ASA システムの導入

この章では、VPN 3000 コンセントレータと Adaptive Security Appliance（ASA; 適応型セキュリティアプライアンス）の主な相違点、特に VPN について説明します。この章は、次の項で構成されています。

- セキュリティ ポリシー機能の概要
- ユーザ管理の相違点
- ASA での PKI 実装
- インターフェイスごとの ASDM セッションおよび WebVPN セッション

セキュリティ ポリシー機能の概要

ASA は、シスコの最も強力なファイアウォールである VPN と侵入保護機能とを結合します。

- ASA は、Web VPN など、VPN 3000 コンセントレータでサポートされているソフトウェア機能のほとんどを提供します。WebVPN には、PIX ファイアウォールではなく ASA デバイス上で動作している ASA ソフトウェアが必要です。
- ASA は、より高速なインターフェイス（10/100/1000）と追加インターフェイス（4）を提供し、追加セキュリティ サービス用のスロットも用意された拡張可能なハードウェアです。
- オペレーティング システムでは IOS に類似の CLI コマンドを使用します。このコマンドは、より強力で柔軟性があり、VPN 3000 コンセントレータのメニューベースのコマンドライン インターフェイスを拡張し、スクリプトを使用して設定プロセスや監視プロセスを自動化する機能を追加します。CLI コマンドは、VPN コンセントレータから ASA に移行した機能をサポートしています。多数の新しいコマンドが VPN 機能専用に設計されています。CLI コマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。
- ASA のパフォーマンスは VPN 3000 コンセントレータのものより優れています。
- ASA はスケーラビリティと投資保護を提供します。同一デバイス内で複数のサービスを使用可能で、後でインターフェイスやサービスを追加することによって拡張できます。
- Adaptive Security Device Manager ソフトウェアは、ASA システムにマルチコンテキスト管理インターフェイスを提供します。

次の項では、ASA と VPN 3000 コンセントレータの概念上の主な相違点を説明します。

ユーザ管理の相違点

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）のセキュリティを管理し、セキュリティ アプライアンスを設定する際は、グループとユーザが中心的な概念になります。グループとユーザにより、VPN へのユーザ アクセスおよび VPN の使用を決定するアトリビュートが指定されます。*グループ*は複数ユーザの集合で、単一のエンティティとして扱われます。*ユーザ*は、自分のアトリビュートを*グループ ポリシー*から取得します。*トンネル グループ*は、特定の接続のグループ ポリシーを特定します。特定のグループ ポリシーをユーザに割り当てない場合、当該接続のデフォルト グループ ポリシーが適用されます。VPN 3000 コンセントレータの場合と異なり、基本グループはありません。

トンネル グループおよびグループ ポリシーを使用することで、システム管理が簡略化されます。セキュリティ アプライアンスにより、設定タスクの効率化に役立つデフォルト LAN 間トンネル グループ、デフォルト リモート アクセス トンネル グループ、デフォルト WebVPN トンネル グループ、およびデフォルト グループ ポリシー（DfltGrpPolicy）が提供されます。デフォルトのトンネル グループおよびグループ ポリシーは、多くのユーザが共通して使用できる可能性のある設定値を提供します。ユーザを追加するときは、グループ ポリシーからパラメータを「継承」するように設定できます。これで、多数のユーザの VPN アクセスをすばやく設定できます。

VPN ユーザすべてに同一の権限を付与するのであれば、特定のトンネル グループまたはグループ ポリシーを設定する必要はありません。しかし実際には、VPN をそのように動作させることはほとんどありません。たとえば、財務グループにプライベート ネットワークの一部へのアクセスを許可し、顧客サポート グループに別の部分へのアクセスを、MIS グループにその他の部分へのアクセスを許可する場合があります。さらに、MIS グループの特定のユーザ数人に、他の MIS ユーザからアクセスできないシステムへのアクセスを許可する場合もあります。トンネル グループとグループ ポリシーには柔軟性があり、このような設定をセキュアに実行できます。

