接続プロファイル、グループ ポリシー、およびユーザー

この章では、VPN 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、およびユーザー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。

接続プロファイル、グループポリシー、およびユーザーの概要

グループとユーザーは、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。グループとユーザーで指定される属性によって、VPN へのユーザー アクセスと VPN の使用方法が決定されます。グループは、ユーザーの集合を 1 つのエンティティとして扱うものです。ユーザーの属性は、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。ユーザー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。

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、ユーザーの集合に関する値が設定されます。その後、ユーザーを設定します。ユーザーはグループの値を継承でき、さらに個別のユーザー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。

（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」は頻繁にほとんど同じ意味で使用されています。

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（DefaultL2Lgroup）、IKEv2 VPN 用のデフォルトのリモートアクセス接続プロファイル（DefaultRAgroup）、クライアントレス SSL および セキュアクライアント SSL 接続用のデフォルトの接続プロファイル（DefaultWEBVPNgroup）、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、多くのユーザーに共通すると考えられる設定が提供されます。ユーザーを追加するときに、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、数多くのユーザーに対して迅速に VPN アクセスを設定できます。

すべての VPN ユーザー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、一般的操作用コンフィギュレーション ガイドの第 20 章「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、ユーザー、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 コンフィギュレーション 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 レコードには存在しないため、セキュリティ アプライアンスは適用する値を見つけるために、ユーザー名および必要に応じてグローバル ポリシーの AAA 属性に移動して検索します。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、トンネルユーザーが認証先サーバー、および接続情報の送信先となるアカウンティング サーバー（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、ユーザー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、IPSEC リモートアクセス接続用の DefaultRAgroup、および SSL VPN（ブラウザベースおよび セキュアクライアント 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、外部サーバーでは設定できません。

（注） 一部のプロファイル（フェーズ 1 の IKEv1 など）は、エンドポイントがリモート アクセスまたは LAN-to-LAN かどうかを判別できないことがあります。トンネル グループを判別できない場合、デフォルトで

```
tunnel-group-map default-group <tunnel-group-name>
```

に設定されます（デフォルト値は *DefaultRAGroup* です）。

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、認可、アカウンティング サーバー：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ーのグループまたはリストを指定します。
  - ユーザーの認証
  - ユーザーがアクセスを認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

サーバー グループは、1 つ以上のサーバーで構成されます。

- 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、ユーザー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 ユーザーを認証または認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 サーバーまたはアドレス プールの値が含まれます。
- 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ーに警告して、パスワードを変更する機会をユーザーに提供できます。
- グループ除去およびレルム除去：これらのパラメータにより、ASAが受信するユーザー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ー名にだけ適用されます。

  領域は @ デリミタ付きでユーザー名に付加される管理ドメインです（user@abc）。レルムを除去する場合、ASAはユーザー名およびグループ（ある場合）を認証に使用します。グループを除去すると、ASA は認証にユーザー名およびレルム（ある場合）を使用します。

  レルム修飾子を除去するには strip-realm コマンドを入力し、認証中にユーザー名からグループ修飾子を削除するには strip-group コマンドを入力します。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。サーバー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。

  さらに、L2TP/IPsecクライアントの場合にstrip-groupコマンドを指定すると、ASAはVPNクライアントが提示したユーザー名からグループ名を取得してユーザー接続の接続プロファイル（トンネル グループ）を選択します。

- 認可の要求：このパラメータを使用すると、ユーザー接続の前に認可を要求したり、またはその要求を取り下げたりできます。

- 認可 DN 属性：このパラメータは、認可を実行するときに使用する認定者名属性を指定します。

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 ID の確認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、エンドユーザー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 ユーザー認証に 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ーし、自分自身の存在をピアに報告できます。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 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 （40 ページ） 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。

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ーに、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ーが取得するためのメカニズムを提供できます。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

次の表は、SSL VPN（セキュア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。

（注） 以前のリリースでは、「接続プロファイル」が「トンネル グループ」と呼ばれていました。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、この 2 つの用語が同義的によく使用されています。

表 *1 : SSL VPN* 用接続プロファイルの属性

	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ー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 サーバー（nbns-server）の名前を指定します。
group-alias	サーバー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、ユーザーはドロップダウン 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ーは、ログイン時にグループを選択する必要はありません。 セキュアクライアント 接続にグループ URL を使用するロードバランシング展開では、クラスタ内の各 ASA ノードで、ノードのロードバランシングのパブリックアドレスのグループ URL と同様に、仮想クラスタアドレスのグループ URL を設定する必要があります。
dns-group	DNS サーバー名、ドメイン名、ネーム サーバー、リトライ回数、および接続ファイルで使用される DNS サーバーのタイムアウト値を指定する DNS サーバー グループを指定します。
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 ユーザー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ー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 サイトツーサイトにのみ適用され、IKEv1 IPSec の セキュアクライアント、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。制限を超えるトンネル 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」メッセージが表示されます。

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


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 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

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 Secure Firewall 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。

- Secure 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）

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 （10 ページ）を使用して無効にすることができます。
- 「リモート アクセス接続プロファイルの一般属性の設定 （11 ページ）」を参照してください。
- 二重認証の設定 （15 ページ）
- 「リモート アクセス接続プロファイルの IPSec IKEv1 属性の設定 （17 ページ）」を参照してください。
- IPSec リモート アクセス接続プロファイルの PPP 属性の設定 （20 ページ）

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

手順

名前とタイプを指定して **tunnel-group** コマンドを入力することで、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。

tunnel-group *tunnel_group_name* **type remote-access**

例：

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。

手順

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 認証サーバー 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。指定したサーバー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)#
```

認証サーバー 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、認証にサーバー 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 使用する認可サーバー 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、ユーザーは接続する認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)#
```

認可サーバー 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、認可サーバーグループ FinGroup を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-groupFinGroup
hostname(config-tunnel-general)#
```

ステップ 4 アカウンティングサーバー 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 サーバー 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ー 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 サーバー（最大 10 サーバー）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 サーバーとアドレス 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 サーバー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 Secure Firewall ASA Series Command Reference』ガイドの 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ーのグループを特定するために、NAC 認証サーバー 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ー 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 ユーザー名を AAA サーバーに渡す前に、ユーザー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。レルムを除去する場合、ASA はユーザー名およびグループ（ある場合）認証を使用します。グループを除去すると、ASA は認証にユーザー名およびレルム（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、認証中にユーザー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。サーバー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 サーバーが RADIUS、RADIUS with NT、または LDAP サーバーの場合、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 サーバー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 サーバーにアクセスするために ASA に設定されている DN が、サーバー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 で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。

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ー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)#
```

サーバーがLDAPサーバーの場合、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、リモートユーザーがログインするときに、ASA は、ユーザー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、ユーザー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、ユーザー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ー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、ユーザーに対して失効が迫っていることを通知しませんが、失効後にユーザー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 （32 ページ）を参照してください。

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。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 サーバーは、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。

（注）
RADIUS サーバー（Cisco ACS など）は、認証要求を別の認証サーバーにプロキシする場合があります。ただし、ASA からは RADIUS サーバーとのみ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 サーバー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 サーバーに対してのみ、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

ステップ 11 証明書から認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認可用のユーザー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 属性を認可用のユーザー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**（ユーザー ID）、および **UPN**（ユーザー プリンシパル ネーム）があります。

ステップ 12 ユーザーに接続を許可する前に、そのユーザーが正常に認可されている必要があるかどうかを指定します。デフォルトでは認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、ユーザーがログイン画面に追加の認証クレデンシャル（2 つ目のユーザー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。

