トンネルグループ、グループポリシー、およびユーザの設定

この章では、VPN のトンネルグループ、グループポリシー、およびユーザの設定方法について説明します。次の事項について説明します。

- トンネルグループ、グループポリシー、およびユーザの概要（P.26-2）
- トンネルグループの設定（P.26-6）
- グループポリシー（P.26-24）
- ユーザ アトリビュートの設定（P.26-60）

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

トンネルグループ、グループポリシー、およびユーザの概要

グループとユーザは、バーチャル プライベート ネットワーク（VPN）のセキュリティ管理とセキュリティ アプライアンスの設定における中核的な概念です。グループとユーザで指定されるアトリビュートによって、VPN へのユーザ アクセスと VPN の使用方法が決定されます。*グループ*は、ユーザの集合を 1 つのエンティティとして扱うものです。*ユーザ*のアトリビュートは、*グループポリシー*から取得されます。*トンネルグループ*は、特定の接続用のグループポリシーを指定します。ユーザに特定のグループポリシーを割り当てない場合は、その接続のデフォルトのグループポリシーが適用されます。

トンネルグループ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、セキュリティ アプライアンスには、デフォルトの LAN-to-LAN トンネルグループ、デフォルトのリモートアクセス トンネルグループ、デフォルトの WebVPN トンネルグループ、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。デフォルトのトンネルグループとグループポリシーでは、多くのユーザに共通すると考えられる設定が提供されます。ユーザを追加するときは、ユーザがグループポリシーからパラメータを「継承」するように指定できます。この指定により、多数のユーザの VPN アクセスを迅速に設定することができます。

すべての VPN ユーザに同一の権限を許可する場合は、特定のトンネルグループ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 の特定のユーザにシステムへのアクセスを許可し、その他の MIS ユーザはアクセスできないようにする場合もあります。トンネルグループとグループポリシーにより、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）　セキュリティ アプライアンスには、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トンネルグループよりも、ACL と関連があります。オブジェクト グループを使用する方法の詳細については、第 13 章「アクセスリストによるトラフィックの指定」を参照してください。

トンネルグループ

トンネルグループは、トンネル接続ポリシーを決定するレコードのセットで構成されます。これらのレコードでは、トンネル ユーザが認証されるサーバ、およびアカウンティング サーバがある場合は接続情報の送信先となるサーバが指定されます。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。トンネルグループには、トンネル自体の作成に関連する少数のアトリビュートが含まれます。また、トンネルグループには、ユーザ関連のアトリビュートを定義するグループポリシーへのポインタも含まれます。

セキュリティ アプライアンスには、LAN-to-LAN 接続用の DefaultL2LGroup とリモートアクセス接続用の DefaultRAGroup、および WebVPN 接続用の DefaultWEBVPNGroup のデフォルト トンネルグループが用意されています。これらのデフォルト トンネルグループは変更できますが、削除はできません。また、環境に固有のトンネルグループを 1 つ以上作成することもできます。トンネルグループは、セキュリティ アプライアンスのローカルな設定であり、外部サーバでは設定できません。

トンネルグループでは、次のアトリビュートが指定されます。

- トンネルグループの一般接続パラメータ（P.26-3）
- トンネルグループの IPSec 接続パラメータ（P.26-4）
- トンネルグループの WebVPN 接続パラメータ（P.26-5）