（注）　セキュリティ アプライアンスには、ネットワーク リストのスーパーセットであるオブジェクト グループの概念も含まれます。オブジェクト グループを使用すると、ネットワークだけでなくポートへの VPN アクセスも定義できます。ACL は、グループ ポリシーやトンネル グループよりも、オブジェクト グループに関連があります。

ASA トンネル グループ

トンネル グループは、トンネル接続ポリシーを決定するレコードのセットで構成されます。これらのレコードは、接続情報の送信先であるアカウンティング サーバ（存在する場合）だけでなく、トンネル ユーザの認証先サーバを特定します。さらに、接続のデフォルト グループ ポリシーを特定します。これらのレコードには、プロトコル固有の接続パラメータが含まれています。トンネル グループには、トンネル自体の作成に関連する少数のアトリビュートがあります。トンネル グループには、ユーザ指向アトリビュートを定義するグループ ポリシーへのポインタが含まれています。

セキュリティ アプライアンスには、LAN 間接続用の DefaultL2LGroup、リモート アクセス接続用の DefaultRAGroup、WebVPN 接続用の DefaultWEBVPNGroup というデフォルト トンネル グループがあります。これらのデフォルト トンネル グループは変更できますが、削除はできません。また、環境に固有のトンネル グループを 1 つ以上作成できます。トンネル グループはセキュリティ アプライアンスのローカルのものであるため、外部サーバでは設定できません。

トンネル グループは次のアトリビュートを指定します。

- 一般パラメータ
- IPSec 接続パラメータ
- WebVPN 接続パラメータ

一般的なトンネル グループ接続パラメータ

一般パラメータは、IPSec 接続と WebVPN 接続の両方に共通です。一般パラメータには、次のものがあります。

- トンネル グループ名：トンネル グループを追加または編集するときにトンネル グループ名を指定します。次の事項を考慮する必要があります。
  - 認証に事前共有鍵を使用するクライアントの場合、トンネル グループ名は、IPSec クライアントがセキュリティ アプライアンスに渡すグループ名と同じです。
  - 認証に証明書を使用するクライアントは、この名前を証明書の一部として渡し、セキュリティ アプライアンスはこの名前を証明書から抽出します。

  トンネル グループ レコードには、トンネル接続ポリシーの情報が含まれています。これらのレコードは、接続情報の送信先であるアカウンティング サーバ（存在する場合）だけでなく、トンネル ユーザの認証先サーバを特定します。さらに、接続のデフォルト グループ ポリシーを特定します。これらのレコードには、プロトコル固有の接続パラメータが含まれています。
- 接続タイプ：接続タイプには、IPSec リモート アクセス、IPSec LAN 間、および WebVPN があります。トンネル グループに設定できる接続タイプは 1 つだけです。
- 認証、認可、アカウンティング サーバ：これらのパラメータは、セキュリティ アプライアンスが次の目的で使用するサーバ グループまたはリストを特定します。
  - ユーザの認証
  - ユーザがアクセスを認可されているサービスに関する情報の取得
  - アカウンティング レコードの格納

  サーバ グループは、1 つ以上のサーバによって構成できます。

- 接続のデフォルト グループ ポリシー：グループ ポリシーは、ユーザ指向アトリビュートのセットです。デフォルト グループ ポリシーは、トンネル ユーザの認証または認可の際にセキュリティ アプライアンスがデフォルトとして使用するアトリビュートを持つグループ ポリシーです。
- クライアント アドレスの割り当て方式：この方式には、セキュリティ アプライアンスがクライアントに割り当てる DHCP サーバやアドレス プールの値が含まれます。
- アカウント無効の上書き：このパラメータを使用すると、AAA サーバから受け取る「アカウント無効」インジケータを上書きできます。
- パスワード管理：このパラメータを使用すると、指定日数（デフォルトは 14 日）が経過すると現在のパスワードの有効期限が切れることをユーザに警告し、パスワードを変更する機会を提供できます。
- グループ除去およびレルム除去：これらのパラメータにより、受信するユーザ名をセキュリティ アプライアンスが処理する方法が決まります。これらのパラメータは、user@realm という形式で受信するユーザ名だけに適用されます。レルムは、ユーザ名に @ デリミタで付加される管理ドメインです（user@abc）。

