CHAPTER 29

VPN

セキュリティ アプライアンスは、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。セキュアな接続はトンネルと呼ばれ、セキュリティ アプライアンス 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。セキュリティ アプライアンスは、双方向のトンネル 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側に送信できます。そのエンドポイントで、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。

セキュリティ アプライアンスは次の VPN 機能を実行します。

- トンネルを確立する。
- トンネル パラメータをネゴシエートする。
- VPN ポリシーを適用する。
- ユーザを認証する。
- ユーザが特定レベルで使用およびアクセスすることを許可する。
- アカウンティング機能を実行する。
- ユーザ アドレスを割り当てる。
- データを暗号化および復号化する。
- セキュリティ キーを管理する。
- トンネルを通したデータ転送を管理する。
- トンネル エンドポイントまたはルータとしての着信データと発信データの転送を管理する。

セキュリティ アプライアンスは、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

VPN Wizard

VPN Wizard では、基本的な LAN-to-LAN 接続とリモート アクセス VPN 接続を設定できます。ASDM を使用して拡張機能を編集および設定してください。

（注） VPN Wizard では、認証用の事前共有キーまたはデジタル証明書のいずれかを割り当てられます。ただし、証明書を使用するには、認証局に登録し、ウィザードを使用する前にトラストポイントを設定しておく必要があります。これらのタスクを実行するには、[ASDM Device Administration] > [Certificate] パネルとオンライン ヘルプを使用してください。

VPN の概要

セキュリティ アプライアンスは、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。

セキュアな接続はトンネルと呼ばれ、セキュリティ アプライアンス 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。セキュリティ アプライアンスは、双方向のトンネル 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側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。

セキュリティ アプライアンスが実行する機能は次のとおりです。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証
- ユーザ アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

VPN Tunnel Type

[VPN Tunnel Type] パネルでは、定義する VPN トンネルのタイプ（リモート アクセスまたは LAN-to-LAN）を選択し、リモート IPSec ピアに接続するインターフェイスを特定します。

フィールド

- [Site-to-Site] : LAN-to-LAN VPN コンフィギュレーションを作成します。2 つの IPSec セキュリティ ゲートウェイの間で使用します。このゲートウェイには、セキュリティ アプライアンス、VPN コンセントレータ、またはサイトツーサイト IPSec 接続をサポートする他のデバイスなどがあります。このオプションを選択すると、VPN Wizard に、サイトツーサイト VPN で必要とされる属性を入力するための一連のパネルが表示されます。
- [Remote Access] : モバイル ユーザなどの VPN クライアントへのセキュアなリモート アクセスを実現するコンフィギュレーションを作成します。このオプションにより、リモート ユーザは、中央集中型ネットワーク リソースに安全にアクセスできます。このオプションを選択すると、VPN Wizard に、リモート アクセス VPN で必要とされる属性を入力するための一連のパネルが表示されます。

- [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。セキュリティ アプライアンス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。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Remote Site Peer

[Remote Site Peer] パネルでは、次のタスクを実行します。

1. この VPN トンネルの終端となるリモート IPSec ピアの IP アドレスを指定する。
2. リモート ピアに対して作成する。
3. 認証方式を選択および設定する。

フィールド

- [Peer IP Address]：VPN トンネルの終端となるリモート IPSec ピアの IP アドレスを入力します。ピアは、別のセキュリティ アプライアンス、VPN コンセントレータ、または IPSec をサポートする他のゲートウェイ デバイスです。
- [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 セキュリティ アプライアンスとリモート 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]：事前共有キーを入力します。最大 127 文字です。

  - [Certificate] : ローカル セキュリティ アプライアンスとリモート 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 つ以上の証明書をセキュリティ アプライアンスにダウンロードしておく必要があります。

    デジタル証明書を使用すると、IPSec トンネルを確立するため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、所有者の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 Certification Authority（CA; 認証局）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] : デジタル証明書に署名するアルゴリズムを、RSA 用の rsa-sig、または DSA 用の dsa-sig から選択します。
  - [Trustpoint Name] : セキュリティ アプライアンスがリモート ピアに送信する証明書を識別する名前を選択します。このリストには、トラストポイントが、証明書の署名アルゴリズム リストで先に選択したタイプの証明書と一緒に表示されます。
  - [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。

- [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ポリシーでは、認証方式を指定し、セキュリティ アプライアンス デフォルト グループ ポリシーを使用します。

