接続プロファイル、グループ ポリシー、およびユーザの設定

この章では、VPN の接続プロファイル（以前は「トンネル グループ」と呼ばれていました）、グループ ポリシー、およびユーザの設定方法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。

要約すると、最初に接続プロファイルを設定して、接続用の値を設定します。次に、グループ ポリシーを設定します。グループ ポリシーでは、ユーザの集合に関する値が設定されます。その後、ユーザを設定します。ユーザはグループの値を継承でき、さらに個別のユーザ単位に特定の値を設定することができます。この章では、これらのエンティティを設定する方法と理由について説明します。

接続プロファイル、グループ ポリシー、およびユーザの概要

グループとユーザは、バーチャル プライベート ネットワーク（VPN）のセキュリティ管理と ASA の設定における中核的な概念です。グループとユーザで指定される属性によって、VPN へのユーザ アクセスと VPN の使用方法が決定されます。*グループ*は、ユーザの集合を 1 つのエンティティとして扱うものです。*ユーザ*の属性は、*グループ ポリシー*から取得されます。*接続プロファイル*では、特定の接続用のグループ ポリシーを指定します。ユーザに対して特定のグループ ポリシーを割り当てない場合は、接続のデフォルト グループ ポリシーが適用されます。

（注） 接続プロファイルは、**tunnel-group** コマンドを使用して設定します。この章では、「接続プロファイル」と「トンネル グループ」という用語が同義的によく使用されています。

接続プロファイルとグループ ポリシーを使用すると、システム管理が簡略化されます。コンフィギュレーション タスクを効率化するために、ASA にはデフォルトの LAN-to-LAN 接続プロファイル、デフォルトのリモート アクセス接続プロファイル、SSL/IKEv2 VPN 用のデフォルトの接続プロファイル、およびデフォルトのグループ ポリシー（DfltGrpPolicy）が用意されています。デフォルトの接続プロファイルとグループ ポリシーでは、多くのユーザに共通すると考えられる設定が提供されます。ユーザを追加するときに、ユーザがグループ ポリシーからパラメータを「継承」するように指定できます。これにより、数多くのユーザに対して迅速に VPN アクセスを設定できます。

すべての VPN ユーザに同一の権限を許可する場合は、特定の接続プロファイルやグループ ポリシーを設定する必要はありませんが、VPN がそのように使用されることはほとんどありません。たとえば、経理グループ、カスタマー サポート グループ、および MIS（経営情報システム）グループが、プライ

ベート ネットワークのそれぞれ異なる部分にアクセスできるようにする場合が考えられます。また、MIS に所属する特定のユーザには、他の MIS ユーザにはアクセスできないシステムにアクセスを許可する場合があります。接続プロファイルとグループ ポリシーにより、このような柔軟な設定を安全に実行することができます。

（注）　ASA には、オブジェクト グループという概念もあります。これは、ネットワーク リストのスーパーセットです。オブジェクト グループを使用すると、ポートやネットワークに対する VPN アクセスを定義することができます。オブジェクト グループは、グループ ポリシーや接続プロファイルよりも、ACL と関連があります。オブジェクト グループの使用方法の詳細については、一般的な操作のコンフィギュレーション ガイドの Chapter 17, “Configuring Objects,” を参照してください。

セキュリティ アプライアンスでは、さまざまなソースから属性値を適用できます。次の階層に従って、属性値を適用します。

1. Dynamic Access Policy（DAP）レコード
2. ユーザ名
3. グループ ポリシー
4. 接続プロファイル用のグループ ポリシー
5. デフォルトのグループ ポリシー

そのため、属性の DAP 値は、ユーザ、グループ ポリシー、または接続プロファイル用に設定された値よりもプライオリティが高くなっています。

DAP レコードの属性をイネーブルまたはディセーブルにすると、ASA はその値を適用して実行します。たとえば、DAP webvpn モードで HTTP プロキシをディセーブルにすると、ASA はそれ以上値を検索しません。代わりに、**http-proxy** コマンドの **no** 値を使用すると、属性は DAP レコードに存在しないため、適用する値を検索するために、セキュリティ アプライアンスはユーザ名の AAA 属性、および必要に応じてグループ ポリシーに移動して適用する値を検出します。ASA クライアントレス SSL VPN コンフィギュレーションは、それぞれ 1 つの http-proxy コマンドと 1 つの https-proxy コマンドのみサポートしています。ASDM を使用して DAP を設定することをお勧めします。

接続プロファイル

接続プロファイルは、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、トンネル ユーザが認証先サーバ、および接続情報の送信先となるアカウンティング サーバ（存在する場合）を特定します。また、これらのレコードには、接続用のデフォルト グループ ポリシーも指定され、さらにプロトコル固有の接続パラメータも含まれています。接続プロファイルには、トンネル自体の作成に関連する少数の属性が含まれます。接続プロファイルには、ユーザ関連の属性を定義するグループ ポリシーへのポインタも含まれます。

ASA には、LAN-to-LAN 接続用の DefaultL2Lgroup、リモートアクセス用の DefaultRAgroup、および SSL VPN（ブラウザベース）接続用の DefaultWEBVPNGroup という、デフォルト接続プロファイルがあります。これらのデフォルト接続プロファイルは変更できますが、削除はできません。また、環境に固有の接続プロファイルを 1 つ以上作成することもできます。接続プロファイルは、ASA のローカルな設定であり、外部サーバでは設定できません。

接続プロファイルでは、次の属性が指定されます。

- 「接続プロファイルの一般接続パラメータ」（P.4-3）
- 「IPSec トンネルグループ接続パラメータ」（P.4-3）
- 「接続プロファイルの SSL VPN セッション接続パラメータ」（P.4-5）

接続プロファイルの一般接続パラメータ

一般パラメータは、すべての VPN 接続に共通です。一般パラメータには、次のものがあります。

- 接続プロファイル名：接続プロファイル名は、接続プロファイルを追加または編集するときに指定します。次の注意事項があります。
  - 認証に事前共有キーを使用するクライアントの場合、接続プロファイル名はクライアントが ASA 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、ASA が証明書からこの名前を抽出します。
- 接続タイプ：接続タイプには、IKEv1 リモート アクセス、IPsec Lan-to-LAN、および Anyconnect（SSL/IKEv2）が含まれます。接続プロファイルでは、1 つの接続タイプだけ指定できます。
- 認証、許可、アカウンティング サーバ：これらのパラメータでは、ASA が次の目的で使用するサーバのグループまたはリストを指定します。
  - ユーザの認証
  - ユーザがアクセスを許可されたサービスに関する情報の取得
  - アカウンティング レコードの保存

  サーバ グループは、1 つ以上のサーバで構成されます。
- 接続用のデフォルト グループ ポリシー：グループ ポリシーは、ユーザ関連の属性のセットです。デフォルト グループ ポリシーは、ASA がトンネル ユーザを認証または許可する際にデフォルトで使用する属性を含んだグループ 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、ASA がクライアントに割り当てる 1 つ以上の DHCP サーバまたはアドレス 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 サーバから受信した「account-disabled」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、現在のパスワードが指定日数（デフォルトは 14 日）で期限切れになることをユーザに警告して、パスワードを変更する機会をユーザに提供できます。
- グループ除去および領域除去：これらのパラメータにより、ASA が受信するユーザ名を処理する方法が決まります。これらは、user@realm の形式で受信するユーザ名にだけ適用されます。領域は @ デリミタ付きでユーザ名に付加される管理ドメインです（user@abc）。

  strip-group コマンドを指定すると、ASA 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によって、ユーザ接続の接続プロファイルを選択します。次に、ASA は、許可および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（ディセーブルになっている場合）、ASA は領域を含むユーザ名全体を送信します。

  レルム除去処理によって、ユーザ名を認証サーバまたは許可サーバに送信するときに、ユーザ名からレルムが削除されます。このコマンドをイネーブルにすると、ASA では、ユーザ名のユーザ部分のみを許可/認証のために送信します。それ以外の場合、ASA ではユーザ名全体を送信します。
- 許可の要求：このパラメータを使用すると、ユーザ接続の前に許可を要求したり、またはその要求を取り下げたりできます。
- 許可 DN 属性：このパラメータは、許可を実行するときに使用する認定者名属性を指定します。

IPSec トンネルグループ接続パラメータ

IPSec 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：事前共有キー、証明書、または両方。
  - 事前共有キーに基づいた IKE 接続の場合、接続ポリシーに関連付けられた英数字のキー自体です（最大 128 文字）。
  - ピア ID 確認の要求：このパラメータでは、ピアの証明書を使用してピアのアイデンティティを確認することを要求するかどうかを指定します。
  - 認証方式に証明書または両方を指定する場合、エンド ユーザは認証のために有効な証明書を指定する必要があります。
- 拡張ハイブリッド認証方式：XAUTH およびハイブリッド XAUTH。

  isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザ認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。
- ISAKMP（IKE）キープアライブの設定：この機能により、ASA はリモート ピアの継続的な存在をモニタし、自分自身の存在をピアに報告します。ピアが応答しなくなると、ASA 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と、IKE ピアが接続を失ったときに接続がハングしません。

  IKE キープアライブにはさまざまな形式があります。この機能が動作するには、ASA とリモート ピア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、次のピアに対して動作します。
  - Cisco AnyConnet VPN Client
  - Cisco VPN Client（Release 3.0 以上）
  - Cisco VPN 3000 Client（Release 2.x）
  - Cisco VPN 3002 Hardware Client
  - Cisco VPN 3000 シリーズ Concentrator
  - 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する場合は、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と、応答しないピアとの接続はタイムアウトになるまでアクティブのままになるため、アイドル タイムアウトを短くすることを推奨します。アイドル タイムアウトを変更するには、「グループ ポリシーの設定」（P.4-44）を参照してください。

（注） ISDN 回線経由で接続するクライアントがグループに含まれる場合は、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てください。通常、ISDN 接続はアイドルになると切断されますが、IKE キープアライブのメカニズムによって接続がアイドル状態にならないため、切断されなくなります。

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 キーと IPSec キーのどちらかの期限が満了した場合にだけ切断されます。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 Peer Timeout Profile 値を持つトンネルから切断されません。

（注）　IKE メイン モードを使用する LAN-to-LAN コンフィギュレーションの場合は、2 つのピアの IKE キープアライブのコンフィギュレーションが同じであることを確認してください。両方のピアで IKE キープアライブがイネーブルになっているか、または両方のピアで IKE キープアライブがディセーブルになっている必要があります。

- 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（ID 証明書と発行するすべての証明書をピアに送信する）か、証明書だけを発行する（ルート証明書とすべての下位 CA 証明書を含む）かを指定できます。
- Windows クライアント ソフトウェアの古いバージョン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、アップデートされたクライアント バージョンをユーザが取得するためのメカニズムを提供できます。VPN 3002 ハードウェア クライアント ユーザの場合は、自動アップデートをトリガーできます。すべての接続プロファイルまたは特定の接続プロファイルに対して、client-update を設定および変更できます。
- デジタル証明書を使用して認証を設定する場合は、IKE ピアに送信する証明書を識別するトラストポイントの名前を指定できます。

接続プロファイルの SSL VPN セッション接続パラメータ

表 4-1 は、SSL VPN（AnyConnect クライアントおよびクライアントレス）接続に固有の接続プロファイルの属性のリストです。これらの属性に加えて、すべての VPN 接続に共通の一般接続プロファイルの属性を設定します。接続プロファイルの設定に関する手順ごとの情報については、「クライアントレス SSL VPN セッションの接続プロファイルの設定」（P.4-21）を参照してください。

（注）　以前のリリースでは、「接続プロファイル」は「トンネル グループ」として知られていました。接続プロファイルは tunnel-group コマンドで設定します。この章では、この 2 つの用語が同義的によく使用されています。

表 4-1　SSL VPN 用接続プロファイルの属性

コマンド	機能
authentication	認証方式、AAA または証明書を設定します。
customization	適用するすでに定義済みのカスタマイゼーションの名前を指定します。カスタマイゼーションによって、ログイン時にユーザに表示されるウィンドウ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、クライアントレス SSL VPN の設定の一部として設定します。
nbns-server	CIFS 名前解決に使用する NetBIOS ネーム サービス サーバ（nbns-server）の名前を指定します。
group-alias	サーバから接続プロファイルを参照できる 1 つ以上の代替名を指定します。ログイン時に、ユーザはドロップダウン メニューからグループ名を選択します。
group-url	1 つ以上のグループ URL を指定します。この属性を設定する場合、指定した URL にアクセスするユーザは、ログイン時にグループを選択する必要はありません。
dns-group	DNS サーバ名、ドメイン名、ネーム サーバ、リトライ回数、および接続ファイルで使用される DNS サーバのタイムアウト値を指定する DNS サーバ グループを指定します。

表 4-1　SSL VPN 用接続プロファイルの属性 （続き）

コマンド	機能
hic-fail-group-policy	Cisco Secure Desktop Manager を使用して、グループベース ポリシー属性を「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合は、VPN 機能ポリシーを指定します。
override-svc-download	AnyConnect VPN クライアントをリモート ユーザにダウンロードするために、設定されているグループ ポリシー属性またはユーザ名属性のダウンロードが上書きされます。
radius-reject-message	認証が拒否されたときに、ログイン画面に RADIUS 拒否メッセージを表示します。

接続プロファイルの設定

ここでは、シングル コンテキスト モードまたはマルチ コンテキスト モードの両方での接続プロファイルの内容および設定について説明します。

（注）　マルチ コンテキスト モードは IKEv1 および IKEv2 サイト間にのみ適用され、IKEv1 IPSec の AnyConnect、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、または cTCP には適用されません。

デフォルトの接続プロファイルを変更し、3 つのトンネルグループ タイプのいずれかで新しい接続プロファイルを設定できます。接続プロファイル内で明示的に設定しない属性に対しては、その値がデフォルトの接続プロファイルから取得されます。デフォルトの接続プロファイル タイプはリモートアクセスです。その後のパラメータは、選択したトンネル タイプによって異なります。デフォルト接続プロファイルも含めて、すべての接続プロファイルの現在のコンフィギュレーションとデフォルトのコンフィギュレーションを確認するには、**show running-config all tunnel-group** コマンドを入力します。

接続プロファイルの最大数

1 つの ASA がサポートできる接続プロファイル（トンネル グループ）の最大数は、プラットフォームの同時 VPN セッションの最大数 + 5 の関数です。たとえば、ASA 5505 は、同時に最大 25 の VPN セッションをサポートし、30 のトンネル グループ（25+5）を許可します。制限値を超えてトンネル グループを追加しようとすると、「ERROR: The limit of 30 configured tunnel groups has been reached」というメッセージが出力されます。

表 4-2 は、各 ASA プラットフォームの VPN セッションと接続プロファイルの最大数を示します。

表 4-2　VPN セッションおよび接続プロファイルの最大数（ASA プラットフォームごと）

	5505 基本 /Security Plus	5510/ 基本 /Security Plus	5520	5540	5550	5580-20	5580-40
VPN セッションの最大数	10/25	250	750	5000	5000	10,000	10,000
接続プロファイルの最大数	15/30	255	755	5005	5005	10,005	10,005

デフォルトの IPsec リモートアクセス接続プロファイルの設定

デフォルトのリモートアクセス接続プロファイルの内容は、次のとおりです。

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no override-account-disable
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

IPSec トンネルグループの一般属性の設定

一般属性は、複数のトンネルグループ タイプに共通です。IPSec リモートアクセス トンネルとクライアントレス SSL VPN トンネルでは、同じ一般属性の大部分を共有しています。IPSec LAN-to-LAN トンネルは、サブセットを使用します。すべてのコマンドの詳細については、『*Cisco ASA Series Command Reference*』を参照してください。ここでは、リモート アクセス接続プロファイルおよび LAN-to-LAN 接続プロファイルを設定する方法について順に説明します。

リモート アクセス接続プロファイルの設定

次のリモート クライアントと中央サイトの ASA の間に接続を設定する場合は、リモート アクセス接続プロファイルを使用します。

- レガシー Cisco VPN Client（IPsec/IKEv1 と接続）
- AnyConnect Secure Mobility Client（SSL または IPsec/IKEv2 と接続）
- クライアントレス SSL VPN（SSL とのブラウザベースの接続）
- Cisco ASA 5500 Easy VPN ハードウェア クライアント（IPsec/IKEv1 と接続）
- Cisco VPM 3002 ハードウェア クライアント（IPsec/IKEv1 と接続）

また、*DfltGrpPolicy* という名前のデフォルト グループ ポリシーも提供します。

リモート アクセス接続プロファイルを設定するには、最初にトンネル グループ一般属性を設定し、次にリモート アクセス属性を設定します。次の項を参照してください。

- 「リモートアクセス接続プロファイルの名前とタイプの指定」（P.4-8）。
- 「リモートアクセス接続プロファイルの一般属性の設定」（P.4-8）。
- 「二重認証の設定」（P.4-13）
- 「リモート アクセス接続プロファイルの IPSec IKEv1 属性の設定」（P.4-14）。
- 「IPSec リモート アクセス接続プロファイルの PPP 属性の設定」（P.4-16）

リモートアクセス接続プロファイルの名前とタイプの指定

tunnel-group コマンドを入力し、名前とタイプを指定して、接続プロファイルを作成します。リモートアクセス トンネルの場合、タイプは **remote-access** です。

```
hostname(config)# tunnel-group tunnel_group_name type remote-access
hostname(config)#
```

たとえば、TunnelGroup1 という名前のリモートアクセス接続プロファイルを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup1 type remote-access
hostname(config)#
```

リモートアクセス接続プロファイルの一般属性の設定

接続プロファイルの一般属性を設定または変更するには、次の手順でパラメータを指定します。

ステップ 1　一般属性を設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで **tunnel-group general-attributes** タスクを入力します。これで、トンネルグループ一般属性コンフィギュレーション モードが開始されます。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

ステップ 2　認証サーバ グループがある場合、使用するグループの名前を指定します。指定したサーバ グループに障害が発生したときにローカル データベースを認証に使用する場合は、キーワード **LOCAL** を追加します。

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

認証サーバ グループの名前は、最大 16 文字です。

オプションで、グループ名の後ろにインターフェイス名を指定することにより、インターフェイス固有の認証を設定することもできます。トンネルの終了場所を指定するインターフェイス名は、丸カッコで囲む必要があります。次のコマンドでは、認証にサーバ servergroup1 を使用する test という名前のインターフェイスのインターフェイス固有の認証が設定されます。

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

ステップ 3　使用する許可サーバ グループの名前を指定します（存在する場合）。この値を設定する場合、ユーザは接続する許可データベースに存在する必要があります。

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

許可サーバ グループの名前は、最大 16 文字です。たとえば、次のコマンドは、許可サーバ グループ FinGroup を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

ステップ 4　アカウンティングサーバ グループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

アカウンティング サーバ グループの名前は、最大 16 文字です。たとえば、次のコマンドは、アカウンティングサーバ グループ comptroller を使用することを指定しています。

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

ステップ 5　デフォルト グループ ポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

グループ ポリシーの名前は、最大 64 文字です。次の例では、デフォルト グループ ポリシーの名前として DfltGrpPolicy を設定しています。

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

ステップ 6　DHCP サーバ（最大 10 サーバ）の名前または IP アドレス、および DHCP アドレス プール（最大 6 プール）の名前を指定します。デフォルトでは、DHCP サーバとアドレス プールは使用されません。**dhcp-server** コマンドにより、VPN クライアントの IP アドレスを取得しようとするときに、指定の DHCP サーバに追加オプションを送信するように ASA を設定できるようになります。詳細については、『*Cisco ASA Series Command Reference*』の **dhcp-server** コマンドを参照してください。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

（注）　インターフェイス名を指定する場合は、丸カッコで囲む必要があります。

アドレス プールは、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して設定します。

ステップ 7　ネットワーク アドミッション コントロールを使用している場合は、ネットワーク アドミッション コントロール ポスチャ検証で使用される認証サーバのグループを特定するために、NAC 認証サーバ グループの名前を指定します。NAC をサポートするように、少なくとも 1 つのアクセス コントロール サーバを設定します。ACS グループの名前を指定するには、**aaa-server** コマンドを使用します。次に、その同じ名前をサーバ グループに使用して、**nac-authentication-server-group** コマンドを使用します。

次に、NAC ポスチャ検証に使用される認証サーバ グループとして acs-group1 を識別する例を示します。

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

次に、デフォルトのリモート アクセス グループから認証サーバ グループを継承する例を示します。

```
hostname(config-group-policy)# no nac-authentication-server-group
hostname(config-group-policy)
```

（注）　NAC を使用するには、リモート ホスト上に Cisco Trust Agent が存在する必要があります。

ステップ 8　ユーザ名を AAA サーバに渡す前に、ユーザ名からグループまたは領域を除去するかどうかを指定します。デフォルトでは、グループ名もレルムも除去されません。

```
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
hostname(config-tunnel-general)#
```

レルムとは管理ドメインのことです。領域を除去する場合、ASA はユーザ名およびグループ（ある場合）認証を使用します。グループを除去すると、ASA は認証にユーザ名およびレルム（ある場合）を使用します。レルム修飾子を削除するには **strip-realm** コマンドを入力し、認証中にユーザ名からグループ修飾子を削除するには strip-group コマンドを使用します。両方の修飾子を削除すると、認証は *username* だけに基づいて行われます。それ以外の場合、認証は *username@realm* 文字列全体または *username<delimiter> group* 文字列に基づいて行われます。サーバでデリミタを解析できない場合は、**strip-realm** を指定する必要があります。

ステップ 9　サーバが RADIUS、RADIUS with NT、または LDAP サーバの場合、オプションで、パスワード管理をイネーブルにできます。

（注）　認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。

Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

詳細については、一般的な操作のコンフィギュレーション ガイドの “Configuring Authorization with LDAP for VPN” section on page 32-18 を参照してください。

この機能はデフォルトでディセーブルになっており、現在のパスワードの有効期限が近づくとユーザに警告を表示します。デフォルトでは、期限切れの 14 日前に警告が開始されます。

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

サーバが LDAP サーバの場合、有効期限が近いことに関する警告が開始されるまでの日数（0 ～ 180）を指定できます。

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

（注）　トンネルグループ一般属性コンフィギュレーション モードで入力した **password-management** コマンドによって、トンネルグループ ipsec 属性モードで事前に入力された非推奨の **radius-with-expiry** コマンドが置き換えられます。

password-management コマンドを設定すると、ASA は、リモート ユーザがログインするときに、そのユーザの現在のパスワードの期限切れが迫っている、または期限が切れたことを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

これによってパスワードが期限切れになるまでの日数が変更されるわけではなく、ASA がパスワードが期限切れになる何日前にユーザへの警告を開始するかが変更されるという点に注意してください。

password-expire-in-days キーワードを指定する場合は、日数も指定する必要があります。

このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。ASA は、ユーザに対して失効が迫っていることを通知しませんが、失効後にユーザはパスワードを変更できます。

詳細については、「パスワード管理用の Microsoft Active Directory の設定」（P.4-30） を参照してください。

（注） ASA Version 7.1 以降では、LDAP または MS-CHAPv2 をサポートする RADIUS 接続で認証を行うときに、AnyConnect VPN Client 接続、Cisco IPSec VPN Client 接続、SSL VPN 完全トンネリング クライアント接続、およびクライアントレス接続に対するパスワード管理が一般的にサポートされています。Kerberos/AD（Windows パスワード）または NT 4.0 ドメインに対するこれらの接続タイプのいずれでも、パスワード管理はサポートされて*いません*。

MS-CHAP をサポートしている一部の RADIUS サーバは、現在 MS-CHAPv2 をサポートしていません。**password-management** コマンドを使用するには、MS-CHAPv2 が必要なため、ベンダーに確認してください。

RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバのみに対して通信しているように見えます。

LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

ステップ 10　オプションで、**override-account-disable** コマンドを入力して、AAA サーバからの account-disabled インジケータを上書きする機能を設定できます。

```
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

（注） override-account-disable を許可することは、潜在的なセキュリティ リスクとなります。

ステップ 11　証明書から許可クエリー用の名前を得るために使用する 1 つまたは複数の属性を指定します。この属性により、サブジェクト DN フィールドのどの部分を許可用のユーザ名として使用するかが指定されます。

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

たとえば、次のコマンドは、CN 属性を許可用のユーザ名として使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes は、**C**（国）、**CN**（通常名）、**DNQ**（DN 修飾子）、**EA**（電子メール アドレス）、**GENQ**（世代修飾子）、**GN**（名）、**I**（イニシャル）、**L**（地名）、**N**（名前）、**O**（組織）、**OU**（組織ユニット）、**SER**（シリアル番号）、**SN**（姓）、**SP**（州または都道府県）、**T**（役職）、**UID**（ユーザ ID）、および **UPN**（ユーザ プリンシパル ネーム）があります。

ステップ 12　ユーザに接続を許可する前に、そのユーザが正常に許可されている必要があるかどうかを指定します。デフォルトでは許可は要求されません。

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

二重認証の設定

二重認証は、ユーザがログイン画面に追加の認証クレデンシャル（2 つ目のユーザ名とパスワードなど）を入力するよう要求するオプションの機能です。二重認証を設定するには、次のコマンドを指定します。

ステップ 1　セカンダリ認証サーバ グループを指定します。このコマンドはセカンダリ AAA サーバとして使用する AAA サーバ グループを指定します。

（注）　このコマンドは、AnyConnect クライアント VPN 接続にだけ適用されます。

セカンダリのサーバ グループでは SDI サーバ グループを指定できません。デフォルトでは、セカンダリ認証は必要ありません。

```
hostname(config-tunnel-general)# secondary-authentication-server-group [interface_name]
{none | LOCAL | groupname [LOCAL]} [use-primary-name]
```

none キーワードを指定すると、セカンダリ認証は要求されません。*groupname* 値は AAA サーバ グループ名を示します。ローカルは内部サーバ データベースを使用することを示し、groupname 値と併用すると、LOCAL はフォールバックを示します。たとえば、プライマリ認証サーバ グループを sdi_group に、セカンダリ認証サーバ グループを ldap_server に設定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# authentication-server-group
hostname(config-tunnel-general)# secondary-authentication-server-group
```

（注）　**use-primary-name** キーワードを使用する場合、ログイン ダイアログは 1 つのユーザ名だけ要求します。また、ユーザ名をデジタル証明書から抽出する場合、プライマリ ユーザ名だけが認証に使用されます。

ステップ 2　セカンダリ ユーザ名を証明書から取得する場合は、**secondary-username-from-certificate** を入力します。

```
hostname(config-tunnel-general)# secondary-username-from-certificate C | CN | ... |
use-script
```

セカンダリ ユーザ名として使用するために証明書から抽出する DN フィールドの値は、プライマリの **username-from-certificate** コマンドと同じです。または、use-script キーワードを指定して、ASDM によって生成されたスクリプト ファイルを使用するよう ASA に指示します。

たとえば、プライマリ ユーザ名フィールドとして通常名を、セカンダリ ユーザ名フィールドとして組織ユニットを指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# username-from-certificate cn
hostname(config-tunnel-general)# secondary-username-from-certificate ou
```

ステップ 3　認証で使用するためにクライアント証明書からセカンダリ ユーザ名を抽出できるようにするには、トンネルグループ webvpn 属性モードで **secondary-pre-fill-username** コマンドを使用します。このコマンドをクライアントレス接続または SSL VPN（AnyConnect）クライアント接続に適用するかどうか、抽出されたユーザ名をエンド ユーザに非表示にするかどうかを指定するキーワードを使用します。この機能はデフォルトで無効に設定されています。クライアントレス オプションと SSL クライアント オプションは同時に使用できますが、それぞれ別個のコマンドで設定する必要があります。

```
hostname(config-tunnel-general)# secondary-pre-fill-username-from-certificate {clientless
| ssl-client} [hide]
```

たとえば、接続のプライマリとセカンダリの両方の認証に pre-fill-username を使用するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# pre-fill-username ssl-client
hostname(config-tunnel-general)# secondary-pre-fill-username ssl-client
```

ステップ 4　接続に適用する許可属性を取得するために使用する認証サーバを指定します。デフォルトの選択は、プライマリ認証サーバです。このコマンドは二重認証でのみ意味を持ちます。