  管理者がグループ除去処理を指定すると、セキュリティ アプライアンスは、VPN クライアントによって提示されたユーザ名からグループ名を取得することで、ユーザ接続のトンネル グループを選択します。次にセキュリティ アプライアンスは、認可または認証のためにユーザ名のユーザ部分だけを送信します。それ以外の場合（ディセーブルの場合）、セキュリティ アプライアンスはレルムを含むユーザ名全体を送信します。

  レルム除去処理では、認証または認可サーバへのユーザ名の送信時にユーザ名からレルムが削除されます。コマンドがイネーブルの場合、セキュリティ アプライアンスはユーザ名認可または認証のユーザ部分だけを送信します。ディセーブルの場合、セキュリティ アプライアンスはユーザ名全体を送信します。
- 認可の要求：このパラメータを使用すると、ユーザ アクセスの前に認可を要求したり、その要求を取り下げたりできます。
- 認可 DN アトリビュート：このパラメータは、認可を実行するときに使用する認定者名アトリビュートを指定します。

IPSec トンネル グループ接続パラメータ

IPSec トンネル グループ パラメータには、次のものがあります。

- クライアント認証方式：事前共有鍵または証明書、あるいは両方。
  - 事前共有鍵に基づいた IKE 接続の場合、接続ポリシーに関連付けられた英数字の鍵自体（最大 128 文字）。
  - ピア ID 確認の要求：このパラメータは、ピアの証明書を使用してピアの ID を確認することを要求するかどうかを指定します。
- ISAKMP（IKE）キープアライブ設定：この機能を使用すると、セキュリティ アプライアンスはリモート ピアが引き続き存在していることを監視し、当該ピアに自身の存在を報告できます。ピアが反応しなくなった場合、セキュリティ アプライアンスは接続を削除します。IKE キープアライブをイネーブルにすることで、IKE ピアが接続を失ったときに接続がハングしないように防止できます。

  IKE キープアライブにはさまざまな形式があります。この機能が正しく動作するには、セキュリティ アプライアンスとそのリモート ピアとが共通の形式をサポートしている必要があります。この機能は次のピアで使用できます。
  - Cisco VPN Client（Release 3.0 以降）
  - Cisco VPN 3000 Client（Release 2.x）
  - Cisco VPN 3002 Hardware Client
  - Cisco VPN 3000 シリーズ コンセントレータ
  - Cisco IOS ソフトウェア

－ Cisco Secure PIX Firewall

シスコ以外の VPN クライアントは IKE キープアライブをサポートしていません。

IKE キープアライブをサポートするピアとサポートしないピアが混在するグループを設定している場合、グループ全体に対して IKE キープアライブをイネーブルにします。この機能をサポートしないピアに影響はありません。

IKE キープアライブをディセーブルにする場合、反応しないピアとの接続はタイムアウトするまでアクティブのままなので、アイドル アイムアウトを短く維持するようお勧めします。

（注） ISDN 回線経由で接続するクライアントがこのグループに含まれる場合、接続コストを削減するために IKE キープアライブをディセーブルにします。通常、ISDN 接続はアイドル時に解除されます。しかし IKE キープアライブ メカニズムによって接続がアイドルにならないため、接続解除されません。

IKE キープアライブをディセーブルにすると、クライアントは IKE 鍵または IPSec 鍵いずれかの有効期限が切れたときにのみ接続解除されます。IKE キープアライブがイネーブルになっている場合とは異なり、障害が発生したトラフィックは、ピア タイムアウト プロファイル値を持つトンネルから接続解除されません。

（注） IKE メイン モードを使用する LAN 間設定がある場合は、2 つのピアが同じ IKE キープアライブ設定を使用していることを確認します。両方のピアで IKE キープアライブをどちらもイネーブルにするか、またはどちらもディセーブルにする必要があります。