手順

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

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

セカンダリのサーバー グループでは SDI サーバー 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 サーバー グループ名を示します。ローカルは内部サーバー 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ー グループを sdi_group に、セカンダリ認証サーバー 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 つのユーザー名だけ要求します。また、ユーザー名をデジタル証明書から抽出する場合、プライマリ ユーザー名だけが認証に使用されます。

ステップ 2 セカンダリ ユーザー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 ユーザー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 に指示できます。

たとえば、プライマリ ユーザー名フィールドとして通常名を、セカンダリ ユーザー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 ユーザー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 クライアント（AnyConnect）接続に適用するかどうか、抽出されたユーザー名をエンドユーザー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 | 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 client
hostname(config-tunnel-general)# secondary-pre-fill-username client
```

ステップ 4 接続に適用する認可属性を取得するために使用する認証サーバーを指定します。デフォルトの選択は、プライマリ認証サーバーです。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ーを指定するには、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ー名（プライマリまたはセカンダリ）を指定します。デフォルト値はプライマリです。二重認証をイネーブルにすると、2 つの別のユーザー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ー名として認証されたユーザー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ー名は、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ー名です。

```
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ー名をセカンダリ認証サーバー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。

手順

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 ID 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 ユーザー認証に 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 ユーザー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 つは **interface** パラメータを使用し、もう 1 つは使用しない場合、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。

手順

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。

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
 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。

手順

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。

tunnel-group *tunnel-group-name* **general-attributes**

例：

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)#
```

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。

ステップ 2 デフォルト グループ ポリシーの名前を指定します。

default-group-policy *policyname*

例：

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。

手順

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 ID 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 ユーザー認証に 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 ユーザー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)#
```

標準ベースの IKEv2 クライアントのトンネル グループについて

トンネル グループは、トンネル接続ポリシーを格納したレコードのセットです。AAA サーバーを識別するトンネル グループを設定し、接続パラメータを指定し、デフォルトのグループ ポリシーを定義します。ASA は、トンネル グループを内部的に保存します。

IPSec リモートアクセスのデフォルト トンネル グループは DefaultRAGroup です。デフォルト トンネル グループは、変更することはできますが、削除することはできません。

IKEv2 では、別のローカルおよびリモート認証 CLI を使用して非対称認証方式を設定できます（つまり、送信元に対しては事前共有キー認証を設定し、応答側に対しては証明書認証または EAP 認証を設定できます）。したがって、IKEv2 を使用すると、両方の側がそれぞれ異なるクレデンシャルで認証する非対称認証を使用できます（事前共有キー、証明書、または EAP）。

DefaultRAGroup は EAP 認証用に設定する必要があります。これは、証明書認証が証明書 DN 照合に使用されていなければ、これらのクライアント接続を特定のトンネル グループにマッピングすることができないためです。

標準ベースの IKEv2 属性のサポート

ASA では、次の IKEv2 属性がサポートされます。

- INTERNAL_IP4_ADDRESS/INTERNAL_IP6_ADDRESS：IPv4 または IPv6 アドレス

（注） デュアル スタック（IPv4 と IPv6 の両方のアドレス割り当て）は、IKEv2 ではサポートされません。IPv4 アドレスと IPv6 アドレスの両方が要求され、両方のアドレスが割り当て可能な場合は、IPv4 アドレスのみが割り当てられます。

- INTERNAL_IP4_NETMASK：IPv4 アドレス ネットワーク マスク
- INTERNAL_IP4_DNS/INTERNAL_IP6_DNS：プライマリ/セカンダリ DNS アドレス
- INTERNAL_IP4_NBNS：プライマリ/セカンダリ WINS アドレス
- INTERNAL_IP4_SUBNET/INTERNAL_IP6_SUBNET：スプリット トンネリングのリスト
- APPLICATION_VERSION：無視されます。セキュリティ上の理由から、ASA のバージョン情報を伝達しないように応答は送信されません。ただし、クライアント設定ペイロード要求にこの属性を含めることができ、文字列が ASA の **vpn-sessiondb** コマンド出力と syslog に表示されます。

DAP のサポート

接続タイプごとの DAP ポリシー設定を許可するには、新しいクライアント タイプの IPsec-IKEv2-Generic-RA を使用してこの接続タイプに特定のポリシーを適用することができます。

リモート アクセス クライアントのトンネル グループ選択

次の表に、リモート アクセス クライアントと使用可能なトンネル グループ オプションのリストを示します。

リモート アクセス クライアント	トンネル グループ リスト	グループ URL	証明書 DN 照合	デフォルト グループ（DefaultRAGroup）	その
AnyConnect VPN クライアント	はい	はい	はい	はい	N/A
Windows L2TP/IPsec（メイン モード IKEv1）	いいえ	非対応	• 対応（ローカル マシンの証明書を使用する場合） • なし（PSK を使用する場合）	○	N/A
標準ベースの IKEv2	いいえ	非対応	• 対応（ローカル マシンの証明書を使用する場合） • なし（EAP 認証を使用する場合）	対応 （注）DefaultRAGroup トンネル グループを使用する必要があります。	N/A

標準ベースの IKEv2 クライアントの認証サポート

次の表に、標準ベースの IKEv2 クライアントとサポートされている認証方式のリストを示します。

（注） 認証方式の制限は、ASA 上ではなく、クライアント上のサポートの有無に基づきます。すべての EAP 方式の認証は、クライアントと EAP サーバー間で ASA によってプロキシされます。EAP 方式のサポートは、クライアントと EAP サーバーの EAP 方式のサポートに基づきます。

クライアントタイプ/認証方式	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	証明書のみ	PSK
Linux 上の StrongSwan	該当なし	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	はい	はい
Android 上の StrongSwan	該当なし	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	非対応	対応	該当なし
Windows 7/8/8.1	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	なし	はい	該当なし
Windows Phone	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	N/A	なし	なし

クライアント タイプ/認証方式	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	証明書のみ	PSK
Samsung Knox	該当なし	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	○	N/A
iOS 8	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	該当なし	対応	はい
Android ネイティブ クライアント	該当なし	• ISE：対応 • ACS：対応 • FreeRadius：対応 • FreeRadius 経由の AD：対応	該当なし	はい	はい

複数証明書認証の追加

マルチ証明書認証のプロトコル交換を定義し、これを両方のセッション タイプで利用できるように、集約認証プロトコルが拡張されました。クライアントがSSL接続を行なって集約認証を開始すると、別の SSL 接続が行なわれ、ASA は、クライアントが証明書認証を必要としクライアント証明書を要求していることを確認します。

ASA は、リモートアクセスタイプのトンネルグループの セキュアクライアント 接続に必要な認証を設定します。トンネルグループ マッピングは、証明書ルール マッピング、group-url などの既存の方法で実行されますが、必要な認証方法はクライアントとネゴシエートされます。

例

tunnel-group <name> webvpn-attributes

authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml] | saml [certificate | multiple-certificate]}

認証オプションは、AAA のみ、証明書のみ、複数証明書のみ、AAA と証明書、AAA と複数証明書、SAML、SAML と証明書、または複数証明書と SAML です。

```
ASA(config)# tunnel-group AnyConnect webvpn-attributes
ASA(config-tunnel-webvpn)# authentication?
tunnel-group-webvpn mode commands/options:
aaa         Use username and password for authentication
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
saml   Use SAML for authentication
ASA(config-tunnel-webvpn)# authentication multiple-certificate?

tunnel-group-webvpn mode commands/options:
aaa  Use username and password for authentication
saml  Use SAML for authentication
<cr>

ASA(config-tunnel-webvpn)# authentication aaa?

tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>ASA(config-tunnel-webvpn)# authentication aaa?

ASA(config-tunnel-webvpn)# authentication saml?
tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>
```