```
hostname(config-tunnel-general)# authentication-attr-from-server {primary | secondary}
```

たとえば、セカンダリ認証サーバを指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authentication-attr-from-server secondary
```

ステップ 5　セッションと関連付ける認証ユーザ名（プライマリまたはセカンダリ）を指定します。デフォルト値は primary です。二重認証をイネーブルにすると、2 つの別のユーザ名でセッションを認証できます。管理者はセッションのユーザ名として認証されたユーザ名のいずれかを指定する必要があります。セッションのユーザ名は、アカウンティング、セッション データベース、syslog、デバッグ出力に提供されるユーザ名です。

```
hostname(config-tunnel-general)# authenticated-session-username {primary | secondary}
```

たとえば、セッションと関連付ける認証ユーザ名をセカンダリ認証サーバから取得するよう指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authenticated-session-username secondary
```

リモート アクセス接続プロファイルの IPSec IKEv1 属性の設定

リモート アクセス接続プロファイルの IPSec IKEv1 属性を設定するには、次の手順を実行します。次の説明は、リモート アクセス接続プロファイルをすでに作成していることを前提としています。リモート アクセス接続プロファイルには、LAN-to-LAN 接続プロファイルよりも多くの属性があります。

ステップ 1　リモート アクセス トンネル グループの IPSec 属性を指定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のコマンドを入力してトンネルグループ ipsec 属性モードを開始します。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

このコマンドにより、トンネル グループ ipsec 属性コンフィギュレーション モードが開始されます。このモードでは、シングル コンテキスト モードまたはマルチ コンテキスト モードでリモート アクセス トンネルグループの IPSec 属性を設定します。

たとえば、次のコマンドは、TG1 という名前の接続プロファイルに関係するトンネルグループ ipsec 属性モードのコマンドが続くことを指定しています。プロンプトが変化して、トンネルグループ ipsec 属性モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

ステップ 2　事前共有キーに基づく IKEv1 接続をサポートするために、事前共有キーを指定します。たとえば、次のコマンドは、IPsec IKEv1 リモート アクセス接続プロファイルの IKEv1 接続をサポートするために、事前共有キー xyzx を指定しています。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

ステップ 3　ピアの証明書を使用してピアのアイデンティティを検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できる*オプション*値は、**req**（必須）、**cert**（証明書でサポートされている場合）、**nocheck**（調べない）です。デフォルトは **req** です。

たとえば、次のコマンドは peer-id 検証が必要なことを指定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

ステップ 4　証明書チェーンを送信できるかどうかを指定します。次のコマンドは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

この属性は、すべての IPsec トンネルグループ タイプに適用されます。

ステップ 5　IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# ikev1 trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

次のコマンドは、IKE ピアに送信する証明書の名前として mytrustpoint を指定しています。

```
hostname(config-ipsec)# ikev1 trust-point mytrustpoint
```

ステップ 6　ISAKMP キープアライブのしきい値と許可されるリトライ回数を指定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

threshold パラメータでは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数（10 ～ 3600）で指定します。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間の間隔です（2 ～ 10 秒）。IKE キープアライブは、デフォルトでイネーブルです。ISAKMP キープアライブをディセーブルにするには、**isakmp keepalive disable** と入力します。

たとえば、次のコマンドは、IKE キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold パラメータのデフォルト値は、リモートアクセスの場合は 300、LAN-to-LAN の場合は 10 です。また、retry パラメータのデフォルト値は 2 です。

中央サイト（セキュア ゲートウェイ）で、ISAKMP モニタリングを決して開始しないように指定する場合は、次のコマンドを入力します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

ステップ 7　ISAKMP ハイブリッド認証方式、XAUTH またはハイブリッド XAUTH を指定します。

isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザ認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。ハイブリッド XAUTH によって、IKE のフェーズ 1 が次の 2 つの手順に分割されます。2 つ合わせてハイブリッド認証と呼ばれます。

a. ASA は、標準の公開キー技術を使用して、リモート VPN ユーザに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。

b. 次に、XAUTH 交換がリモート VPN ユーザを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注） 認証タイプをハイブリッドに設定するには、事前に認証サーバを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

isakmp ikev1-user-authentication コマンドとオプションの **interface** パラメータを使用して、特定のインターフェイスを指定できます。**interface** パラメータを省略すると、このコマンドはすべてのインターフェイスに適用され、インターフェイスごとにコマンドが指定されていない場合のバックアップとして機能します。接続プロファイルに 2 つの **isakmp ikev1-user-authentication** コマンドを指定していて、1 つで **interface** パラメータを使用し、もう 1 つで使用しない場合、インターフェイスを指定するコマンドはその特定のインターフェイスを優先します。

たとえば、次のコマンドは、example-group と呼ばれる接続プロファイルの内部インターフェイスでハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

IPSec リモート アクセス接続プロファイルの PPP 属性の設定

リモート アクセス接続プロファイルのポイントツーポイント プロトコル属性を設定するには、次の手順を実行します。PPP 属性は、IPSec リモート アクセスの接続プロファイルにだけ適用されます。次の説明は、IPSec リモート アクセス接続プロファイルをすでに作成していることを前提としています。

ステップ 1　トンネルグループ ppp 属性コンフィギュレーション モードに入ります。このモードで、次のコマンドを入力して、リモートアクセス トンネルグループ PPP 属性を設定します。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name type remote-access
hostname(config)# tunnel-group tunnel-group-name ppp-attributes
hostname(config-tunnel-ppp)#
```

たとえば、次のコマンドは、TG1 という名前の接続プロファイルに関係するトンネルグループ ppp 属性モードのコマンドが続くことを指定しています。プロンプトが変化して、トンネルグループ ppp 属性モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ppp-attributes
hostname(config-tunnel-ppp)#
```

ステップ 2　PPP 接続に対する固有のプロトコルを使用する認証をイネーブルにするかどうかを指定します。プロトコルの値は次のいずれかになります。

- pap：PPP 接続で Password Authentication Protocol（パスワード認証プロトコル）の使用をイネーブルにします。
- chap：PPP 接続で Challenge Handshake Authentication（チャレンジ ハンドシェイク認証プロトコル）の使用をイネーブルにします。
- ms-chap-v1 または ms-chap-v2：PPP 接続で Microsoft Challenge Handshake Authentication Protocol（Microsoft チャレンジ ハンドシェイク認証プロトコル）のバージョン 1 またはバージョン 2 の使用をイネーブルにします。
- eap：PPP 接続で Extensible Authentication Protocol（拡張認証プロトコル）の使用をイネーブルにします。

CHAP と MSCHAPv1 は、デフォルトでイネーブルになっています。

このコマンドの構文は次のとおりです。

```
hostname(config-tunnel-ppp)# authentication protocol
hostname(config-tunnel-ppp)#
```

特定のプロトコルの認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-tunnel-ppp)# no authentication protocol
hostname(config-tunnel-ppp)#
```

たとえば、次のコマンドは PPP 接続で PAP プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

次のコマンドは、PPP 接続で MS-CHAP バージョン 2 プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp)# authentication ms-chap-v2
hostname(config-tunnel-ppp)#
```

次のコマンドは、PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

次のコマンドは、PPP 接続で MS-CHAP バージョン 1 プロトコルの使用をディセーブルにします。

```
hostname(config-tunnel-ppp)# no authentication ms-chap-v1
hostname(config-tunnel-ppp)#
```

LAN-to-LAN 接続プロファイルの設定

IPSec LAN-to-LAN VPN 接続プロファイルは、LAN-to-LAN IPSec クライアント接続にだけ適用されます。設定するパラメータの多くは IPSec リモート アクセスの接続プロファイルのものと同じですが、LAN-to-LAN トンネルの方がパラメータの数は少なくなります。ここでは、LAN-to-LAN 接続プロファイルを設定する方法について説明します。

- 「LAN-to-LAN 接続プロファイルの名前とタイプの指定」（P.4-18）
- 「LAN-to-LAN 接続プロファイルの一般属性の設定」（P.4-18）
- 「LAN-to-LAN IPSec IKEv1 属性の設定」（P.4-19）

デフォルトの LAN-to-LAN 接続プロファイルのコンフィギュレーション

デフォルトの LAN-to-LAN 接続プロファイルの内容は、次のとおりです。

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 no accounting-server-group
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

LAN-to-LAN 接続プロファイルのパラメータはリモートアクセス接続プロファイルのパラメータより少なく、そのほとんどはどちらのグループでも同じです。実際に接続を設定する場合の利便性を考え、ここではこのグループのパラメータを個別に説明します。明示的に設定しないパラメータはすべて、デフォルトの接続プロファイルからその値を継承します。

LAN-to-LAN 接続プロファイルの名前とタイプの指定

接続プロファイルの名前とタイプを指定するには、次のように **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

LAN-to-LAN トンネルの場合、タイプは **ipsec-l2l** になります。たとえば、docs という名前の LAN-to-LAN 接続プロファイルを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

LAN-to-LAN 接続プロファイルの一般属性の設定

接続プロファイルの一般属性を設定するには、次の手順を実行します。

ステップ 1　シングル コンテキスト モードまたはマルチ コンテキスト モードで general-attributes キーワードを指定して、トンネルグループ一般属性モードを開始します。

```
hostname(config)# tunnel-group_tunnel-group-name general-attributes
hostname(config-tunnel-general)#
```

プロンプトが変化して、config-general モードに入ったことがわかります。トンネルグループの一般属性は、このモードで設定します。

たとえば、docs という名前の接続プロファイルの場合は、次のコマンドを入力します。

```
hostname(config)# tunnel-group_docs general-attributes
hostname(config-tunnel-general)#
```

ステップ 2　アカウンティングサーバ グループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドはアカウンティングサーバ グループ acctgserv1 の使用を指定しています。

```
hostname(config-tunnel-general)# accounting-server-group acctgserv1
hostname(config-tunnel-general)#
```

ステップ 3　デフォルト グループ ポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、デフォルト グループ ポリシーの名前に MyPolicy を指定しています。

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

LAN-to-LAN IPSec IKEv1 属性の設定

IPsec IKEv1 属性を設定するには、次の手順を実行します。

ステップ 1　トンネルグループ IPSec IKEv1 属性を設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで IPSec-attributes キーワードを指定して tunnel-group コマンドを入力し、トンネルグループ ipsec 属性コンフィギュレーション モードを開始します。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドでは、config-ipsec モードを開始し、TG1 という名前の接続プロファイルのパラメータを設定できます。

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

プロンプトが変化して、トンネルグループ ipsec 属性コンフィギュレーション モードに入ったことがわかります。

ステップ 2　事前共有キーに基づく IKEv1 接続をサポートするために、事前共有キーを指定します。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、LAN-to-LAN 接続プロファイルの IKEv1 接続をサポートするために、事前共有キー XYZX を指定しています。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

ステップ 3　ピアの証明書を使用してピアのアイデンティティを検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できるオプションは、**req**（必須）、**cert**（証明書でサポートされている場合）、**nocheck**（調べない）です。デフォルトは **req** です。たとえば、次のコマンドは、peer-id-validate オプションを **nocheck** に設定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

ステップ 4　証明書チェーンを送信できるかどうかを指定します。次のアクションは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

この属性は、すべてのトンネル グループ タイプに適用できます。

ステップ 5　IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、トラストポイント名を mytrustpoint に設定しています。

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

この属性は、すべてのトンネル グループ タイプに適用できます。

ステップ 6　ISAKMP（IKE）キープアライブのしきい値と許可されるリトライ回数を指定します。**threshold** パラメータでは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数（10 ～ 3600）で指定します。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間の間隔です（2 ～ 10 秒）。IKE キープアライブは、デフォルトでイネーブルです。IKE キープアライブをディセーブルにするには、**isakmp** コマンドの **no** 形式を入力します。

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、ISAKMP キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold パラメータのデフォルト値は、LAN-to-LAN の場合は 10 です。retry パラメータのデフォルト値は 2 です。

中央サイト（セキュア ゲートウェイ）で、ISAKMP モニタリングを決して開始しないように指定する場合は、次のコマンドを入力します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

ステップ 7　ISAKMP ハイブリッド認証方式、XAUTH またはハイブリッド XAUTH を指定します。

isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザ認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。ハイブリッド XAUTH によって、IKE のフェーズ 1 が次の 2 つの手順に分割されます。2 つ合わせてハイブリッド認証と呼ばれます。

a. ASA は、標準の公開キー技術を使用して、リモート VPN ユーザに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。

b. 次に、XAUTH 交換がリモート VPN ユーザを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注）　認証タイプをハイブリッドに設定するには、事前に認証サーバを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

たとえば、次のコマンドは、example-group と呼ばれる接続プロファイルのハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
```

```
hostname(config-tunnel-ipsec)#
```

クライアントレス SSL VPN セッションの接続プロファイルの設定

クライアントレス SSL VPN 接続プロファイル用のトンネルグループ一般属性は、トンネルグループのタイプが webvpn で、**strip-group** コマンドと **strip-realm** コマンドが適用されない点を除いて、IPSec リモートアクセスの接続プロファイルのものと同じです。クライアントレス SSL VPN に固有の属性は別々に定義します。次の項では、クライアントレス SSL VPN 接続プロファイルを設定する方法について説明します。

- 「クライアントレス SSL VPN セッションの一般トンネルグループ属性の設定」（P.4-21）
- 「クライアントレス SSL VPN セッションのトンネルグループ属性の設定」（P.4-24）

クライアントレス SSL VPN セッションの一般トンネルグループ属性の設定

接続プロファイルの一般属性を設定または変更するには、次の手順でパラメータを指定します。

ステップ 1　一般属性を設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで **tunnel-group general-attributes** コマンドを入力します。これで、トンネルグループ一般属性コンフィギュレーション モードが開始されます。プロンプトが変化することに注意してください。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

前の項で作成した TunnelGroup3 の一般属性を設定するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup3 general-attributes
hostname(config-tunnel-general)#
```

ステップ 2　認証サーバ グループがある場合、使用するグループの名前を指定します。指定したサーバ グループに障害が発生したときにローカル データベースを認証に使用する場合は、キーワード LOCAL を追加します。

```
hostname(config-tunnel-general)# authentication-server-group groupname [LOCAL]
hostname(config-tunnel-general)#
```

たとえば、test という名前の認証サーバ グループを設定し、認証サーバ グループで障害が発生したときにローカル サーバにフォールバックするようにするには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# authentication-server-group test LOCAL
hostname(config-tunnel-general)#
```

authentication-server-group 名で、事前に設定した認証サーバまたはサーバのグループを指定します。認証サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。

グループ名の前にある丸カッコ内にインターフェイス名を指定することにより、インターフェイス固有の認証を設定することもできます。次のインターフェイスはデフォルトで使用可能になっています。

- inside：インターフェイス GigabitEthernet0/1 の名前
- outside：インターフェイス GigabitEthernet0/0 の名前

（注）　ASA の外部インターフェイス アドレス（IPv4 と IPv6 の両方）は、プライベート側のアドレス空間と重複していてはなりません。

interface コマンドを使用して設定したその他のインターフェイスも使用可能です。次のコマンドは、認証にサーバ servergroup1 を使用する outside という名前のインターフェイスのインターフェイス固有の認証を設定しています。

```
hostname(config-tunnel-general)# authentication-server-group (outside) servergroup1
hostname(config-tunnel-general)#
```

ステップ 3　オプションで、使用する許可サーバ グループの名前を指定します（存在する場合）。許可を使用していない場合は、ステップ 6 に進んでください。この値を設定する場合、ユーザは接続する許可データベースに存在する必要があります。

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

許可サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。

たとえば、次のコマンドは、許可サーバ グループ FinGroup を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

ステップ 4　ユーザに接続を許可する前に、そのユーザが正常に許可されている必要があるかどうかを指定します。デフォルトでは許可は要求されません。

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

ステップ 5　証明書から許可クエリー用の名前を得るために使用する 1 つまたは複数の属性を指定します。この属性により、サブジェクト DN フィールドのどの部分を許可用のユーザ名として使用するかが指定されます。

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

たとえば、次のコマンドは、CN 属性を許可用のユーザ名として使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes は、**C**（国）、**CN**（通常名）、**DNQ**（DN 修飾子）、**EA**（電子メール アドレス）、**GENQ**（世代修飾子）、**GN**（名）、**I**（イニシャル）、**L**（地名）、**N**（名前）、**O**（組織）、**OU**（組織ユニット）、**SER**（シリアル番号）、**SN**（姓）、**SP**（州または都道府県）、**T**（役職）、**UID**（ユーザ ID）、および **UPN**（ユーザ プリンシパル ネーム）があります。

ステップ 6　オプションで、使用するアカウンティングサーバ グループの名前を指定します（存在する場合）。アカウンティングを使用していない場合は、ステップ 7 に進んでください。アカウンティング サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、アカウンティングサーバ グループ comptroller を使用することを指定しています。

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

ステップ 7　オプションで、デフォルト グループ ポリシーの名前を指定します。デフォルト値は DfltGrpPolicy です。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

次の例では、デフォルト グループ ポリシーの名前として MyDfltGrpPolicy を設定しています。

```
hostname(config-tunnel-general)# default-group-policy MyDfltGrpPolicy
hostname(config-tunnel-general)#
```

ステップ 8　オプションで、DHCP サーバ（最大 10 サーバ）の名前または IP アドレス、および DHCP アドレス プール（最大 6 プール）の名前を指定します。リスト項目はスペースで区切ります。デフォルトでは、DHCP サーバとアドレス プールは使用されません。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

（注）　インターフェイス名は丸カッコで囲む必要があります。

アドレス プールは、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して設定します。アドレス プールの設定の詳細については、第 5 章「VPN の IP アドレスの設定」を参照してください。

ステップ 9　サーバが RADIUS、RADIUS with NT、または LDAP サーバの場合、オプションで、パスワード管理をイネーブルにできます。

（注）　認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

- Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

詳細については、一般的な操作のコンフィギュレーション ガイドの“Configuring Authorization with LDAP for VPN” section on page 32-18 を参照してください。

この機能はデフォルトでイネーブルになっており、現在のパスワードの有効期限が近づくとユーザに警告を表示します。デフォルトでは、期限切れの 14 日前に警告が開始されます。

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

サーバが LDAP サーバの場合、有効期限が近いことに関する警告が開始されるまでの日数（0 ～ 180）を指定できます。

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

（注）　トンネルグループ一般属性コンフィギュレーション モードで入力した **password-management** コマンドによって、トンネルグループ ipsec 属性モードで事前に入力された非推奨の **radius-with-expiry** コマンドが置き換えられます。

このコマンドを設定すると、リモート ユーザがログインするときに、ASA は、ユーザの現在のパスワードの有効期限が近づいていること、または期限が切れていることを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

これによってパスワードが期限切れになるまでの日数が変更されるわけではなく、ASA がパスワードが期限切れになる何日前にユーザへの警告を開始するかが変更されるという点に注意してください。

password-expire-in-days キーワードを指定する場合は、日数も指定する必要があります。

詳細については、「パスワード管理用の Microsoft Active Directory の設定」（P.4-30）を参照してください。

ステップ 10　このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。ASA は、期限切れが近いことをユーザに通知しませんが、ユーザは期限切れ後にパスワードを変更できます。オプションで、**override-account-disable** コマンドを入力して、AAA サーバからの account-disabled インジケータを上書きする機能を設定できます。

```
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

クライアントレス SSL VPN セッションのトンネルグループ属性の設定

クライアントレス SSL VPN 接続プロファイルに固有のパラメータを設定するには、この項の次の手順を実行します。クライアントレス SSL VPN は、以前は WebVPN として知られていました。これらの属性は、トンネルグループ webvpn 属性モードで設定します。

ステップ 1　クライアントレス SSL VPN トンネルグループの属性を指定するには、次のコマンドを入力してトンネルグループ webvpn 属性モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name webvpn-attributes
hostname(config-tunnel-ipsec)#
```

たとえば、sales という名前のクライアントレス SSL VPN トンネルグループの webvpn 属性を指定するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)#
```

ステップ 2　AAA、デジタル証明書、または両方を使用するための認証方式を指定するには、**authentication** コマンドを入力します。AAA、証明書、または両方を任意の順序で指定できます。

```
hostname(config-tunnel-webvpn)# authentication authentication_method
hostname(config-tunnel-webvpn)#
```

たとえば、次のコマンドは AAA と証明書の両方の認証を許可します。

```
hostname(config-tunnel-webvpn)# authentication aaa certificate
hostname(config-tunnel-webvpn)#
```

カスタマイゼーションの適用

カスタマイゼーションによって、ログイン時にユーザに表示されるウィンドウ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、クライアントレス SSL VPN の設定の一部として設定します。

ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するために、事前に定義した Web ページ カスタマイゼーションを適用するには、ユーザ名 webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-username-webvpn)# customization {none | value customization_name}
hostname(config-username-webvpn)#
```

たとえば、blueborder という名前のカスタマイゼーションを使用するには、次のコマンドを入力します。

```
hostname(config-username-webvpn)# customization value blueborder
hostname(config-username-webvpn)#
```

カスタマイゼーション自体は、webvpn モードで **customization** コマンドを入力して設定します。

次の例は、「123」という名前のカスタマイゼーションを最初に確立するコマンド シーケンスを示しています。このコマンド シーケンスによって、パスワード プロンプトが定義されます。この例では、「test」という名前のクライアントレス SSL VPN トンネルグループを定義して、**customization** コマンドを使用し、「123」という名前のカスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# customization value 123
hostname(config-tunnel-webvpn)#
```

ステップ 3　ASA は、NetBIOS 名を IP アドレスにマップするために NetBIOS ネーム サーバにクエリーを送信します。クライアントレス SSL VPN では、リモート システムのファイルをアクセスまたは共有するための NetBIOS が必要です。クライアントレス SSL VPN では、NetBIOS と CIFS プロトコルを使用して、リモート システムのファイルをアクセスまたは共有します。Windows コンピュータにそのコンピュータ名を使用してファイル共有接続をしようとすると、指定されたファイル サーバはネットワーク上のリソースを識別する特定の NetBIOS 名と対応します。

NBNS 機能を動作させるには、少なくとも 1 台の NetBIOS サーバ（ホスト）を設定する必要があります。冗長性を実現するために NBNS サーバを 3 つまで設定できます。ASA は、リストの最初のサーバを NetBIOS/CIFS 名前解決に使用します。クエリーが失敗すると、次のサーバが使用されます。

CIFS 名前解決に使用する NBNS（NetBIOS ネーム サービス）サーバの名前を指定するには、**nbns-server** コマンドを使用します。サーバ エントリは 3 つまで入力できます。冗長性のために、設定する最初のサーバはプライマリ サーバで、その他のサーバはバックアップです。これが（ただの WINS サーバではなく）マスター ブラウザであるかどうか、タイムアウト間隔、およびリトライ回数も指定できます。WINS サーバまたはマスター ブラウザは、通常、ASA と同じネットワーク上か、そのネットワークから到達可能な場所に設定されます。タイムアウト間隔はリトライ回数の前に指定する必要があります。

```
hostname(config-tunnel-webvpn)# nbns-server {host-name | IP_address} [master]
[timeout seconds] [retry number]
hostname(config-tunnel-webvpn)#
```

たとえば、nbnsprimary という名前のサーバをプライマリ サーバとして設定し、サーバ 192.168.2.2 をセカンダリ サーバとして設定し、それぞれに 3 回のリトライを許可し、5 秒のタイムアウトを設定するには、次のコマンドを入力します。

```
hostname(config)# name 192.168.2.1 nbnsprimary
```

```
hostname(config-tunnel-webvpn)# nbns-server nbnsprimary master timeout 5 retry 3
hostname(config-tunnel-webvpn)# nbns-server 192.168.2.2 timeout 5 retry 3
hostname(config-tunnel-webvpn)#
```

タイムアウト間隔の範囲は 1 ～ 30 秒（デフォルトは 2）、リトライ回数は 0 ～ 10（デフォルトは 2）です。

トンネルグループ webvpn 属性コンフィギュレーション モードで **nbns-server** コマンドを使用すると、webvpn コンフィギュレーション モードで非推奨の **nbns-server** コマンドが置き換えられます。

ステップ 4　グループの代替名を指定するには、**group-alias** コマンドを使用します。グループ エイリアスを指定すると、ユーザがトンネルグループを参照できる 1 つ以上の代替名が作成されます。ここで指定するグループ エイリアスは、ユーザのログイン ページにあるドロップダウン リストに表示されます。各グループに対して複数のエイリアスを指定することも、エイリアスを指定しないこともできます。それぞれを別のコマンドで指定します。この機能は、同じグループが「Devtest」や「QA」などの複数の通常名で指定されている場合に便利です。

各グループ エイリアスに対して、**group-alias** コマンドを入力します。各エイリアスはデフォルトでイネーブルになっています。各エイリアスは、オプションで明示的にイネーブルまたはディセーブルにできます。

```
hostname(config-tunnel-webvpn)# group-alias alias [enable | disable]
hostname(config-tunnel-webvpn)#
```

たとえば、QA という名前のトンネルグループのエイリアスの QA と Devtest をイネーブルにするには、次のコマンドを入力します。

```
hostname(config-tunnel-webvpn)# group-alias QA enable
hostname(config-tunnel-webvpn)# group-alias Devtest enable
hostname(config-tunnel-webvpn)#
```

（注） webvpn tunnel-group-list は、表示する（ドロップダウン）グループ リストに対してイネーブルにする必要があります。

ステップ 5　グループの着信 URL または IP アドレスを指定するには、**group-url** コマンドを使用します。グループの URL または IP アドレスを指定すると、ユーザがログイン時にグループを選択する必要がなくなります。ユーザがログインすると、ASA は、tunnel-group-policy テーブル内のユーザの着信 URL またはアドレスを検索します。URL またはアドレスが見つかり、group-url が接続プロファイル内でイネーブルになっている場合、ASA は、関連の接続プロファイルを自動的に選択して、ログイン ウィンドウにユーザ名フィールドとパスワード フィールドだけを表示します。これによりユーザ インターフェイスが簡素化され、グループ リストがユーザに表示されなくなるという利点が追加されます。ユーザに表示するログイン ウィンドウには、その接続プロファイル用に設定されたカスタマイゼーションが使用されます。

URL またはアドレスがディセーブルになっており、group-alias が設定されている場合、グループのドロップダウン リストも表示され、ユーザは選択を行う必要があります。

1 つのグループに対して複数の URL またはアドレスを設定できます（何も設定しないこともできます）。各 URL またはアドレスは、個別にイネーブルまたはディセーブルにできます。指定した各 URL またはアドレスに対しては、別々の **group-url** コマンドを使用する必要があります。http または https プロトコルを含め、URL またはアドレス全体を指定する必要があります。

同じ URL またはアドレスを複数のグループに関連付けることはできません。ASA は、接続プロファイルの URL またはアドレスを受け入れる前にその URL またはアドレスの固有性を検証します。

各グループ URL またはアドレスに対して、**group-url** コマンドを入力します。各 URL またはエイリアスは、オプションで明示的にイネーブル（デフォルト）またはディセーブルにできます。

```
hostname(config-tunnel-webvpn)# group-url url [enable | disable]
```

```
hostname(config-tunnel-webvpn)#
```

Url は、このトンネル グループの URL または IP アドレスを指定します。

たとえば、RadiusServer という名前のトンネルグループに対してグループ URL http://www.example.com と http://192.168.10.10 をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
hostname(config-tunnel-webvpn)# group-url http://www.example.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

多数の例については、「クライアントレス SSL VPN セッションのユーザ用ログイン ウィンドウのカスタマイズ」（P.4-29）を参照してください。

ステップ 6　グループ URL のいずれかを入力した場合に、接続プロファイルごとに実行中の Cisco Secure Desktop から特定のユーザを免除するには、次のコマンドを入力します。

