよびリモート ネットワークを指定します。これらのネットワークでは、IPsec 暗号化を使用してトラフィックが保護されます。

- [Local Networks]：IPsec トンネルで使用されるホストを指定します。
- [Remote Networks]：IPsec トンネルで使用されるネットワークを指定します。

セキュリティ

このステップでは、ピアデバイスとの認証の方法を設定します。単純な設定を選択するか、事前共有キーを指定できます。またさらに詳細なオプションについては、以下に説明する [Customized Configuration] を選択できます。

- [IKE Version]：どちらのバージョンを使用するかに応じて、[IKEv1] または [IKEv2] チェックボックスをオンにします。
- IKE version 1 Authentication Methods
  - [Pre-shared Key]：事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

    IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモート サイトの管理者と事前共有キーを交換してください。
  - [Device Certificate]：ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。

    デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP

アドレスなどの、ユーザーまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

- IKE version 2 Authentication Methods
  - [Local Pre-shared Key]：IPsec IKEv2 認証方式と暗号化アルゴリズムを指定します。
  - [Local Device Certificate]：VPN アクセスの認証を、セキュリティ アプライアンスを通して行います。
  - [Remote Peer Pre-shared Key]：ローカル ASA とリモート IPsec ピア間の認証で事前共有キーを使用する場合にクリックします。
  - [Remote Peer Certificate Authentication]：このチェックボックスがオンのときは、ピアデバイスが証明書を使用してこのデバイスに対して自身の認証を行うことができます。

- [Encryption Algorithms]：このタブでは、データの保護に使用する暗号化アルゴリズムのタイプを選択します。
  - [IKE Policy]：IKEv1/IKEv2 認証方式を指定します。
  - [IPsec Proposal]：IPsec 暗号化アルゴリズムを指定します。

- Perfect Forward Secrecy
  - [Enable Perfect Forwarding Secrecy (PFS)]：フェーズ 2 IPsec キーの生成において、Perfect Forward Secrecy を使用するかどうか、および使用する番号のサイズを指定します。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPsec ネゴシエーションでは、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成に Diffie-Hellman 方式が採用されています。

    PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

    PFS は、接続の両側でイネーブルにする必要があります。
  - [Diffie-Hellman Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトのグループ 14（2048 ビット Diffie-Hellman）。

NAT Exempt

- [Exempt ASA side host/network from address translation]：ドロップダウン リストを使用して、アドレス変換から除外するホストまたはネットワークを選択します。

セキュアクライアント VPN ウィザード

このウィザードは、 Cisco Secure Clientの AnyConnect VPN モジュールからの VPN 接続を受け入れるように ASA を設定するときに使用します。このウィザードでは、フル ネットワーク アクセスができるように IPsec（IKEv2）プロトコルまたは SSL VPN プロトコルを設定します。VPN 接続が確立したときに、ASA によって自動的に Cisco Secure Client の AnyConnect VPN モジュールがエンドユーザーのデバイスにアップロードされます。

Connection Profile Identification

[Connection Profile Identification] では、リモート アクセス ユーザーに対する ASA を指定します。

- [Connection Profile Name]：リモート アクセス ユーザーが VPN 接続のためにアクセスする名前を指定します。
- [VPN Access Interface]：リモート アクセス ユーザーが VPN 接続のためにアクセスするインターフェイスを選択します。

VPN Protocols

この接続プロファイルに対して許可する VPN プロトコルを指定します。

セキュアクライアント のデフォルトは SSL です。接続プロファイルの VPN トンネル プロトコルとして IPsec をイネーブルにした場合は、IPsec をイネーブルにしたクライアント プロファイルを作成して展開することも必要になります（作成するには、ASDM のプロファイル エディタを使用します）。

WebLaunch の代わりに セキュアクライアント を事前展開する場合は、最初のクライアント接続に SSL を使用し、セッション中に ASA からクライアントプロファイルを受け取ります。以降の接続では、クライアントはそのプロファイルで指定されたプロトコル（SSL または IPsec）を使用します。IPsec が指定されたプロファイルをクライアントとともに事前展開した場合は、最初のクライアント接続で IPsec が使用されます。IPsec をイネーブルにした状態のクライアントプロファイルを事前展開する方法の詳細については、『*Secure Client Administrator Guide*』を参照してください。

- SSL
- IPsec (IKE v2)
- [Device Certificate]：リモート アクセス クライアントに対する ASA を指定します。セキュアクライアント の機能の中には、Always on や IPsec/IKEv2 のように、有効なデバイス証明書が ASA に存在することを要件とするものがあります。
- [Manage]：[Manage] を選択すると [Manage Identity Certificates] ウィンドウが開きます。
  - [Add]：ID 証明書とその詳細情報を追加するには、[Add] を選択します。