EAP ID を取得するためのクエリ ID オプションの設定

Microsoft Windows 7 IKEv2 クライアントは、Cisco ASA サーバーがトンネル グループ検索に使用できないようにするために、IP アドレスをインターネット キー交換（IKE）ID として送信します。ASA は、ASA がクライアントから有効な EAP ID を取得できるように、EAP 認証用の **query-identity** オプションを使用して設定する必要があります。

証明書ベースの認証の場合は、次のように、ASA サーバーと Microsoft Windows 7 クライアントの証明書に拡張キー使用法（EKU）フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバー証明書では、EKU フィールド = サーバー認証証明書です。

証明書は、Microsoft Certificate Server またはその他の CA サーバーから取得できます。

EAP 認証の場合は、Microsoft Windows 7 IKEv2 クライアントが他の EAP 要求の前に EAP ID 要求を待ちます。クライアントに EAP ID 要求を送信するには、IKEv2 ASA サーバー上のトンネ

ル グループ プロファイル内で **query-identity** キーワードが設定されていることを確認してください。

（注） Windows でスプリット トンネリングが実行できるように IKEv2 では DHCP 代行受信がサポートされます。この機能は、IPv4 スプリット トンネリング属性でのみ動作します。

手順

ステップ 1 接続タイプを IPsec リモート アクセスに設定するには、 **tunnel-group** コマンドを入力します。構文は、**tunnel-group** *name***type** *type* です。ここで、name はトンネル グループに割り当てる名前であり、type はトンネルのタイプです。

次の例では、IKEv2 事前共有キーが 44kkaol59636jnfx に設定されます。

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

（注）
認証を完了するには、**ikev2 remote-authentication pre-shared-key** コマンドまたは **ikev2 remote-authentication certificate** コマンドを設定する必要があります。

ステップ 2 標準ベースのサードパーティ IKEv2 リモート アクセス クライアントを使用したユーザー認証をサポートする方式として拡張認証プロトコル（EAP）を指定するには、**ikev2 remote-authentication eap** [**query-identity**] コマンドを使用します。

（注）
リモート認証でEAPをイネーブルにするには、証明書を使用してローカル認証を設定し、**ikev2 local-authentication** {**certificate** *trustpoint*} コマンドを使用して有効なトラストポイントを設定する必要があります。そうしなかった場合は、EAP 認証要求が拒否されます。

クライアントが、リモート認証用に設定されたオプションのすべてではなく、一部を使用できるようにする複数のオプションがあります。

IKEv2 接続の場合、トンネル グループのマッピングで、リモート認証に使用できる認証方式（PSK、証明書、およびEAP）とローカル認証に使用できる認証方式（PSKおよび証明書）、およびローカル認証で使用するトラストポイントを特定する必要があります。現在、マッピングの実行には、ピアまたはピア証明書のフィールドの値から取得（証明書マップを使用）された IKE ID が使用されます。両方のオプションが失敗した場合は、着信接続がデフォルトのリモート アクセス トンネル グループ DefaultRAGroup にマッピングされます。証明書マップは、リモート ピアが証明書で認証された場合にのみ適用されるオプションです。このマップにより、異なるトンネル グループへのマッピングが可能です。証明書認証の場合のみ、ルールまたはデフォルトの設定を使用してトンネル グループの参照が行われます。EAP 認証および PSK 認証の場合は、クライアント（トンネル グループ名が一致するクライアント）の IKE ID またはデフォルトの設定を使用してトンネル グループの参照が行われます。

EAP認証で、クライアントがIKE IDとユーザー名を個別に設定できない場合は、DefaultRAGroup トンネル グループを使用する必要があります。

次の例では、EAP 認証要求が拒否されています。

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

ステップ 3 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

トンネルが稼働中であることを確認するには、**show vpn-sessiondb summary** または **show crypto ipsec sa** コマンドを使用します。

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

認証に LDAP ディレクトリ サーバー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 サーバーにアクセスするために ASA に設定されている DN が、サーバーのデフォルト 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 で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。

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 の用語に言及しています。この項では、認証に LDAP ディレクトリ サーバー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ーに強制するための Active Directory の使用

次回ログイン時にユーザー パスワードの変更をユーザーに強制するには、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。

手順

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

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。

このユーザーが次回ログインするときに、ASA で次のプロンプトが表示されます「New password required. Password change required. You must enter a new password with a minimum length *n* to continue.」最小必須パスワード長 *n* は、[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] > [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] で Active Directory 設定の一部として設定できます。[Minimum password length] 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。ユーザー 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。

（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。

手順

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。

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。

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。

手順

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。

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。

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。

手順

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。

パスワードの複雑性の強制は、ユーザー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。

セキュアクライアント 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 サーバーにプロキシする RADIUS サーバー経由でクライアントに配信されるユーザー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。

（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ーでだけサポートされます。

リモート ユーザーが 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 サーバーと通信を行い、次に、認証について SDI サーバーと通信を行います。

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。このメッセージ テキストは、ASA が SDI サーバーと直接通信している場合と RADIUS プロキシを経由して通信している場合とで異なります。そのため、セキュアクライアントにネイティブ SDI サーバーとして認識させるために、ASA は RADIUS サーバー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が、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、セキュア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 （35 ページ） クライアントと SDI サーバー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、セキュアクライアント ユーザー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。

手順

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 サーバー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 サーバーに認証されるユーザーは、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。

例：

```
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 サーバー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。

次の表に、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であるとします。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照合します。

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。

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-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。

グループ ポリシーは、IPSec 接続用のユーザー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 サーバーに保存されます。接続プロファイルでは、トンネル確立後、ユーザー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、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

ユーザーにグループ ポリシーを割り当てたり、特定のユーザーのグループ 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ーに設定されます。グループ ポリシーには、次の属性があります。

- Identity
- サーバーの定義
- 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
- Filters
- 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 ポリシーの変更

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 ポリシーから継承されます。

（注） DfltGrpPolicy に設定されている（その後に割り当てられた）すべての セキュアクライアント プロファイルタイプ（Network Access Manager、Cisco Umbrella など）を含むセキュアクライアント プロファイルは、他のグループポリシーが DfltGrpPolicy から継承するように明示的に設定されていない限り、他のグループポリシーによって継承されません。つまり、特定のセキュアクライアントプロファイルがグループポリシーで設定されている場合、DfltGrpPolicy に関連付けられている セキュアクライアント プロファイルは継承されません。

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。コマンドの構文は、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
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client

 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

  http-proxy disable

  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

  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

  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable

  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 サイトツーサイトにのみ適用され、IKEv1 IPSec の AnyConnect、クライアントレス SSL VPN、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ー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 サーバー グループを特定し、その外部 AAA サーバー 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。外部認証サーバーを使用していて、外部グループ ポリシー属性が、認証する予定のユーザーと同じ RADIUS サーバーにある場合、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 での外部グループ名は、RADIUS サーバーのユーザー名を参照しています。つまり、ASA に外部グループ X を設定した場合、RADIUS サーバーはクエリーをユーザー X に対する認証要求と見なします。したがって、外部グループは、ASA にとって特別な意味を持つ RADIUS サーバー上のユーザー アカウントにすぎません。外部グループ属性が認証する予定のユーザーと同じ RADIUS サーバーに存在する場合、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 サーバーでのユーザー認証をサポートしています。外部サーバーを使用するように ASA を設定する前に、適切な ASA 認可属性を指定してサーバーを設定し、それらの属性のサブセットから個々のユーザーに対する特定の許可を割り当てる必要があります。外部サーバーを設定するには、VPN の外部 AAA サーバーの設定 の説明に従ってください。

手順

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 名とパスワードとともにグループ 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 サーバー 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 サーバーから取得され、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）
VPN の外部 AAA サーバーの設定 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 サーバーが 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 サーバーでは、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 （42 ページ）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 500 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。

VPN リモート クライアントでのログイン後に表示される全体的なバナーの長さは、ASA バージョン 9.5.1 で 510 ～ 4000 文字に増加しました。

（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

始める前に

IPv4 アドレス プールを作成します。

手順

ステップ 1 グループ ポリシー コンフィギュレーション モードを開始します。

group-policy *value* **attributes**

例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

ステップ 2 ipv4-pool1、ipv4-pool2、および ipv4-pool3 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。

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)#
```