```
hostname(config-tunnel-webvpn)# without-csd
hostname(config-tunnel-webvpn)#
```

（注）　このコマンドを入力すると、これらのセッションのエンドポイント状態が検出されないため、Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）コンフィギュレーションを調整する必要があります。

ステップ 7　クライアントレス SSL VPN セッションの接続プロファイルに使用する DNS サーバ グループを指定するには、**dns-group** コマンドを使用します。指定するグループは、グローバル コンフィギュレーション モードで（**dns server-group** コマンドおよび **name-server** コマンドを使用して）設定済みのグループである必要があります。

デフォルトでは、接続プロファイルは DNS サーバ グループ *DefaultDNS* を使用します。ただし、セキュリティ アプライアンスで DNS 要求を解決する前にこのグループを設定する必要があります。

次の例は、*corp_dns* という名前の新規 DNS サーバ グループを設定し、接続プロファイル *telecommuters* のサーバ グループを指定します。

```
hostname(config)# dns server-group corp_dns
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 209.165.200.224

hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group corp_dns
hostname(config-tunnel-webvpn)#
```

ステップ 8　（任意）認証および許可で使用するためにクライアント証明書からユーザ名を抽出するには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドを使用します。デフォルト値はありません。

```
hostname(config)# pre-fill-username {ssl-client | clientless}
```

pre-fill-username コマンドは、ユーザ名 / パスワードの認証および許可のユーザ名として、**username-from-certificate** コマンド（トンネルグループ一般属性モード）で指定した証明書フィールドから抽出されるユーザ名の使用をイネーブルにします。証明書機能からこの事前充填ユーザ名を使用するには、両方のコマンドを設定する必要があります。

（注） バージョン 8.0.4 では、ユーザ名は事前に入力されません。ユーザ名フィールド内の送信されたデータは無視されます。

次の例では、グローバル コンフィギュレーション モードで入力された、remotegrp という名前の IPSec リモート アクセス トンネル グループを作成し、証明書からのユーザ名の取得をイネーブルにして、SSL VPN クライアント認証または許可のクエリーのための名前がデジタル証明書から派生している必要があることを指定します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# username-from-certificate CN OU
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)# pre-fill-username ssl-client
hostname(config-tunnel-webvpn)#
```

ステップ 9　（任意）AnyConnect または SSL VPN クライアントをダウンロードするためにグループ ポリシーまたはユーザ名属性コンフィギュレーションを上書きするかどうかを指定するには、**override-svc-download** コマンドを使用します。この機能はデフォルトで無効に設定されています。

セキュリティ アプライアンスは、**vpn-tunnel-protocol** コマンドによってグループ ポリシーまたはユーザ名属性でクライアントレスや SSL VPN がイネーブルになっているかどうかに基づいて、リモート ユーザに対してクライアントレス接続または AnyConnect クライアント接続を許可します。**anyconnect ask** コマンドはさらに、クライアントをダウンロードするか、または WebVPN ホームページに戻るようにユーザに要求して、クライアントのユーザ エクスペリエンスを変更します。

ただし、特定のトンネルグループでログインしているクライアントレス ユーザには、ダウンロード プロンプトが終了するまで待たせることなく、クライアントレス SSL VPN ホームページを表示することができます。**override-svc-download** コマンドを使用すると、接続プロファイル レベルでこのようなユーザに対する遅延を防止できます。このコマンドにより、接続プロファイル経由でログインするユーザには、**vpn-tunnel-protocol** コマンドまたは **anyconnect ask** コマンドの設定に関係なく、ただちにクライアントレス SSL VPN ホームページが表示されるようになります。

次の例では、接続プロファイル *engineering* のトンネルグループ webvpn 属性コンフィギュレーション モードに入り、クライアント ダウンロード プロンプトのグループ ポリシーとユーザ名属性設定を上書きする接続プロファイルをイネーブルにします。

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# override-svc-download
```

ステップ 10　（任意）認証が拒否されたときのログイン画面への RADIUS 拒否メッセージの表示をイネーブルにするには、**radius-eject-message** コマンドを使用します。

次に、engineering という名前の接続プロファイルに対して RADIUS 拒否メッセージの表示をイネーブルにする例を示します。

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# radius-reject-message
```

クライアントレス SSL VPN セッションのユーザ用ログイン ウィンドウのカスタマイズ

カスタマイゼーション プロファイルと接続プロファイルの組み合わせを使用することで、さまざまなグループに対して異なるログイン ウィンドウをセットアップできます。たとえば、salesgui と呼ばれるカスタマイゼーション プロファイルを作成してある場合、そのカスタマイゼーション プロファイルを使用する sales と呼ばれるクライアントレス SSL VPN セッション用の接続プロファイルを、次のように作成できます。

ステップ 1　webvpn モードで、クライアントレス SSL VPN アクセスのカスタマイゼーションを定義します。この場合は、salesgui という名前で、デフォルトのロゴを mycompanylogo.gif に変更します。mycompanylogo.gif を ASA のフラッシュ メモリに事前にロードし、設定を保存している必要があります。詳細については、第 11 章「クライアントレス SSL VPN の設定」を参照してください。

```
hostname# webvpn
hostname (config-webvpn)# customization value salesgui
hostname(config-webvpn-custom)# logo file disk0:\mycompanylogo.gif
hostname(config-webvpn-custom)#
```

ステップ 2　グローバル コンフィギュレーション モードで、ユーザ名をセットアップし、先ほど定義したクライアントレス SSL VPN 用のカスタマイゼーションと関連付けます。

```
hostname# username seller attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value salesgui
hostname(config-username-webvpn)# exit
hostname(config-username)# exit
hostname#
```

ステップ 3　グローバル コンフィギュレーション モードで、sales という名前のクライアントレス SSL VPN セッションのトンネルグループを作成します。

```
hostname# tunnel-group sales type webvpn
hostname(config-tunnel-webvpn)#
```

ステップ 4　この接続プロファイルに対して salesgui カスタマイゼーションを使用することを指定します。

```
hostname# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)# customization salesgui
```

ステップ 5　ASA にログインするためにユーザがブラウザに入力するアドレスに対するグループ URL を設定します。たとえば、ASA に IP アドレス 192.168.3.3 が設定されている場合は、グループ URL を https://192.168.3.3 に設定します。

```
hostname(config-tunnel-webvpn)# group-url https://192.168.3.3.
hostname(config-tunnel-webvpn)#
```

ログインを成功させるためにポート番号が必要な場合は、コロンに続けてポート番号を指定します。ASA は、この URL を sales 接続プロファイルにマッピングし、ユーザが https://192.168.3.3 にログインしたときに表示されるログイン画面に salesgui カスタマイゼーション プロファイルを適用します。

パスワード管理用の Microsoft Active Directory の設定

（注）　認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

- Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

詳細については、一般的な操作のコンフィギュレーション ガイドの“Configuring Authorization with LDAP for VPN” section on page 32-18 を参照してください。

Microsoft Active Directory でパスワード管理を使用するには、一定の Active Directory パラメータを設定し、ASA でパスワード管理を設定する必要があります。この項では、さまざまなパスワード管理アクションに関連する Active Directory の設定について説明します。これらの説明は、ASA でのパスワード管理がイネーブルになっていて、対応するパスワード管理属性が設定されていることを前提としています。この項の特定の手順では、Windows 2000 における Active Directory の用語に言及し、次の項目を取り上げます。

- 「次回ログイン時にパスワードの変更をユーザに強制するための Active Directory の使用」（P.4-30）。
- 「Active Directory を使用したパスワードの最大有効日数の指定」（P.4-32）。
- 「Active Directory を使用した Account Disabled AAA インジケータの上書き」（P.4-33）
- 「Active Directory を使用したパスワードの複雑性の強制」（P.4-35）。

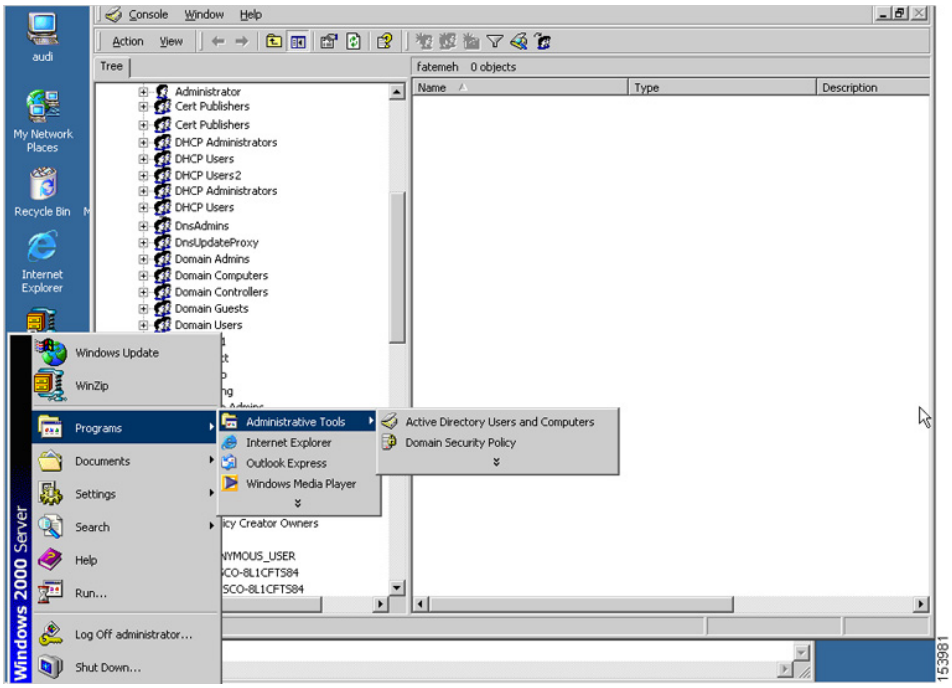
この項では、認証に LDAP ディレクトリ サーバを使用していることを前提としています。

次回ログイン時にパスワードの変更をユーザに強制するための Active Directory の使用

次回ログイン時にユーザ パスワードの変更をユーザに強制するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを指定して、Active Directory で次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] を選択します（図 4-1）。

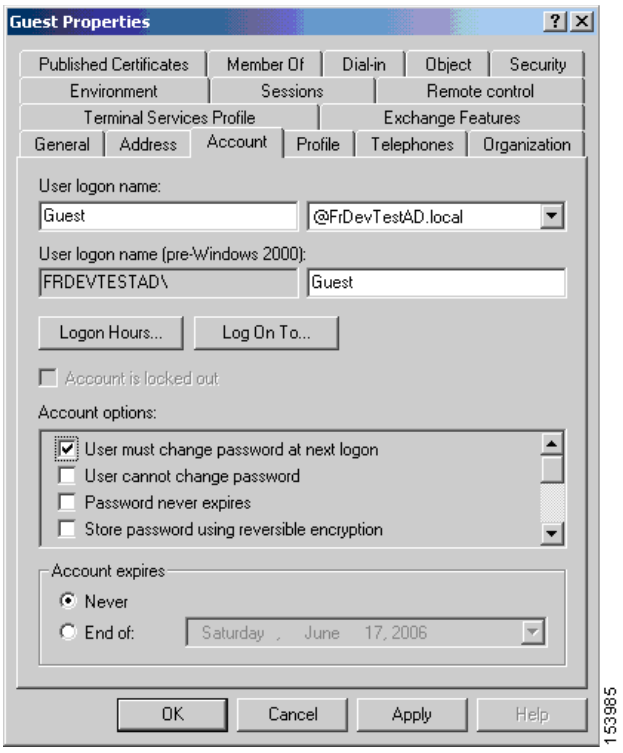
図 4-1　Active Directory : [Administrative Tools] メニュー



ステップ 2　右クリックして、[Username] > [Properties] > [Account] を選択します。

ステップ 3　[User must change password at next logon] チェックボックスをオンにします（図 4-2）。

図 4-2　Active Directory：ログイン時のパスワード変更要求



このユーザが次回ログインするときに、ASA が「New password required.Password change required.You must enter a new password with a minimum length *n* to continue.」というプロンプトを表示します。[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] > [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択し、Active Directory コンフィギュレーションの一部として、パスワードの最小の長さ *n* を設定できます。[Minimum password length] パスワードの最小の長さを選択します。

Active Directory を使用したパスワードの最大有効日数の指定

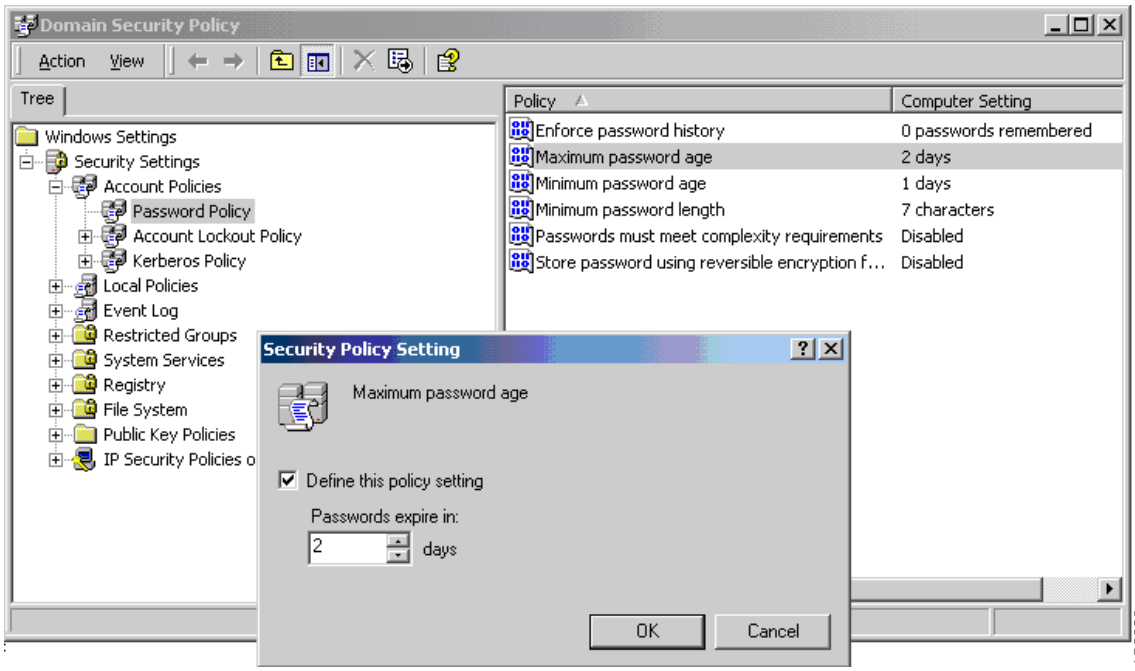
セキュリティを強化するために、一定の日数経過後パスワードが期限切れになるように指定できます。ユーザ パスワードの最大有効日数を指定するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを指定し、Active Directory で次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] > [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。

ステップ 2　[Maximum password age] をダブルクリックします。[Security Policy Setting] ダイアログボックスが表示されます。

ステップ 3　[Define this policy setting] チェックボックスをオンにして、許可する [Maximum password age] を日単位で指定します。

図 4-3　Active Directory：パスワードの最大有効日数



（注）　以前、パスワードの有効日数の設定機能を実行するためにトンネルグループ リモートアクセス コンフィギュレーションの一部として設定されていた **radius-with-expiry** コマンドは非推奨になっています。このコマンドは、トンネルグループ一般属性モードで入力される **password-management** コマンドに置き換えられます。

Active Directory を使用した Account Disabled AAA インジケータの上書き

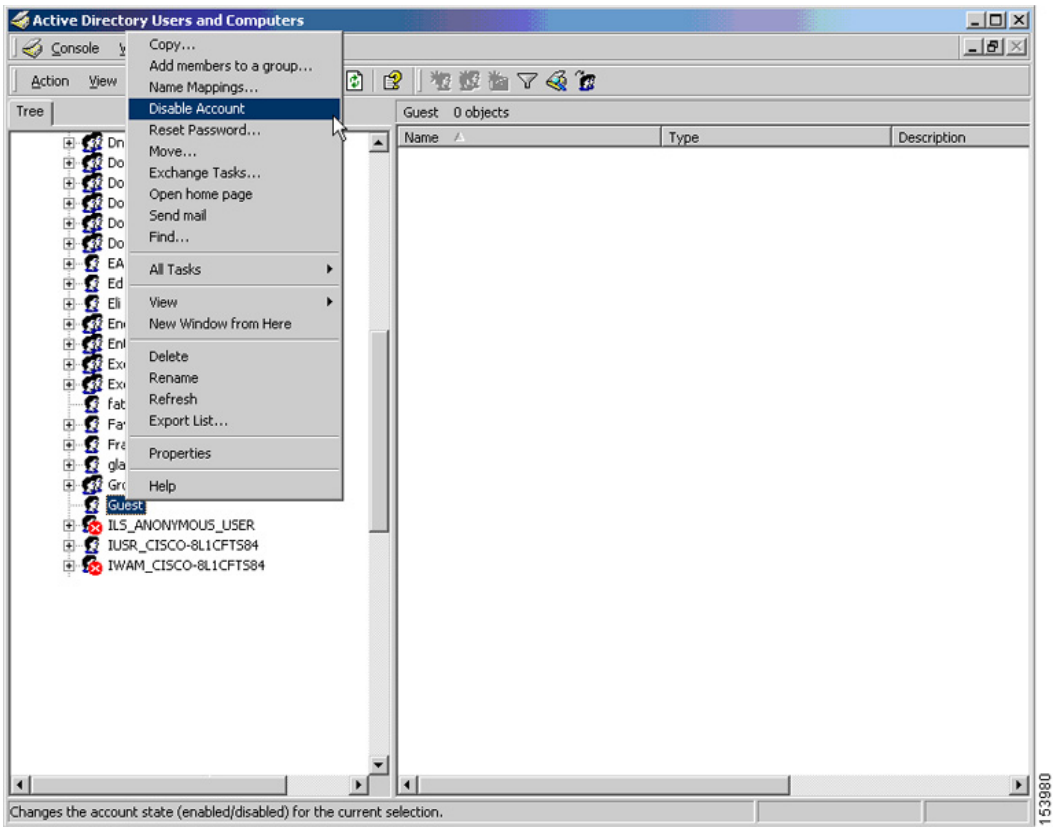
AAA サーバからの account-disabled 表示を上書きするには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **override-account-disable** コマンドを使用し、Active Directory で次の手順を実行します。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] を選択します。

ステップ 2　[Username] > [Properties] > [Account] を右クリックして、メニューから [Disable Account] を選択します。

図 4-4　Active Directory：アカウント無効の上書き



AAA サーバを介して account-disabled インジケータが表示されていても、ユーザは正常にログインできます。

Active Directory を使用した最小パスワード長の強制

パスワードの最小長を強制するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを指定し、Active Directory で次の手順を実行します。

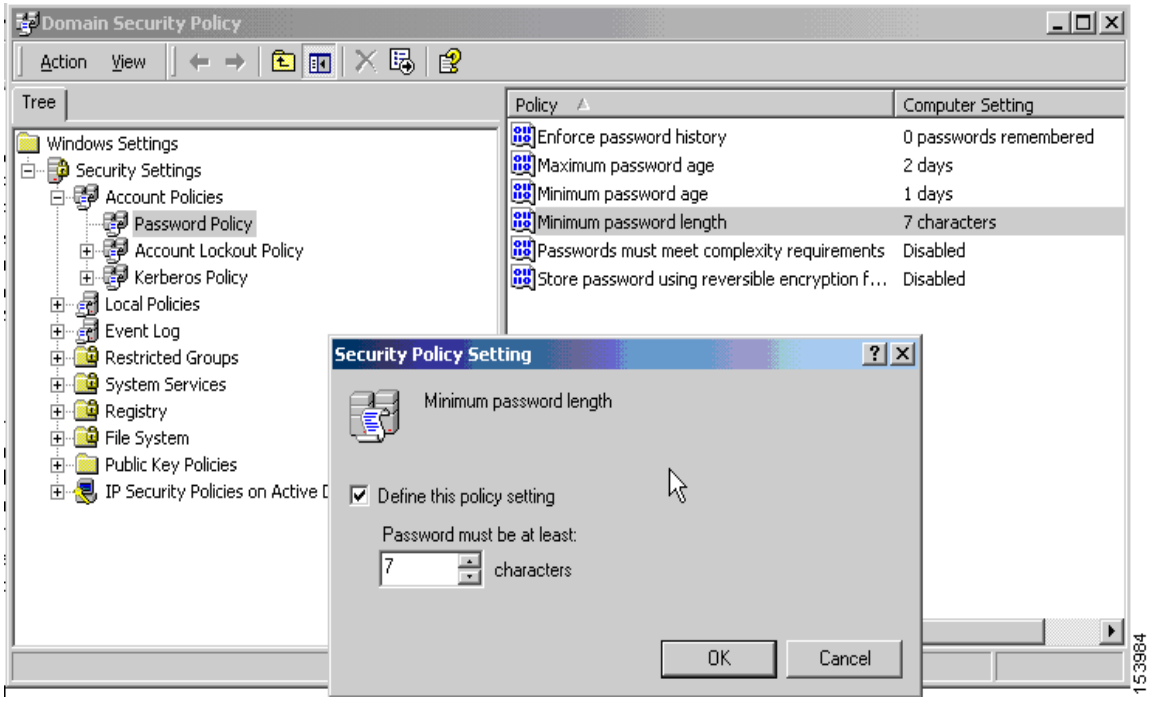
ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] を選択します。

ステップ 2　[Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。

ステップ 3　[Minimum Password Length] をダブルクリックします。[Security Policy Setting] ダイアログボックスが表示されます。

ステップ 4　[Define this policy setting] チェックボックスをオンにして、パスワードに含める必要がある最小文字数を指定します。

図 4-5　Active Directory：最小パスワード長



Active Directory を使用したパスワードの複雑性の強制

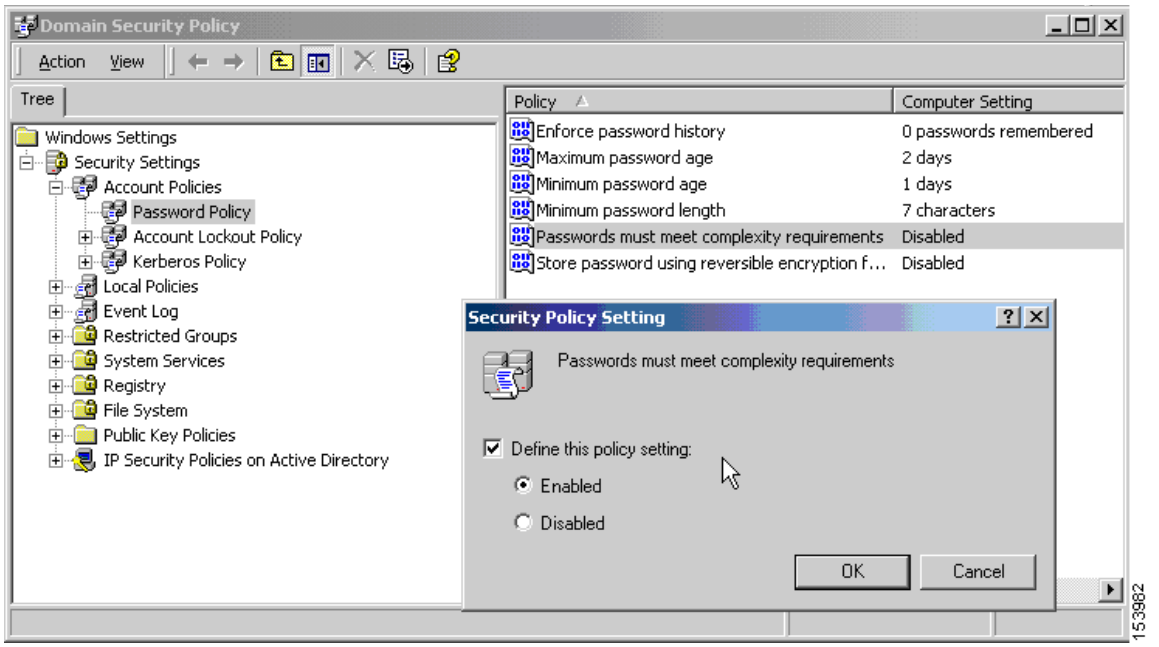
複雑なパスワード、たとえば、大文字と小文字、数字、および特殊文字を含むパスワードを要求するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを入力し、Active Directory で次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] を選択します。[Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。

ステップ 2　[Password must meet complexity requirements] をダブルクリックして、[Security Policy Setting] ダイアログボックスを開きます。

ステップ 3　[Define this policy setting] チェックボックスをオンにして、[Enable] を選択します。

図 4-6　Active Directory：パスワードの複雑性の強制



パスワードの複雑性の強制は、ユーザがパスワードを変更するときにだけ有効になります。たとえば、次回ログイン時にパスワード変更を強制する、または *n* 日後にパスワードが期限切れになるように設定した場合です。ログイン時に、新しいパスワードの入力を求めるプロンプトが表示され、システムは複雑なパスワードだけを受け入れます。

AnyConnect クライアントをサポートする RADIUS/SDI メッセージの接続プロファイルの設定

この項では、RSA SecureID ソフトウェア トークンを使用する AnyConnect VPN クライアントが、SDI サーバにプロキシする RADIUS サーバ経由でクライアントに配信されるユーザ プロンプトに正しく応答できるようにする手順について説明します。ここでは、次の内容について説明します。

- AnyConnect クライアントと RADIUS/SDI サーバのインタラクション
- RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

（注）　二重認証機能を設定した場合、SDI 認証はプライマリ認証サーバでだけサポートされます。

AnyConnect クライアントと RADIUS/SDI サーバのインタラクション

リモート ユーザが AnyConnect VPN クライアントで ASA に接続し、RSA SecurID トークンを使用して認証を試みると、ASA は RADIUS サーバと通信を行い、次に、RADIUS サーバは認証について SDI サーバと通信を行います。

認証の間に、RADIUS サーバは ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。メッセージ テキストは、ASA が SDI サーバと直接通信している場合と、RADIUS プロキシ経由で通信している場合とでは異なります。そのため、AnyConnect クライアントにネイティブ SDI サーバとして認識させるために、ASA は RADIUS サーバからのメッセージを解釈する必要があります。

また、SDI メッセージは SDI サーバで設定可能であるため、ASA のメッセージ テキストの全体または一部が、SDI サーバのメッセージ テキストと一致する必要があります。一致しない場合、リモート クライアント ユーザに表示されるプロンプトは、認証中に必要とされるアクションに対して適切でない場合があります。そのため、AnyConnect クライアントが応答できずに、認証が失敗する可能性があります。

「RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定」（P.4-37）では、クライアントと SDI サーバ間の認証を確実に成功させるように ASA を設定する方法について説明します。

RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

SDI 固有の RADIUS 応答メッセージを解釈し、AnyConnect ユーザに適切なアクションを求めるプロンプトを表示するように ASA を設定するには、次の手順を実行します。

ステップ 1　トンネルグループ webvpn コンフィギュレーション モードで **proxy-auth sdi** コマンドを使用して、SDI サーバとの直接通信をシミュレートする方法で、RADIUS 応答メッセージを転送するための接続プロファイル（トンネルグループ）を設定します。SDI サーバに認証されるユーザは、この接続プロファイルを介して接続する必要があります。

たとえば、次のように入力します。

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

ステップ 2　トンネルグループ webvpn コンフィギュレーション モードで **proxy-auth_map sdi** コマンドを使用して、RADIUS サーバによって送信されるメッセージ テキストと全体または一部が一致する RADIUS 応答メッセージ テキストを ASA で設定します。

ASA が使用するデフォルトのメッセージ テキストは、Cisco Secure Access Control Server（ACS）で使用されるデフォルトのメッセージ テキストです。Cisco Secure ACS を使用していて、デフォルトのメッセージ テキストを使用している場合、ASA でメッセージ テキストを設定する必要はありません。それ以外の場合は、**proxy-auth_map sdi** コマンドを使用して、メッセージ テキストが一致するようにします。

表 4-3 は、メッセージ コード、デフォルトの RADIUS 応答メッセージ テキスト、および各メッセージの機能を示しています。セキュリティ アプライアンスは、テーブルに表示される順番に文字列を検索するため、メッセージ テキストに使用する文字列は別の文字列のサブセットではないようにする必要があります。