- デジタル証明書を使用して認証を設定する場合、証明書チェーン全体を送信するか（つまりピアに ID 証明書およびすべての発行証明書を送信する）、または ID 証明書のみを送信するかを指定できます。
- 古いバージョンの Windows クライアント ソフトウェアを使用しているユーザに、クライアントをアップデートする必要があることを通知し、クライアントのアップデート バージョンを取得するためのメカニズムをそのユーザに提供できます。VPN 3002 Hardware Client ユーザの場合、自動アップデートをトリガーできます。クライアント アップデートの設定と変更は、すべてのトンネル グループまたは特定のトンネル グループのどちらに対しても実行できます。
- デジタル証明書を使用して認証を設定する場合、IKE ピアに送信する証明書を特定するトラストポイントの名前を指定する必要があります。

WebVPN トンネル グループ接続パラメータ

次のアトリビュートは WebVPN 接続に固有です。

- 認証方式。AAA または証明書。
- 適用するカスタマイゼーションの名前。カスタマイゼーションにより、WebVPN ポータル ページの外観が決まります。カスタマイゼーション パラメータは WebVPN の設定の一環として設定します。
- DNS サーバ グループ名。DNS サーバ グループは、DNS サーバ名、ドメイン名、ネーム サーバ、リトライ回数、および DNS サーバがトンネル グループに使用するタイムアウト値を指定します。
- 1 つまたは複数のグループ エイリアス。これらは、トンネル グループへの参照にサーバが使用する代替名です。ログイン時、ユーザはグループ名をドロップダウン メニューから選択します。
- 1 つまたは複数のグループ URL。このパラメータを設定すると、指定 URL に参加するユーザは、ログイン時にグループを選択する必要がありません。

- デフォルト グループ ポリシーとは異なるアクセス権を WebVPN ユーザに付与するグループ ポリシー。
- CIFS 名前解決に使用する NetBIOS Name Service サーバの名前（nbns-server）。

グループ ポリシー

グループ ポリシーは、IPSec 接続用のユーザ指向アトリビュートと値のペアのセットで、内部的（ローカル）にデバイスに格納されるか、または外部的に RADIUS サーバに格納されます。トンネル グループでは、トンネルが確立されると、ユーザ接続の条件を設定するグループ ポリシーを使用します。グループ ポリシーを使用すると、ユーザまたはユーザのグループごとに各アトリビュートを個別に指定する必要がなく、ユーザにアトリビュートのセット全体を適用できます。

グループ ポリシーをユーザに割り当てる、または特定ユーザのグループ ポリシーを変更するには、グローバル コンフィギュレーション モードで **group-policy** コマンドを入力します。

セキュリティ アプライアンスにはデフォルト グループ ポリシーがあります。デフォルト グループ ポリシー（変更できますが削除はできません）に加えて、環境に固有のグループ ポリシーを 1 つまたは複数作成できます。

内部グループおよび外部グループについてポリシーを設定できます。内部グループは、セキュリティ アプライアンスの内部データベースに設定されます。外部グループは、RADIUS などの外部認証サーバに設定されます。グループ ポリシーには、次のアトリビュートが含まれます。

- ID
- サーバ定義
- クライアント ファイアウォールの設定
- トンネリング プロトコル
- IPSec の設定
- ハードウェア クライアントの設定
- フィルタ
- クライアント設定の設定値
- WebVPN 機能
- 接続設定

デフォルト グループ ポリシー

セキュリティ アプライアンスは、デフォルト グループ ポリシーを提供します。このデフォルト グループ ポリシーは変更できますが、削除できません。DfltGrpPolicy という名前のデフォルト グループ ポリシーはセキュリティ アプライアンスに常に存在します。しかしこのデフォルト グループ ポリシーは、セキュリティ アプライアンスで使用するように設定しない限り、有効になりません。他のグループ ポリシーを設定する場合、明示的に指定しないアトリビュートがあると、そのアトリビュートはデフォルト グループ ポリシーから値を取得します。デフォルト グループ ポリシーを表示するには、次のコマンドを入力します。

