VPN ウィザード

ASA では、ほぼすべてのインターネット接続環境からの Secure Socket Layer（SSL）リモート アクセス接続機能を提供します。Web ブラウザとそのネイティブの SSL 暗号化機能だけでアクセスが可能です。クライアントレスでブラウザベースの VPN により、適応型セキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを、Web ブラウザを使用して確立できます。認証されると、ユーザにはポータル ページが表示され、サポートされる特定の内部リソースにアクセスできるようになります。ネットワーク管理者は、グループ単位でユーザにリソースへのアクセス権限を付与します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

Cisco AnyConnect VPN クライアントは ASA へのセキュアな SSL 接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN トンネリングが可能となります。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および設定され、セキュア接続が確立されます。接続終了時にクライアントが残されるか、アンインストールされるかは、ASA の設定で決まります。事前にクライアントがインストールされている場合は、ユーザの認証時に、ASA がクライアントのリビジョンを検査し、必要に応じてクライアントをアップグレードします。

IKEv2 のサポートがリリース 8.4 で追加されたことにより、AnyConnect クライアント セッションで使用されるトンネリング プロトコルに関係なく、エンド ユーザには同じユーザ エクスペリエンスが提供されます。この追加の結果、他ベンダーの VPN クライアントが ASA に接続できるようになります。このサポートによってセキュリティが強化されるとともに、IPsec リモート アクセスに関して国や地方自治体が定める要件も満たされます。

VPN ウィザードでは、基本的な LAN-to-LAN およびリモート アクセス VPN 接続を設定して、認証のための事前共有キーまたはデジタル証明書を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。

VPN の概要

ASA は、ユーザがプライベートな接続と見なす 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。

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ときに、セキュリティ アプライアンスで VPN トンネルがサポートされるのは、両方のピアが Cisco ASA 5500 シリーズ セキュリティ アプライアンスであり、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）場合です。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。

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、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向トンネル エンドポイントとして機能します。つまり、プレーン パケットを受信してカプセル化し、トンネルの反対側に送信できます。送信されたパケットはカプセル化が解除され、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。

ここでは、次の 4 つの VPN ウィザードについて説明します。

- IPsec IKEv1 Remote Access Wizard
- IPsec Site-to-Site VPN Wizard
- AnyConnect VPN Wizard
- Clientless SSL VPN Wizard

IPsec IKEv1 Remote Access Wizard

IKEv1 Remote Access Wizard を使用して、モバイル ユーザなどの VPN クライアントの安全なリモート 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。

フィールド

- [VPN Tunnel 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。
- [Enable inbound IPsec sessions to bypass interface access lists]：セキュリティ アプライアンスによって常に許可される（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、IPsec 認証の着信セッションをイネーブルにします。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、およびダウンロードされた ACL は適用されます。

Remote Access Client

さまざまなタイプのリモート アクセス ユーザが、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。

フィールド

- VPN Client Type
  - Cisco VPN Client, Release 3.x or higher, or an 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 の認証プロセスを外部の RADIUS 認証サーバに代行させます。

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。

フィールド

- [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 ピアの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 ピアの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、あらかじめ CA への登録を済ませ、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）。
  - [Challenge/response authentication (CRACK)]：クライアントが RADIUS などの一般的な方式を使用して認証を行い、サーバが公開キーによる認証方式を使用している場合に、強力な相互認証を実現します。セキュリティ アプライアンスは、Nokia 92xx Communicator Series デバイスで Nokia VPN Client を認証するために、IKE オプションとして CRACK をサポートしています。

- [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、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では、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。

Client Authentication

[Client Authentication] ペインでは、ASA がリモート ユーザを認証するときに使用する方法を選択します。

フィールド

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 ユーザ認証で外部サーバ 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 グループを選択します。
  - [New ...]：新しい AAA サーバ 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 データベースに新しいユーザを追加します。

フィールド

- このセクションのフィールドを使用してユーザを追加します。
  - [Username]：ユーザ名を入力します。
  - [Password]：（任意）パスワードを入力します。
  - [Confirm Password]：（任意）パスワードを再入力します。
- [Add]：ユーザ名と任意指定のパスワードを入力した後でクリックすると、データベースにユーザが追加されます。
- [Delete]：データベースからユーザを削除するには、該当するユーザ名を強調表示させ、[Delete] をクリックします。

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。

フィールド

- [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]（任意）ペインでは、DNS サーバと WINS サーバおよびデフォルト ドメイン名についての情報をリモート アクセス クライアントに渡す動作を ASA に実行させます。

フィールド

- [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 サーバの IP アドレスを入力します。
- [Secondary DNS Server]：セカンダリ DNS サーバの IP アドレスを入力します。
- [Primary WINS Server]：プライマリ WINS サーバの IP アドレスを入力します。
- [Secondary WINS Server]：セカンダリ WINS サーバの 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。次の項目があります。

- 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。
- 暗号キー判別アルゴリズムを強化する Diffie-Hellman グループ。このアルゴリズムを使用して、ASA は暗号キーとハッシュ キーを導出します。

フィールド

- [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。

アルゴリズム	説明
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。ただし、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。デフォルトの Group 2（1024 ビット Diffie-Hellman）は、Group 5（1536 ビット）と比較して、CPU の実行時間は短いですが、安全性は低くなります。