たとえば、「new PIN」が new-pin-sup と next-ccode-and-reauth の両方に対するデフォルトのメッセージ テキストのサブセットだとします。new-pin-sup を「new PIN」として設定した場合、セキュリティ アプライアンスは RADIUS サーバから「new PIN with the next card code」を受信すると、next-ccode-and-reauth コードではなく new-pin-sup コードとテキストを一致させます。

表 4-3　SDI 操作コード、デフォルトのメッセージ テキスト、およびメッセージの機能

メッセージ コード	デフォルトの RADIUS 応答メッセージ テキスト	機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。
new-pin-reenter	Reenter PIN:	ユーザが提供した PIN の確認のために ASA が内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。
next-ccode-and-reauth	new PIN with the next card code	PIN 操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	ユーザがシステム生成の PIN に対する準備ができていることを示すために ASA が内部的に使用します。

次の例では、aaa-server-host モードに入り、RADIUS 応答メッセージ new-pin-sup のテキストを変更します。

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup "This is your new PIN"
```

グループ ポリシー

この項では、グループ ポリシーとその設定方法について説明します。説明する項目は次のとおりです。

- 「デフォルトのグループ ポリシー」（P.4-39）
- 「グループ ポリシーの設定」（P.4-44）

グループ ポリシーは、IPSec 接続用のユーザ関連の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の RADIUS サーバに保存されます。接続プロファイルでは、トンネル確立後、ユーザ接続の条件を設定するグループ ポリシーが使用されます。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に属性セット全体を適用できるので、ユーザごとに各属性を個別に指定する必要がありません。

ユーザにグループ ポリシーを割り当てたり、特定のユーザのグループ ポリシーを変更したりするには、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。

ASA には、デフォルトのグループ ポリシーが含まれています。変更はできても削除はできないデフォルトのグループ ポリシーに加え、自分の環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

内部グループ ポリシーと外部グループ ポリシーを設定できます。内部グループは ASA の内部データベースで設定されます。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、次の属性があります。

- アイデンティティ
- サーバの定義
- 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 コンフィギュレーションの設定
- 接続の設定

デフォルトのグループ ポリシー

ASA では、デフォルトのグループ ポリシーが提供されます。このデフォルト グループ ポリシーは変更できますが、削除はできません。デフォルトのグループ ポリシーは、DfltGrpPolicy という名前で ASA に常に存在していますが、このデフォルトのグループ ポリシーは、ASA でそれを使用するように設定しない限り有効にはなりません。その他のグループ ポリシーを設定する場合、明示的に指定しない属性の値はデフォルトのグループ ポリシーから取得されます。デフォルトのグループ 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)#
```

デフォルトのグループ ポリシーを設定するには、次のコマンドを入力します。

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```

（注） デフォルトのグループ ポリシーは、常に内部（internal）です。コマンド構文は、hostname(config)# group-policy DfltGrpPolicy {internal | external} ですが、タイプを外部（external）に変更することはできません。

デフォルトのグループ ポリシーの任意の属性を変更する場合は、**group-policy attributes** コマンドを使用して属性モードに入り、その後、変更対象の属性を変更するためのコマンドを指定します。

```
hostname(config)# group-policy DfltGrpPolicy attributes
```

（注） 属性モードは内部グループ ポリシーにだけ適用されます。

ASA で提供されるデフォルトのグループ ポリシー DfltGrpPolicy は、次のとおりです。

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
```

```
dns-server value 10.10.10.1.1
dhcp-network-scope none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
ipv6-vpn-filter none
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp disable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain value cisco.com
split-dns none
split-tunnel-all-dns disable
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
client-bypass-protocol disable
gateway-fqdn none
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
msie-proxy pac-url none
msie-proxy lockdown enable
vlan none
nac-settings none
address-pools none
ipv6-address-pools none
smartcard-removal-disconnect enable
scep-forwarding-url none
client-firewall none
client-access-rule none
webvpn
 url-list none
 filter none
 homepage none
 html-content-filter none
 port-forward name Application Access
 port-forward disable
 http-proxy disable
 sso-server none
 anyconnect ssl dtls enable
 anyconnect mtu 1406
 anyconnect firewall-rule client-interface private none
 anyconnect firewall-rule client-interface public none
 anyconnect keep-installer installed
 anyconnect ssl keepalive 20
 anyconnect ssl rekey time none
```

```
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression lzs
  anyconnect modules none
  anyconnect profiles none
  anyconnect ask none
  customization none
  keep-alive-ignore 4
  http-comp gzip
  download-max-size 2147483647
  upload-max-size 2147483647
  post-max-size 2147483647
  user-storage none
  storage-objects value cookies,credentials
  storage-key none
  hidden-shares none
  smart-tunnel disable
  activex-relay enable
  unix-auth-uid 65534
  unix-auth-gid 65534
  file-entry enable
  file-browsing enable
  url-entry enable
  deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features. Contact your IT administrator for more information
  smart-tunnel auto-signon disable
  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable
  smart-tunnel tunnel-policy tunnelall
  always-on-vpn profile-setting
```

デフォルト グループ ポリシーは変更可能です。また、環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

グループ ポリシー

この項では、グループ ポリシーとその設定方法について説明します。説明する項目は次のとおりです。

- 「デフォルトのグループ ポリシー」（P.4-39）
- 「グループ ポリシーの設定」（P.4-44）

グループ ポリシーは、IPSec 接続用のユーザ関連の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の RADIUS サーバに保存されます。接続プロファイルでは、トンネル確立後、ユーザ接続の条件を設定するグループ ポリシーが使用されます。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に属性セット全体を適用できるので、ユーザごとに各属性を個別に指定する必要がありません。

ユーザにグループ ポリシーを割り当てたり、特定のユーザのグループ ポリシーを変更したりするには、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。

ASA には、デフォルトのグループ ポリシーが含まれています。変更はできても削除はできないデフォルトのグループ ポリシーに加え、自分の環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

内部グループ ポリシーと外部グループ ポリシーを設定できます。内部グループは ASA の内部データベースで設定されます。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、次の属性があります。

- アイデンティティ
- サーバの定義
- 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 コンフィギュレーションの設定
- 接続の設定

デフォルトのグループ ポリシー

ASA では、デフォルトのグループ ポリシーが提供されます。このデフォルト グループ ポリシーは変更できますが、削除はできません。デフォルトのグループ ポリシーは、DfltGrpPolicy という名前で ASA に常に存在していますが、このデフォルトのグループ ポリシーは、ASA でそれを使用するように設定しない限り有効にはなりません。その他のグループ ポリシーを設定する場合、明示的に指定しない属性の値はデフォルトのグループ ポリシーから取得されます。デフォルトのグループ 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)#
```

デフォルトのグループ ポリシーを設定するには、次のコマンドを入力します。

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```

（注） デフォルトのグループ ポリシーは、常に内部（internal）です。コマンド構文は、hostname(config)# group-policy DfltGrpPolicy {internal | external} ですが、タイプを外部（external）に変更することはできません。

デフォルトのグループ ポリシーの任意の属性を変更する場合は、**group-policy attributes** コマンドを使用して属性モードに入り、その後、変更対象の属性を変更するためのコマンドを指定します。

```
hostname(config)# group-policy DfltGrpPolicy attributes
```

（注） 属性モードは内部グループ ポリシーにだけ適用されます。

ASA で提供されるデフォルトのグループ ポリシー DfltGrpPolicy は、次のとおりです。

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
```

```
dns-server value 10.10.10.1.1
dhcp-network-scope none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
ipv6-vpn-filter none
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp disable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain value cisco.com
split-dns none
split-tunnel-all-dns disable
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
client-bypass-protocol disable
gateway-fqdn none
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
msie-proxy pac-url none
msie-proxy lockdown enable
vlan none
nac-settings none
address-pools none
ipv6-address-pools none
smartcard-removal-disconnect enable
scep-forwarding-url none
client-firewall none
client-access-rule none
webvpn
 url-list none
 filter none
 homepage none
 html-content-filter none
 port-forward name Application Access
 port-forward disable
 http-proxy disable
 sso-server none
 anyconnect ssl dtls enable
 anyconnect mtu 1406
 anyconnect firewall-rule client-interface private none
 anyconnect firewall-rule client-interface public none
 anyconnect keep-installer installed
 anyconnect ssl keepalive 20
 anyconnect ssl rekey time none
```

```
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression lzs
  anyconnect modules none
  anyconnect profiles none
  anyconnect ask none
  customization none
  keep-alive-ignore 4
  http-comp gzip
  download-max-size 2147483647
  upload-max-size 2147483647
  post-max-size 2147483647
  user-storage none
  storage-objects value cookies,credentials
  storage-key none
  hidden-shares none
  smart-tunnel disable
  activex-relay enable
  unix-auth-uid 65534
  unix-auth-gid 65534
  file-entry enable
  file-browsing enable
  url-entry enable
  deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features. Contact your IT administrator for more information
  smart-tunnel auto-signon disable
  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable
  smart-tunnel tunnel-policy tunnelall
  always-on-vpn profile-setting
```

デフォルト グループ ポリシーは変更可能です。また、環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

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。どちらの場合も、パラメータが明示的に指定されていなければ、そのグループはデフォルト グループ ポリシーの値を使用します。

設定タスクは、シングル コンテキスト モードまたはマルチ コンテキスト モードの両方で実行できます。

（注） マルチ コンテキスト モードは IKEv1 および IKEv2 サイト間にのみ適用され、IKEv1 IPSec の AnyConnect、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、または cTCP には適用されません。

外部グループ ポリシーの設定

外部グループ ポリシーの属性値には、指定する外部サーバの値が取得されます。外部グループ ポリシーの場合は、ASA が属性のクエリーを実行できる AAA サーバ グループを特定し、その外部 AAA サーバ グループから属性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て、外部グループ ポリシー属性が、認証する予定のユーザと同じ RADIUS サーバにある場合、それらの間で名前が重複しないようにする必要があります。

（注）　ASA の外部グループ名は、RADIUS サーバのユーザ名を参照しています。つまり、ASA に外部グループ X を設定する場合、RADIUS サーバはクエリーをユーザ X に対する認証要求と見なします。そのため、外部グループは実際には、ASA にとって特別な意味を持つ、RADIUS サーバ上のユーザ アカウントということになります。外部グループ属性が認証する予定のユーザと同じ RADIUS サーバに存在する場合、それらの間で名前を重複させることはできません。

ASA は、外部 LDAP または RADIUS サーバでのユーザ認証をサポートしています。外部サーバを使用するように ASA を設定する前に、正しい ASA 認証属性でサーバを設定し、それらの属性のサブセットから個々のユーザに対する個別の許可を割り当てる必要があります。外部サーバを設定するには、付録 14「許可および認証用の外部サーバの設定」の説明に従ってください。

外部グループ ポリシーを設定するには、次の手順を実行して、server-group 名と password とともにグループ ポリシーの名前とタイプを指定します。

```
hostname(config)# group-policy group_policy_name type server-group server_group_name
password server_password
hostname(config)#
```

（注）　外部グループ ポリシーの場合、サポートされる AAA サーバ タイプは RADIUS だけです。

たとえば、次のコマンドは、ExtGroup という名前の外部グループ ポリシーが作成します。このグループ ポリシーの属性は、ExtRAD という名前の外部 RADIUS サーバから取得され、属性を取得するときに使用されるパスワードが newpassword に指定されます。

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

（注）　付録 14「許可および認証用の外部サーバの設定」に説明されているように、いくつかのベンダー固有属性（VSA）を設定できます。RADIUS サーバが Class 属性（#25）を返すように設定されている場合、ASA は、グループ名の認証にその属性を使用します。RADIUS サーバでは、属性は次の形式で指定する必要があります。OU=*groupname*。ここで、*groupname* は、ASA で設定されたグループ名と同一です。例、OU=Finance。

内部グループ ポリシーの作成

内部グループ ポリシーを設定するには、コンフィギュレーション モードを開始します。group-policy コマンドを使用して、グループ ポリシーの名前と **internal** タイプを指定します。

```
hostname(config)# group-policy group_policy_name internal
hostname(config)#
```

たとえば、次のコマンドは GroupPolicy1 という名前の内部グループ ポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

（注）　いったん作成したグループ ポリシーの名前は変更できません。

キーワード **from** を追加して既存のポリシーの名前を指定することにより、既存のグループ ポリシーの値をコピーして、内部グループ ポリシーの属性を設定できます。

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
```

```
hostname(config-group-policy)#
```

たとえば、次のコマンドは GroupPolicy1 の属性をコピーして、GroupPolicy2 という名前の内部グループ ポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy2 internal from GroupPolicy1
hostname(config-group-policy)#
```

一般的な内部グループ ポリシー属性の設定

グループ ポリシー名

グループ ポリシーの名前は内部グループ ポリシーの作成時に選択されています。いったん作成されたグループ ポリシーの名前は変更できません。詳細については、「内部グループ ポリシーの作成」（P.4-45）を参照してください。

グループ ポリシーのバナー メッセージの設定

表示するバナーまたは初期メッセージ（ある場合）を指定します。デフォルトでは、バナーは表示されません。指定したメッセージは、リモート クライアントが接続したときに、そのクライアントに表示されます。バナーを指定するには、グループ ポリシー コンフィギュレーション モードで **banner** コマンドを入力します。バナー テキストの長さは 510 文字までです。復帰改行を挿入する場合は、「\n」シーケンスを入力します。

（注）　バナー内の復帰改行は、2 文字として数えられます。

バナーを削除するには、このコマンドの **no** 形式を入力します。このコマンドの **no** 形式を使用すると、グループ ポリシーのすべてのバナーが削除されることに注意してください。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、次のように、バナー文字列の値を指定する代わりに **none** キーワードを入力します。

```
hostname(config-group-policy)# banner {value banner_string | none}
```

次の例は、FirstGroup という名前のグループ ポリシーにバナーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems ASA 9.0.
```

リモート アクセス接続のアドレス プールの指定

リモート アクセス クライアントが ASA に接続する場合、ASA は、接続に指定されたグループ ポリシーに基づいて IPv4 または IPv6 アドレスをクライアントに割り当てることができます。

ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

内部グループ ポリシーへの IPv4 アドレス プールの割り当て

前提条件

IPv4 アドレス プールを作成します。第 5 章「VPN の IP アドレスの設定」を参照してください。

手順の詳細

	コマンド	目的

ステップ 1	`group-policy value attributes`
	
	例：
	`hostname> en`
	`hostname# config t`
	`hostname(config)# group-policy FirstGroup attributes`
	`hostname(config-group-policy)#`
		グループ ポリシー コンフィギュレーション モードを開始します。

ステップ 2	**address-pools value** *pool-name1 pool-name2 pool-name6*
	
	例：
	`asa4(config-group-policy)# address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3`
	`asa4(config-group-policy)#`
		ipv4 pool1、ipv4 pool2、および ipv4pool3 という名前のアドレス プールを FirstGroup グループ ポリシーに割り当てます。
		グループ ポリシーには、最大 6 個のアドレス プールを指定できます。

ステップ 3	（任意）
	no address-pools value pool-name1 pool-name2 pool-name6
	
	例：
	`hostname(config-group-policy)# no address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3`
	`hostname(config-group-policy)#`
		グループ ポリシー設定からアドレス プールを削除し、アドレス プール設定を戻して DefltGroupPolicy などの他のソースからのアドレス プール情報を継承するには、**no address-pools value pool-name** コマンドを使用します。

ステップ 4	（任意）
	address-pools none
	
	例：
	`hostname(config-group-policy)# address-pools none`
	`hostname(config-group-policy)#`
		address-pools none コマンドは、ポリシーの別のソース（DefltGrpPolicy など）からこの属性を継承することをディセーブルにします。

ステップ 5	（任意）
	no address-pools none
	
	例：
	`hostname(config-group-policy)# no address-pools none`
	`hostname(config-group-policy)#`
		no address pools none コマンドは、**address-pools none** コマンドをグループ ポリシーから削除して、デフォルト値（継承の許可）に戻します。

内部グループ ポリシーへの IPv6 アドレス プールの割り当て

前提条件

IPv6 アドレス プールを作成します。第 5 章「VPN の IP アドレスの設定」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	group-policy *value* attributes **例：** hostname**> en** hostname# **config t** hostname(config)# **group-policy FirstGroup attributes** hostname(config-group-policy)#	グループ ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**ipv6-address-pools value** *pool-name1 pool-name2 pool-name6* **例：** hostname(config-group-policy)# **ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3** hostname(config-group-policy)#	ipv6-pool という名前のアドレス プールを FirstGroup グループ ポリシーに割り当てます。 グループ ポリシーには、最大 6 個の IPv6 アドレス プールを割り当てることができます。 この例では、ipv6-pool1、ipv6-pool2、および ipv6-pool3 が FirstGroup グループ ポリシーに割り当てられています。
ステップ 3	（任意） **no ipv6-address-pools value pool-name1 pool-name2 pool-name6** **例：** hostname(config-group-policy)# **no ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3** hostname(config-group-policy)#	グループ ポリシー設定からアドレス プールを削除し、アドレス プール設定を戻して DfltGroupPolicy などの他のソースからのアドレス プール情報を継承するには、**no ipv6-address-pools value pool-name** コマンドを使用します。
ステップ 4	（任意） **ipv6-address-pools none** **例：** hostname(config-group-policy)# **ipv6-address-pools none** hostname(config-group-policy)#	**ipv6-**address-pools none コマンドは、この属性が DfltGrpPolicy など他のポリシーから継承されないようにします。
ステップ 5	（任意） **no ipv6-address-pools none** **例：** hostname(config-group-policy)# **no ipv6-address-pools none** hostname(config-group-policy)#	**no ipv6-address pools none** コマンドは、**ipv6-address-pools none** コマンドをグループ ポリシーから削除して、デフォルト値（継承の許可）に戻します。

グループ ポリシーのトンネリング プロトコルの指定

グループ ポリシー コンフィギュレーション モードで **vpn-tunnel-protocol {ikev1 | ikev2 | l2tp-ipsec | ssl-client | ssl-clientless}** コマンドを入力して、このグループ ポリシーの VPN トンネル タイプを指定します。

デフォルト値は、デフォルト グループ ポリシーの属性を継承することです。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

このコマンドのパラメータの値は、次のとおりです。

- **ikev1**：2 つのピア（Cisco VPN Client または別のセキュア ゲートウェイ）間の IPsec IKEv1 トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **ikev2**：2 つのピア（AnyConnect Secure Mobility Client または別のセキュア ゲートウェイ）間の IPsec IKEv2 トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **l2tp-ipsec**：L2TP 接続用の IPsec トンネルをネゴシエートします。
- **ssl-client**：AnyConnect Secure Mobility Client で TLS または DTLS を使用して、SSL トンネルをネゴシエートします。
- **ssl-clientless**：HTTPS 対応の Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは必要ありません。

このコマンドを入力して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

次の例は、FirstGroup という名前のグループ ポリシーに IPsec IKEv1 トンネリング モードを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

リモート アクセスの VLAN の指定またはグループ ポリシーへの統合アクセス コントロール ルール

フィルタは、ASA を経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。グループ ポリシーの IPv4 または IPv6 統合アクセス コントロール リストを指定するか、またはデフォルト グループ ポリシーで指定された ACL を継承するようにできます。新しい統合 ACL を設定して、グループで使用するには、一般的な操作のコンフィギュレーション ガイドの“Adding ACLs and ACEs” section on page 22-2を参照してください。

次のオプションのいずれかを選択して、リモート アクセス用の出力 VLAN（「VLAN マッピング」とも呼ばれる）、またはトラフィックをフィルタリングする ACL を指定します。

- グループ ポリシー コンフィギュレーション モードで次のコマンドを入力して、このグループ ポリシーまたはこのグループ ポリシーを継承するグループ ポリシーに割り当てられているリモートアクセス VPN セッション用の出力 VLAN を指定します。

  ```
  hostname(config-group-policy)# [no] vlan {vlan_id |none}
  ```

  no vlan は、グループ ポリシーから *vlan_id* を削除します。グループ ポリシーは、デフォルトのグループ ポリシーから vlan 値を継承します。

  none は、グループ ポリシーから *vlan_id* を削除し、このグループ ポリシーに対する VLAN マッピングをディセーブルにします。グループ ポリシーは、デフォルトのグループ ポリシーから vlan 値を継承しません。

  vlan_id は、このグループ ポリシーを使用するリモート アクセス VPN セッションに割り当てる VLAN の番号（10 進表記）です。VLAN は一般的な操作のコンフィギュレーション ガイドの“Configuring VLAN Subinterfaces and 802.1Q Trunking” section on page 10-31の説明に従い、この ASA に設定する必要があります。

（注） 出力 VLAN は、HTTP 接続では機能しますが、FTP と CIFS では機能しません。

- グループ ポリシー モードで **vpn-filter** コマンドを使用して、VPN セッションに適用するアクセス コントロール ルール（ACL）の名前を指定します vpn-filter コマンドを使用して、IPv4 または IPv6 ACL を指定できます。

（注） ipv6-vpn-filter コマンドは ASA 9.0 から非推奨になりました。IPv4 および IPv6 エントリの両方で統合フィルタを設定するには、「vpn-filter」CLI を使用する必要があります。この IPv6 フィルタは、「vpn-filter」によって指定されたアクセス リストに IPv6 エントリがない場合にのみ使用されます。

（注） この属性はユーザ名モードで設定することもできます。その場合、ユーザ名の下で設定された値がグループ ポリシーの値よりも優先されます。

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

ACL を設定して、このグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを入力して、これらの ACL を適用します。

vpn-filter none コマンドを入力して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、ACL 名を指定する代わりに、**none** キーワードを入力します。**none** キーワードは、ACL がないことを示します。このキーワードにより、ヌル値が設定され、ACL が拒否されます。

次に、FirstGroup という名前のグループ ポリシーの、acl_vpn という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

vpn-filter コマンドは、トンネルから出た後の、復号化後のトラフィックとトンネルに入る前の、暗号化前のトラフィックに適用されます。vpn-filter に使用される ACL を interface access-group にも使用することはできません。**vpn-filter** コマンドを、リモート アクセス VPN クライアント接続を制御するグループ ポリシーに適用する場合は、ACL の **src_ip** の位置のクライアント割り当て IP アドレスおよび ACL の **dest_ip** の位置のローカル ネットワークに対して ACL を設定する必要があります。

vpn-filter コマンドを、LAN-to-LAN VPN 接続を制御するグループ ポリシーに適用する場合は、ACL の **src_ip** の位置のリモート ネットワークおよび ACL の **dest_ip** の位置のローカル ネットワークに対して ACL を設定する必要があります。

vpn-filter 機能で使用するために ACL を設定する場合は、注意する必要があります。ACL は、復号化後のトラフィックに対して構築されていることに留意してください。ただし、ACL は反対方向のトラフィックに対しても適用されます。トンネル宛ての、暗号化前のこのトラフィックについては、ACL は **src_ip** の位置と **dest_ip** の位置を入れ替えたものに対して構築されています。

次の例では、vpn-filter をリモート アクセス VPN クライアントと共に使用します。
この例では、クライアント割り当て IP アドレスを 10.10.10.1/24、ローカル ネットワークを 192.168.1.0/24 としています。

次の ACE によって、リモート アクセス VPN クライアントがローカル ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

次の ACE によって、ローカル ネットワークがリモート アクセス クライアントに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq
23 192.168.1.0 255.255.255.0
```

（注）　ACE の **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23** によって、ローカル ネットワークは、送信元ポート 23 を使用している場合に任意の TCP ポートでのリモート アクセス クライアントへの接続開始が許可されます。ACE の **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0** によって、リモート アクセス クライアントは、送信元ポート 23 を使用している場合に任意の TCP ポートでのローカル ネットワークへの接続開始が許可されます。

次の例では、vpn-filter を LAN-to-LAN VPN 接続と共に使用します。この例では、リモート ネットワークを 10.0.0.0/24、ローカル ネットワークを 192.168.1.0/24 としています。
次の ACE によって、リモート ネットワークがローカル ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0
192.168.1.0 255.255.255.0 eq 23
```

次の ACE によって、ローカル ネットワークがリモート ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```

（注）　ACE の **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23** によって、ローカル ネットワークは、送信元ポート 23 を使用している場合に任意の TCP ポートでのリモート ネットワークへの接続開始が許可されます。ACE の **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0** によって、リモート ネットワークは、送信元ポート 23 を使用している場合に任意の TCP ポートでのローカル ネットワークへの接続開始が許可されます。

グループ ポリシーに対する NAC ポリシーの指定

このコマンドでは、このグループ ポリシーに適用するネットワーク アドミッション コントロール ポリシーの名前を選択します。オプションの NAC ポリシーを各グループ ポリシーに割り当てることができます。デフォルト値は --None-- です。

前提条件

NAC ポリシーを作成します。「ネットワーク アドミッション コントロールの設定」（P.7-1）を参照してください。

手順の詳細

	コマンド	目的

ステップ 1	`group-policy value attributes`
	
	例：
	`hostname> en`
	`hostname# config t`
	`hostname(config)# group-policy FirstGroup attributes`
	`hostname(config-group-policy)#`
		グループ ポリシー コンフィギュレーション モードを開始します。

ステップ 2	**nac-settings value** *nac-policy-name* **例：** hostname(config-group-policy)# **nac-settings value nac-policy-1** hostname(config-group-policy)#	nac-policy-1 という名前の NAC ポリシーを FirstGroup グループ ポリシーに割り当てます。

グループ ポリシーの VPN アクセス時間の指定

前提条件

時間の範囲を作成します。一般的な操作のコンフィギュレーション ガイドの“Configuring Time Ranges” section on page 17-18を参照してください。

手順の詳細

	コマンド	目的

ステップ 1	`group-policy value attributes`
	
	例：
	`hostname> en`
	`hostname# config t`
	`hostname(config)# group-policy FirstGroup attributes`
	`hostname(config-group-policy)#`
		グループ ポリシー コンフィギュレーション モードを開始します。

ステップ 2	`hostname(config-group-policy)#` **vpn-access-hours value** {*time-range-name* **| none**} **例：** `hostname(config-group-policy)#` **vpn-access-hours value business-hours** hostname(config-group-policy)#	グループ ポリシー コンフィギュレーション モードで **vpn-access-hours** コマンドを使用して、グループ ポリシーと設定済みの time-range ポリシーを関連付けることによって、VPN アクセス時間を設定できます。 このコマンドは、business-hours という名前の VPN アクセス時間範囲を FirstGroup という名前のグループ ポリシーに割り当てます。 グループ ポリシーは、デフォルトまたは指定されたグループ ポリシーの time-range の値を継承することができます。この継承が発生しないようにするには、このコマンドで time-range の名前ではなく **none** キーワードを入力します。このキーワードにより、VPN アクセス時間がヌル値に設定され、time-range ポリシーは許可されなくなります。

グループ ポリシーの同時 VPN ログインの指定

グループ ポリシー コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用して、任意のユーザに許可される同時ログイン数を指定します。

```
hostname(config-group-policy)# vpn-simultaneous-logins integer
```