- [Show Details]：特定の証明書を選択して [Show Details] をクリックすると、[Certificate Details] ウィンドウが開き、その証明書の発行対象者と発行者が表示されるほか、シリアル番号、使用方法、対応するトラストポイント、有効期間などが表示されます。
- [Delete]：削除する証明書を強調表示して [Delete] をクリックします。
- [Export]：証明書を強調表示して [Export] をクリックすると、その証明書をファイルにエクスポートできます。このときに、暗号化パスフレーズを付けるかどうかを指定できます。
- [Enroll ASA SSL VPN with Entrust]：Entrust からの SSL Advantage デジタル証明書を使用すると、すぐに ASA SSL VPN アプライアンスの稼働を開始できます。

Client Images

ASA は、クライアントデバイスがエンタープライズ ネットワークにアクセスするときに、最新の セキュアクライアント パッケージをそのデバイスに自動的にアップロードすることができます。ブラウザのユーザーエージェントとイメージとの対応を、正規表現を使用して指定できます。また、接続の設定に要する時間を最小限にするために、最もよく使用されるオペレーティング システムをリストの先頭に移動できます。

認証方法

この画面では、認証情報を指定します。

- [AAA server group]：ASA がリモート AAA サーバー グループにアクセスしてユーザーを認証できるようにします。AAA サーバー グループを、事前設定されたグループのリストから選択するか、[New] をクリックして新しいグループを作成します。
- [Local User Database Details]：ASA に格納されているローカル データベースに新しいユーザーを追加します。
  - [Username]：ユーザーのユーザー名を作成します。
  - [Password]：ユーザー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ーを追加またはデータベースから削除します。

Client Address Assignment

リモート セキュアクライアント ユーザのための IP アドレス範囲を指定します。

- [IPv4 Address Pools]：SSL VPN クライアントは、ASA に接続したときに新しい 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。既存の IP アドレス プールを選択するか、[New] をクリックして新しいプールを作成します。

[New] を選択した場合は、開始と終了の IP アドレスおよびサブネット マスクを指定する必要があります。

- [IPv6 Address Pool]：既存の IP アドレス プールを選択するか、[New] をクリックして新しいプールを作成します。

（注） IPv6アドレス プールは、IKEv2接続プロファイル用には作成できません。

Network Name Resolution Servers

リモートユーザーが内部ネットワークにアクセスするときにどのドメイン名を解決するかを指定します。

- [DNS Servers]：DNS サーバーの IP アドレスを入力します。
- [WINS Servers]：WINS サーバーの IP アドレスを入力します。
- [Domain Name]：デフォルトのドメイン名を入力します。

NAT Exempt

ASA 上でネットワーク変換がイネーブルに設定されている場合は、VPN トラフィックに対してこの変換を免除する必要があります。

セキュアクライアント の導入

次の2つの方法のいずれかを使用して、セキュアクライアントプログラムをクライアントデバイスにインストールできます。

- [Web起動（Web launch）]：セキュアクライアント パッケージは、Web ブラウザを使用して ASA にアクセスしたときに自動的にインストールされます。

（注） Web launch はマルチ コンテキスト モードではサポートされません。

- [事前展開（Pre-deployment）]：手動で セキュアクライアント パッケージをインストールします。

[Allow Web Launch] は、すべての接続に影響が及ぶグローバル設定です。このチェックボックスがオフ（許可しない）の場合は、セキュアクライアント SSL 接続とクライアントレス SSL 接続は機能しません。

事前展開の場合は、disk0:/test2_client_profile.xml プロファイル バンドルの中に .msi ファイルがあり、このクライアントプロファイルを ASA からセキュアクライアント パッケージに入れておく必要があります。これは、IPsec 接続を期待したとおりに確実に動作させるためです。

IPsec IKEv1 Remote Access Wizard

（注） Cisco VPN Client は耐用年数末期で、サポートが終了しています。Secure Clientにアップグレードする必要があります。

IKEv1 Remote Access Wizard を使用して、モバイル ユーザーなどの VPN クライアントに安全なリモート アクセスを設定し、リモート IPsec ピアに接続するインターフェイスを指定します。