ステップ 3 （任意） 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。

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)#
```

ステップ 4 （任意） **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。

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

ステップ 5 （任意） **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。

```
hostname(config-group-policy)# no address-pools none
hostname(config-group-policy)#
```

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

始める前に

IPv6 アドレス プールを作成します。VPN の IP アドレスを参照してください。

手順

ステップ 1 グループ ポリシー コンフィギュレーション モードを開始します。

group-policy *value* **attributes**

例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

ステップ 2 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。

例：

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。

```
hostname(config-group-policy)# ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

ステップ 3 （任意） 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。

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)#
```

ステップ 4 （任意） この属性が DfltGrpPolicy など他のポリシーのソースから継承されないようにするには、**ipv6-address-pools none** コマンドを使用します。

```
hostname(config-group-policy)# ipv6-address-pools none
hostname(config-group-policy)#
```

ステップ 5 （任意） **no ipv6-address pools none** コマンドを使用して、 **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。

```
hostname(config-group-policy)# no ipv6-address-pools none
hostname(config-group-policy)#
```

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} 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には次のものがあります。

- 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（セキュアクライアント 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 接続の IPsec トンネルをネゴシエートします。
- ssl-client：セキュアクライアント 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。

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ーには、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 ルールの適用

フィルタは複数のルールから構成されています。これらのルールは、ASA を介して着信したトンネリング データ パケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。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。

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。

（注） IPv6 を使用して VLAN マッピングを実行する場合、復号化されたトラフィックが内部ネットワークにルーティングされるようにするために、外部（宛先）アドレスは VLAN ごとに固有にする必要があります。異なる VLAN およびルート メトリックに対して同じ宛先ネットワークを使用することはできません。

- 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。

  [**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、一般的操作用コンフィギュレーション ガイドの「Configuring VLAN Subinterfaces and 802.1Q Trunking」の手順に従って、この ASA で設定する必要があります。

（注） クライアントレス VPN 接続の場合、出力 VLAN 機能は HTTP プロトコルでのみ機能します。

- 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） この属性はユーザー名モードで設定することもできます。その場合、ユーザー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。

VPN フィルタは初期接続にのみ適用されることにも留意してください。アプリケーション インスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。

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 ポリシーの VPN アクセス時間の指定

始める前に

時間の範囲を作成します。一般的操作用コンフィギュレーション ガイドの「Configuring Time Ranges」を参照してください。

手順

ステップ 1 グループ ポリシー コンフィギュレーション モードを開始します。

group-policy *value* **attributes**

例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
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 **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。

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 ポリシーの同時 VPN ログインの指定

特定のユーザーがグループポリシーに対して維持できる同時セッション数の制限を設定できます。デフォルトの同時セッション数は 3 です。

失効したセキュアクライアント、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、同じユーザー名で「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。

許可される同時セッション数が 1 で、異常終了後に同じユーザーが再度ログインした場合、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、同じユーザーが別の 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。

許可される同時セッション数が 1 より大きい場合、その最大数に達した状態でユーザーが再度ログインを試みると、最もアイドル時間が長いセッションがログオフされます。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。

最大セッション制限に達すると、システムが最も古いセッションを削除するまでに時間がかかります。そのため、ユーザーはすぐにログオンできず、削除が正常に完了する前に新しい接続を再試行する必要が生じる場合があります。ユーザーが想定どおりにログオフした場合、これは問題になりません。必要に応じて、削除の完了を待たずにすぐに新しいユーザー接続を許可するようにシステムを設定することで、遅延を解消できます。

手順

	コマンドまたはアクション	目的

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 **vpn-simultaneous-logins** *integer* コマンドを使用して、任意のユーザーに許可される同時ログイン数を指定します。	**vpn-simultaneous-logins**整数
		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ー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`
		（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。
		• 異なるグループポリシーを使用して異なるトンネルグループに接続すると、 **vpn-simultaneous-logins** は、既存のセッションで異なるグループポリシーが使用されている場合でも、ユーザー セッションを削除します。

ステップ 2	（オプション）同時ログインの制限に達した場合に、最も古いセッションが削除	**vpn-simultaneous-login-delete-no-delay** このオプションはデフォルトでは無効になっています。

	コマンドまたはアクション	目的
	されるのを待たずに新しいセッションを確立するようにシステムを設定します。	`hostname(config)# group-policy FirstGroup attributes` `hostname(config-group-policy)# vpn-simultaneous-login-delete-no-delay`

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のみアクセスするようにリモートユーザー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 がユーザー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、そのユーザー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、ユーザーを制限します。一致していない場合、ASA はユーザーが接続できないようにします。グループロックを設定しない場合、ASA は、割り当てられたグループとは関係なく、ユーザーを認証します。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。

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

手順

ステップ 1 （任意） 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ー名コンフィギュレーション モードで **vpn-session-timeout** {*minutes* コマンドを使用して、VPN 接続の最大時間を設定します。

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。

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)#
```

次の例は、anyuser という名前のユーザーに 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
hostname(config-username)#
```

[**no**] **vpn-session-timeout** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- このポリシーから属性を削除し、継承を許可するには、このコマンドの **no vpn-session-timeout** 形式を入力します。
- 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、**vpn-session-timeout none** を入力します。

ステップ 2 **vpn-session-timeout alert-interval** {*minutes* | } 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ー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ーに伝えます。次に、VPN セッションが切断される 20 分前にユーザーに通知されるよう指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
```

[**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- 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。

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- **vpn-session-timeout alert-interval none** は、ユーザーが通知を受信しないことを示します。

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

手順

ステップ 1 （任意） VPN アイドル タイムアウト期間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで **vpn-idle-timeout** *minutes* コマンドを使用します。

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。最小時間は 1 分、最大時間は 35791394 分であり、デフォルトは 30 分です。