デフォルト値は 3 です。値の範囲は 0 ～ 2147483647 の整数です。グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。次に、FirstGroup という名前のグループ ポリシーに対して最大 4 つの同時ログインを許可する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
hostname(config-group-policy)#
```

（注） 同時ログイン数の最大制限は非常に大きい値ですが、複数の同時ログインを許可すると、セキュリティが侵害されたり、パフォーマンスが低下したりすることがあります。

失効した AnyConnect、IPsec クライアント、またはクライアントレス セッション（異常終了したセッション）は、同じユーザ名で「新しい」セッションが確立されても、セッション データベースに残る場合があります。

vpn-simultaneous-logins の値が 1 の場合は、異常終了後に同じユーザが再度ログインすると、失効したセッションはデータベースから削除され、新しいセッションが確立されます。ただし、既存のセッションがまだアクティブな接続である場合は、同じユーザが別の PC などから再度ログインすると、最初のセッションがログオフし、データベースから削除されて、新しいセッションが確立されます。

同時ログイン数が 1 より大きい値の場合、その最大数に達した状態で再度ログインしようとすると、最もアイドル時間の長いセッションがログオフします。現在のすべてのセッションが同じくらい長い間アイドル状態の場合は、最も古いセッションがログオフします。このアクションにより、セッションが解放されて新しいログインが可能になります。

特定の接続プロファイルへのアクセスの制限

グループ ポリシー コンフィギュレーション モードで **group-lock** コマンドを使用して、接続プロファイルを介してだけアクセスするようにリモート ユーザを制限するかどうかを指定します。

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

tunnel-grp-name 変数は、ASA がユーザの接続に関して要求する既存の接続プロファイルの名前を指定します。group-lock は、VPN クライアントで設定されたグループが、そのユーザが割り当てられている接続プロファイルと同じかどうかをチェックすることによって、ユーザを制限します。同一ではなかった場合、ASA はユーザによる接続を禁止します。グループ ロックを設定しなかった場合、ASA は、割り当てられているグループに関係なくユーザを認証します。グループのロックは、デフォルトではディセーブルになっています。

group-lock 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

group-lock をディセーブルにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。none キーワードにより、group-lock はヌル値に設定され、group-lock の制限が拒否されます。また、デフォルトまたは指定されたグループ ポリシーから group-lock の値が継承されなくなります。

グループ ポリシーの VPN の最大接続時間の指定

ステップ 1　グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用して、VPN 接続の最大時間を設定します。

```
hostname(config-group-policy)# vpn-session-timeout {minutes | none}
hostname(config-group-policy)#
```

最小時間は 1 分で、最大時間は 35791394 分です。デフォルト値はありません。この期間が終了すると、ASA は接続を終了します。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、分を指定する代わりに **none** キーワードを指定して、このコマンドを入力します。**none** キーワードを指定すると、無制限のセッション タイムアウト期間が許可されます。セッション タイムアウトにはヌル値が設定され、セッション タイムアウトが拒否されます。

次に、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

ステップ 2　**vpn-session-timeout alert-interval** {minutes | none} コマンドを使用して、セッション タイムアウトのアラート メッセージがユーザに表示される時間を設定します。このアラート メッセージは、VPN セッションが自動的に切断されるまでに何分あるかをユーザに伝えます。

次に、VPN セッションが切断される 20 分前にユーザに通知されるよう **vpn-session-timeout alert-interval** を設定する例を示します。1 ～ 30 分の範囲を指定できます。

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

none パラメータは、ユーザが通知を受信しないことを示します。

VPN セッション タイムアウト アラート間隔属性がデフォルト グループ ポリシーから継承されることを示すには、このコマンドの no 形式を使用します。

```
no vpn-session-timeout alert-interval
```

グループ ポリシーの VPN セッション アイドル タイムアウトの指定

ステップ 1　グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを入力して、ユーザ タイムアウト期間を設定します。

```
hostname(config-group-policy)# vpn-idle-timeout {minutes | none}
hostname(config-group-policy)#
```

AnyConnect（SSL IPsec/IKEv2）：次のコマンドで設定されたグローバル WebVPN default-idle-timeout 値（秒単位）を使用します。**hostname(config-webvpn)# default-idle-timeout**

WebVPN **default-idle-timeout** コマンドにおけるこの値の範囲は、60 ～ 86400 秒です。デフォルトのグローバル WebVPN アイドル タイムアウト（秒単位）は、1800 秒（30 分）です。

（注）　すべての AnyConnect 接続では、ASA によってゼロ以外のアイドル タイムアウト値が要求されます。

WebVPN ユーザの場合、**default-idle-timeout** 値は、vpn-idle-timeout none がグループ ポリシー/ユーザ名属性に設定されている場合にのみ有効です。

サイト間（IKEv1、IKEv2）および IKEv1 リモート アクセス：タイムアウトをディセーブルにし、無制限のアイドル期間を許可します。

次の例は、FirstGroup という名前のグループ ポリシーに 15 分の VPN アイドル タイムアウトを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

ステップ 2　**vpn-idle-timeout alert-interval {minutes | none}** コマンドを使用して、アイドルタイムアウトのアラート メッセージがユーザに表示される時間を設定します。このアラート メッセージは、VPN セッションが非アクティブ状態のため切断されるまでに何分あるかをユーザに伝えます。

次に、VPN セッションが非アクティブ状態のため切断される 20 分前にユーザに通知されるよう vpn-idle-timeout alert-interval を設定する例を示します。1 ～ 30 分の範囲を指定できます。

```
hostname(config-webvpn)# vpn-idle-timeout alert-interval 20
```

none パラメータは、ユーザが通知を受信しないことを示します。

VPN アイドル タイムアウト アラート間隔属性がデフォルト グループ ポリシーから継承されることを示すには、このコマンドの no 形式を使用します。

```
no vpn-idle-timeout alert-interval
```

グループ ポリシーの WINS サーバと DNS サーバの設定

プライマリおよびセカンダリの WINS サーバと DNS サーバを指定できます。それぞれのデフォルト値は none です。これらのサーバを指定するには、次の手順を実行します。

ステップ 1　プライマリとセカンダリの WINS サーバを指定します。

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

最初に指定する IP アドレスがプライマリ WINS サーバの IP アドレスです。2 番目（任意）の IP アドレスはセカンダリ WINS サーバの IP アドレスです。IP アドレスではなく **none** キーワードを指定すると、WINS サーバにヌル値が設定されます。この設定により、WINS サーバは許可されず、デフォルトまたは指定のグループ ポリシーから値が継承されなくなります。

wins-server コマンドを入力するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定してから WINS サーバ y.y.y.y を設定すると、2 番めのコマンドによって最初の設定が上書きされ、y.y.y.y が唯一の WINS サーバになります。サーバを複数設定する場合も同様です。設定済みのサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときに、すべての WINS サーバの IP アドレスを含めます。

次の例は、FirstGroup という名前のグループ ポリシーに、IP アドレスが 10.10.10.15 と 10.10.10.30 である WINS サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

ステップ 2　プライマリとセカンダリの DNS サーバを指定します。

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

最初に指定する IP アドレスがプライマリ DNS サーバの IP アドレスです。2 番目（任意）の IP アドレスはセカンダリ DNS サーバの IP アドレスです。IP アドレスではなく **none** キーワードを指定すると、DNS サーバにヌル値が設定されます。この設定により、DNS サーバは許可されず、デフォルトまたは指定のグループ ポリシーから値が継承されなくなります。最大 4 つの DNS サーバ アドレス、2 つの IPv4 アドレス、および 2 つの IPv6 アドレスを指定できます。

dns-server コマンドを入力するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、次に DNS サーバ y.y.y.y を設定した場合、2 番めのコマンドは最初のコマンドを上書きし、y.y.y.y が唯一の DNS サーバになります。サーバを複数設定する場合も同様です。以前に設定された DNS サーバを上書きする代わりにサーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを含めます。

次に、FirstGroup という名前のグループ ポリシーで、IP アドレスが 10.10.10.15、10.10.10.30、2001:DB8::1、および 2001:DB8::2 の DNS サーバを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30 2001:DB8::1
2001:DB8::2
hostname(config-group-policy)#
```

ステップ 3　**DeafultDNS DNS サーバ グループ**にデフォルトのドメイン名が指定されていない場合は、デフォルトドメインを指定する必要があります。**example.com** などのドメイン名とトップ レベル ドメインを使用します。

```
asa4(config)# group-policy FirstGroup attributes
asa4(config-group-policy)# default-domain value example.com
asa4(config-group-policy)#
```

ステップ 4　DHCP ネットワーク スコープを次のように設定します。

```
hostname(config-group-policy)# dhcp-network-scope {ip_address | none}
hostname(config-group-policy)#
```

DHCP スコープでは、ASA DHCP サーバがこのグループ ポリシーのユーザにアドレスを割り当てるために使用する IP アドレスの範囲（つまり、サブネットワーク）を指定します。

次の例は、First Group という名前のグループ ポリシーに IP サブネットワーク 10.10.85.0（アドレス範囲 10.10.85.0 ～ 10.10.85.255 を指定）を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

グループ ポリシーのスプリット トンネリング属性の設定

スプリット トンネリングを使用すると、リモート アクセス クライアントは、条件に応じて、パケットを暗号化された形式で VPN トンネルを介して誘導したり、クリア テキスト形式でネットワーク インターフェイスに誘導したりすることができます。スプリット トンネリングがイネーブルになっている場合、宛先がトンネルの反対側でないパケットは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが必要ありません。**split-tunnel-policy** コマンドでは、このスプリット トンネリング ポリシーが特定のネットワークに適用されます。

サブネット内でのトラフィックのクライアント スプリット トンネリング動作の違い

AnyConnect クライアントおよびレガシー Cisco VPN（IPsec/IKEv1 クライアント）は、ASA によって割り当てられた IP アドレスと同じサブネット内のサイトにトラフィックを渡す場合、動作が異なります。AnyConnect では、クライアントは、設定済みのスプリット トンネリング ポリシーで指定されたすべてのサイト、および ASA によって割り当てられた IP アドレスと同じサブネット内に含まれるすべてのサイトにトラフィックを渡します。たとえば、ASA によって割り当てられた IP アドレスが 10.1.1.1、マスクが 255.0.0.0 の場合、エンドポイント デバイスは、スプリット トンネリング ポリシーに関係なく、10.0.0.0/8 を宛先とするすべてのトラフィックを渡します。

これとは対照的に、レガシー Cisco VPN Client は、クライアントに割り当てられたサブネットに関係なく、スプリット トンネリング ポリシーで指定されたアドレスだけにトラフィックを渡します。

そのため、割り当てられた IP アドレスが、期待されるローカル サブネットを適切に参照するように、ネットマスクを使用します。

スプリット トンネリング ポリシーの設定

IPv4 トラフィックのスプリット トンネリング ポリシーを指定して、トラフィックのトンネリング ルールを設定します。

```
hostname(config-group-policy)# split-tunnel-policy {tunnelall | tunnelspecified |
excludespecified}
hostname(config-group-policy)# no split-tunnel-policy
```

IPv6 トラフィックのスプリット トンネリング ポリシーを指定して、トラフィックのトンネリング ルールを設定します。

```
hostname(config-group-policy)# ipv6-split-tunnel-policy {tunnelall | tunnelspecified |
excludespecified}
hostname(config-group-policy)# no ipv6-split-tunnel-policy
```

デフォルトでは、**すべてのトラフィックがトンネリング**されます。スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを入力します。**split-tunnel-policy** 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、別のグループ ポリシーのスプリット トンネリングの値を継承できます。

トラフィックがクリア テキストで送信されるネットワークのリストは、**excludespecified** キーワードで定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザにとって役立ちます。このオプションは、Cisco VPN Client に対してだけ適用されます。

tunnelall キーワードを指定すると、すべてのトラフィックがクリア テキストとして送信されなくなるか、ASA 以外の宛先に送信されなくなります。この指定では、実質的にスプリット トンネリングはディセーブルになります。リモート ユーザは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。これがデフォルトのオプションです。

tunnelspecified キーワードを指定すると、指定されたネットワークとの間のすべてのトラフィックがトンネリングされます。このオプションによって、スプリット トンネリングがイネーブルになります。トンネリングするアドレスのネットワーク リストを作成できるようになります。その他すべてのアドレスに対するデータは、クリア テキストで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

（注） スプリット トンネリングは、本来は、セキュリティ機能ではなくトラフィック管理機能です。最大限のセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

次に、FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

スプリット トンネリング用のネットワーク リストの指定

前提条件

- 「スプリット トンネリング ポリシーの設定」（P.4-57）に従って、IPv4 または IPv6、あるいはその両方のスプリット トンネル ポリシーを設定します。
- IPv4 または IPv6 統合 ACL を作成して、スプリット トンネルのためのネットワーク リストとして指定します。IPv4 ネットワークおよび IPv6 ネットワークの両方のスプリット トンネル ポリシーを設定した場合は、コマンドで指定するネットワーク リスト（統合 ACL）が両方のプロトコルで使用されます。このため、ネットワーク リストには、IPv4 および IPv6 の両方のトラフィックのアクセス コントロール エントリ（ACE）が含まれている必要があります。これらの統合 ACL を作成していない場合は、一般的な操作のコンフィギュレーション ガイドの“Adding ACLs and ACEs” section on page 22-2を参照してください。

手順

グループ ポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用して、スプリット トンネリング用のネットワーク リスト（統合 ACL）を指定します。

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

スプリット トンネリング ネットワーク リストによって、トラフィックがトンネルを通過する必要があるネットワークと、トンネリングを必要としないネットワークが区別されます。ASA は、ネットワーク リストに基づいてスプリット トンネリングを実行するかどうかを決定します。ネットワーク リストは、プライベート ネットワーク上のアドレスのリストで構成された ACL です。

拡張 ACL を使用する場合は、ソース ネットワークがスプリットトンネリング ネットワークを決定します。この場合、宛先ネットワークは無視されます。また、*any* という名前の IP アドレスまたはネットワーク アドレスは存在しないので、ACL のソースにはこの名前を使用しないでください。

value *access-list name* パラメータでは、トンネリングを実行する、または実行しないネットワークを列挙した ACL を指定します。ACL には、IPv4 と IPv6 の両方のアドレスを指定する ACE が含まれている統合 ACL を指定できます。

none キーワードは、スプリット トンネリング用のネットワーク リストが存在しないことを示し、ASA はすべてのトラフィックをトンネリングします。**none** キーワードを指定すると、スプリット トンネリングのネットワーク リストにヌル値が設定され、スプリット トンネリングが拒否されます。また、これにより、デフォルトまたは指定されたグループ ポリシーから、デフォルトのスプリット トンネリング ネットワーク リストが継承されなくなります。

ネットワーク リストを削除するには、このコマンドの **no** 形式を入力します。すべてのスプリット トンネリング ネットワーク リストを削除するには、引数を指定せずに **no split-tunnel-network-list** コマンドを入力します。このコマンドにより、**none** キーワードを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのネットワーク リストが削除されます。

スプリット トンネリング ネットワーク リストがない場合、ユーザはデフォルトのグループ ポリシーまたは指定したグループ ポリシー内に存在するネットワーク リストを継承します。ユーザがこのようなネットワーク リストを継承しないようにするには、**split-tunnel-network-list none** コマンドを入力します。

次に、FirstGroup という名前のグループ ポリシーに対して FirstList という名前のネットワーク リストを設定する例を示します。

```
hostname(config)# show runn group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list value FirstList
```

show runn group-policy attributes コマンドを実行して、設定を確認します。次の例は、管理者が IPv4 と IPv6 の両方のネットワーク ポリシーを設定し、両方のポリシーに対してネットワーク リスト（統合 ACL）**FirstList** を使用したことを示しています。

```
hostname(config-group-policy)# show runn group-policy FirstGroup attributes
group-policy FirstGroup attributes
 split-tunnel-policy tunnelspecified
 ipv6-split-tunnel-policy tunnelspecified
 split-tunnel-network-list value FirstList
```

トンネリング用のドメイン属性の設定

トンネリングされたパケットのデフォルト ドメイン名、またはスプリット トンネルを経由して解決されるドメインのリストを指定できます。この項では、これらのドメインを設定する方法について説明します。次の項目を取り上げます。

トンネリングされたパケットのデフォルト ドメイン名の定義

ASA は、ドメイン フィールドを省略した DNS クエリーに付加するために、デフォルト ドメイン名を IPsec クライアントに渡します。デフォルト ドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。グループ ポリシーのユーザのデフォルト ドメイン名を指定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを入力します。ドメイン名を削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

value *domain-name* パラメータは、グループのデフォルト ドメイン名を指定します。デフォルト ドメイン名が存在しないことを指定するには、**none** キーワードを入力します。このコマンドにより、デフォルト ドメイン名にヌル値が設定され、デフォルト ドメイン名が拒否されます。また、デフォルトまたは指定されたグループ ポリシーからデフォルト ドメイン名が継承されなくなります。

すべてのデフォルト ドメイン名を削除するには、引数を指定せずに **no default-domain** コマンドを入力します。このコマンドにより、**none** キーワードを指定して **default-domain** コマンドを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのデフォルト ドメイン名が削除されます。**no** 形式を使用すると、ドメイン名の継承が許可されます。

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

スプリット トンネリング用のドメイン リストの定義

スプリット トンネルを介して解決されるドメインのリストを入力します。グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを入力します。リストを削除するには、このコマンドの **no** 形式を入力します。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルトのグループ ポリシー内に存在するリストを継承します。ユーザがこのようなスプリット トンネリング ドメイン リストを継承しないようにするには、**none** キーワードを指定して **split-dns** コマンドを入力します。

すべてのスプリット トンネリング ドメイン リストを削除するには、引数を指定せずに **no split-dns** コマンドを入力します。これにより、**none** キーワードを指定して **split-dns** コマンドを発行して作成したヌル リストを含めて、設定済みのすべてのスプリット トンネリング ドメイン リストが削除されます。

パラメータ **value** *domain-name* では、ASA がスプリット トンネルを介して解決するドメイン名を指定します。**none** キーワードは、スプリット DNS リストが存在しないことを示します。また、このキーワードにより、スプリット DNS リストにヌル値が設定されます。そのため、スプリット DNS リストは拒否され、デフォルトまたは指定されたグループ ポリシーのスプリット DNS リストが継承されなくなります。このコマンドの構文は次のとおりです。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2...
domain-nameN] | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

ドメインのリスト内で各エントリを区切るには、スペースを 1 つ入力します。エントリ数に制限はありませんが、ストリング全体の長さは 255 文字以下にします。英数字、ハイフン（-）、およびピリオド（.）のみを使用できます。デフォルト ドメイン名がトンネルを介して解決される場合は、そのドメイン名をこのリストに明示的に含める必要があります。

次の例は、FirstGroup という名前のグループ ポリシーで、Domain1、Domain2、Domain3、Domain4 の各ドメインがスプリット トンネリングを介して解決されるように設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

DHCP 代行受信の設定

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、ASA で送信ルートの数を 27 ～ 40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信を使用することにより、Microsoft Windows XP クライアントで ASA とともにスプリット トンネリングを使用できます。ASA は、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows XP 以前の Windows クライアントの場合、DHCP 代行受信によってドメイン名とサブネット マスクが提供されます。これは、DHCP サーバを使用するのが効果的でない環境で役立ちます。

intercept-dhcp コマンドは、DHCP 代行受信をイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

netmask 変数で、トンネル IP アドレスのサブネット マスクを提供します。このコマンドの **no** 形式は、コンフィギュレーションから DHCP 代行受信を削除します。

```
[no] intercept-dhcp
```

次に、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

Web セキュリティのスプリット除外ポリシーの設定

クラウド Web セキュリティに関する情報

AnyConnect Web セキュリティ モジュールは、Cisco クラウド Web セキュリティが評価する Cisco クラウド Web セキュリティ スキャニング プロキシに HTTP トラフィックをルーティングするエンドポイント コンポーネントです。Cisco クラウド Web セキュリティは、Web ページの各要素を同時に分析できるように、これらの要素を分解します。これにより、潜在的に危険なコンテンツがブロックされ、問題のないコンテンツが通過します。

多数の Cisco クラウド Web セキュリティ スキャニング プロキシが世界各国に普及することで、AnyConnect Web セキュリティを活用するユーザは、遅延を最小限に抑えるために、応答時間が最も早い Cisco クラウド Web セキュリティ スキャニング プロキシにトラフィックをルーティングできます。

ユーザが VPN セッションを確立した場合は、すべてのネットワーク トラフィックが VPN トンネル経由で送信されます。ただし、AnyConnect ユーザが Web セキュリティを使用している場合、エンドポイントで発信された HTTP トラフィックはトンネルから除外され、クラウド Web セキュリティ スキャニング プロキシに直接送信される必要があります。

クラウド Web セキュリティ スキャニング プロキシ用のトラフィックのスプリット トンネル除外を設定するには、グループ ポリシーで [Set up split exclusion for Web Security] ボタンを使用します。

前提条件

- ASDM を使用して ASA にアクセスできる必要があります。この手順は、コマンドライン インターフェイスを使用して実行できません。
- Web セキュリティは AnyConnect クライアントで使用するように設定する必要があります。『*AnyConnect Secure Mobility Client Administrator Guide*』の「Configuring Web Security」を参照してください。
- グループ ポリシーを作成し、Web セキュリティで設定された AnyConnect クライアントの接続プロファイルに割り当てます。

手順の詳細

ステップ 1　設定するヘッド エンドの ASDM セッションを開始し、[Remote Access VPN] > [Configuration] > [Group Policies] の順に選択します

ステップ 2　設定するグループ ポリシーを選択し、[Edit] をクリックします。

ステップ 3　[Advanced] > [Split Tunneling] の順に選択します。

ステップ 4　[Set up split exclusion for Web Security] をクリックします。

ステップ 5　Web セキュリティのスプリット除外に使用される新しい ACL を入力するか、既存のアクセス リストを選択します。ASDM は、ネットワーク リストで使用する ACL を設定します。

ステップ 6　新しいリストの場合は [Create Access List] をクリックし、既存のリストの場合は [Update Access List] をクリックします。

ステップ 7　[OK] をクリックします。

次の実施手順

追加スキャニング プロキシを追加した場合は、この手順で作成した統合 ACL を新しい情報で更新します。

リモート アクセス クライアントで使用するためのブラウザ プロキシ設定の設定

クライアントのプロキシ サーバ パラメータを設定するには、次の手順を実行します。

ステップ 1　グループ ポリシー コンフィギュレーション モードで **msie-proxy server** コマンドを入力し、クライアントデバイスのブラウザのプロキシ サーバとポート番号を設定します。

```
hostname(config-group-policy)# msie-proxy server {value server[:port] | none}
hostname(config-group-policy)#
```

デフォルト値は **none** です。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy server
hostname(config-group-policy)#
```

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、ブラウザ プロキシ サーバとして IP アドレス 192.168.10.1 を設定し、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象にする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

ステップ 2　グループ ポリシー コンフィギュレーション モードで **msie-proxy method** コマンドを入力して、クライアントデバイスのブラウザ プロキシ アクション（「メソッド」）を設定します。

```
hostname(config-group-policy)# msie-proxy method [auto-detect | no-modify | no-proxy |
use-server]
hostname(config-group-policy)#
```

デフォルト値は **use-server** です。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy method [auto-detect | no-modify | no-proxy |
use-server]
hostname(config-group-policy)#
```

使用できる方法は、次のとおりです。

- **auto-detect**：クライアントデバイスのブラウザでプロキシ サーバの自動検出の使用をイネーブルにします。
- **no-modify**：このクライアントデバイスで使用しているブラウザの HTTP ブラウザ プロキシ サーバの設定をそのままにします。
- **no-proxy**：クライアントデバイスで使用しているブラウザの HTTP プロキシの設定をディセーブルにします。
- **use-server**：**msie-proxy server** コマンドに設定された値を使用するように、ブラウザの HTTP プロキシ サーバ設定を設定します。

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、FirstGroup というグループ ポリシーのブラウザ プロキシ設定として自動検出を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

次に、クライアントデバイスのサーバとしてサーバ QASERVER、ポート 1001 を使用するように、FirstGroup というグループ ポリシーのブラウザ プロキシ設定を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

ステップ 3　グループ ポリシー コンフィギュレーション モードで **msie-proxy except-list** コマンドを入力して、クライアントデバイスのブラウザがローカルでプロキシをバイパスするために使用するプロキシの例外リストを設定します。これらのアドレスは、プロキシ サーバによってアクセスされません。このリストは、[Proxy Stteings] ダイアログボックスにある [Exceptions] ボックスに相当します。

```
hostname(config-group-policy)# msie-proxy except-list {value server[:port] | none}
hostname(config-group-policy)#
```

コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy except-list
hostname(config-group-policy)#
```

- **value** *server:port*：このクライアントデバイスに適用する MSIE サーバの IP アドレスまたは名前、およびポートを指定します。ポート番号は任意です。
- **none**：IP アドレスまたはホスト名とポートがないことを示し、例外リストを継承しません。

デフォルトでは、msie-proxy except-list はディセーブルになっています。

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、ブラウザのプロキシ例外リストを設定する例を示します。IP アドレス 192.168.20.1 のサーバで構成され、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象とします。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

ステップ 4　グループ ポリシー コンフィギュレーション モードで **msie-proxy local-bypass** コマンドを入力し、クライアントデバイスで使用するブラウザが、プロキシをローカルでバイパスする設定をイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

デフォルトでは、msie-proxy local-bypass はディセーブルになっています。

次に、FirstGroup というグループ ポリシーのブラウザのプロキシ ローカル バイパスをイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

AnyConnect Secure Mobility Client 接続のグループ ポリシー属性の設定

第 12 章「AnyConnect VPN Client 接続の設定」に示すように、AnyConnect クライアント接続をイネーブルにした後は、グループ ポリシーの AnyConnect 機能をイネーブルまたは必須にできます。グループ ポリシー webvpn コンフィギュレーション モードで次の手順を実行します。

ステップ 1　グループ ポリシー webvpn コンフィギュレーション モードを開始します。たとえば、次のように入力します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

ステップ 2　エンドポイント コンピュータ上で AnyConnect クライアントの永続的なインストールをディセーブルにするには、**none** キーワードで **anyconnect keep-installer** コマンドを使用します。たとえば、次のように入力します。

```
hostname(config-group-webvpn)# anyconnect keep-installer none
hostname(config-group-webvpn)#
```

デフォルトでは、クライアントの永続的なインストールはイネーブルになっています。クライアントは、AnyConnect セッションの終了時にエンドポイントにインストールされたままになります。

ステップ 3　グループ ポリシーの AnyConnect SSL 接続経由で HTTP データの圧縮をイネーブルにするには、**anyconnect ssl compression** コマンドを入力します。デフォルトでは、圧縮は **none**（ディセーブル）に設定されています。圧縮をイネーブルにするには、**deflate** キーワードを使用します。たとえば、次のように入力します。

```
hostname(config-group-webvpn)# anyconnect compression deflate
hostname(config-group-webvpn)#
```

ステップ 4　ASA で Dead Peer Detection（DPD; デッド ピア検出）をイネーブルにし、AnyConnect または ASA が DPD を実行する頻度を設定するには、**anyconnect dpd-interval** コマンドを使用します。

anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

デフォルトでは、ASA と AnyConnect クライアントの両方が 30 秒間隔で DPD を実行します。

ゲートウェイは、ASA のことです。ASA が DPD テストを実行する頻度を、30 ～ 3600 秒（1 時間）の範囲で指定できます。**none** を指定すると、ASA が実行する DPD テストはディセーブルになります。値 300 が推奨されます。

クライアントは、AnyConnect クライアントのことです。クライアントが DPD テストを実行する頻度は、30 ～ 3600 秒（1 時間）の範囲で指定できます。**none** を指定すると、クライアントが実行する DPD テストはディセーブルになります。値 30 が推奨されます。

次の例では、ASA（ゲートウェイ）で実行される DPD の頻度を 300 秒に設定し、クライアントで実行される DPD の頻度を 30 秒に設定します。

```
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 300
hostname(config-group-webvpn)# anyconnect dpd-interval client 30
hostname(config-group-webvpn)#
```

ステップ 5　デバイスが接続のアイドル状態を維持する時間を制限する場合でも、**anyconnect ssl keepalive** コマンドを使用してキープアライブ メッセージの頻度を調整することで、プロキシ、ファイアウォール、または NAT デバイス経由の AnyConnect 接続を開いたままにすることができます。

anyconnect ssl keepalive {none | *seconds***}**

また、キープアライブを調整すると、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベース アプリケーションをアクティブに実行していない場合でも、AnyConnect クライアントは切断および再接続されません。

次の例では、AnyConnect クライアントがキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるようにセキュリティ アプライアンスを設定します。