（注） VPN 3000 シリーズ コンセントレータのデフォルト値は MD5 です。ASA と VPN コンセントレータの間の接続では、接続の両方の側で、フェーズ 1 と 2 の IKE ネゴシエーションの認証方式を同じにする必要があります。

IPsec Settings（任意）

[IPsec Settings]（任意）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。デフォルトにより ASA は、ダイナミックまたはスタティックのネットワーク アドレス変換（NAT）を使用して、内部ホストおよびネットワークの本当の 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。

フィールド

- [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、暗号化なしでインターネットに直接送り出され、ASA は関与しません。
- [Enable Perfect Forwarding Secrecy (PFS)] : フェーズ 2 IPsec キーを生成するときに Perfect Forward Secrecy を使用するかどうか、および使用する値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 Group 2（1024 ビット Diffie-Hellman）は、Group 5（1536 ビット）と比較して、CPU の実行時間は短いですが、安全性は低くなります。

Summary

[Summary] ペインには、この VPN LAN-to-LAN 接続の属性すべてが設定どおりに表示されます。

フィールド

[Back] : 変更するには、目的のペインに到達するまで [Back] をクリックします。

[Finish] : 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。

[Cancel] : このコンフィギュレーションを削除するには、[Cancel] をクリックします。

IPsec Site-to-Site VPN Wizard

このウィザードは、新しいサイトツーサイト VPN トンネルを設定するときに使用します。2 台のデバイス間のトンネルを「サイトツーサイト トンネル」と呼び、これは双方向です。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

ピア VPN デバイスを指定するには、その IP アドレスと、ピアへのアクセスに使用するインターフェイスを指定します。

フィールド

- [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。
- IKEv2

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。

フィールド

- [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。

Security

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。単純な設定のいずれかを選択し、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。

[Authentication] タブ

IKE バージョン 1

- [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 ピアの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 バージョン 2

- [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 ピアの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。

暗号化アルゴリズム

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 バージョン 1

- [IKE Policy] : IKEv1 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。

IKE バージョン 2

- [IKE Policy] : 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。

NAT Excempt

フィールド

- [Exempt ASA side host/network from address translation] : ドロップダウンを使用して、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。

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。サポートされる VPN プロトコルがサマリーに表示されるほか、[VPN Connection Type] ウィンドウで選択された IKE バージョンも表示されます。

AnyConnect VPN Wizard

このウィザードは、AnyConnect VPN クライアントからの 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 AnyConnect VPN クライアントがエンド ユーザのデバイスにアップロードされます。

このウィザードを実行しても、事前展開シナリオにおいて自動的に IKEv2 プロファイルが適用されるわけではないことについてユーザに注意を促します。IKEv2 を正常に事前展開するのに必要な指示または手順を示す必要があります。

Connection Profile Identification

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

フィールド

- [Connection Profile Name] : リモート アクセス ユーザが 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。

AnyConnect 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）。

AnyConnect クライアントの WebLaunch の代わりに事前展開する場合は、最初のクライアント接続で SSL を使用し、クライアント プロファイルをセッション中に ASA から受け取ります。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、『AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

フィールド

- 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。

（注） AnyConnect 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 Cisco 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 AnyConnect 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 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。

フィールド

- Add
- Replace
- Delete

Authentication Methods

この画面では、認証情報を指定します。

フィールド

- [AAA server group]：ASA 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 サーバ 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 上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。

Client Address Assignment

リモート SSL VPN ユーザのための IP アドレス範囲を指定します。

フィールド

- [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

このステップでは、リモート ユーザ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。

フィールド

- [DNS Servers]：DNS サーバの IP アドレスを入力します。
- [WINS Servers]：WINS サーバの 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。

フィールド

- Exempt VPN traffic from network address translation

AnyConnect Client Deployment

次の 2 つの方法のいずれかを使用して、AnyConnect 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。

- WebLaunch：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します。
- 事前展開：手動で AnyConnect クライアント パッケージをインストールします。

フィールド

- [Allow Web Launch]：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、AnyConnect 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 AnyConnect 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。

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。サポートされる VPN プロトコルが、選択された IKE バージョンとともにサマリーに表示されます。

Clientless SSL VPN Wizard

このウィザードでは、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。

SSL VPN Interface

接続プロファイルと、SSL VPN ユーザの接続先となるインターフェイスを指定します。

フィールド

- Connection Profile Name
- [SSL VPN Interface]：SSL VPN 接続のためにユーザがアクセスするインターフェイスです。
- [Digital Certificate]：ASA の認証のためにセキュリティ アプライアンスからリモート Web ブラウザに何を送信するかを指定します。
  - [Certificate]：ドロップダウン メニューから選択します。
- Accessing the Connection Profile

- [Connection Group Alias/URL]: グループ エイリアスはログイン時に [Group] ドロップダウン リストから選択されます。この URL が Web ブラウザに入力されます。
- Display Group Alias list at the login page

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]：ASA 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、[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]：ASA 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。

Group Policy

グループ ポリシーによって、ユーザ グループの共通属性を設定します。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 ポリシーを作成できます。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。

Bookmark List

グループ イントラネット Web サイトのリストを設定します。これらのサイトは、ポータル ページにリンクとして表示されます。例としては、https://intranet.acme.com、rdp://10.120.1.2、vnc://100.1.1.1 などがあります。

フィールド

- Bookmark List
- Manage

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。