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)#
```

[**no**] **vpn-idle-timeout** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- VPN アイドル タイムアウトを無効にし、タイムアウト値を継承しないようにするには、**vpn-idle-timeout none** を入力します。

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

  これにより、セキュアクライアント（SSL と IPsec/IKEv2 の両方）およびクライアントレス VPN がグローバル webvpn **default-idle-timeout** *seconds* 値を使用するようになります。このコマンドは、webvpn コンフィギュレーション モードで入力します。たとえば、`hostnamee(config-webvpn)# default-idle-timeout 300` のように入力します。デフォルトは 1800 秒（30 分）で、範囲は 60 ～ 86400 秒です。

  すべての webvon 接続において、**default-idle-timeout** 値が適用されるのは、グループ ポリシー/ユーザー名属性に **vpn-idle-timeout none** が設定されている場合のみです。すべてのセキュアクライアント 接続で、ASA によりゼロ以外のアイドルタイムアウト値が要求されます。

  サイト間（IKEv1、IKEv2）および IKEv1 リモート アクセス VPN の場合は、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することを推奨します。

- このグループ ポリシーまたはユーザー ポリシーのアイドル タイムアウトを無効にするには、**no vpn-idle-timeout** を入力します。値は継承されます。

- **vpn-idle-timeout** をまったく設定しない場合、値は継承されます。デフォルトは 30 分です。

ステップ 2 （任意） オプションで、**vpn-idle-timeout alert-interval** {*minutes*} 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ーに表示される時間を設定できます。

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ーに伝えます。デフォルトのアラート間隔は 1 分です。

次の例は、anyuser という名前のユーザーに 3 分の VPN アイドル タイムアウト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 alert-interval 3
hostname(config-username)#
```

[**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- **none** パラメータは、ユーザーが通知を受信しないことを示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- このグループまたはユーザー ポリシーのアラート間隔を削除するには、**no vpn-idle-timeout alert-interval** を入力します。値は継承されます。
- このパラメータをまったく設定しない場合、デフォルトのアラート間隔は 1 分です。

グループ ポリシーの WINS サーバーと DNS サーバーの設定

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

手順

ステップ 1 プライマリとセカンダリの WINS サーバーを指定します。

```
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 サーバーの 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 サーバーの 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 サーバーにヌル値が設定されます。この設定により、WINS サーバーは許可されず、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、既存の設定がオーバーライドされます。たとえば、WINS サーバー x.x.x.x を設定してから WINS サーバー 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 サーバーになります。サーバーを複数設定する場合も同様です。設定済みのサーバーを上書きするのではなく、WINS サーバーを追加するには、このコマンドを入力するときに、すべての WINS サーバーの 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 サーバー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 サーバーを指定します。

```
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 サーバーの 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 サーバーの 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 サーバーにヌル値が設定されます。この設定により、DNS サーバーは許可されず、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。DNS サーバー アドレスは最大 4 つ、IPv4 アドレスと IPv6 アドレスで 2 つずつ指定できます。

dns-server コマンドを入力するたびに、既存の設定がオーバーライドされます。たとえば、DNS サーバー x.x.x.x を設定し、次に DNS サーバー 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 サーバーになります。サーバーを複数設定する場合も同様です。以前に設定された DNS サーバーを上書きする代わりにサーバーを追加するには、このコマンドを入力するときにすべての DNS サーバーの 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 サーバー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 DefaultDNS DNS サーバー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。たとえば、**example.com.** というドメイン名およびトップ 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 （オプション）DHCP ネットワーク スコープを次のように設定します。

dhcp-network-scope {*ip_address* | **none**}

接続プロファイルのアドレスプールに DHCP サーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用する DHCP サーバーで定義されているアドレスプールのサブセットを選択できます。

ネットワーク スコープを定義しない場合、DHCP サーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

スコープを指定するには、目的のプールと同じサブネット上にあり、そのプール内にはないルーティング可能なアドレスを入力します。DHCP サーバは、この IP アドレスが属するサブネットを判別し、そのプールからの IP アドレスを割り当てます。

ルーティングの目的で可能な場合は常に、インターフェイスの IP アドレスを使用することを推奨します。たとえば、プールが 10.100.10.2 ～ 10.100.10.254 で、インターフェイスアドレスが 10.100.10.1/24 の場合、DHCP スコープとして 10.100.10.1 を使用します。ネットワーク番号は使用しないでください。DHCP は IPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

none を指定すると、たとえば、デフォルトまたは継承されたグループポリシーから DHCP アドレスが割り当てられなくなります。

例：

次の例では、FirstGroup の属性コンフィギュレーション モードを開始し、DHCP スコープを 10.100.10.1 に設定します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

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。

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

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。

ipv6-split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no ipv6-split-tunnel-policy

ポリシー オプションは次のとおりです。

- **tunnelspecified**：トンネルを通じてネットワーク リストに指定されているネットワークに対するすべてのトラフィックをトンネリングします。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 ユーザーのインターネット サービス プロバイダーによってルーティングされます。

  ASA 9.1.4 以降のバージョンでは、インクルード リストを指定するときに、インクルード範囲内のサブネットにエクスクルードリストも指定できます。除外されたサブネットのアドレスは、トンネリングされず、インクルードリストの残りの部分がトンネリングされます。エクスクルージョンリストのネットワークはトンネルを介して送信されません。エクスクルージョン リストは拒否エントリを使用して指定され、インクルージョン リストは許可エントリを使用して指定されます。

- **excludespecified**ネットワークリストに指定されているネットワークとの双方向のトラフィックをトンネリングしません。その他すべてのアドレスに対するトラフィックはトンネリングされます。を使用します。クライアント上でアクティブになっている VPN クライアント プロファイルでは、ローカル LAN アクセスを有効にしておく必要があります。このオプションは、セキュアクライアント クライアントでのみ機能します。

（注） インクルード リストのサブネットではないエクスクルージョン リスト内のネットワークは、クライアントで無視されます。

- **tunnelall —**すべてのトラフィックがトンネルを通過するよう指定します。このポリシーは、スプリット トンネリングをディセーブルにします。リモート ユーザーは企業ネットワークにアクセスできますが、ローカルネットワークへ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。

（注） スプリット トンネリング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。

例

次に、IPv4 と IPv6 の 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

スプリットトンネリングでは、トンネルを通過するネットワークトラフィックがネットワークリストによって決定されます。セキュアクライアント は、ACL である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に関する決定を行います。

```
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]
```

- **value** access-list name：トンネリングを実行するネットワーク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** ：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、ユーザー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。ユーザー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。

例

次に、FirstList という名前のネットワーク リストを作成し、FirstGroup という名前のグループ ポリシーに追加する例を示します。FistList はエクスクルージョン リストであり、エクスクルージョン リストのサブネットであるインクルージョン リストです。

```
hostname(config)# split-tunnel-policy tunnelspecified
hostname(config)# access-list FirstList deny ip 10.10.10.0 255.255.255.0 any
hostname(config)# access-list FirstList permit ip 10.0.0.0 255.0.0.0 any

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

次に、v6 という名前のネットワーク リストを作成し、GroupPolicy_ipv6-ikev2 という名前のグループ ポリシーに v6 スプリット トンネル ポリシーを追加する例を示します。v6 はエクスクルージョン リストであり、エクスクルージョン リストのサブネットであるインクルージョン リストです。

```
hostname(config)# access-list v6 extended permit ip fd90:5000::/32 any6
hostname(config)# access-list v6 extended deny ip fd90:5000:3000:2880::/64 any6

hostname(config)# group-policy GroupPolicy_ipv6-ikev2 internal
hostname(config)# group-policy GroupPolicy_ipv6-ikev2 attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value v6
```

スプリット トンネル設定の確認

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
```

スプリット トンネリング用のドメイン属性の設定

デフォルト ドメイン名、またはスプリット トンネルを介して解決する、スプリット DNS と呼ばれるドメインのリストを指定できます。

AnyConnect 3.1 は、Windows および Mac OS X のプラットフォームのトゥルー スプリット DNS 機能をサポートします。セキュリティ アプライアンスのグループ ポリシーにより Split-Include トンネリングがイネーブルになっており、トンネリング対象の DNS 名が指定されている場合、AnyConnect は、この名前に一致するすべての DNS クエリーをプライベート DNS サーバーにトンネリングします。トゥルー スプリット DNS を使用すると、ASA によってクライアントにプッシュダウンされたドメインに一致する DNS 要求へのトンネル アクセスのみが許可されます。これらの要求は、クリア テキストでは送信されません。一方、DNS 要求が ASA によってプッシュダウンされたドメインに一致しない場合は、AnyConnect は、クライアントのオペレーティング システムにある DNS リゾルバから、DNS 解決に使用されるホスト名を暗号化せずに送信させます。