```
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
hostname(config-group-webvpn)#
```

ステップ 6　AnyConnect クライアントが SSL セッションでキーを再生成できるようにするには、**anyconnect ssl rekey** コマンドを使用します。

anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}}

デフォルトでは、キー再生成はディセーブルになっています。

method を new-tunnel に指定すると、SSL キーの再生成中に AnyConnect クライアントが新しいトンネルを確立することが指定されます。method を **none** に指定すると、キー再生成はディセーブルになります。method を **ssl** に指定すると、SSL の再ネゴシエーションはキー再生成中に行われます。method を指定する代わりに、セッションの開始からキー再生成が行われるまでの時間を 1 ～ 10080（1 週間）の分数で指定できます。

次の例では、キー再生成中に AnyConnect クライアントが SSL と再ネゴシエートするように設定し、キー再生成がセッション開始の 30 分後に発生するように設定しています。

```
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
hostname(config-group-webvpn)#
```

ステップ 7　クライアント プロトコル バイパス機能を使用すると、ASA が IPv6 トラフィックだけを予期しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定することができます。

AnyConnect クライアントが ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ASA が AnyConnect 接続に IPv4 アドレスまたは IPv6 アドレスだけを割り当てた場合に、ASA が IP アドレスを割り当てなかったネットワーク トラフィックについて、クライアント プロトコル バイパスによってそのトラフィックをドロップさせるか、または ASA をバイパスしてクライアントからの暗号化なし、つまりクリア テキストとしての送信を許可するかを設定できるようになりました。

たとえば、ASA が AnyConnect 接続に IPv4 アドレスだけを割り当てたが、そのエンドポイントがデュアル スタックであるとします。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコル機能がディセーブルの場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルがイネーブルの場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

client-bypass-protocol コマンドを使用して、クライアント バイパス プロトコル機能をイネーブルまたはディセーブルにします。コマンド構文は次のとおりです。

```
client-bypass-protocol {enable | disable}
```

次に、クライアント バイパス プロトコルをイネーブルにする例を示します。

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

次に、クライアント バイパス プロトコルをデイセーブルにする例を示します。

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

次に、イネーブルまたはディセーブルになっているクライアント バイパス プロトコル設定を削除する例を示します。

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

ステップ 8　ASA 間にロード バランシングを設定した場合は、VPN セッションの再確立に使用される ASA IP アドレスを解決するために、ASA の FQDN を指定します。この設定は、さまざまな IP プロトコルのネットワーク間のクライアント ローミングをサポートするうえで重要です（IPv4 から IPv6 など）。

AnyConnect プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロード バランシング シナリオの正しいデバイス（トンネルが確立されているデバイス）と一致しない場合があります。

デバイスの FQDN がクライアントに配信されない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル（IPv4 から IPv6）のネットワーク間のローミングをサポートするには、AnyConnect は、トンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDN の名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、使用可能な場合の、常に、ASA によってプッシュされた（また、グループ ポリシーで管理者が設定した）デバイス FQDN を使用します（使用可能な場合）。FQDN が設定されていない場合、ASA は、[Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得（およびクライアントに送信）します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

gateway-fqdn コマンドを使用して、ASA の FQDN を設定します。コマンド構文は次のとおりです。

```
gateway-fqdn value {FQDN_Name | none}
no gateway-fqdn
```

次に、ASA の FQDN を ASAName.example.cisco.com として定義する例を示します。

```
hostname(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
hostname(config-group-policy)#
```

次に、グループ ポリシーから ASA の FQDN を削除する例を示します。グループ ポリシーは、デフォルト グループ ポリシーからこの値を継承します。

```
hostname(config-group-policy)# no gateway-fqdn
hostname(config-group-policy)#
```

次に、FQDN を空の値として定義する例を示します。hostname コマンドおよび domain-name コマンドを使用して設定されたグローバル FQDN が使用されます（使用可能な場合）。

```
hostname(config-group-policy)# gateway-fqdn none
hostname(config-group-policy)#
```

IPSec（IKEv1）クライアントのグループ ポリシー属性の設定

IPSec（IKEv1）クライアントのセキュリティ属性の設定

グループのセキュリティ設定を指定するには、次の手順を実行します。

ステップ 1　グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **password-storage** コマンドを使用し、ユーザがログイン パスワードをクライアント システムに保存できるようにするかどうかを指定します。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを使用します。

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

セキュリティ上の理由から、パスワード保存はデフォルトでディセーブルになっています。セキュア サイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。

password-storage 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

no 形式を指定すると、password-storage の値を別のグループ ポリシーから継承することができます。

このコマンドは、対話的なハードウェア クライアント認証やハードウェア クライアントの個別ユーザ認証には適用されません。

次に、FirstGroup という名前のグループ ポリシーに対してパスワードの保管をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

ステップ 2　デフォルトではディセーブルになっている IP 圧縮をイネーブルにするかどうかを指定します。

（注）　IPSec IKEv2 接続では、IP 圧縮はサポートされていません。

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

LZS IP 圧縮をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-comp** コマンドを入力します。IP 圧縮をディセーブルにするには、**disable** キーワードを指定して **ip-comp** コマンドを入力します。

ip-comp 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、別のグループ ポリシーの値を継承できます。

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

データ圧縮をイネーブルにすると、モデムで接続するリモート ダイヤルイン ユーザのデータ伝送レートが向上する場合があります。

注意　データ圧縮を使用すると、ユーザ セッションごとのメモリ要求と CPU 使用率が増加し、結果として ASA のスループット全体が低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。

ステップ 3　グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **re-xauth** コマンドを使用し、IKE キーが再生成される際にユーザが再認証を受ける必要があるかどうかを指定します。

（注）　IKEv2 接続では、IKE キー再生成はサポートされていません。

IKE キー再生成時の再認証をイネーブルにすると、ASA では、最初のフェーズ 1 IKE ネゴシエーションにおいてユーザに対してユーザ名とパスワードの入力が求められ、その後 IKE キー再生成が行われるたびにユーザ認証が求められます。再認証によって、セキュリティが強化されます。

設定されているキー再生成間隔が極端に短い場合、ユーザは認証を繰り返し求められることに不便を感じることがあります。許可要求が何度も繰り返されないようにするには、再認証をディセーブルにします。設定されているキー再生成インターバルを確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを入力して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータのキロバイト単位のライフタイムを表示します。IKE キーが再生成される際のユーザの再認証をディセーブルにするには、**disable** キーワードを入力します。IKE キーが再生成される際の再認証は、デフォルトではディセーブルになっています。

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

IKE キーが再生成される際の再認証用の値を別のグループ ポリシーから継承することをイネーブルにするには、このコマンドの **no** 形式を入力して、実行コンフィギュレーションから re-xauth 属性を削除します。

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

（注）　接続先にユーザが存在しない場合、再認証は失敗します。

ステップ 4　完全転送秘密をイネーブルにするかどうかを指定します。IPsec ネゴシエーションでは、完全転送秘密により、新しい各暗号キーは以前のどのキーとも関連性がないことが保証されます。グループ ポリシーは、別のグループ ポリシーから完全転送秘密の値を継承できます。完全転送秘密は、デフォルトではディセーブルになっています。完全転送秘密をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **pfs** コマンドを使用します。

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

完全秘密転送をディセーブルにするには、**disable** キーワードを指定して **pfs** コマンドを入力します。

完全秘密転送属性を実行コンフィギュレーションから削除して、値を継承しないようにするには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

IKEv1 クライアントの IPsec-UDP 属性の設定

IPsec over UDP（IPsec through NAT と呼ばれることもあります）を使用すると、Cisco VPN Client またはハードウェア クライアントは、NAT を実行している ASA に UDP 経由で接続できます。この機能はデフォルトではディセーブルになっています。IPsec over UDP は、リモートアクセス接続だけに適用される専用の機能で、モード コンフィギュレーションが必要です。ASA は、SA のネゴシエート時にクライアントとの間でコンフィギュレーション パラメータをやり取りします。IPSec over UDP を使用すると、システム パフォーマンスが若干低下します。

IPsec over UDP をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、次のように **enable** キーワードを指定して **ipsec-udp** コマンドを設定します。

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

IPsec over UDP を使用するには、この項の説明に従って、**ipsec-udp-port** コマンドも設定する必要があります。

IPsec over UDP をディセーブルにするには、**disable** キーワードを入力します。IPSec over UDP 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、別のグループ ポリシーから IPSec over UDP の値を継承できるようになります。

また、IPsec over UDP を使用するように Cisco VPN Client を設定しておく必要があります（Cisco VPN Client は、デフォルトで IPsec over UDP を使用するように設定されています）。VPN 3002 では、IPsec over UDP を使用するためのコンフィギュレーションが必要ありません。

次に、FirstGroup というグループ ポリシーの IPSec over UDP を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

IPsec over UDP をイネーブルにした場合は、グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドも設定する必要があります。このコマンドにより、IPSec over UDP 用の UDP ポート番号が設定されます。IPSec ネゴシエーションでは、ASA は設定されたポートでリッスンし、他のフィルタ ルールで UDP トラフィックがドロップされていても、そのポート宛ての UDP トラフィックを転送します。ポート番号の範囲は 4001 ～ 49151 です。デフォルトのポート値は 10000 です。

UDP ポートをディセーブルにするには、このコマンドの **no** 形を入力します。これにより、別のグループ ポリシーから IPsec over UDP ポートの値を継承できるようになります。

```
hostname(config-group-policy)# ipsec-udp-port port
```

次に、FirstGroup というグループ ポリシーの IPsec UDP ポートをポート 4025 に設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

VPN ハードウェア クライアントの属性の設定

この項では、セキュア ユニット認証およびユーザ認証をイネーブルまたはディセーブルにし、VPN ハードウェア クライアントのユーザ認証タイムアウト値を設定する方法について説明します。これらのコマンドは、Cisco IP Phone および LEAP パケットで個別のユーザ認証をバイパスすることを許可し、ネットワーク拡張モードを使用するハードウェア クライアントの接続を許可することもできます。

セキュア ユニット認証の設定

セキュア ユニット認証では、VPN ハードウェア クライアントがトンネルを開始するたびにユーザ名とパスワードを使用した認証を要求することで、セキュリティが強化されます。この機能をイネーブルにすると、ハードウェア クライアントではユーザ名とパスワードが保存されません。セキュア ユニット認証はデフォルトでディセーブルになっています。

（注） この機能をイネーブルにした場合に VPN トンネルを確立するには、ユーザがユーザ名とパスワードを入力する必要があります。

セキュア ユニット認証では、ハードウェア クライアントが使用する接続プロファイルに対して認証サーバ グループが設定されている必要があります。プライマリ ASA でセキュア ユニット認証が必要な場合は、すべてのバックアップ サーバに対してもセキュア ユニット認証を設定する必要があります。

グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **secure-unit-authentication** コマンドを入力し、セキュア ユニット認証をイネーブルにするかどうかを指定します。

```
hostname(config-group-policy)# secure-unit-authentication {enable | disable}
hostname(config-group-policy)# no secure-unit-authentication
```

セキュア ユニット認証をディセーブルにするには、**disable** キーワードを入力します。セキュア ユニット認証の属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを指定すると、他のグループ ポリシーからセキュア ユニット認証の値を継承できます。

次に、FirstGroup という名前のグループ ポリシーに対して、セキュア ユニット認証をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

ユーザ認証の設定

ユーザ認証はデフォルトでディセーブルになっています。ユーザ認証をイネーブルにすると、ハードウェア クライアントの背後にいる個々のユーザは、トンネルを介してネットワークにアクセスするために認証を受けることが必要となります。個々のユーザは、設定した認証サーバの順序に従って認証されます。

グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **user-authentication** コマンドを入力し、ユーザ認証をイネーブルにするかどうかを指定します。

```
hostname(config-group-policy)# user-authentication {enable | disable}
hostname(config-group-policy)# no user-authentication
```

ユーザ認証をディセーブルにするには、**disable** キーワードを入力します。ユーザ認証属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、別のグループ ポリシーからユーザ認証の値を継承できます。

プライマリ ASA でユーザ認証が必要な場合は、バックアップ サーバでも同様にユーザ認証を設定する必要があります。

次の例は、FirstGroup という名前のグループ ポリシーのユーザ認証をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

アイドル タイムアウトの設定

グループ ポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを入力して、ハードウェア クライアントの背後の個々のユーザにアイドル タイムアウトを設定します。アイドル タイムアウト期間中にハードウェア クライアントの背後のユーザによる通信アクティビティがない場合、ASA はそのクライアントのアクセスを終了します。

```
hostname(config-group-policy)# user-authentication-idle-timeout {minutes | none}
hostname(config-group-policy)# no user-authentication-idle-timeout
```

（注）　このタイマーは、VPN トンネル自体ではなく、VPN トンネルを通過するクライアント アクセスだけを終了します。

show uauth コマンドへの応答で示されるアイドル タイムアウトは、常に Cisco Easy VPN リモート デバイスのトンネルを認証したユーザのアイドル タイムアウト値になります。

minutes パラメータで、アイドル タイムアウト時間（分単位）を指定します。最短時間は 1 分、デフォルトは 30 分、最長時間は 35791394 分です。

アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、他のグループ ポリシーからアイドル タイムアウト値を継承できます。

アイドル タイムアウト値を継承しないようにするには、**none** キーワードを指定して **user-authentication-idle-timeout** コマンドを入力します。このコマンドにより、アイドル タイムアウトにヌル値が設定されます。この設定によってアイドル タイムアウトが拒否され、デフォルトまたは指定されたグループ ポリシーからユーザ認証のアイドル タイムアウト値が継承されなくなります。

次の例は、FirstGroup という名前のグループ ポリシーに 45 分のアイドル タイムアウト値を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

IP Phone Bypass の設定

Cisco IP Phone は、ハードウェア クライアントの背後の個別のユーザ認証をバイパスさせることができます。IP Phone Bypass をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-phone-bypass** コマンドを入力します。IP Phone Bypass を使用すると、ハードウェア クライアントの背後にある IP 電話が、ユーザ認証プロセスなしで接続できます。IP Phone Bypass は、デフォルトでディセーブルになっています。イネーブルの場合、セキュア ユニット認証は有効のままになります。

IP Phone Bypass をディセーブルにするには、**disable** キーワードを入力します。IP Phone Bypass 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、IP Phone Bypass の値を別のグループ ポリシーから継承できます。

```
hostname(config-group-policy)# ip-phone-bypass {enable | disable}
hostname(config-group-policy)# no ip-phone-bypass
```

（注）　mac-exempt を設定してクライアントの認証を免除する必要があります。詳細については、「デバイス パススルーの設定」（P.8-9）を参照してください。

LEAP Bypass の設定

LEAP Bypass がイネーブルの場合、VPN 3002 ハードウェア クライアントの背後の無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過します。このアクションによって、Cisco ワイヤレス アクセス ポイント デバイスを使用するワークステーションは、LEAP 認証を確立し、その後ユーザ認証ごとに認証を再度実行できます。LEAP Bypass は、デフォルトでディセーブルになっています。

シスコの無線アクセス ポイントからの LEAP パケットが個々のユーザ認証をバイパスできるようにするには、グループ ポリシー コンフィギュレーション モードで **enable** キーワードを指定して **leap-bypass** コマンドを入力します。LEAP Bypass をディセーブルにするには、**disable** キーワードを

入力します。LEAP Bypass の属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、LEAP Bypass の値を別のグループ ポリシーから継承できます。

```
hostname(config-group-policy)# leap-bypass {enable | disable}
hostname(config-group-policy)# no leap-bypass
```

（注） IEEE 802.1X は、有線および無線ネットワークにおける認証規格です。この規格では、クライアントと認証サーバの間で強力な相互認証を実現し、ユーザ単位およびセッション単位のダイナミックな無線暗号化秘密（WEP）キーの使用を可能にして、スタティックな WEP キーの場合に介在する面倒な管理作業やセキュリティ上の問題を軽減することができます。

シスコは、Cisco LEAP と呼ばれる 802.1X 無線認証タイプを開発しました。LEAP（Lightweight Extensible Authentication Protocol）は、無線クライアントと RADIUS サーバの間の接続における相互認証を実装します。パスワードなど、認証に使用されるクレデンシャルは、ワイヤレス媒体を経由して送信される前に必ず暗号化されます。

Cisco LEAP では、無線クライアントを RADIUS サーバに対して認証します。RADIUS アカウンティング サービスは提供されません。

インタラクティブ ハードウェア クライアント認証をイネーブルにした場合、この機能は正常に動作しません。

注意 認証されていないトラフィックがトンネルを通過できるようにすると、ネットワークにセキュリティ リスクを招くおそれがあります。

次の例は、FirstGroup という名前のグループ ポリシーに LEAP Bypass を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

ネットワーク拡張モードのイネーブル化

ネットワーク拡張モードを使用すると、ハードウェア クライアントは、単一のルーティング可能なネットワークを VPN トンネルを介してリモート プライベート ネットワークに提供できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークから ASA の背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、ASA の背後にあるデバイスは、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。トンネルはハードウェア クライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。

グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **nem** コマンドを入力し、ハードウェア クライアントの Network Extension Mode（NEM; ネットワーク拡張モード）をイネーブルにします。

```
hostname(config-group-policy)# nem {enable | disable}
hostname(config-group-policy)# no nem
```

NEM をディセーブルにするには、**disable** キーワードを入力します。この NEM の属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

次に、FirstGroup というグループ ポリシーの NEM を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

バックアップ サーバ属性の設定

バックアップ サーバを設定します（使用する予定がある場合）。IPsec バックアップ サーバを使用すると、VPN クライアントはプライマリ ASA が使用不可の場合も中央サイトに接続することができます。バックアップ サーバを設定すると、ASA は、IPsec トンネルを確立するときにクライアントにサーバ リストを渡します。クライアント上またはプライマリ ASA 上にバックアップ サーバを設定しない限り、バックアップ サーバは存在しません。

バックアップ サーバは、クライアント上またはプライマリ ASA 上に設定します。ASA 上にバックアップ サーバを設定すると、適応型セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュして、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

（注） ホスト名を使用する場合は、バックアップ DNS サーバおよびバックアップ WINS サーバを、プライマリ DNS サーバおよびプライマリ WINS サーバとは別のネットワーク上に配置することを推奨します。このようにしないと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得している場合、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報と WINS 情報があると、DHCP リースが期限切れになるまでクライアントを更新できなくなります。また、ホスト名を使用している場合に DNS サーバが使用不可になると、大幅な遅延が発生するおそれがあります。

バックアップ サーバを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを入力します。

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

バックアップ サーバを削除するには、バックアップ サーバを指定してこのコマンドの **no** 形式を入力します。backup-servers 属性を実行コンフィギュレーションから削除し、backup-servers の値を他のグループ ポリシーから継承できるようにするには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

clear-client-config キーワードは、クライアントでバックアップ サーバを使用しないことを指定します。ASA は、ヌルのサーバ リストをプッシュします。

keep-client-config キーワードは、ASA がバックアップ サーバ情報をクライアントに送信しないことを指定します。クライアントは、独自のバックアップ サーバ リストを使用します（設定されている場合）。これはデフォルトです。

server1 server 2....server10 パラメータ リストは、プライマリの ASA が使用不可の場合に VPN クライアントが使用するサーバをプライオリティ順にスペースで区切ったリストです。このリストには、サーバを IP アドレスまたはホスト名で指定します。このリストの長さは 500 文字までで、格納できるエントリは最大 10 個までです。

次の例は、FirstGroup という名前のグループ ポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップ サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

ネットワーク アドミッション コントロールのパラメータの設定

この項で説明するグループ ポリシー NAC コマンドには、すべてデフォルトの値があります。どうしても必要な場合を除き、これらのパラメータのデフォルト値は変更しないでください。

ASA は、拡張認証プロトコル（EAP）over UDP（EAPoUDP）のメッセージを使用して、リモート ホストのポスチャを確認します。ポスチャ検証では、リモート ホストにネットワーク アクセス ポリシーを割り当てる前に、そのホストがセキュリティの必要条件を満たしているかどうかが調べられます。セキュリティ アプライアンスでネットワーク アドミッション コントロールを設定する前に、NAC 用に Access Control Server を設定しておく必要があります。

Access Control Server は、システムのモニタリング、レポートの作成、デバッグ、およびロギングに役立つ情報を示すポスチャ トークン（ACS で設定可能な文字列）をセキュリティ アプライアンスにダウンロードします。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。ポスチャ検証またはクライアントなしの認証が終わると、ACS はセッション用のアクセス ポリシーをセキュリティ アプライアンスにダウンロードします。

デフォルトのグループ ポリシーまたは代替グループ ポリシーのネットワーク アドミッション コントロールを設定するには、次の手順を実行します。

ステップ 1　（任意）ステータス クエリー タイマーの期間を設定します。セキュリティ アプライアンスは、ポスチャ検証が問題なく終わり、ステータス クエリーの応答を受け取るたびに、ステータス クエリーのタイマーを始動させます。このタイマーが切れると、ホスト ポスチャの変化を調べるクエリー（ステータス クエリーと呼ばれる）がトリガーされます。タイマーの期限を 30 ～ 1800 の秒数で入力します。デフォルトの設定は 300 秒です。

ネットワーク アドミッション コントロールのセッションで、ポスチャ検証が問題なく終わり、ポスチャの変更を調べる次のクエリーが発行されるまでの間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-sq-period** コマンドを使用します。

```
hostname(config-group-policy)# nac-sq-period seconds
hostname(config-group-policy)#
```

デフォルトのグループ ポリシーからステータス クエリー タイマーの値を継承するには、継承元の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac-sq-period [seconds]
hostname(config-group-policy)#
```

次に、ステータス クエリー タイマーの値を 1800 秒に変更する例を示します。

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)
```

次の例では、デフォルト グループ ポリシーからステータス クエリー タイマーの値を継承しています。

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)#
```

ステップ 2　（*任意*）NAC の再検証の期間を設定します。セキュリティ アプライアンスは、ポスチャ検証が問題なく終わるたびに、再検証タイマーを始動させます。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。セキュリティ アプライアンスは、それまでと同じ方法でポスチャを再検証します。ポスチャ検証または再検証中にアクセス コントロール サーバが使用できない場合、デフォルトのグループ ポリシーが有効になります。ポスチャを検証する間隔を秒数で入力します。範囲は 300 ～ 86400 秒です。デフォルトの設定は 36000 秒です。

ネットワーク アドミッション コントロールのセッションでポスチャを検証する間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-reval-period** コマンドを使用します。

```
hostname(config-group-policy)# nac-reval-period seconds
hostname(config-group-policy)#
```

再検証タイマーの値をデフォルト グループ ポリシーから継承するには、継承元の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac-reval-period [seconds]
hostname(config-group-policy)#
```

次に、再検証タイマーを 86400 秒に変更する例を示します。

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーから再検証タイマーの値を継承しています。

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)#
```

ステップ 3　（*任意*）NAC のデフォルト ACL を設定します。セキュリティ アプライアンスは、ポスチャを検証できない場合に、選択された ACL に関連付けられているセキュリティ ポリシーを適用します。**none** または拡張 ACL を指定します。デフォルト設定は **none** です。**none** に設定すると、セキュリティ アプライアンスは、ポスチャを検証できなかったときにデフォルトのグループ ポリシーを適用します。

ポスチャを検証できなかったネットワーク アドミッション コントロール セッションのデフォルト ACL として使用される ACL を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-default-acl** コマンドを使用します。

```
hostname(config-group-policy)# nac-default-acl {acl-name | none}
hostname(config-group-policy)#
```

デフォルトのグループ ポリシーから ACL を継承するには、継承元の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac-default-acl [acl-name | none]
hostname(config-group-policy)#
```

このコマンドの要素は次のとおりです。

- *acl-name*：**aaa-server host** コマンドを使用して ASA に設定されている、ポスチャを検証するサーバ グループの名前を指定します。この名前は、そのコマンドに指定された server-tag 変数に一致する必要があります。
- **none**：デフォルト グループ ポリシーからの ACL の継承をディセーブルにし、NAC セッションでポスチャ検証ができなかったときに ACL を適用しません。

NAC はデフォルトでディセーブルになっているため、ASA を通過する VPN トラフィックは、NAC がイネーブルになるまで、NAC デフォルトの ACL の影響は受けません。

次の例では、ポスチャを検証できなかったときに、acl-1 という ACL を適用するように指定しています。

```
hostname(config-group-policy)# nac-default-acl acl-1
hostname(config-group-policy)
```

次の例では、デフォルト グループ ポリシーから ACL を継承しています。

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)
```

次の例では、デフォルト グループ ポリシーからの ACL の継承をディセーブルにし、NAC セッションでポスチャを検証できなかったときに ACL を適用しません。

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

ステップ 4　VPN の NAC 免除を設定します。デフォルトでは、免除リストは空になっています。フィルタ属性のデフォルト値は **none** です。ポスチャ検証を免除するリモート ホストのオペレーティング システム（および ACL）ごとに **vpn-nac-exempt** コマンドを 1 回入力します。

ポスチャ検証を免除するリモート コンピュータのタイプのリストにエントリを追加するには、グループ ポリシー コンフィギュレーション モードで **vpn-nac-exempt** コマンドを使用します。

```
hostname(config-group-policy)# vpn-nac-exempt os "os name" [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

継承をディセーブルにし、すべてのホストをポスチャ検証の対象にするには、**vpn-nac-exempt** のすぐ後ろに **none** キーワードを入力します。

```
hostname(config-group-policy)# vpn-nac-exempt none
hostname(config-group-policy)#
```

免除リストのエントリを削除するには、このコマンドの **no** 形式を使用し、削除するオペレーティング システム（および ACL）を指定します。

```
hostname(config-group-policy)# no vpn-nac-exempt [os "os name"] [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

このグループ ポリシーに関連付けられている免除リストにある全エントリを削除し、デフォルト グループ ポリシーの免除リストを継承するには、キーワードを指定せずにこのコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

このコマンドの構文要素は次のとおりです。

- *acl-name*：ASA のコンフィギュレーションに存在する ACL の名前。
- **disable**：免除リストのエントリを削除せずにディセーブルにします。
- **filter**：（任意）コンピュータのオペレーティング システムの名前が一致したときにトラフィックをフィルタリングするために ACL に適用するフィルタ。
- **none**：このキーワードを **vpn-nac-exempt** のすぐ後ろに入力した場合は、継承がディセーブルになり、すべてのホストがポスチャ検証の対象になります。このキーワードを **filter** のすぐ後ろに入力した場合は、エントリで ACL を指定しないことを示します。
- **OS**：オペレーティング システムをポスチャ検証から免除します。
- *os name*：オペレーティング システムの名前です。引用符は、オペレーティング システムの名前にスペースが入っている場合（"Windows XP" など）だけ必要です。

次に、ポスチャ検証を免除するコンピュータのリストに Windows XP を実行するすべてのホストを追加する例を示します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows XP"
hostname(config-group-policy)
```

次の例では、Windows 98 を実行しているホストのうち、acl-1 という名前の ACL にある ACE に一致するものがすべて免除されます。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次の例では、上と同じエントリが免除リストに追加されますが、ディセーブルにされます。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1 disable
hostname(config-group-policy)
```

次の例では、同じエントリが、ディセーブルかどうかにかかわらず、免除リストから削除されます。

```
hostname(config-group-policy)# no vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次の例では、継承がディセーブルにされ、すべてのホストがポスチャ検証の対象にされます。

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

次に、免除リストからすべてのエントリを削除する例を示します。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

ステップ 5　次のコマンドを入力して、ネットワーク アドミッション コントロールをイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# nac {enable | disable}
hostname(config-group-policy)#
```

デフォルト グループ ポリシーから NAC の設定を継承するには、継承元の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac [enable | disable]
hostname(config-group-policy)#
```

デフォルトでは、NAC はディセーブルになっています。NAC をイネーブルにすると、リモートアクセスでポスチャ検証が必要になります。リモート コンピュータのポスチャが正しいことが確認されると、ACS サーバが ASA で使用するアクセス ポリシーをダウンロードします。NAC は、デフォルトではディセーブルになっています。

Access Control Server はネットワーク上に存在する必要があります。

次の例では、グループ ポリシーに対して NAC をイネーブルにします。

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)#
```