  デフォルトでは、ASDM は、このボックスにピア IP アドレスの値を入力します。この名前は変更できます。最大 64 文字です。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

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] パネルでは、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、セキュリティ アプライアンス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 を確立するためにセキュリティ アプライアンスが使用する、対称暗号化アルゴリズムを選択します。セキュリティ アプライアンスは、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。
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、セキュリティ アプライアンスで使用される Keyed-Hash Message Authentication Code（HMAC）バージョンはこの攻撃を防ぎます。
- [DH Group] : Diffie-Hellman グループ ID を選択します。2 つのピアは、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。セキュリティ アプライアンスと 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。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IPSec Encryption and Authentication

[IPSec Encryption and Authentication] パネルでは、セキュアな VPN トンネルを作成するフェーズ 2 IKE ネゴシエーションで使用する暗号化方式と認証方式を選択します。これらの値は、両方のピアでまったく同じにする必要があります。

フィールド

- [Encryption]：VPN トンネルを確立するためにセキュリティ アプライアンスが使用する対称暗号化アルゴリズムを選択します。セキュリティ アプライアンスは、暗号化を使用してトンネルを通過するデータを保護し、プライバシーを守ります。有効な暗号化方式には、次のものがあります。

暗号化方式	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 3 回暗号化します。
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。ただし、セキュリティ アプライアンスで使用される Keyed-Hash Message Authentication Code（HMAC）バージョンはこの攻撃を防ぎます。

（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。セキュリティ アプライアンスと 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 とフェーズ 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。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Hosts and Networks

[Hosts and Networks] パネルでは、この LAN-to-LAN IPSec トンネルを使用してデータを送受信することができる、ローカルおよびリモートのホストとネットワークを特定します。

IPSec に従って動作するには、LAN-to-LAN 接続における両方のピアのホストおよびネットワークのエントリが、互換性を持っている必要があります。このパネルでローカルのホストとネットワークとして設定するホストおよびネットワークは、LAN-to-LAN 接続のリモート サイトにあるデバイスのリモートのホストとネットワークとして設定する必要があります。ローカルのセキュリティ アプライアンスとリモート デバイスには、この LAN-to-LAN 接続で使用する共通のトランスフォーム セットが少なくとも 1 つ必要です。

フィールド

- [Action]：ローカル ネットワークとリモート ネットワークの間を移動するデータを保護するかどうかを指定します。
- [Local networks]：ローカルのホストとネットワークを選択します。
- [Remote networks]：リモートのホストとネットワークを選択します。
- [Exempt ASA side host/network from address translation]：トラフィックがアドレス変換なしでセキュリティ アプライアンスを通過できるようにします。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Summary

[Summary] パネルには、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、目的のパネルに到達するまで [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。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Remote Access Client

[Remote Access Client] パネルでは、この接続を使用するリモート アクセス ユーザのタイプを特定します。

フィールド

- [Cisco VPN Client Release 3.x or higher, or other Easy VPN Remote product]：ここで名前が指定されたもの以外の互換性のあるソフトウェア クライアントとハードウェア クライアントを含む、IPSec 接続の場合にクリックします。
- [Microsoft Windows client using L2TP over IPSec]：パブリック IP ネットワークを経由する、Microsoft Windows クライアントおよび Microsoft Windows Mobile クライアントからの接続をイネーブルにする場合にクリックします。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。次の PPP 認証プロトコルの 1 つ以上をイネーブルにします。
  - [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]：EAP をイネーブルにします。これによってセキュリティ アプライアンスは、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。
- [Client will send the tunnel group name as username@tunnelgroup]：セキュリティ アプライアンスが、L2TP over IPSec 接続を確立する別々のユーザを異なるトンネル グループと関連付けることができるようにします。各トンネル グループはそれぞれの AAA サーバ グループと IP アドレス プールを持つため、ユーザはそのトンネル グループ特定の方法で認証を受けられます。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

VPN Client Authentication Method and Tunnel Group Name

[VPN Client Authentication Method and Tunnel Group Name] パネルでは、認証方式を設定し、トンネル グループを作成します。

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 セキュリティ アプライアンスとリモート 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]：事前共有キーを入力します。
  - [Certificate]：ローカル セキュリティ アプライアンスとリモート 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 つ以上の証明書をセキュリティ アプライアンスにダウンロードしておく必要があります。