（注） スプリット DNS は、標準クエリーおよび更新クエリー（A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR、CNAME など）をサポートしています。トンネリングされたネットワークのいずれかに一致する PTR クエリーは、トンネル経由で許可されます。

Mac OS X の場合、AnyConnect は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのトゥルー スプリット DNS を使用できます。

- グループ ポリシーで、スプリット DNS が 1 つの IP プロトコル（IPv4 など）に設定されており、クライアント バイパス プロトコルがもう片方の IP プロトコル（IPv6 など）に設定されている（後者の IP プロトコルにはアドレス プールは設定されていない）。
- スプリット DNS が両方の IP プロトコルに設定されている。

デフォルトのドメイン名の定義

ASA は セキュアクライアント にデフォルトドメイン名を渡します。クライアントは、ドメイン フィールドを省略した DNS クエリーにドメイン名を追加します。このドメイン名は、トンネルパケットにだけ適用されます。デフォルトのドメイン名がない場合、ユーザーはデフォルト 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 ポリシーのユーザーのデフォルト 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 ドメイン名を識別します。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、**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

デフォルトのドメイン名のほかに、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、ユーザー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。ユーザー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 492 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
```

（注） スプリット DNS を設定する場合、指定したプライベート DNS サーバーが、クライアント プラットフォームに設定されている DNS サーバーと重複していないことを確認します。重複していると、名前解決が正しく動作せず、クエリーがドロップされる可能性があります。

Windows XP およびスプリット トンネリング用の 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 代行受信によって、Microsoft Windows XP クライアントは ASA でスプリット トンネリングを使用できるようになります。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 サーバー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
```

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 サーバー パラメータを設定するには、次の手順を実行します。

手順

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 サーバーとポートを設定します。

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

デフォルト値は **none** で、クライアント デバイスのブラウザでプロキシ サーバーの設定を指定していません。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)#
```

プロキシサーバーの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 サーバーとして 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 **no-modify** 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 サーバー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 サーバーの設定をそのままにします。
- **no-proxy—**このクライアントデバイスでは、ブラウザのHTTPプロキシ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 サーバー設定を設定します。

プロキシサーバーの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 デバイスのサーバーとしてサーバー 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、プロキシサーバー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 サーバーの 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または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。

プロキシサーバーの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 のサーバーで構成され、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)#
```

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。

手順

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、ユーザーがログイン 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ー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保存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 ユーザーのデータ伝送レートが向上する場合があります。

ヒント
データ圧縮を使用すると、ユーザー 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ー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ーに対してユーザー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ー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、ユーザー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。認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ー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）
接続先にユーザーが存在しない場合、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、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。

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 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

手順

ステップ 1 （任意） 次のコマンドを使用して、ネットワーク拡張モードを設定します。

[no] nem [enable |disable]

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。PAT は適用されません。したがって、Easy VPN サーバーの背後にあるデバイスは、Easy VPN リモートの背後にあるプライベート ネットワーク上のデバイスに、トンネルを介して（トンネルを介してのみ）直接アクセスできます。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。

例：

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
```

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 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。

ステップ 2 （任意） 次のコマンドを使用して、セキュア ユニット認証を設定します。

[no] secure-unit-authentication [enable |disable]

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ー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 クライアントは保存されているユーザー名とパスワードを使用しません（設定されている場合）。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。

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ー 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、どのバックアップ サーバーにもセキュア ユニット認証を設定する必要があります。

（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。

例：

次の例は、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方法を示しています。

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

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。

ステップ 3 （任意） 次のコマンドを使用して、ユーザー認証を設定します。

[**no**] **user-authentication** [**enable** | **disable**]

ユーザー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ーは、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。個々のユーザーは、設定した認証サーバーの順序に従って認証されます。ユーザー認証はデフォルトでディセーブルになっています。

プライマリ ASA でユーザー認証が必要な場合は、どのバックアップ サーバーにもユーザー認証を設定する必要があります。

例：

次の例は、FirstGroup という名前のグループ ポリシーに対して、ユーザー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
```

ユーザー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。ユーザー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ー認証の値を継承できます。

ステップ 4 次のコマンドを使用して、認証した個々のユーザーのアイドル タイムアウトを設定します。

[**no**] **user-authentication-idle-timeout** *minutes* | **none**]

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 タイムアウト期間中にハードウェア クライアントの背後のユーザー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させます。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のアクセスだけを終了します。

例：

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 enable
hostname(config-group-policy)#user-authentication-idle-timeout 45
```

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。ヌル値を設定すると、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ー認証のアイドル タイムアウト値が継承されなくなります。

（注）
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ーのアイドル タイムアウト値になります。

ステップ 5 次のコマンドを使用して、IP Phone Bypass を設定します。

ip-phone-bypass enable

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 フォンが、ユーザー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。これは、IUA がイネーブルになっている場合にのみ適用されます。

（注）
また、これらのクライアントの認証を免除するには、クライアントに MAC アドレス免除を設定する必要があります。

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。このオプションにより、別のグループ ポリシーから IP Phone Bypass の値を継承できます。

ステップ 6 次のコマンドを使用して、LEAP Bypass を設定します。

leap-bypass enable

LEAP Bypass は、**user-authentication** がイネーブルになっている場合にのみ適用されます。このコマンドにより、Cisco ワイヤレス アクセス ポイント デバイスからの LEAP パケットは、

LEAP 認証を確立してから、ユーザー認証ごとに認証を実行できるようになります。LEAP Bypass は、デフォルトでディセーブルになっています。

ハードウェア クライアントの後ろにいる LEAP ユーザーには、面倒な問題があります。トンネルで中央サイト デバイスの後ろにある RADIUS サーバーにクレデンシャルを送信することができないため、LEAP 認証をネゴシエートできません。トンネル経由でクレデンシャルを送信できない理由は、無線ネットワークで認証されていないためです。この問題を解決するために、LEAP バイパスは、個別のユーザー認証の前に LEAP パケット（LEAP パケットだけ）をトンネルで転送し、RADIUS サーバーへの無線接続を認証できるようにします。これによって、ユーザーは、個別のユーザー認証に進むことができます。

LEAP Bypass は、次の条件下で適切に機能します。

- **secure-unit-authentication** がディセーブルになっていること。インタラクティブ ユニット認証がイネーブルの場合、トンネルを使用して LEAP デバイスが接続できるようになる前に、非 LEAP（有線）デバイスがハードウェア クライアントを認証する必要があります。
- **user-authentication** がイネーブルになっていること。イネーブルになっていないと、LEAP Bypass が適用されません。
- 無線環境のアクセス ポイントが、Cisco Discovery Protocol（CDP）を実行している Cisco Aironet Access Point であること。PC の NIC カードは、他のブランドの製品でもかまいません。

例：

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)# user-authentication enable
hostname(config-group-policy)# leap-bypass enable
```

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 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。

セキュアクライアント 接続のグループポリシー属性の設定

「AnyConnect VPN Client 接続」に示すように、セキュアクライアント 接続をイネーブルにした後は、グループポリシーのセキュアクライアント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。