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

グループ ポリシーの設定

グループ ポリシーは、すべての種類のトンネルに適用できます。いずれの場合でも、パラメータを明示的に定義しないと、グループはデフォルト グループ ポリシーから値を取得します。グループ ポリシーは、外部と内部のどちらも設定できます。グループ ポリシーを設定するには、まずグループ ポリシーの名前とタイプを指定し、次に、内部グループ ポリシーの場合はアトリビュートを指定します。

外部グループ ポリシーの設定

外部グループ ポリシーは、指定の外部サーバからアトリビュート値を取得します。外部グループ ポリシーの場合、セキュリティ アプライアンスがアトリビュートについて照会できる AAA サーバ グループを特定し、その外部 AAA サーバ グループからアトリビュートを取得するときに使用するパスワードを指定する必要があります。外部認証サーバを使用している場合は、ユーザ名とグループ名が一意である必要があるので注意してください。グループに名前を付けるときは、外部ユーザの名前と一致するものを選択しないようにします。逆に、外部ユーザに名前を割り当てるときは、既存のグループの名前を選択しないようにします。

（注） セキュリティ アプライアンスは、外部 LDAP サーバまたは外部 RADIUS サーバでのユーザ認可をサポートしています。外部サーバを使用するようにセキュリティ アプライアンスを設定する前に、正しいセキュリティ アプライアンス認可アトリビュートでサーバを設定し、これらのアトリビュートのサブセットから、個々のユーザに特定の権限を割り当てる必要があります。外部グループ ポリシーの場合、サポートされている AAA サーバ タイプは RADIUS だけです。

内部グループ ポリシーの設定

内部グループ ポリシー用のアトリビュートと値のペアは、内部的（ローカル）にセキュリティ アプライアンスに格納されます。内部グループ ポリシーを設定するには、グループ ポリシーの名前とタイプを指定し、次にアトリビュートを指定します。内部グループ ポリシーのアトリビュートは、キーワード ***from*** を付加し、以前から存在しているグループ ポリシーの名前を指定することで、その既存グループ ポリシーの値に初期設定できます。内部グループ ポリシーには次のアトリビュートを指定できます。

- プライマリとセカンダリの WINS サーバおよび DNS サーバ
- VPN 固有のアトリビュート（アクセス時間、同時ログインの回数、VPN アイドル タイムアウトとセッション タイムアウト、VPN 接続に使用する ACL の名前、このグループ ポリシーの VPN トンネル タイプ（IPSec リモート アクセス、LAN 間、または WebVPN））
- セキュリティ設定（パスワード ストレージ、IP 圧縮、IKE 鍵の再生成でユーザ再認証を要求するかどうか、リモート ユーザのアクセスをトンネル グループのみに制限するかどうか、完全転送秘密をイネーブルにするかどうか）
- バナー メッセージ
- IPSec over UDP（IPSec through NAT と呼ばれる場合もある）
- スプリットトンネリング ポリシーとネットワーク リスト
- ドメイン アトリビュート
- VPN 3002 Hardware Client のアトリビュート（セキュア ユニット認証、ユーザ認証、ユーザ認証アイドル タイムアウト、IP Phone バイパス、LEAP バイパス、およびネットワーク拡張モード）
- バックアップ サーバ アトリビュート
- クライアント ファイアウォール ポリシー
- クライアント アクセス規則

明示的に指定しないアトリビュートがある場合、グループ ポリシーにはデフォルト グループから値が継承されます。

グループ ポリシー WebVPN アトリビュートの設定

WebVPN では、ユーザは、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。ソフトウェア クライアントとハードウェア クライアントはいずれも必要ありません。WebVPN では、多様な Web リソースおよび Web 対応アプリケーションへのアクセスが、HTTPS インターネット サイトに到達可能なコンピュータほとんどすべてで容易になります。WebVPN では、SSL およびその後継バージョンである TLS1 が使用され、中央サイトで設定済みの特定のサポート対象内部リソースとリモート ユーザとの間にセキュアな接続が提供されます。セキュリティ アプライアンスはプロキシ処理が必要な接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。デフォルトでは、WebVPN はディセーブルです。