- [VPN Tunnel Interface]：リモート アクセス クライアントで使用するインターフェイスを選択します。ASA に複数のインターフェイスがある場合は、このウィザードを実行する前に ASA でインターフェイスを設定します。
- [Enable inbound IPsec sessions to bypass interface access lists]：IPsec 認証済みの着信セッションを ASA によって常に許可するようにします（つまり、インターフェイスの access-list 文をチェックしないようにします）。着信セッションがバイパスするのは、インターフェイス ACL だけです。設定されたグループ ポリシー、ユーザー、およびダウンロードされた ACL は適用されます。

リモート アクセス クライアント

さまざまなタイプのリモート アクセス ユーザーが、この ASA への VPN トンネルを開くことができます。このトンネルの VPN クライアントのタイプを選択します。

- VPN Client Type
  - [Easy VPN Remote product]
  - [Microsoft Windows client using L2TP over IPsec]：PPP 認証プロトコルを指定します。選択肢は、PAP、CHAP、MS-CHAP-V1、MS-CHAP-V2、および EAP-PROXY です。

    [PAP]：認証中にクリアテキストのユーザー名とパスワードを渡すので、安全ではありません。

    [CHAP]：サーバーのチャレンジに対する応答で、クライアントは暗号化されたチャレンジとパスワードおよびクリアテキストのユーザー名を返します。このプロトコルは、PAP より安全ですが、データは暗号化されません。

    [MS-CHAP, Version 1]：CHAP と似ていますが、サーバーは、CHAP のようなクリアテキストのパスワードではなく、暗号化したパスワードだけを保存および比較するので安全です。

[MS-CHAP, Version 2]：MS-CHAP, Version 1 以上のセキュリティ強化機能が含まれています。

[EAP-Proxy]：EAP をイネーブルにします。これによって ASA は、PPP 認証プロセスを外部の RADIUS 認証サーバーに代行させることができます。

リモートクライアントでプロトコルが指定されていない場合は、指定しないでください。

- 指定するのは、クライアントからトンネル グループ名が username@tunnelgroup として送信される場合です。

VPN クライアント認証方式とトンネル グループ名

認証方式を設定し、接続ポリシー（トンネル グループ）を作成するには、[VPN Client Authentication Method and Name] ペインを使用します。

- [Authentication Method]：リモート サイト ピアは、事前共有キーか証明書のいずれかを使用して認証します。
  - [Pre-shared Key]：ローカル ASA とリモート IPsec ピア間の認証で事前共有キーを使用する場合にクリックします。

    事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

    IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモート サイトの管理者と事前共有キーを交換してください。

  - [Pre-shared Key]：1～128 文字の英数字文字列を入力します。

  - [Certificate]：ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、事前に CA に登録し、1 つ以上の証明書を ASA にダウンロードしておく必要があります。

    デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザーまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

    デジタル証明書を使用するには、デジタル証明書を発行する認証局（CA）に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

    2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

[Certificate Signing Algorithm]：デジタル証明書署名アルゴリズムを表示します（RSA の場合は rsa-sig）。

- [Tunnel Group Name]：名前を入力して、この IPsec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウンティング サーバー、デフォルト グループ ポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定する接続ポリシーは、認証方式を指定し、ASA のデフォルトのグループ ポリシーを使用します。

クライアント認証

[Client Authentication] ペインでは、ASA がリモート ユーザーを認証するときに使用する方法を選択します。次のオプションのいずれかを選択します。

- [Authenticate using the local user database]：ASA の内部の認証方式を使用する場合にクリックします。この方式は、ユーザーの数が少なくて安定している環境で使用します。次のペインでは、ASA に個々のユーザーのアカウントを作成できます。
- [Authenticate using an AAA server group]：リモート ユーザー認証で外部サーバー グループを使用する場合にクリックします。
  - [AAA Server Group Name]：先に構成された AAA サーバー グループを選択します。
  - [New ...]：新しい AAA サーバー グループを設定する場合にクリックします。

User Accounts

[User Accounts] ペインでは、認証を目的として、ASA の内部ユーザー データベースに新しいユーザーを追加します。

Address Pool

[Address Pool] ペインでは、ASA がリモート VPN クライアントに割り当てるローカル IP アドレスのプールを設定します。

- [Tunnel Group Name]：このアドレス プールが適用される接続プロファイル（トンネル グループ）の名前が表示されます。この名前は、[VPN Client Name and Authentication Method] ペイン（ステップ 3）で設定したものです。
- [Pool Name]：アドレス プールの記述 ID を選択します。
- [New...]：新しいアドレス プールを設定します。
- [Range Start Address]：アドレス プールの開始 IP アドレスを入力します。
- [Range End Address]：アドレス プールの終了 IP アドレスを入力します。
- [Subnet Mask]：（任意）これらの IP アドレスのサブネット マスクを選択します。