手順

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。次に例を示します。

```
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 セキュアクライアント の永続的なインストールをディセーブルにするには、**none** キーワードを指定して anyconnect keep-installer コマンドを使用します。次に例を示します。

```
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、セキュアクライアント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 セキュアクライアント 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。次に例を示します。

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

ステップ 4 デッドピア検出の設定

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、プロキシ、ファイアウォール、または NAT デバイス経由の セキュアクライアント 接続を開いたままにすることができます。これを行うには、**anyconnect ssl keepalive command:** を使用してキープアライブメッセージの頻度を調整します。

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

また、キープアライブを調整すると、リモートユーザーが 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、セキュアクライアント 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、セキュアクライアント 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 セキュアクライアント 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、SVC キーの再生成中に セキュアクライアント が新しいトンネルを確立するように指定されます。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 セキュアクライアント 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、セキュアクライアントが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。

セキュアクライアント 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 がセキュアクライアント 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 がセキュアクライアント 接続に IPv4 アドレスのみを割り当て、エンドポイントがデュアルスタックされていると想定します。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。

SSL 接続ではなく IPsec トンネルを確立している場合は、クライアントで IPv6 が有効になっているかどうかが ASA に通知されないため、ASA は常にクライアント バイパス プロトコル設定をプッシュダウンします。

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）。

セキュアクライアント 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、セキュアクライアントは、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、使用可能な場合は常に、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。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**} または **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)#
```

バックアップ サーバー属性の設定

バックアップ サーバーを設定します（使用する予定がある場合）。IPsec バックアップ サーバーを使用すると、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 サーバーを設定すると、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ー 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 サーバーを設定しない限り、バックアップ サーバーは存在しません。

バックアップ サーバーは、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 サーバーを設定すると、バックアップ サーバー ポリシーがグループ内のクライアントにプッシュされ、クライアント上のバックアップ サーバー リスト（設定されている場合）が置き換わります。

（注） ホスト名を使用する場合は、バックアップ DNS サーバーおよびバックアップ WINS サーバーを、プライマリ DNS サーバーおよびプライマリ WINS サーバー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 サーバーとの接続が失われ、バックアップ サーバーに異なる 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 サーバー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 **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 サーバーを削除するには、バックアップ サーバー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 サーバーを使用しないことを指定します。ASA は、ヌルのサーバー 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 サーバー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 サーバー 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ー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、サーバーを 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 サーバー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 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。

手順

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。このタイマーの期限が切れると、ホストのポスチャの変更を調べるクエリー（ステータス クエリー）が発行されます。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 サーバー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 用デフォルト 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ー 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**：（オプション）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 を適用します。
- **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。名前にスペースが含まれている場合にのみ引用符が必要です（たとえば "Windows XP"）。

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 サーバーが 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 ユーザーがスプリット 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、ファイアウォールが、インターネットまたはユーザーのローカルLANを経由する不正侵入からユーザーのコンピュータを保護し、ひいては企業ネットワー

クも保護します。VPN クライアントを使用して ASA に接続しているリモート ユーザーは、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、ユーザー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。ユーザー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。

[Client Firewall] タブの [Add or Edit Group Policy] ダイアログボックスでは、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 ユーザーの 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ーします。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ーするからです。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と認識します）。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、ユーザー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 ポリシーとして指定します。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。

セキュアクライアント ファイアウォールポリシーの設定

セキュアクライアント のファイアウォールルールでは、IPv4 アドレスおよび IPv6 アドレスを指定できます。

始める前に

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。

手順

ステップ 1 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。

webvpn

例：

```
hostname(config)# group-policy ac-client-group attributes
hostname(config-group-policy)# webvpn
```

ステップ 2 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 インターフェイスに適用されるルールです。

anyconnect firewall-rule client-interface {private | public} value *[RuleName]*

```
hostname(config-group-webvpn)# anyconnect firewall-rule client-interface private value
ClientFWRule
```

ステップ 3 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。

show runn group-policy [value]

例：

```
hostname(config-group-webvpn)# show run group-policy FirstGroup
group-policy FirstGroup internal
group-policy FirstGroup attributes
webvpn
  anyconnect firewall-rule client-interface private value ClientFWRule
```

ステップ 4 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。

no anyconnect firewall-rule client-interface private value [*RuleName*]

例：

```
hostname(config-group-webvpn)# no anyconnect firewall-rule client-interface private value
```

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

Zone Labs Integrity サーバーの使用

この項では Zone Labs Integrity サーバー（Check Point Integrity サーバーとも呼ばれる）について説明し、Zone Labs Integrity サーバー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 サーバーは、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 サーバー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 サーバーおよび 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。

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 サーバー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 サーバー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 サーバー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 サーバーの間だけで確立されます。
4. Integrity サーバーは、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 サーバーから 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 サーバーは、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ーを続けます。

（注） ユーザー インターフェイスが最大 5 つの Integrity サーバー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 サーバーは 1 つです。アクティブな Integrity サーバーに障害が発生した場合は、ASA 上に別の Integrity サーバーを設定してから、VPN クライアント セッションを再度確立します。

Integrity サーバーを設定するには、次の手順を実行します。

手順

ステップ 1 IP アドレス 10.0.0.5 を使用して Integrity サーバーを設定します。

```
zonelabs-Integrity server-address {hostname1 | ip-address1}
```

例：

```
hostname(config)# zonelabs-Integrity server-address 10.0.0.5
```

ステップ 2 ポート 300 を指定します（デフォルト ポートは 5054 です）。

```
zonelabs-integrity port port-number
```

例：

```
hostname(config)# zonelabs-integrity port 300
```

ステップ 3 Integrity サーバーとの通信用に内部インターフェイスを指定します。

```
zonelabs-integrity interface interface
```

例：

```
hostname(config)# zonelabs-integrity interface inside
```

ステップ 4 Integrity サーバー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 サーバーからの応答を 12 秒間待つようにします。

（注）
ASA と Integrity サーバー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 サーバー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 サーバー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。

```
zonelabs-integrity fail-timeout timeout
```

例：

```
hostname(config)# zonelabs-integrity fail-timeout 12
```

ステップ 5 ASA と Zone Labs Integrity サーバー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。

```
zonelabs-integrity fail-close
```

例：

```
hostname(config)# zonelabs-integrity fail-close
```

ステップ 6 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。

zonelabs-integrity fail-open

例：

```
hostname(config)# zonelabs-integrity fail-open
```

ステップ 7 Integrity サーバーが ASA のポート 300（デフォルトはポート 80）に接続して、サーバー SSL 証明書を要求するように指定します。

zonelabs-integrity ssl-certificate-port cert-port-number

例：

```
hostname(config)# zonelabs-integrity ssl-certificate-port 300
```

ステップ 8 サーバーの SSL 証明書が常に認証される間、Integrity サーバーのクライアント SSL 証明書が認証されるように指定します。

zonelabs-integrity ssl-client-authentication {enable | disable}

例：

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
```

ファイアウォール クライアント タイプの Zone Labs への設定

手順

	コマンドまたはアクション	目的
ステップ 1	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。 例： `hostname(config)# client-firewall req zonelabs-integrity`	**client-firewall {opt | req} zonelabs-integrity**

次のタスク

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 （81 ページ）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 サーバー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 （81 ページ）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 サーバー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 *2 : 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?」という確認メッセージが表示されます。応答がない場合は、ASA によって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 サーバー 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。
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。許可ルールを定義しないと、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 rul 3 deny type * version 3.*** では、バージョン 3.x のソフトウェア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 command** 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、ユーザー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。