WebVPN 設定は、特定の内部グループ ポリシー用にカスタマイズできます。

（注） グローバル コンフィギュレーション モードから移行する WebVPN モードでは、WebVPN のグローバル設定値を設定できます。この項で説明する WebVPN モード（グループ ポリシー コンフィギュレーション モードから移行するモード）では、特定のグループ ポリシーの WebVPN 設定をカスタマイズできます。

グループ ポリシーの WebVPN コンフィギュレーション モードでは、すべての機能について設定値を継承するか、または次のパラメータをカスタマイズするかを指定できます。

- WebVPN 機能（自動ダウンロード、Citrix、ファイル アクセス、ファイル参照、ファイル エントリ、フィルタ、HTTP プロキシ、MAPI、ポート転送、URL エントリ）。
- ACL とフィルタ対象トラフィックのタイプ。
- ログイン時にユーザに表示されるウィンドウのルックアンドフィールを変更するカスタマイゼーション。
- HTML コンテンツ フィルタ。
- ホームページ。
- WebVPN セッションの Java、ActiveX、イメージ、スクリプト、および cookie のフィルタリング。
- このグループの WebVPN 接続で使用するアクセス コントロール リスト。
- このグループの WebVPN ホームページに表示される URL リスト。
- ポート転送とポート転送表示名。
- デッド ピア検知アトリビュート。
- シングル サインオン サーバ（SSO サーバ）。WebVPN でのみ可能なシングル サイン オンのサポートにより、ユーザは、ユーザ名とパスワードを入力し直すことなく、さまざまなサーバからさまざまなセキュア サービスにアクセスできます。
- 自動サインオン。WebVPN ユーザのログイン資格情報を内部サーバに自動的に送信します。
- ログオンに成功するが VPN 特権を持っていない WebVPN ユーザへの拒否メッセージ。
- SSL VPN Client（SVC）アトリビュート。SVC は、IPSec VPN クライアントの利点をリモート ユーザが活用できる VPN トンネリング テクノロジーです。これを使用すると、ネットワーク管理者が IPSec VPN クライアントをリモート コンピュータにインストールして設定する必要はありません。

- SVC キープアライブ アトリビュート。キープアライブ メッセージの頻度を調整し（*seconds* で指定）、プロキシ、ファイアウォール、または NAT デバイス経由の SVC 接続をオープンのまま維持します。接続のアイドル状態が維持される時間がデバイスで制限されている場合でも同様に機能します。
- SVC インストールの維持。この設定により、リモート コンピュータへの SVC 常時インストールがイネーブルになります。

（注）　WebVPN は **vpn-filter** コマンドで定義された ACL を使用しません。

多くの場合、WebVPN の設定の一環として WebVPN アトリビュートを定義し、その後、グループ ポリシー WebVPN アトリビュートを設定するときにそれらの定義を特定のグループに適用します。WebVPN アトリビュートの設定の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』および『*Cisco Security Appliance Command Reference*』にある WebVPN の説明を参照してください。

ユーザ アトリビュートの設定

デフォルトでは、ユーザは割り当てられたグループ ポリシーからすべてのユーザ アトリビュートを継承します。セキュリティ アプライアンスでは、個々のアトリビュートをユーザ レベルに割り当て、そのユーザに適用されるグループ ポリシーの値を上書きすることもできます。たとえば、業務時間中のアクセスをすべてのユーザに許可するグループ ポリシーを指定し、その後で、特定のユーザに 24 時間のアクセスを設定することができます。