    デジタル証明書を使用すると、IPSec トンネルを確立するため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、所有者の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 Certification Authority（CA; 認証局）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。
  - [Trustpoint Name]：セキュリティ アプライアンスがリモート ピアに送信する証明書を識別する名前を選択します。
  - [Certificate Signing Algorithm]：デジタル証明書に署名するアルゴリズムを、RSA 用の rsa-sig、または DSA 用の dsa-sig から選択します。

  - [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。

- [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ポリシーでは、認証方式を指定し、セキュリティ アプライアンス デフォルト グループ ポリシーを使用します。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

クライアント認証

[Client Authentication] パネルでは、セキュリティ アプライアンスがリモート 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] : セキュリティ アプライアンス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。次のパネルでは、セキュリティ アプライアンス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] : 前に設定されている 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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

New Authentication Server Group

[New Authentication Server Group] パネルでは、新しい AAA サーバを 1 つ以上定義します。

フィールド

サーバを 1 つだけ含む AAA サーバ グループを設定するには、次の情報を入力します。

- [Server Group Name]：サーバ グループの名前を入力します。この名前は、このサーバを使用して認証する対象のユーザに関連付けます。
- [Authentication Protocol]：サーバで使用する認証プロトコルを選択します。オプションには、TACACS+、RADIUS、SDI、NT、および Kerberos などがあります。
- [Server IP Address]：AAA サーバの IP アドレスを入力します。
- [Interface]：AAA サーバが常駐するセキュリティ アプライアンスのインターフェイスを選択します。
- [Server Secret Key]：大文字と小文字が区別される最大 127 文字の英数字キーワードを入力します。サーバとセキュリティ アプライアンスは、そのキーを使用して両者の間を移動するデータを暗号化します。キーは、セキュリティ アプライアンスとサーバの両方で同じにする必要があります。スペース以外の特殊文字を使用することができます。
- [Confirm Server Secret Key]：もう一度秘密キーを入力します。

この新しいグループにサーバを追加するか、または他の AAA サーバの設定を変更するには、[Configuration] > [Features] > [Properties] > [AAA] に移動します。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

User Accounts

[User Accounts] パネルでは、認証を目的として、セキュリティ アプライアンスの内部ユーザ データベースに新しいユーザを追加します。

フィールド

次の情報を入力します。

- 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。
- [Change user password]：ユーザ パスワードを変更する場合にオンにします。

- [User authentication using MSCHAP]：ユーザ認証用に MS-CHAP を使用する場合にオンにします。
- [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。
- [Edit]：データベースに追加したユーザを編集する場合にクリックします。
- [Access Restriction]：次のオプションのいずれかを選択します。
  - Full access (ASDM, SSH, Telnet, and console)

    [Privilege Level]：ドロップダウン リストから適切なものを選択します。管理者は、通常、使用できるうち最高の 15 を割り当てています。
  - CLI login prompt for SSH, Telnet, and console (no ASDM access)
  - No ASDM, SSH, Telnet, or console access
- [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。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Address Pool

[Address Pool] パネルでは、セキュリティ アプライアンスがリモート 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

- [Name]：アドレス プールが適用されるトンネル グループの名前を表示します。この名前は、[VPN Client Name and Authentication Method] パネル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。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Attributes Pushed to Client

[Attributes Pushed to Client (Optional)] パネルでは、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セキュリティ アプライアンスに実行させます。

フィールド

リモート アクセス クライアントで使用する情報を入力します。

- ：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] パネル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。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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Address Translation Exemption

[Address Translation Exemption (Optional)] パネルを使用して、アドレス変換を必要としないローカル ホスト/ネットワークを識別します。デフォルトによりセキュリティ アプライアンスは、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、このパネル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

- [Host/Network to Be Added] : これらのフィールドに値を入力して、NAT から特定のホストまたはネットワークを免除します。
  - [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。
  - [IP address] : ホストまたはネットワークの IP アドレスを選択します。IP アドレスを入力するか、または隣の [...] ボタンをクリックしてネットワーク図を表示し、ホストまたはネットワークを選択します。
- [Add] : 適切なフィールドへの入力を済ませた後に、ホストまたはネットワークを [Selected Hosts/Networks] リストに追加します。
- [Selected Hosts/Networks] : NAT から免除するホストとネットワークを表示します。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、このリストには何も入力しません。
- [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、セキュリティ アプライアンスは、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、セキュリティ アプライアンスの背後にある 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、セキュリティ アプライアンスは関与しません。

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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—