ユーザーがクライアント 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]
```

次の表に、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 *3 : 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。値の小さいプライオリティ 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*	フリー形式の文字列を介してデバイスのタイプを識別します。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。

パラメータ	説明
version version	7.0 などの自由形式の文字列を使用して、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。

ユーザー属性の設定

この項では、ユーザー属性とその設定方法について説明します。

デフォルトでは、ユーザーは、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ー属性を継承します。また、ASA では、ユーザー レベルで個別に属性を割り当て、そのユーザー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、すべてのユーザーに営業時間内のアクセスを許可し、特定のユーザーに 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。

ユーザー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、すべてのユーザー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、すべてのユーザーまたは特定のユーザー（ユーザー名を指定した場合）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 というユーザーを指定した場合の出力を示します。

```
hostname# show running-config all username testuse
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

個々のユーザーの属性の設定

特定のユーザーを設定するには、**username** コマンドを使用してユーザー名モードに入り、ユーザーにパスワード（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。

内部ユーザー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ー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。ユーザーを 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。ユーザーを削除するには、削除するユーザー名を指定して、このコマンドの **no** バージョンを使用します。すべてのユーザー名を削除するには、ユーザー名を指定せずに、**clear configure username** コマンドを使用します。

ユーザーのパスワードと特権レベルの設定

ユーザー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、このユーザー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、このユーザー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]
```

下記の表に、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。

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	このユーザーにパスワードが必要ないことを示します。
password password	このユーザー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。

キーワード/変数	意味
privilege priv_level	このユーザー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 ユーザー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ー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)#
```

ユーザー属性の設定

ユーザーのパスワード（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、ユーザー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 ユーザー属性の設定

VPN ユーザー属性は、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

ユーザーが、それまでにユーザー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。このユーザー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 ユーザーにはグループ 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
```

ユーザー名モードで使用できる属性の場合、ユーザー名モードで設定すると、特定のユーザーに関してグループ 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ー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、このユーザー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ーを 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

このユーザー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ー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ーに最大 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

手順

ステップ 1 （任意） VPN アイドル タイムアウト期間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで **vpn-idle-timeout** *minutes* コマンドを使用します。

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。最小時間は 1 分、最大時間は 35791394 分であり、デフォルトは 30 分です。

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)#
```

[**no**] **vpn-idle-timeout** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- VPN アイドル タイムアウトを無効にし、タイムアウト値を継承しないようにするには、**vpn-idle-timeout none** を入力します。

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

  これにより、セキュアクライアント（SSL と IPsec/IKEv2 の両方）およびクライアントレス VPN がグローバル webvpn **default-idle-timeout** *seconds* 値を使用するようになります。このコマンドは、webvpn コンフィギュレーション モードで入力します。たとえば、`hostnamee(config-webvpn)# default-idle-timeout 300` のように入力します。デフォルトは 1800 秒（30 分）で、範囲は 60 ～ 86400 秒です。

  すべての webvon 接続において、**default-idle-timeout** 値が適用されるのは、グループ ポリシー/ユーザー名属性に **vpn-idle-timeout none** が設定されている場合のみです。すべてのセキュアクライアント 接続で、ASA によりゼロ以外のアイドルタイムアウト値が要求されます。

  サイト間（IKEv1、IKEv2）および IKEv1 リモート アクセス VPN の場合は、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することを推奨します。

- このグループ ポリシーまたはユーザー ポリシーのアイドル タイムアウトを無効にするには、**no vpn-idle-timeout** を入力します。値は継承されます。

- **vpn-idle-timeout** をまったく設定しない場合、値は継承されます。デフォルトは 30 分です。

ステップ 2 （任意） オプションで、**vpn-idle-timeout alert-interval** {*minutes*} 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ーに表示される時間を設定できます。

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ーに伝えます。デフォルトのアラート間隔は 1 分です。

次の例は、anyuser という名前のユーザーに 3 分の VPN アイドル タイムアウト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 alert-interval 3
hostname(config-username)#
```

[**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- **none** パラメータは、ユーザーが通知を受信しないことを示します。

  ```
  hostname(config)# username anyuser attributes
  hostname(config-username)# vpn-idle-timeout none
  hostname(config-username)#
  ```

- このグループまたはユーザー ポリシーのアラート間隔を削除するには、**no vpn-idle-timeout alert-interval** を入力します。値は継承されます。
- このパラメータをまったく設定しない場合、デフォルトのアラート間隔は 1 分です。

最大接続時間の設定

手順

ステップ 1 （任意） 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ー名コンフィギュレーション モードで **vpn-session-timeout** {*minutes* コマンドを使用して、VPN 接続の最大時間を設定します。

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。

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)#
```

次の例は、anyuser という名前のユーザーに 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
```

```
hostname(config-username)#
```

[**no**] **vpn-session-timeout** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- このポリシーから属性を削除し、継承を許可するには、このコマンドの **no vpn-session-timeout** 形式を入力します。
- 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、**vpn-session-timeout none** を入力します。

ステップ 2 **vpn-session-timeout alert-interval** {*minutes* | } 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ー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ーに伝えます。次に、VPN セッションが切断される 20 分前にユーザーに通知されるよう指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
```

[**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} コマンドを使用したその他のアクションは次のとおりです。

- 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。

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- **vpn-session-timeout alert-interval none** は、ユーザーが通知を受信しないことを示します。

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ー固有の 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、グループ ポリシーから値を継承できます。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。VPN フィルタは初期接続にのみ適用されます。アプリケーション インスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。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 では、**vpn-filter** コマンドで定義された ACL は使用されません。

次に、anyuser という名前のユーザーの、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)# 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

特定のユーザーに割り当てる 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ーに 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ーに、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

特定のユーザーに割り当てる 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ーに 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

このユーザーが使用できる 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 ユーザー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ーには、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ー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 ユーザー 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 ユーザーを制限します。group-lock は、VPN クライアントで設定されたグループが、そのユーザー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、ユーザーを制限します。一致していない場

合、ASA はユーザーが接続できないようにします。グループロックを設定しない場合、ASA は、割り当てられたグループとは関係なく、ユーザーを認証します。

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** 形式を入力します。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ーにグループ 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 ユーザーのパスワード保存のイネーブル化

ユーザーがログイン 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。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。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ー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ー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)
```

VPN フィルタ ACL の設定と調整に関するベストプラクティス

このセクションでは、トラフィックの中断なしに既存の VPN フィルタ ACL を更新する際に従うべきベストプラクティスを示します。

既存の VPN フィルタ ACL を更新する

ASA デバイスに適用されている vpn-filter ACL を更新するには、次の手順を実行します。

1. システムで新しい vpn-filter ACL を作成します（例：*new_acl.txt*）。
2. デバイスから現在の vpn-filter ACL をダウンロードします（例：*old_acl.txt*）。
3. 次のように、ACL の変更手順を作成します。

```
* Add update in-progress to ACL remark
echo ?access-list <name> line 1 ACL update in-progress? > push.txt
* Delete old rules
sed ?s/^/no /g? old.acl >> push.txt
 * Add new rules
cat new.acl >> push.txt
 * Remove update in-progress to ACL remark
echo ?no access-list <name> ACL update in-progress? >> push.txt
```

4. push.txt をデバイスにアップロードします。

既存の VPN フィルタ ACL を新しいものに置き換える

ASA デバイスに適用されている vpn-filter ACL を置き換えるには、次の手順を実行します。

1. 既存の vpn-filter ACL を置き換えるときは毎回新しいものを作成します。
2. 作成した vpn-filter ACL を使用してグループポリシーを更新します。
3. デバイスに適用されていた古い vpn-filter ACL を削除します。

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