特定ユーザのアトリビュートの設定

特定のユーザのアトリビュートを設定するには、**username** コマンドを使用してユーザ名モードを開始し、1 つ（またはゼロ個）のパスワード、およびその他の値をユーザに割り当てます。指定しないアトリビュートはグループ ポリシーから継承されます。

内部ユーザ認証データベースは、**username** コマンドによって入力されたユーザで構成されます。セキュリティ アプライアンス データベースにユーザを追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除対象のユーザ名に対してこのコマンドの **no** バージョンを使用します。ユーザ名をすべて削除するには、ユーザ名を付加せずに **clear configure username** コマンドを使用します。

指定できるユーザ名アトリビュートは、次のとおりです。

- このユーザのパスワードと特権レベル
- 明示的に設定されていないアトリビュートの値の継承元であるグループ ポリシー
- VPN アクセス時間と許可されている同時ログイン回数
- VPN アイドル タイムアウトと最大接続時間
- VPN 接続のフィルタとして使用する、以前に設定されたユーザ固有の ACL の名前
- このユーザに割り当てる IP アドレスとネットマスク
- このユーザが使用できる VPN トンネル タイプ（IPSec リモート アクセスまたは WebVPN）
- リモート ユーザのアクセスを、以前から存在している指定のトンネル グループ経由のみに制限するかどうか
- ログイン パスワードをユーザがクライアント システムに格納することを許可するかどうか

特定ユーザの WebVPN の設定

WebVPN では、ユーザは、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。ソフトウェア クライアントとハードウェア クライアントはいずれも必要ありません。WebVPN では、多様な Web リソースおよび Web 対応アプリケーションへのアクセスが、HTTPS インターネット サイトに到達可能なコンピュータほとんどすべてで容易になります。WebVPN では、SSL およびその後継バージョンである TLS1 が使用され、中央サイトで設定済みの特定のサポート対象内部リソースとリモート ユーザとの間にセキュアな接続が提供されます。セキュリティ アプライアンスはプロキシ処理が必要な接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

特定ユーザの WebVPN 設定をカスタマイズするには、ユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用することにより、ユーザ名 WebVPN コンフィギュレーション モードを開始します。ユーザ名に対して **webvpn** コマンドを使用すると、ファイル、MAPI プロキシ、URL および TCP アプリケーションへの WebVPN 経由のアクセスを定義できます。さらに、ACL とフィルタ対象トラフィックのタイプも特定できます。WebVPN は、デフォルトではディセーブルです。これらの **webvpn** コマンドは、設定元のユーザ名にのみ適用されます。

ユーザ名 WebVPN コンフィギュレーション モードでは、すべての機能について設定値を継承するか、または次のパラメータをカスタマイズするかを指定できます。

- WebVPN 機能（自動ダウンロード、Citrix、ファイル アクセス、ファイル参照、ファイル エントリ、フィルタ、HTTP プロキシ、MAPI、ポート転送、URL エントリ）。
- ログイン時にユーザに表示されるウィンドウのルックアンドフィールを変更するカスタマイゼーション。
- HTML コンテンツ フィルタ。
- ホームページ。
- WebVPN セッションの Java、ActiveX、イメージ、スクリプト、および cookie のフィルタリング。
- このグループの WebVPN 接続で使用するアクセス コントロール リスト。
- このグループの WebVPN ホームページに表示される URL リスト。
- ポート転送とポート転送表示名。
- デッド ピア検知アトリビュート。
- シングル サインオン サーバ（SSO サーバ）。WebVPN でのみ可能なシングル サイン オンのサポートにより、ユーザは、ユーザ名とパスワードを入力し直すことなく、さまざまなサーバからさまざまなセキュア サービスにアクセスできます。
- 自動サインオン（WebVPN ユーザのログイン資格情報を内部サーバに自動的に送信します）。
- ログオンに成功するが VPN 特権を持っていない WebVPN ユーザへの拒否メッセージ。
- SSL VPN Client（SVC）アトリビュート。SVC は、IPSec VPN クライアントの利点をリモート ユーザが活用できる VPN トンネリング テクノロジーです。これを使用すると、ネットワーク管理者が IPSec VPN クライアントをリモート コンピュータにインストールして設定する必要はありません。
- SVC キープアライブ アトリビュート。キープアライブ メッセージの頻度を調整し（*seconds* で指定）、プロキシ、ファイアウォール、または NAT デバイス経由の SVC 接続をオープンのまま維持します。接続のアイドル状態が維持される時間がデバイスで制限されている場合でも同様に機能します。
- SVC インストールの維持。この設定により、リモート コンピュータへの SVC 常時インストールがイネーブルになります。