Attributes Pushed to Client (任意)

[Attributes Pushed to Client (Optional)] ペインでは、DNS サーバーと WINS サーバーに関する情報およびデフォルト ドメイン名をリモート アクセス クライアントに渡すように、ASA を設定します。

- [Tunnel Group]：アドレス プールが適用される接続ポリシーの名前を表示します。この名前は、[VPN Client Name and Authentication Method] ペインで設定したものです。
- [Primary DNS Server]：プライマリ DNS サーバーの IP アドレスを入力します。
- [Secondary DNS Server]：セカンダリ DNS サーバーの IP アドレスを入力します。
- [Primary WINS Server]：プライマリ WINS サーバーの IP アドレスを入力します。
- [Secondary WINS Server]：セカンダリ WINS サーバーの IP アドレスを入力します。
- [Default Domain Name]：デフォルトのドメイン名を入力します。

IKE Policy

Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれる IKE は、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。各 IKE ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。フェーズ 1 は、以後の IKE ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ2では、データを保護するトンネルが作成されます。

[IKE Policy] ペインでは、フェーズ 1 IKE ネゴシエーションの条件を設定します。この条件には、データを保護し、プライバシーを守る暗号化方式、ピアの ID を確認する認証方式、および暗号キー判別アルゴリズムを強化する Diffie-Hellman グループが含まれます。ASA はこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。

- [Encryption]：フェーズ 2 ネゴシエーションを保護するフェーズ 1 SA を確立するために ASA が使用する、対称暗号化アルゴリズムを選択します。ASA は、次の暗号化アルゴリズムをサポートしています。

アルゴリズム	説明
DES	データ暗号規格。56 ビット キーを使用します。
3DES	Triple DES。56 ビット キーを使用して暗号化を 3 回実行します。
AES-128	高度暗号化規格。128 ビット キーを使用します。
aes-192	192 ビット キーを使用する AES。
AES-256	256 ビット キーを使用する AES。

デフォルトの 3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。同様に、AESオプションによるセキュリティは強力ですが、必要な処理量も増大します。

- [Authentication]：認証やデータ整合性の確保のために使用するハッシュ アルゴリズムを選択します。デフォルトは SHA です。MD5 のダイジェストは小さく、SHA よりもわずかに速いとされています。MD5 は、（きわめて困難ですが）攻撃により破れることが実証されています。しかし、ASA で使用される Keyed-Hash Message Authentication Code（HMAC）バージョンはこの攻撃を防ぎます。
- [Diffie-Hellman Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルト DH グループ 14（2048 ビット）は、グループ 2 およびグループ 5 よりも安全性が高いと見なされます。

IPsec Settings（任意）

[IPsec Settings (Optional)] ペインでは、アドレス変換が不要なローカル ホスト/ネットワークを指定します。デフォルトでは、ASA は、ダイナミックまたはスタティックなネットワーク アドレス変換（NAT）を使用して、内部のホストおよびネットワークの実 IP アドレスを外部ホストから隠します。NAT は、信頼できない外部ホストによる攻撃の危険性を最小限に抑えますが、VPN によって認証および保護されているホストに対しては不適切な場合があります。

たとえば、ダイナミック NAT を使用する内部ホストは、プールから無作為に選択したアドレスと照合することにより、その IP アドレスを変換させます。外部ホストからは、変換されたアドレスだけが見えるようになります。本当の IP アドレスにデータを送信することによってこれらの内部ホストに到達しようとするリモート VPN クライアントは、NAT 免除ルールを設定しない限り、これらのホストには接続できません。

（注） すべてのホストとネットワークを NAT から免除する場合は、このペインでは何も設定しません。エントリが 1 つでも存在すると、他のすべてのホストとネットワークは NAT に従います。

- [Interface]：選択したホストまたはネットワークに接続するインターフェイスの名前を選択します。
- [Exempt Networks]：選択したインターフェイス ネットワークから免除するホストまたはネットワークの IP アドレスを選択します。
- [Enable split tunneling]：リモート アクセス クライアントからのパブリック インターネット宛のトラフィックを暗号化せずに送信する場合に選択します。スプリット トンネリングにより、保護されたネットワークのトラフィックが暗号化され、保護されていないネットワークのトラフィックは暗号化されません。スプリット トンネリングをイネーブルにすると、ASA は、認証後に IP アドレスのリストをリモート VPN クライアントにプッシュします。リモート VPN クライアントは、ASA の背後にある IP アドレスへのトラフィックを暗号化します。他のすべてのトラフィックは暗号化されずに直接インターネットに送り出され、ASA は関与しません。
- [Enable Perfect Forwarding Secrecy (PFS)]：フェーズ 2 IPsec キーの生成において、Perfect Forward Secrecy を使用するかどうか、および使用する番号のサイズを指定します。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトで

す。IPsec ネゴシエーションでは、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成に Diffie-Hellman 方式が採用されています。

PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

PFS は、接続の両側でイネーブルにする必要があります。

- [Diffie-Hellman Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルト DH グループ 14（2048 ビット）は、グループ 2 およびグループ 5 よりも安全性が高いと見なされます。

Summary

設定に問題なければ、[Finish] をクリックします。ASDM によって LAN-to-LAN のコンフィギュレーションが保存されます。[Finish] をクリックした後は、この VPN ウィザードを使用してこのコンフィギュレーションを変更することはできません。ASDM を使用して拡張機能を編集および設定してください。

IPsec IKEv2 Remote Access Wizard

IKEv2 Remote Access Wizard を使用して、モバイル ユーザーなどの VPN クライアントに安全なリモート アクセスを設定し、リモート IPsec ピアに接続するインターフェイスを指定します。

Connection Profile Identification

[Connection Profile Name] に接続プロファイルの名前を入力し、[VPN Access Interface] で IPsec IKEv2 リモート アクセスに使用する VPN アクセス インターフェイスを選択します。

- [Connection Profile Name]：名前を入力して、この IPsec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウンティング サーバー、デフォルト グループ ポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定する接続ポリシーは、認証方式を指定し、ASA のデフォルトのグループ ポリシーを使用します。
- [VPN Access Interface]：リモート IPsec ピアとのセキュアなトンネルを確立するインターフェイスを選択します。ASA に複数のインターフェイスがある場合は、このウィザードを実行する前に VPN コンフィギュレーションを計画し、セキュアな接続を確立する予定のリモート IPsec ピアごとに、使用するインターフェイスを特定しておく必要があります。

標準規格に基づく IPSec（IKEv2）認証ページ

[IKE Peer Authentication]：リモート サイト ピアは、事前共有キー、証明書、または EAP を使用したピア認証のいずれかを使用して認証します。

- [Pre-shared Key]：1～128 文字の英数字文字列を入力します。

  事前共有キーを使用すると、リモートピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

  IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモートサイトの管理者と事前共有キーを交換してください。

- [Enable Certificate Authentication]：オンにすると、認証に証明書を使用できます。
- [Enable peer authentication using EAP]：オンにすると、認証に EAP を使用できます。このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。
- [Send an EAP identity request to the client]：リモート アクセス VPN クライアントに EAP 認証要求を送信できます。

Mobike RRC

- [Enable Return Routability Check for mobike]：Mobike が有効になっている IKE/IPSEC セキュリティ アソシエーションにおけるダイナミック IP アドレスの変更をチェックする Return Routability を有効にします。

[IKE Local Authentication]

- ローカル認証をイネーブルにして、事前共有キーまたは証明書のいずれかを選択します。
  - [Preshared Key]：1 ～ 128 文字の英数字文字列を入力します。
  - [Certificate]：ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、事前に CA に登録し、1 つ以上の証明書を ASA にダウンロードしておく必要があります。

    デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザーまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

    デジタル証明書を使用するには、デジタル証明書を発行する認証局（CA）に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

    2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

認証方法

IPsec IKEv2 リモート アクセスでは RADIUS 認証のみがサポートされています。

- [AAA Server Group]：先に構成された AAA サーバー グループを選択します。
- [New]：新しい AAA サーバー グループを設定する場合にクリックします。
- [AAA Server Group Details]：この領域を使用して、AAA サーバー グループを必要に応じて変更します。

Client Address Assignment

IPv4 および IPv6 のアドレス プールを作成するか、選択します。リモート アクセス クライアントには、IPv4 または IPv6 のプールのアドレスが割り当てられます。両方を設定した場合は、IPv4 アドレスが優先されます。詳細については、「ローカル *IP* アドレス プールの設定」を参照してください。

Network Name Resolution Servers

リモートユーザーが内部ネットワークにアクセスするときにどのようにドメイン名を解決するかを指定します。

- [DNS Servers]：DNS サーバーの IP アドレスを入力します。
- [WINS Servers]：WINS サーバーの IP アドレスを入力します。
- [Default Domain Name]：デフォルトのドメイン名を入力します。

NAT Exempt

- [Exempt VPN traffic from Network Address Translation]：ASA で NAT がイネーブルになっている場合は、このチェックボックスをオンにする必要があります。

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