VPN クライアント ファイアウォール ポリシーの設定

*ファイアウォール*は、データの着信パケットと発信パケットをそれぞれ検査して、パケットのファイアウォール通過を許可するか、またはパケットをドロップするかどうかを決定することにより、コンピュータをインターネットから分離して保護します。ファイアウォールは、グループのリモート ユーザがスプリット トンネリングを設定している場合、セキュリティの向上をもたらします。この場合ファイアウォールにより、インターネットまたはユーザのローカル LAN を経由する不正侵入からユーザのコンピュータが保護され、ひいては企業ネットワークも保護されます。VPN クライアントを使用して ASA に接続しているリモート ユーザは、適切なファイアウォール オプションを選択できます。

グループ ポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用して、ASA が IKE トンネル ネゴシエーション中に VPN クライアントに配信するパーソナル ファイアウォール ポリシーを設定します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を入力します。

すべてのファイアウォール ポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを入力します。このコマンドにより、**none** キーワードを指定して **client-firewall** コマンドを入力して作成したヌル ポリシーがあればそれも含めて、設定済みのすべてのファイアウォール ポリシーが削除されます。

ファイアウォール ポリシーがなくなると、ユーザはデフォルトまたはその他のグループ ポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがこのようなファイアウォール ポリシーを継承しないようにするには、**none** キーワードを指定して **client-firewall** コマンドを入力します。

[Add or Edit Group Policy] ダイアログボックスの [Client Firewall] タブでは、追加または変更するグループ ポリシーに対して VPN クライアントのファイアウォール設定を指定できます。

（注） これらのファイアウォール機能を使用できるのは、Microsoft Windows を実行する VPN クライアントだけです。現在、ハードウェア クライアントまたは他（Windows 以外）のソフトウェア クライアントでは、これらの機能は使用できません。

最初のシナリオでは、リモート ユーザの PC 上にパーソナル ファイアウォールがインストールされています。VPN クライアントは、ローカル ファイアウォールで定義されているファイアウォール ポリシーを適用し、そのファイアウォールが実行されていることを確認するためにモニタします。ファイアウォールの実行が停止すると、VPN クライアントは ASA への通信をドロップします。（このファイアウォール適用メカニズムは *Are You There（AYT）* と呼ばれます。VPN クライアントが定期的に「are you there?」メッセージを送信することによってファイアウォールをモニタするからです。応答が返されない場合、VPN クライアントは、ファイアウォールがダウンしたため ASA への接続が終了したことを認識します）ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合もありますが、この方法を使用すれば、ユーザは各自の設定をカスタマイズできます。

第 2 のシナリオでは、VPN クライアント PC のパーソナル ファイアウォールに中央集中型ファイアウォール ポリシーを適用することが選択されることがあります。一般的な例としては、スプリット トンネリングを使用してグループのリモート PC へのインターネット トラフィックをブロックすることが挙げられます。この方法は、トンネルが確立されている間、インターネット経由の侵入から PC を保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、*プッシュ ポリシー* または *Central Protection Policy（CPP）* と呼ばれます。ASA では、VPN クライアントに適用するトラフィック管理ルールのセットを作成し、これらのルールをフィルタに関連付けて、そのフィルタをファイアウォール ポリシーに指定します。ASA は、このポリシーを VPN クライアントまで配信します。その後、VPN クライアントはポリシーをローカル ファイアウォールに渡し、そこでポリシーが適用されます。

AnyConnect クライアント ファイアウォール ポリシーの設定

AnyConnect クライアントのファイアウォール ルールでは、IPv4 および IPv6 のアドレスを指定できます。

前提条件

IPv6 アドレスが指定された統合アクセス ルールを作成します。ACL を作成していない場合は、一般的な操作のコンフィギュレーション ガイドの“Adding ACLs and ACEs” section on page 22-2 を参照してください。

表 4-1

	コマンド	説明
ステップ 1	**webvpn** **例：** hostname(config)# **group-policy ac-client-group attributes** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)#	webvpn グループ ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**anyconnect firewall-rule client-interface {private | public} value** *[RuleName]* **例：** hostname(config-group-webvpn)# **anyconnect fireall-rule client-iterface private value** *ClientFWRule*	プライベートまたはパブリック ネットワーク ルールのアクセス コントロール ルールを指定します。プライベート ネットワーク ルールが、クライアントの VPN 仮想アダプタに適用されるルールです。
ステップ 3	**show runn group-policy** [value] **例：** hostname(config-group-webvpn)# **show runn group-policy FirstGroup** group-policy FirstGroup internal group-policy FirstGroup attributes webvpn anyconnect firewall-rule client-interface private value ClientFWRule	グループ ポリシーのグループ ポリシー属性と webvpn ポリシー属性を表示します。
ステップ 4	（任意） **no anyconnect firewall-rule client-ineterface private value [***RuleName***]** **例：** hostname(config-group-webvpn)#**no anyconnect firewall-rule client-ineterface private value** hostname(config-group-webvpn)#	プライベート ネットワーク ルールからクライアント ファイアウォール ルールが削除されます。

Zone Labs Integrity サーバのサポート

この項では Zone Labs Integrity サーバ（Check Point Integrity サーバとも呼ばれる）について説明し、Zone Labs Integrity サーバをサポートするように ASA を設定する手順の例を示します。Integrity サーバは、リモート PC 上でセキュリティ ポリシーを設定および実行するための中央管理ステーションです。リモート PC が Integrity サーバによって指定されたセキュリティ ポリシーと適合しない場合、Integrity サーバおよびASAが保護するプライベート ネットワークへのアクセス権が与えられません。

この項では、次のトピックについて取り上げます。

- 「Integrity サーバと ASA とのインタラクションの概要」（P.4-80）
- 「Integrity サーバのサポートの設定」（P.4-80）

Integrity サーバと ASA とのインタラクションの概要

VPN クライアント ソフトウェアと Integrity クライアント ソフトウェアは、リモート PC 上に共に常駐しています。次の手順では、リモート PC と企業のプライベート ネットワーク間にセッションを確立する際のリモート PC、ASA、および Integrity サーバのアクションをまとめます。

1. VPN クライアント ソフトウェア（Integrity クライアント ソフトウェアと同じリモート PC に常駐）は、ASA に接続し、それがどのタイプのファイアウォール クライアントであるかを ASA に知らせます。
2. ASA でクライアント ファイアウォールのタイプが承認されると、ASA から Integrity クライアントに Integrity サーバのアドレス情報が返されます。
3. ASA はプロキシとして動作し、Integrity クライアントは Integrity サーバとの制限付き接続を確立します。制限付き接続は、Integrity クライアントと Integrity サーバの間だけで確立されます。
4. Integrity サーバは、Integrity クライアントが指定されたセキュリティ ポリシーに準拠しているかどうかを特定します。Integrity クライアントがセキュリティ ポリシーに準拠している場合、Integrity サーバから ASA に対して、接続を開いて接続の詳細をクライアントに提供するように指示されます。
5. リモート PC では、VPN クライアントから Integrity クライアントに接続の詳細が渡され、ポリシーの実施がただちに開始されること、また、Integrity クライアントがプライベート ネットワークに接続できることが知らされます。
6. VPN 接続が確立すると、Integrity サーバは、クライアント ハートビート メッセージを使用して Integrity クライアントの状態のモニタを続けます。

（注） ユーザ インターフェイスが最大 5 つの Integrity サーバのコンフィギュレーションをサポートしている場合でも、現在のリリースの ASA が一度にサポートする Integrity サーバは 1 つです。アクティブな Integrity サーバに障害が発生した場合は、ASA 上に別の Integrity サーバを設定してから、VPN クライアント セッションを再度確立します。

Integrity サーバのサポートの設定

この項では、Zone Labs Integrity サーバをサポートするように ASA を設定するための手順の例を示します。この手順には、アドレス、ポート、接続障害タイムアウトおよび障害の状態、および SSL 証明書パラメータの設定が含まれます。

Integrity サーバを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**zonelabs-Integrity server-address** {*hostname1* | *ip-address1*} **例：** `hostname(config)# zonelabs-Integrity server-address 10.0.0.5`	IP アドレス 10.0.0.5 を使用して Integrity サーバを設定します。
ステップ 2	**zonelabs-integrity port** *port-number* **例：** `hostname(config)# zonelabs-integrity port 300`	ポート 300 を指定します（デフォルト ポートは 5054 です）。

	コマンド	目的
ステップ 3	**zonelabs-integrity interface** *interface* **例：** `hostname(config)# zonelabs-integrity interface inside`	Integrity サーバとの通信用に内部インターフェイスを指定します。
ステップ 4	**zonelabs-integrity fail-timeout** *timeout* **例：** `hostname(config)# zonelabs-integrity fail-timeout 12`	Integrity サーバに障害があることを宣言して VPN クライアント接続を閉じる前に、ASA がアクティブまたはスタンバイ Integrity サーバからの応答を 12 秒間待つようにします。 **（注）** ASA と Integrity サーバの間の接続で障害が発生した場合、エンタープライズ VPN が Integrity サーバの障害によって中断されないように、デフォルトで VPN クライアント接続は開いたままになります。ただし、Zone Labs Integrity サーバに障害が発生した場合、必要に応じて VPN 接続を閉じることができます。
ステップ 5	**zonelabs-integrity fail-close** **例：** `hostname(config)# zonelabs-integrity fail-close`	ASA と Zone Labs Integrity サーバとの接続に障害が発生した場合に VPN クライアントとの接続が閉じるよう、ASA を設定します。
ステップ 6	**zonelabs-integrity fail-open** **例：** `hostname(config)# zonelabs-integrity fail-open`	設定された VPN クライアント接続の障害状態をデフォルトに戻して、クライアント接続が開いたままになるようにします。
ステップ 7	**zonelabs-integrity ssl-certificate-port** *cert-port-number* **例：** `hostname(config)# zonelabs-integrity ssl-certificate-port 300`	Ipntegrity サーバが ASA のポート 300（デフォルトはポート 80）に接続して、サーバ SSL 証明書を要求するように指定します。
ステップ 8	**zonelabs-integrity ssl-client-authentication {enable | disable}** **例：** `hostname(config)# zonelabs-integrity ssl-client-authentication enable`	サーバの SSL 証明書は常に認証されますが、Integrity サーバのクライアント SSL 証明書も認証されるように指定します。

ファイアウォール クライアント タイプを Zone Labs Integrity タイプに設定するには、次のコマンドを入力します。

コマンド	目的
client-firewall {opt | req} zonelabs-integrity **例：** hostname(config)# client-firewall req zonelabs-integrity	詳細については、「VPN クライアント ファイアウォール ポリシーの設定」（P.4-77）を参照してください。ファイアウォールのタイプが **zonelabs-integrity** の場合、Integrity サーバによってこれらのポリシーが決定されるため、ファイアウォール ポリシーを指定するコマンド引数は使用されません。

クライアント ファイアウォールのパラメータの設定

次のコマンドを入力して、適切なクライアント ファイアウォールのパラメータを設定します。各コマンドに設定できるインスタンスは 1 つだけです。詳細については、「VPN クライアント ファイアウォール ポリシーの設定」（P.4-77）を参照してください。

Cisco 統合ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated acl-in ACL
acl-out ACL
```

Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

ファイアウォールなし

```
hostname(config-group-policy)# client-firewall none
```

カスタム ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num product-id
num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

Zone Labs ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```

（注） ファイアウォールのタイプを **zonelabs-integrity** にする場合は、引数を指定しないでください。ポリシーは、Zone Labs Integrity サーバによって決められます。

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm policy {AYT
| CPP acl-in ACL acl-out ACL}

hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarmorpro policy
{AYT | CPP acl-in ACL acl-out ACL}

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in ACL acl-out
ACL}
```

Sygate Personal ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro
hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

Network Ice、Black Ice ファイアウォール：

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

表 4-4　client-firewall コマンドのキーワードと変数

パラメータ	説明
acl-in *ACL*	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out *ACL*	クライアントが発信トラフィックに使用するポリシーを指定します。
AYT	クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御することを指定します。ASA はファイアウォールが実行されていることを確認します。「Are You There?」と表示され、応答がない場合は、ASA によりトンネルが切断されます。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。
cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。
CPP	VPN クライアントのファイアウォール ポリシーのソースとして Policy Pushed を指定します。
custom	カスタム ファイアウォール タイプを指定します。
description *string*	ファイアウォールの説明を示します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーにヌル値を設定して、ファイアウォール ポリシーを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからファイアウォール ポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。
req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。
sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォールのベンダーを指定します。
zonelabs-integrity	Zone Labs Integrity サーバ ファイアウォール タイプを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。

表 4-4　client-firewall コマンドのキーワードと変数 （続き）

zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

次に、FirstGroup という名前のグループ ポリシーについて、Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

クライアント アクセス ルールの設定

グループ ポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用して、ASA を介して IPsec で接続できるリモート アクセス クライアントのタイプとバージョンを制限するルールを設定します。次のガイドラインに従ってルールを作成します。

- ルールを定義しない場合、ASA はすべての接続タイプを許可します。
- クライアントがいずれのルールにも一致しない場合、ASA は接続を拒否します。拒否ルールを定義する場合は、許可ルールも 1 つ以上定義する必要があります。定義しない場合、ASA はすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントのどちらでも、タイプとバージョンは **show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。
- ***** 文字はワイルドカードです。ワイルドカードは各ルールで複数回入力することができます。たとえば、**client-access rule 3 deny type * version 3.*** では、バージョン 3.x のソフトウェア リリースを実行しているすべてのクライアント タイプを拒否する、プライオリティ 3 のクライアント アクセス ルールが作成されます。
- 1 つのグループ ポリシーにつき最大 25 のルールを作成できます。
- ルール セット全体に対して 255 文字の制限があります。
- クライアントのタイプまたはバージョン（あるいはその両方）を送信しないクライアントには、n/a を入力できます。

ルールを削除するには、このコマンドの **no** 形式を入力します。このコマンドは、次のコマンドと同等です。

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version
4.0
```

すべてのルールを削除するには、引数を指定せずに **no client-access-rule** コマンドを入力します。これにより、**none** キーワードを指定して **client-access-rule** コマンドを発行して作成したヌル ルールがあればそれも含めて、設定済みのすべてのルールが削除されます。

デフォルトでは、アクセス ルールはありません。クライアント アクセス ルールがない場合、ユーザはデフォルトのグループ ポリシー内に存在するすべてのルールを継承します。

ユーザがクライアント アクセス ルールを継承しないようにするには、**none** キーワードを指定して **client-access-rule** コマンドを入力します。このコマンドの結果、すべてのタイプとバージョンのクライアントが接続できるようになります。

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type type
version {version | none}
```

```
hostname(config-group-policy)# no client-access rule [priority {permit | deny} type type
version version]
```

表 4-5 に、これらのコマンドのキーワードとパラメータの意味を示します。

表 4-5　client-access rule コマンドのキーワードと変数

パラメータ	説明
deny	特定のタイプとバージョンのデバイスの接続を拒否します。
none	クライアント アクセス ルールを許可しません。client-access-rule をヌル値に設定します。これにより制限が許可されなくなります。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンのデバイスの接続を許可します。
priority	ルールのプライオリティを決定します。最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアントのタイプとバージョン（またはこのいずれか）に一致する最も小さい整数のルールが、適用されるルールとなります。プライオリティの低いルールに矛盾がある場合、ASA はそのルールを無視します。
type *type*	VPN 3002 などの自由形式のストリングを使用して、デバイス タイプを指定します。文字列は、**show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。
version *version*	7.0 などの自由形式のストリングを使用して、デバイス バージョンを指定します。文字列は、**show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。

次に、FirstGroup という名前のグループ ポリシーのクライアント アクセス ルールを作成する例を示します。これらのルールは、バージョン 4.x のソフトウェアを実行する Cisco VPN Client を許可し、すべての Windows NT クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client" version 4.*
```

（注）　「type」フィールドは、任意の値が許可される自由形式の文字列ですが、その値は、接続時にクライアントから ASA に送信される固定値と一致している必要があります。

グループ ポリシーのクライアントレス SSL VPN セッションの属性の設定

クライアントレス SSL VPN によってユーザは、Web ブラウザを使用して ASA へのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。クライアントレス SSL VPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。クライアントレス SSL VPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間のセキュアな接続を提供します。ASA はプロキシで処理する必要がある接続を認識し、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、クライアントレス SSL VPN はディセーブルになっています。

特定の内部グループ ポリシー用のクライアントレス SSL VPN のコンフィギュレーションを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 モードから入る webvpn モードでは、クライアントレス SSL VPN セッションのグローバル設定を構成できます。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 モードから入ります）を使用すると、クライアントレス SSL VPN セッションに固有のグループ ポリシーのコンフィギュレーションをカスタマイズできます。

グループ ポリシー webvpn コンフィギュレーション モードでは、すべての機能の設定を継承するか、または次のパラメータをカスタマイズするかどうかを指定できます。各パラメータについては、後述の項で説明します。

- customizations
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server（シングル サインオン サーバ）
- auto-signon
- deny message
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

多くの場合、クライアントレス SSL VPN の設定の一部として webvpn 属性を定義した後、グループ ポリシーの webvpn 属性を設定するときにこれらの定義を特定のグループに適用します。グループ ポリシー コンフィギュレーション モードで **webvpn** コマンドを使用して、グループ ポリシー webvpn コンフィギュレーション モードに入ります。グループ ポリシー用の webvpn コマンドは、ファイル、URL、および TCP アプリケーションへのクライアントレス SSL VPN セッション経由のアクセスを定義します。ACL およびフィルタリングするトラフィックのタイプも指定します。クライアントレス SSL VPN は、デフォルトではディセーブルになっています。クライアントレス SSL VPN セッションの属性の設定の詳細については、*第 11 章「クライアントレス SSL VPN の設定」*の説明を参照してください。

グループ ポリシー webvpn コンフィギュレーション モードで入力されたすべてのコマンドを削除するには、このコマンドの **no** 形式を入力します。これらの webvpn コマンドは、設定元のユーザ名またはグループ ポリシーに適用されます。

```
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# no webvpn
```

次の例は、FirstGroup という名前のグループ ポリシーのグループ ポリシー webvpn コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

カスタマイゼーションの適用

カスタマイゼーションによって、ログイン時にユーザに表示されるウィンドウ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、クライアントレス SSL VPN の設定の一部として設定します。定義済みの Web ページ カスタマイゼーションを適用して、ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するには、グループ ポリシー webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-group-webvpn)# customization customization_name
hostname(config-group-webvpn)#
```

たとえば、blueborder という名前のカスタマイゼーションを使用するには、次のコマンドを入力します。

```
hostname(config-group-webvpn)# customization blueborder
hostname(config-group-webvpn)#
```

カスタマイゼーション自体は、webvpn モードで **customization** コマンドを入力して設定します。

次の例は、123 という名前のカスタマイゼーションを最初に確立するコマンド シーケンスを示しています。このコマンド シーケンスによって、パスワード プロンプトが定義されます。次の例は、testpolicy という名前のグループ ポリシーを定義し、**customization** コマンドを使用して、クライアントレス SSL VPN セッションに 123 という名前のカスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# group-policy testpolicy nopassword
hostname(config)# group-policy testpolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# customization value 123
hostname(config-group-webvpn)#
```

「拒否」メッセージの指定

グループ ポリシー webvpn コンフィギュレーション モードで、**deny-message** コマンドを入力すると、クライアントレス SSL VPN セッションに正常にログインできるが VPN 特権を持たないリモート ユーザに送信されるメッセージを指定できます。

```
hostname(config-group-webvpn)# deny-message value "message"
hostname(config-group-webvpn)# no deny-message value "message"
hostname(config-group-webvpn)# deny-message none
```

no deny-message value コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

no deny-message none コマンドは、接続プロファイル ポリシーのコンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

メッセージは、特殊文字、スペース、および句読点を含む英数字で最大 491 文字まで指定できますが、囲みの引用符はカウントされません。テキストは、ログイン時にリモート ユーザのブラウザに表示されます。**deny-message value** コマンドへのストリングの入力時は、コマンドがラップしている場合でも引き続き入力します。

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」

次の例の最初のコマンドは、group2 という名前の内部グループ ポリシーを作成します。後続のコマンドは、そのポリシーに関連付けられている webvpn 拒否メッセージが含まれた属性を変更します。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
you have not been granted rights to use the VPN features. Contact your administrator for
more information."
hostname(config-group-webvpn)
```

グループ ポリシーのクライアントレス SSL VPN セッションのフィルタ属性の設定

webvpn モードで **html-content-filter** コマンドを使用して、このグループ ポリシーのクライアントレス SSL VPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするかどうかを指定します。HTML フィルタリングは、デフォルトでディセーブルです。

コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**none** キーワードを指定して **html-content-filter** コマンドを発行して作成したヌル値を含めて、すべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。HTML コンテンツ フィルタを継承しないようにするには、**none** キーワードを指定して **html-content-filter** コマンドを入力します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

```
hostname(config-group-webvpn)# html-content-filter {java | images | scripts | cookies |
none}

hostname(config-group-webvpn)# no html-content-filter [java | images | scripts | cookies |
none]
```

表 4-6 に、このコマンドで使用するキーワードの意味を示します。

表 4-6　filter コマンドのキーワード

キーワード	意味
cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを提供します。
images	イメージへの参照を削除します（<IMG> タグを削除します）。
java	Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> の各タグを削除）。
none	フィルタリングを行わないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
scripts	スクリプトへの参照を削除します（<SCRIPT> タグを削除します）。

次に、FirstGroup という名前のグループ ポリシーに対して JAVA と ActiveX、クッキー、およびイメージのフィルタリングを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
hostname(config-group-webvpn)#
```

ユーザ ホームページの指定

グループ ポリシー webvpn コンフィギュレーション モードで **homepage** コマンドを使用して、このグループのユーザのログイン時に表示される Web ページの URL を指定します。デフォルトのホームページはありません。

homepage none コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。ホームページを継承しないようにするには、**homepage none** コマンドを入力します。

none キーワードは、クライアントレス SSL VPN セッションのホームページがないことを示します。これにより、ヌル値が設定されてホームページが拒否され、ホームページが継承されなくなります。

キーワード *value* の後ろの **url-string** 変数で、ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

```
hostname(config-group-webvpn)# homepage {value url-string | none}
hostname(config-group-webvpn)# no homepage
hostname(config-group-webvpn)#
```

自動サインオンの設定

auto-signon コマンドは、クライアントレス SSL VPN セッションのユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のためにログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名がグループに優先し、グループがグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、使用する認証の対象範囲によって異なります。

特定のサーバへの特定のユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URL を指定してこのコマンドの **no** 形式を使用します。すべてのサーバへの認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。

次の例では、グループ ポリシー webvpn コンフィギュレーション モードで入力し、基本認証を使用して、10.1.1.0 から 10.1.1.255 の範囲の IP アドレスを持つサーバへの anyuser という名前のユーザの自動サインオンを設定します。

次のコマンド例では、基本認証または NTLM 認証を使用して、クライアントレス SSL VPN セッションのユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
hostname(config-group-webvpn)#
```

次のコマンド例では、基本認証または NTLM 認証を使用して、クライアントレス SSL VPN セッションのユーザに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type all
hostname(config-group-webvpn)#
```

クライアントレス SSL VPN セッションに使用する ACL の指定

webvpn モードで **filter** コマンドを使用して、このグループ ポリシーまたはユーザ名でクライアントレス SSL VPN セッションに使用する ACL の名前を指定します。**filter** コマンドを入力して指定するまで、クライアントレス SSL VPN ACL は適用されません。

filter none コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

filter コマンドを入力して指定するまで、クライアントレス SSL VPN セッションの ACL は適用されません。

ACL を設定して、このグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを入力して、これらの ACL をクライアントレス SSL VPN トラフィックに適用します。

```
hostname(config-group-webvpn)# filter {value ACLname | none}
hostname(config-group-webvpn)# no filter
```

none キーワードは、**webvpntype** ACL がないことを示します。これにより、ヌル値が設定されて ACL が拒否され、別のグループ ポリシーから ACL が継承されなくなります。

キーワード *value* の後ろの **ACLname** 文字列で、事前に設定されている ACL の名前を指定します。

（注） クライアントレス SSL VPN セッションは、**vpn-filter** コマンドで定義されている ACL を使用しません。

次に、FirstGroup という名前のグループ ポリシーの、*acl_in* という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
hostname(config-group-webvpn)#
```

URL リストの適用

グループ ポリシーのクライアントレス SSL VPN ホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して、1 つ以上の名前付きリストを作成する必要があります。特定のグループ ポリシーにクライアントレス SSL VPN セッションのサーバと URL のリストを適用して、特定のグループ ポリシーのリストにある URL にアクセスできるようにするには、グループ ポリシー webvpn コンフィギュレーション モードで **url-list** コマンドを実行する際に、作成するリスト（複数可）の名前を使用します。デフォルトの URL リストはありません。

url-list none コマンドを使用して作成したヌル値を含めて、リストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。URL リストを継承しないようにするには、**url-list none** コマンドを入力します。コマンドを 2 回使用すると、先行する設定が上書きされます。

```
hostname(config-group-webvpn)# url-list {value name | none} [index]
hostname(config-group-webvpn)# no url-list
```

表 4-7 に、**url-list** コマンドのパラメータとその意味を示します。

表 4-7　url-list コマンドのキーワードと変数

パラメータ	意味
index	ホームページ上の表示のプライオリティを指定します。
none	URL リストにヌル値を設定します。デフォルトまたは指定したグループ ポリシーからリストが継承されないようにします。
value *name*	設定済み URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

次の例では、FirstGroup という名前のグループ ポリシーに FirstGroupURLs という名前の URL リストを設定し、これがホームページに表示される最初の URL リストになるように指定します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
hostname(config-group-webvpn)#
```

グループ ポリシーの ActiveX Relay のイネーブル化

ActiveX Relay を使用すると、クライアントレス SSL VPN セッションを確立したユーザが、ブラウザを使用して Microsoft Office アプリケーションを起動できるようになります。アプリケーションは、セッションを使用して Microsoft Office ドキュメントのダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。

クライアントレス SSL VPN セッションで ActiveX コントロールをイネーブルまたはディセーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードで次のコマンドを入力します。

activex-relay {**enable** | **disable**}

デフォルト グループ ポリシーから **activex-relay** コマンドを継承するには、次のコマンドを入力します。

no activex-relay

次のコマンドは、特定のグループ ポリシーに関連付けられているクライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

グループ ポリシーのクライアントレス SSL VPN セッションのアプリケーション アクセスのイネーブル化

このグループ ポリシーのアプリケーション アクセスをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート フォワーディングは、デフォルトではディセーブルになっています。

グループ ポリシー webvpn コンフィギュレーション モードで **port-forward** コマンドを入力し、アプリケーション アクセスをイネーブルにする前に、クライアントレス SSL VPN セッションでユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

port-forward none コマンドを発行して作成したヌル値を含めて、グループ ポリシー コンフィギュレーションからポート転送属性を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、リストを別のグループ ポリシーから継承できます。ポート転送リストを継承しないよ

うにするには、**none** キーワードを指定して **port-forward** コマンドを入力します。**none** キーワードは、フィルタリングが実行されないことを示します。これにより、ヌル値が設定されてフィルタリングが拒否され、フィルタリング値が継承されなくなります。

このコマンドの構文は次のとおりです。

```
hostname(config-group-webvpn)# port-forward {value listname | none}
hostname(config-group-webvpn)# no port-forward
```

キーワード *value* の後ろの **listname** 文字列で、クライアントレス SSL VPN セッションのユーザがアクセスできるアプリケーションのリストを指定します。webvpn コンフィギュレーション モードで port-forward コマンドを入力し、このリストを定義します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

次の例は、FirstGroup という名前の内部グループ ポリシーに *ports1* というポート転送リストを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
hostname(config-group-webvpn)#
```

ポート転送表示名の設定

グループ ポリシー webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用して、特定のユーザまたはグループ ポリシーでエンド ユーザへの TCP ポート転送を識別する表示名を設定します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するには、このコマンドの **no** 形式を入力します。**no** オプションは、デフォルト名の、Application Access を復元します。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。このコマンドの構文は次のとおりです。

```
hostname(config-group-webvpn)# port-forward-name {value name | none}
hostname(config-group-webvpn)# no port-forward-name
```