（注）　WebVPN は **vpn-filter** コマンドで定義された ACL を使用しません。

多くの場合、WebVPN の設定の一環として WebVPN アトリビュートを定義し、その後、ユーザ名 WebVPN アトリビュートを設定するときにそれらの定義を特定のユーザ名に適用します。WebVPN アトリビュートの設定の詳細については、Web VPN の説明を参照してください。ユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用することにより、ユーザ名 WebVPN コンフィギュレーション モードを開始します。ユーザ名に対して WebVPN 関連のコマンドを使用すると、ファイル、MAPI プロキシ、URL および TCP アプリケーションへの WebVPN 経由のアクセスを定義できます。さらに、ACL とフィルタ対象トラフィックのタイプも特定できます。WebVPN は、デフォルトではディセーブルです。

ASA での PKI 実装

ASA における PKI 実装は、VPN 3000 コンセントレータの実装とは異なります。ASA 上の PKI モデルの重要な概念はトラストポイントです。トラストポイントには、次の特性があります。

- トラストポイントは、ローカル ID と 1 対 1 の関係を持ちます。
- トラストポイントは、CA ID と 多対 1 の関係を持ちます。
- トラストポイントは、登録要求の内容、デフォルト、および登録方法を指定します。
- トラストポイントは、CRL コンフィギュレーション パラメータを指定します。

ASA では、CLI でトラストポイントを設定するために **crypto ca trustpoint** コマンドが用意されています。このコマンドには、IOS オプションのサブセットと、既存の VPN 3000 機能を ASA に移行するための追加パラメータが含まれています。このコマンドと、そのサブコマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。すべての PKI 機能は、ASDM で設定できます（詳細については、このマニュアルの「デジタル証明書の登録」を参照してください）。

表 2-1 は、その他の新しい PKI コマンドのリストを示しています。

表 2-1　ASA の新しい PKI コマンド

コマンド セット	アクション
crypto key	RSA または DSA の鍵ペアを生成します。
crl configure	**crypto ca trustpoint** 下でこのコマンドを使用すると、**crl** コンフィギュレーション モードを開始して CRL パラメータを設定できます。
crl	VPN 3000 コンセントレータから引き継いだ多数のパラメータを設定できます。
crypto ca authenticate	認証局から証明書をダウンロードまたはペーストすることで、CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca import（新しいコマンドではありません）	手動登録要求への応答として CA から受信した証明書をインストールします。
crypto ca crl request	指定したコンフィギュレーションの設定に基づいて、証明書失効リストを要求します。
crypto ca certificate map	証明書マッピング規則の優先順位付きリストを管理します。このコマンドは、VPN 3000 コンセントレータでの証明書グループのマッチング用に提供されています。
tunnel-group-map	証明書ベースの IKE セッションをトンネル グループにマッピングするためのポリシーと規則を設定します。

インターフェイスごとの ASDM セッションおよび WebVPN セッション

ASA Version 7.1(1) 以降は、インターフェイス上で WebVPN 管理セッションおよび ASDM 管理セッションの両方を同時にサポートします。唯一の制約は、これらの機能にそれぞれ異なるポートを割り当てる必要があるという点です。たとえば、HTTPS トラフィック用にポート 443 を使用して WebVPN を実行する場合、ASDM 管理セッションには別のポートを割り当てます。

ASDM を使用して、Configuration > VPN > WebVPN > WebVPN Access ウィンドウでポートを設定します。