次の例は、*FirstGroup* という名前の内部グループ ポリシーに Remote Access TCP Applications という名前を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
hostname(config-group-webvpn)#
```

セッション タイマーを更新のために無視する最大オブジェクト サイズの設定

ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回路が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定したサイズ以下のすべてのメッセージをキープアライブ メッセージと見なし、セッション タイマーの更新時にトラフィックと見なさないよう ASA に指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

トランザクションごとに無視する HTTP/HTTPS トラフィックの上限を指定するには、グループ ポリシー属性 webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#

The no form of the command removes this specification from the configuration:
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

HTTP 圧縮の指定

グループ ポリシー webvpn モードで、**http-comp** コマンドを入力して、特定のグループまたはユーザのクライアントレス SSL VPN セッションで HTTP データの圧縮をイネーブルにします。

```
hostname(config-group-webvpn)# http-comp {gzip | none}
hostname(config-group-webvpn)#
```

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# no http-comp {gzip | none}
hostname(config-group-webvpn)#
```

このコマンドの構文は次のとおりです。

- **gzip**：圧縮がグループまたはユーザに対してイネーブルになることを指定します。768 ビットは、デフォルト値です。
- **none**：圧縮がグループまたはユーザに対してディセーブルになることを指定します。

クライアントレス SSL VPN セッションの場合、グローバル コンフィギュレーション モードで設定された **compression** コマンドは、グループ ポリシー モードおよびユーザ名 webvpn モードで設定された **http-comp** コマンドを上書きします。

次に、グローバル ポリシー sales の圧縮をディセーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
hostname(config-group-webvpn)#
```

SSO サーバの指定

クライアントレス SSL VPN セッションだけに使用できるシングル サインオンのサポートを使用すると、ユーザはユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。グループ ポリシー webvpn モードで **sso-server value** コマンドを入力すると、SSO サーバをグループ ポリシーに割り当てることができます。

グループ ポリシーに SSO サーバを割り当てるには、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 **sso-server value** コマンドを使用します。このコマンドでは、コンフィギュレーションに CA SiteMinder コマンドが含まれている必要があります。

```
hostname(config-group-webvpn)# sso-server value server_name
hostname(config-group-webvpn)#
```

割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。デフォルト ポリシーが継承されないようにするには、**sso-server none** コマンドを使用します。

```
hostname(config-group-webvpn)# sso-server {value server_name | none}
hostname(config-group-webvpn)# [no] sso-server value server_name
```

SSO サーバに割り当てられているデフォルト ポリシーは DfltGrpPolicy です。

次の例では、グループ ポリシー「my-sso-grp-pol」を作成して、「example」という名前の SSO サーバに割り当てます。

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
```

```
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

ユーザ属性の設定

この項では、ユーザ属性とその設定方法について説明します。内容は次のとおりです。

デフォルトでは、ユーザは、割り当てられているグループ ポリシーからすべてのユーザ属性を継承します。また、ASA では、ユーザ レベルで個別に属性を割り当て、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ができます。たとえば、すべてのユーザに営業時間内のアクセスを許可し、特定のユーザに 24 時間のアクセスを許可するグループ ポリシーを指定することができます。

ユーザ名のコンフィギュレーションの表示

グループ ポリシーから継承したデフォルト値も含めて、すべてのユーザ名のコンフィギュレーションを表示するには、次のように、**all** キーワードを指定して **show running-config username** コマンドを入力します。

```
hostname# show running-config all username
hostname#
```

このコマンドは、すべてのユーザまたは特定のユーザ（ユーザ名を指定した場合）の 暗号化されたパスワードと特権レベルを表示します。**all** キーワードを省略すると、明示的に設定された値だけがこのリストに表示されます。次の例は、このコマンドで testuser というユーザを指定した場合の出力を示します。

```
hostname# show running-config all username testuser
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

個々のユーザの属性の設定

特定のユーザを設定するには、**username** コマンドを使用してユーザ名モードに入り、ユーザにパスワード（パスワードなしも可）と属性を割り当てます。指定しなかったすべての属性は、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** コマンドを使用して入力されたユーザで構成されています。**login** コマンドでは、このデータベースを認証用に使用します。ユーザを ASA データベースに追加するには、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、削除するユーザ名を指定して、このコマンドの **no** 形式を使用します。すべてのユーザ名を削除するには、ユーザ名を指定せずに **clear configure username** コマンドを使用します。

ユーザのパスワードと特権レベルの設定

ユーザにパスワードと特権レベルを割り当てるには、**username** コマンドを入力します。**nopassword** キーワードを入力すると、このユーザにパスワードが不要であることを指定できます。パスワードを指定する場合は、そのパスワードを暗号化形式で保存するかどうかを指定できます。

オプションの **privilege** キーワードにより、このユーザの特権レベルを設定できます。特権レベルの範囲は 0（最低）～ 15 です。一般に、システム管理者は最高の特権レベルを持ちます。デフォルトのレベルは 2 です。

```
hostname(config)# username name {nopassword | password password [encrypted]} [privilege
priv_level]}

hostname(config)# no username [name]
```

表 4-8 に、このコマンドで使用するキーワードと変数の意味を示します。

表 4-8　username コマンドのキーワードと変数

キーワード / 変数	意味
encrypted	パスワードの暗号化を指定します。
name	ユーザの名前を指定します。
nopassword	このユーザにパスワードが必要ないことを示します。
password *password*	このユーザにパスワードが存在することを示し、パスワードを指定します。
privilege *priv_level*	このユーザの特権レベルを設定します。範囲は 0 ～ 15 です。この数値が低いほど、コマンドの使用や ASA の管理に関する機能が限定されます。デフォルトの特権レベルは 2 です。システム管理者の通常の特権レベルは 15 です。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。すべての値を明示的に設定する必要があります。

次の例は、暗号化されたパスワードが pw_12345678 で、特権レベルが 12 の anyuser という名前のユーザを設定する方法を示しています。

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege 12
hostname(config)#
```

ユーザ属性の設定

ユーザのパスワード（存在する場合）と特権レベルの設定後は、その他の属性を設定します。これらは任意の順序で設定できます。任意の属性と値のペアを削除するには、このコマンドの **no** 形式を入力します。

attributes キーワードを指定して **username** コマンドを入力して、ユーザ名モードに入ります。

```
hostname(config)# username name attributes
hostname(config-username)#
```

プロンプトが変化し、新しいモードになったことが示されます。これで属性を設定できます。

VPN ユーザ属性の設定

VPN ユーザ属性は、次の項で説明するように、VPN 接続に固有の値を設定します。

継承の設定

ユーザが、それまでにユーザ名レベルで設定されていない属性の値をグループ ポリシーから継承するようにできます。このユーザが属性を継承するグループ ポリシーの名前を指定するには、**vpn-group-policy** コマンドを入力します。デフォルトでは、VPN ユーザにはグループ ポリシーが関連付けられていません。

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

ユーザ名モードで使用できる属性の場合、ユーザ名モードで設定すると、特定のユーザに関してグループ ポリシーにおける属性の値を上書きできます。

次に、FirstGroup という名前のグループ ポリシーから属性を使用するように anyuser という名前のユーザを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

アクセス時間の設定

設定済みの time-range ポリシーの名前を指定して、このユーザがシステムへのアクセスを許可される時間を関連付けます。

この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、他のグループ ポリシーから time-range 値を継承できます。値を継承しないようにするには、**vpn-access-hours none** コマンドを入力します。デフォルトでは、アクセスは無制限です。

```
hostname(config-username)# vpn-access-hours value {time-range | none}
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

次の例は、anyuser という名前のユーザを 824 と呼ばれる time-range ポリシーに関連付ける方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

最大同時ログイン数の設定

このユーザに許可される同時ログインの最大数を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトの同時ログイン数は、3 です。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)# vpn-session-timeout alert-interval none
```

（注） 同時ログインの最大数の制限は非常に大きなものですが、複数の同時ログインを許可すると、セキュリティが低下し、パフォーマンスに影響を及ぼすことがあります。

次の例は、anyuser という名前のユーザに最大 4 つの同時ログインを許可する方法を示しています。

```
hostname(config)# username anyuser attributes
```

```
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

アイドル タイムアウトの設定

アイドル タイムアウト期間を分単位で指定するか、**none** を入力してアイドル タイムアウトをディセーブルにします。この期間中に接続上で通信アクティビティがない場合、ASA は接続を終了します。任意でアラート間隔を設定することも、1 分のデフォルト設定のままにすることもできます。

範囲は 1 ～ 35791394 分です。デフォルトは 30 分です。無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**none** キーワードを指定して **vpn-idle-timeout** コマンドを入力します。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-idle-timeout {minutes | none} alert-interval {minutes}
hostname(config-username)# no vpn-idle-timeout alert-interval
hostname(config-username)# vpn-idle-timeout alert-interval none
```

次の例は、anyuser という名前のユーザに 15 分の VPN アイドル タイムアウトおよび 3 分のアラート間隔を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout 30 alert-interval 3
hostname(config-username)#
```

最大接続時間の設定

ユーザの最大接続時間を分単位で指定するか、**none** を入力して無制限の接続時間を許可し、この属性の値を継承しないようにします。この期間が終了すると、ASA は接続を終了します。任意でアラート間隔を設定することも、1 分のデフォルト設定のままにすることもできます。

範囲は 1 ～ 35791394 分です。デフォルトのタイムアウトはありません。無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**none** キーワードを指定して **vpn-session-timeout** コマンドを入力します。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-session-timeout {minutes | none} alert-interval {minutes}
hostname(config-username)# no vpn-session-timeout alert-interval
hostname(config-username)#
```

次の例は、anyuser という名前のユーザに 180 分の VPN セッション タイムアウトを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180 alert-interval {minutes}
hostname(config-username)#
```

ACL フィルタの適用

VPN 接続用のフィルタとして使用する、事前に設定されたユーザ固有の ACL の名前を指定します。ACL を拒否し、グループ ポリシーから ACL を継承しないようにするには、none キーワードを指定して **vpn-filter** コマンドを入力します。**vpn-filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。このコマンドには、デフォルトの動作や値はありません。

ACL を設定して、このユーザについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを使用して、それらの ACL を適用します。

```
hostname(config-username)# vpn-filter {value ACL_name | none}
hostname(config-username)# no vpn-filter
hostname(config-username)#
```

（注）　クライアントレス SSL VPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次に、anyuser という名前のユーザの、acl_vpn という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

IPv4 アドレスとネットマスクの指定

特定のユーザに割り当てる IP アドレスとネットマスクを指定します。IP アドレスを削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)
```

次に、anyuser という名前のユーザに IP アドレス 10.92.166.7 を設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)
```

前の手順で指定した IP アドレスに使用するネットワーク マスクを指定します。**no vpn-framed-ip-address** コマンドを使用した場合は、ネットワーク マスクを指定しないでください。サブネット マスクを削除するには、このコマンドの **no** 形式を入力します。デフォルトの動作や値はありません。

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

次の例は、anyuser という名前のユーザに、サブネット マスク 255.255.255.254 を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

IPv6 アドレスとネットマスクの指定

特定のユーザに割り当てる IPv6 アドレスとネットマスクを指定します。IP アドレスを削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-framed-ipv6-address {ip_address}
hostname(config-username)# no vpn-framed-ipv6-address
hostname(config-username)
```

次に、anyuser という名前のユーザに IP アドレスとネットマスク 2001::3000:1000:2000:1/64 を設定する例を示します。このアドレスは、プレフィックス値 2001:0000:0000:0000 およびインターフェイス ID 3000:1000:2000:1 を示しています。

```
hostname(config)# username anyuser attributes
```

```
hostname(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
hostname(config-username)
```

トンネル プロトコルの指定

このユーザが使用できる VPN トンネルのタイプ（IPsec またはクライアントレス SSL VPN）を指定します。デフォルトは、デフォルト グループ ポリシーから取得される値で、IPsec になります。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPsec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPsec]
hostname(config-username)
```

このコマンドのパラメータの値は、次のとおりです。

- **IPsec**：2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IPsec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **webvpn**：HTTPS 対応 Web ブラウザ経由でリモート ユーザにクライアントレス SSL VPN アクセスを提供します。クライアントは不要です。

このコマンドを入力して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

次の例は、anyuser という名前のユーザにクライアントレス SSL VPN および IPsec トンネリング モードを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPsec
hostname(config-username)
```

リモート ユーザ アクセスの制限

value キーワードを指定して **group-lock** 属性を設定することにより、指定した既存の接続プロファイルだけを介してアクセスするようにリモート ユーザを制限します。group-lock は、VPN クライアントで設定されたグループが、そのユーザが割り当てられている接続プロファイルと同じかどうかをチェックすることによって、ユーザを制限します。同一ではなかった場合、ASA はユーザによる接続を禁止します。グループ ロックを設定しなかった場合、ASA は、割り当てられているグループに関係なくユーザを認証します。

group-lock 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値をグループ ポリシーから継承できます。group-lock をディセーブルにし、デフォルトまたは指定されたグループ ポリシーから group-lock の値を継承しないようにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

次の例は、anyuser という名前のユーザにグループ ロックを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel-group-name
hostname(config-username)
```

ソフトウェア クライアント ユーザのパスワード保存のイネーブル化

ユーザがログイン パスワードをクライアント システム上に保存するかどうかを指定します。パスワード保存は、デフォルトでディセーブルになっています。パスワード保存は、セキュアなサイトにあることがわかっているシステムでのみイネーブルにします。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを入力します。password-storage 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、password-storage の値をグループ ポリシーから継承できます。

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

このコマンドは、ハードウェア クライアントのインタラクティブ ハードウェア クライアント認証または個別ユーザ認証には関係ありません。

次の例は、anyuser という名前のユーザでパスワード保存をイネーブルにする方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
hostname(config-username)
```

特定ユーザのクライアントレス SSL VPN アクセスの設定

次の各項では、特定のユーザのクライアントレス SSL VPN セッションの設定をカスタマイズする方法について説明します。ユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用して、ユーザ名 webvpn コンフィギュレーション モードに入ります。クライアントレス SSL VPN によってユーザは、Web ブラウザを使用して ASA へのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。クライアントレス SSL VPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。クライアントレス SSL VPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間のセキュアな接続を提供します。ASA はプロキシで処理する必要がある接続を認識し、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。

ユーザ名 webvpn コンフィギュレーション モードのコマンドは、ファイル、URL、および TCP アプリケーションへのクライアントレス SSL VPN セッション経由のアクセスを定義します。ACL およびフィルタリングするトラフィックのタイプも指定します。クライアントレス SSL VPN は、デフォルトではディセーブルになっています。これらの **webvpn** コマンドは、設定を行ったユーザ名にだけ適用されます。プロンプトが変化して、ユーザ名 webvpn コンフィギュレーション モードに入ったことがわかります。

```
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

ユーザ名 webvpn コンフィギュレーション モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username)# no webvpn
hostname(config-username)#
```

電子メール プロキシを使用するためにクライアントレス SSL VPN を設定する必要はありません。

（注）　グローバル コンフィギュレーション モードから入る webvpn モードでは、クライアントレス SSL VPN セッションのグローバル設定を構成できます。この項で説明した、ユーザ名モードから入ったユーザ名 webvpn コンフィギュレーション モードを使用すると、特定のユーザのクライアントレス SSL VPN セッションのコンフィギュレーションをカスタマイズできます。

ユーザ名 webvpn コンフィギュレーション モードでは、次のパラメータをカスタマイズできます。各パラメータについては、後続の手順で説明します。

- customizations
- deny message
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server（シングル サインオン サーバ）
- auto-signon
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

次の例は、ユーザ名 anyuser の属性のユーザ名 webvpn コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

HTML からフィルタリングするコンテンツとオブジェクトの指定

このユーザのクライアントレス SSL VPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするには、ユーザ名 webvpn コンフィギュレーション モードで **html-content-filter** コマンドを入力します。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**html-content-filter none** コマンドを発行して作成したヌル値を含めて、すべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。HTML コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを入力します。HTML フィルタリングは、デフォルトでディセーブルです。

次回このコマンドを使用すると、前回までの設定が上書きされます。

```
hostname(config-username-webvpn)# html-content-filter {java | images | scripts | cookies |
none}

hostname(config-username-webvpn)# no html-content-filter [java | images | scripts |
cookies | none]
```

このコマンドで使用するキーワードは、次のとおりです。

- **cookies**：イメージからクッキーを削除して、アドバタイズメント フィルタリングを制限し、プライバシーを保持します。
- **images**：イメージへの参照を削除します（<IMG> タグを削除）。
- **java**：Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> の各タグを削除）。
- **none**：フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
- **scripts**：スクリプトへの参照を削除します（<SCRIPT> タグを削除）。

次の例は、anyuser という名前のユーザに、Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# html-content-filter java cookies images
hostname(config-username-webvpn)#
```

ユーザ ホームページの指定

このユーザがクライアントレス SSL VPN セッションにログインするときに表示される Web ページの URL を指定するには、ユーザ名 webvpn コンフィギュレーション モードで **homepage** コマンドを入力します。**homepage none** コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。ホームページを継承しないようにするには、**homepage none** コマンドを入力します。

none キーワードは、クライアントレス SSL VPN ホームページがないことを示します。これにより、ヌル値が設定されてホームページが拒否され、ホームページが継承されなくなります。

キーワード *value* の後ろの **url-string** 変数で、ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

デフォルトのホームページはありません。

```
hostname(config-username-webvpn)# homepage {value url-string | none}
hostname(config-username-webvpn)# no homepage
hostname(config-username-webvpn)#
```

次の例は、anyuser という名前のユーザのホームページとして www.example.com を指定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# homepage value www.example.com
hostname(config-username-webvpn)#
```

カスタマイゼーションの適用

カスタマイゼーションによって、ログイン時にユーザに表示されるウィンドウ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、クライアントレス SSL VPN の設定の一部として設定します。ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するために、事前に定義した Web ページ カスタマイゼーションを適用するには、ユーザ名 webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-username-webvpn)# customization {none | value customization_name}
hostname(config-username-webvpn)#
```

たとえば、blueborder という名前のカスタマイゼーションを使用するには、次のコマンドを入力します。

```
hostname(config-username-webvpn)# customization value blueborder
hostname(config-username-webvpn)#
```

カスタマイゼーション自体は、webvpn モードで **customization** コマンドを入力して設定します。

次の例は、123 という名前のカスタマイゼーションを最初に確立するコマンド シーケンスを示しています。このコマンド シーケンスによって、パスワード プロンプトが定義されます。次に test という名前のトンネルグループを定義し、**customization** コマンドを使用して、123 という名前のカスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# username testuser nopassword
hostname(config)# username testuser attributes
hostname(config-username-webvpn)# webvpn
hostname(config-username-webvpn)# customization value 123
hostname(config-username-webvpn)#
```

「拒否」メッセージの指定

ユーザ名 webvpn コンフィギュレーション モードで、**deny-message** コマンドを入力すると、クライアントレス SSL VPN セッションに正常にログインできるが VPN 特権を持たないリモート ユーザに送信されるメッセージを指定できます。

```
hostname(config-username-webvpn)# deny-message value "message"
hostname(config-username-webvpn)# no deny-message value "message"
hostname(config-username-webvpn)# deny-message none
```

no deny-message value コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

no deny-message none コマンドは、接続プロファイル ポリシーのコンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

メッセージは、特殊文字、スペース、および句読点を含む英数字で最大 491 文字まで指定できますが、囲みの引用符はカウントされません。テキストは、ログイン時にリモート ユーザのブラウザに表示されます。**deny-message value** コマンドへのストリングの入力時は、コマンドがラップしている場合でも引き続き入力します。

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」

次の例の最初のコマンドは、ユーザ名モードに入り、anyuser という名前のユーザに属性を設定します。後続のコマンドは、ユーザ名 webvpn コンフィギュレーション モードに入り、そのユーザに関連付けられている拒否メッセージを変更します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# deny-message value "Your login credentials are OK.
However, you have not been granted rights to use the VPN features. Contact your
administrator for more information."
hostname(config-username-webvpn)
```

クライアントレス SSL VPN セッションに使用する ACL の指定

このユーザのクライアントレス SSL VPN セッションに使用する ACL の名前を指定するには、ユーザ名 webvpn コンフィギュレーション モードで **filter** コマンドを入力します。**filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

filter コマンドを入力して指定するまで、クライアントレス SSL VPN ACL は適用されません。

ACL を設定して、このユーザについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを入力して、これらの ACL をクライアントレス SSL VPN トラフィックに適用します。

```
hostname(config-username-webvpn)# filter {value ACLname | none}
hostname(config-username-webvpn)# no filter
hostname(config-username-webvpn)#
```

none キーワードは、**webvpntype** ACL がないことを示します。これにより、ヌル値が設定されて ACL が拒否され、別のグループ ポリシーから ACL が継承されなくなります。

キーワード *value* の後ろの **ACLname** 文字列で、事前に設定されている ACL の名前を指定します。

（注） クライアントレス SSL VPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次に、anyuser という名前のユーザの、*acl_in* という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# filter acl_in
hostname(config-username-webvpn)#
```

URL リストの適用

クライアントレス SSL VPN セッションを確立したユーザのホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して、1 つ以上の名前付きリストを作成する必要があります。クライアントレス SSL VPN の特定のユーザにサーバと URL のリストを適用するには、ユーザ名 webvpn コンフィギュレーション モードで **url-list** コマンドを入力します。

url-list none コマンドを使用して作成したヌル値を含めて、リストを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。URL リストを継承しないようにするには、**url-list none** コマンドを入力します。

```
hostname(config-username-webvpn)# url-list {listname displayname url | none}
hostname(config-username-webvpn)# no url-list
```

このコマンドで使用するキーワードと変数は、次のとおりです。

- *displayname* : URL の名前を指定します。この名前は、クライアントレス SSL VPN セッションのポータル ページに表示されます。
- *listname* : URL をグループ化する名前を指定します。
- **none** : URL のリストが存在しないことを示します。ヌル値を設定して、URL リストを拒否します。URL リストの値を継承しないようにします。
- *url* : クライアントレス SSL VPN のユーザがアクセスできる URL を指定します。

デフォルトの URL リストはありません。

次回このコマンドを使用すると、前回までの設定が上書きされます。

次の例は、anyuser という名前のユーザに AnyuserURLs という URL リストを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# url-list value AnyuserURLs
hostname(config-username-webvpn)#
```

ユーザの ActiveX Relay のイネーブル化

ActiveX Relay を使用すると、クライアントレス SSL VPN セッションを確立したユーザが、ブラウザを使用して Microsoft Office アプリケーションを起動できるようになります。アプリケーションは、セッションを使用して Microsoft Office ドキュメントのダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。

クライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルまたはディセーブルにするには、ユーザ名 webvpn コンフィギュレーション モードで次のコマンドを入力します。

activex-relay {**enable | disable**}

グループ ポリシーから **activex-relay** コマンドを継承するには、次のコマンドを入力します。

no activex-relay

次のコマンドは、特定のユーザ名に関連付けられているクライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルにします。

```
hostname(config-username-policy)# webvpn
hostname(config-username-webvpn)# activex-relay enable
hostname(config-username-webvpn)
```

クライアントレス SSL VPN セッションのアプリケーション アクセスのイネーブル化

このユーザのアプリケーション アクセスをイネーブルにするには、ユーザ名 webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート フォワーディングは、デフォルトではディセーブルになっています。

port-forward none コマンドを発行して作成したヌル値を含めて、コンフィギュレーションからポート転送属性を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、リストをグループ ポリシーから継承できます。フィルタリングを拒否してポート転送リストを継承しないようにするには、**none** キーワードを指定して **port-forward** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward {value listname | none}
hostname(config-username-webvpn)# no port-forward
hostname(config-username-webvpn)#
```

キーワード *value* の後ろの **listname** 文字列で、クライアントレス SSL VPN のユーザがアクセスできるアプリケーションのリストを指定します。コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

ユーザ名 webvpn コンフィギュレーション モードで **port-forward** コマンドを入力し、アプリケーション アクセスをイネーブルにする前に、クライアントレス SSL VPN セッションでユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

次の例は、ports1 というポート転送リストを設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward value ports1
hostname(config-username-webvpn)#
```

ポート転送表示名の設定

ユーザ名 webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用して、特定のユーザでエンド ユーザへの TCP ポート転送を識別する表示名を設定します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するには、このコマンドの **no** 形式を入力します。**no** オプションは、デフォルト名の、Application Access を復元します。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward-name {value name | none}
hostname(config-username-webvpn)# no port-forward-name
```

次の例は、ポート転送名 test を設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward-name value test
hostname(config-username-webvpn)#
```

セッション タイマーを更新のために無視する最大オブジェクト サイズの設定

ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回路が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定したサイズ以下のすべてのメッセージをキープアライブ メッセージと見なし、セッション タイマーの更新時にトラフィックと見なさないよう ASA に指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

トランザクションごとに無視する HTTP/HTTPS トラフィックの上限を指定するには、グループ ポリシー属性 webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#

The no form of the command removes this specification from the configuration:
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

自動サインオンの設定

NTLM、基本 HTTP 認証、またはその両方を使用する内部サーバに、特定のクライアントレス SSL VPN のユーザのログイン クレデンシャルを自動的に渡すには、ユーザ名 webvpn コンフィギュレーション モードで **auto-signon** コマンドを使用します。

auto-signon コマンドは、クライアントレス SSL VPN セッションのユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のためにログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名がグループに優先し、グループがグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、使用する認証の対象範囲によって異なります。

特定のサーバへの特定のユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URL を指定してこのコマンドの **no** 形式を使用します。すべてのサーバへの認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、値をグループ ポリシーから継承できます。

次のコマンド例では、基本認証または NTLM 認証を使用して、anyuser という名前のクライアントレス SSL VPN のユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
```

次のコマンド例では、基本認証または NTLM 認証を使用して、anyuser という名前のクライアントレス SSL VPN のユーザに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
all
hostname(config-username-webvpn)#
```

HTTP 圧縮の指定

ユーザ名 webvpn コンフィギュレーション モードで、**http-comp** コマンドを入力し、特定のユーザのクライアントレス SSL VPN セッションで HTTP データの圧縮をイネーブルにします。

```
hostname(config-username-webvpn)# http-comp {gzip | none}
hostname(config-username-webvpn)#
```

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# no http-comp {gzip | none}
hostname(config-username-webvpn)#
```

このコマンドの構文は次のとおりです。

- **gzip**：圧縮がグループまたはユーザに対してイネーブルになることを指定します。768 ビットは、デフォルト値です。
- **none**：圧縮がグループまたはユーザに対してディセーブルになることを指定します。

クライアントレス SSL VPN セッションの場合、グローバル コンフィギュレーション モードで設定された **compression** コマンドは、グループ ポリシー モードおよびユーザ名 webvpn モードで設定された **http-comp** コマンドを上書きします。

次の例は、testuser というユーザ名で圧縮をディセーブルにしています。

```
hostname(config)# username testuser internal
hostname(config)# username testuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# http-comp none
hostname(config-username-webvpn)#
```

SSO サーバの指定

クライアントレス SSL VPN セッションだけに使用できるシングル サインオンのサポートを使用すると、ユーザはユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。**sso-server value** コマンドをユーザ名 webvpn モードで入力すると、SSO サーバをユーザに割り当てることができます。

SSO サーバをユーザに割り当てるには、ユーザ名 webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。このコマンドでは、コンフィギュレーションに CA SiteMinder コマンドが含まれている必要があります。

```
hostname(config-username-webvpn)# sso-server value server_name
hostname(config-username-webvpn)#
```

割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。デフォルト ポリシーが継承されないようにするには、**sso-server none** コマンドを使用します。

```
hostname(config-username-webvpn)# sso-server {value server_name | none}
hostname(config-username-webvpn)# [no] sso-server value server_name
```

SSO サーバに割り当てられているデフォルト ポリシーは DfltGrpPolicy です。

次の例は、example という名前の SSO サーバを anyuser という名前のユーザに割り当てます。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value example
hostname(config-username-webvpn)#
```