トンネルグループの一般接続パラメータ

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

- トンネルグループ名：トンネルグループを追加または編集する場合にトンネルグループ名を指定します。次の考慮事項が適用されます。
  - 認証に事前共有キーを使用するクライアントの場合、トンネルグループ名は IPSec クライアントがセキュリティ アプライアンスに渡すグループ名と同じです。
  - 認証に証明書を使用するクライアントはこの名前を証明書の一部として渡し、セキュリティ アプライアンス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、IPSec リモートアクセス、IPSec LAN-to-LAN、および WebVPN があります。トンネルグループでは、接続タイプを 1 つだけ指定できます。
- 認証、認可、アカウンティング サーバ：これらのパラメータでは、セキュリティ アプライアンスが次の目的で使用するサーバのグループまたはリストを指定します。
  - ユーザの認証
  - ユーザがアクセスを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 グループは、1 つ以上のサーバで構成されます。
- 接続用のデフォルト グループポリシー：グループポリシーは、ユーザ関連のアトリビュートのセットです。デフォルト グループポリシーは、セキュリティ アプライアンスがトンネル ユーザを認証または認可する際にデフォルトで使用するアトリビュート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、セキュリティ アプライアンスがクライアントに割り当てる 1 つ以上の DHCP サーバまたはアドレス プールの値が含まれます。
- account-disabled の上書き：このパラメータにより、AAA サーバから受信した「account-disabled」インジケータを上書きできます。
- パスワード管理：このパラメータにより、現在のパスワードが指定された日数（デフォルトでは 14 日）で有効期限が切れることをユーザに警告して、パスワードを変更する機会をユーザに提供できます。

- グループの除去と領域の除去：これらのパラメータは、セキュリティ アプライアンスが受信したユーザ名を処理する方法を指示します。これらが適用されるのは、user@realm という形式で受信したユーザ名だけです。領域とは、ユーザ名に @ デリミタが負荷されている管理ドメインです（user@abc）。

  strip-group コマンドを指定する場合、セキュリティ アプライアンスは、VPN クライアントによって提示されるユーザ名からグループ名を取得してユーザ接続のトンネルグループを選択します。その後、セキュリティ アプライアンスは認可 / 認証のためにユーザ名のユーザ部分だけを送信します。それ以外の場合（ディセーブルになっている場合）、セキュリティ アプライアンスは領域を含むユーザ名全体を送信します。

  strip-realm コマンドの処理は、ユーザ名を認証または認可サーバに送信するときにユーザ名から領域を削除します。コマンドがイネーブルになっている場合、セキュリティ アプライアンスはユーザ名認可 / 認証のユーザ部分だけを送信します。それ以外の場合、セキュリティ アプライアンスはユーザ名全体を送信します。

- 認可の要求：このパラメータにより、ユーザのアクセス前に認可を要求するか、またはその要求を取り下げることができます。
- 認可 DN アトリビュート：このパラメータは、認可の実行時に使用する認定者名アトリビュートを指定します。

トンネルグループの IPSec 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、またはその両方。
  - 事前共有キーに基づく IKE 接続の場合は、接続ポリシーに関連付けられている英数字キー自体（長さ 128 文字まで）。
  - ピア ID 確認要求：このパラメータはピアの証明書を使用してピアの ID を確認することを要求するかどうかを指定します。
- ISAKMP（IKE）キープアライブの設定。この機能により、セキュリティ アプライアンスはリモート ピアの継続的な存在を監視し、自分自身の存在をピアに報告します。ピアが応答しなくなると、セキュリティ アプライアンスは接続を削除します。IKE キープアライブをイネーブルにすると、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、セキュリティ アプライアンスとリモート 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 VPN Client（Release 3.0 以上）
  - Cisco VPN 3000 Client（Release 2.x）
  - Cisco VPN 3002 ハードウェア クライアント
  - Cisco VPN 3000 シリーズ コンセントレータ
  - Cisco IOS ソフトウェア
  - Cisco Secure PIX Firewall

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

  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、P.26-26 の「グループポリシーの設定」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に、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のみ切断されます。IKE キープアライブがイネーブルになっている場合とは異なり、障害が発生したトラフィックは Peer Timeout Profile 値を持つトンネルから切断されません。

（注）　IKE メイン モードを使用する LAN-to-LAN コンフィギュレーションの場合は、2 つのピアの IKE キープアライブの設定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、（ID 証明書とすべての発行証明書をピアに送信する）証明書チェーン全体を送信するか、または発行証明書（ルート証明書とすべての下位 CA 証明書を含む）だけを送信するかを指定できます。
- Windows クライアント ソフトウェアの古いバージョンを使用しているユーザに、クライアントをアップデートする必要があることを通知できるため、アップデートされたクライアント バージョンを取得するためのメカニズムを提供できます。VPN 3002 ハードウェア クライアントのユーザの場合、自動アップデートをトリガーできます。すべてのトンネルグループまたは特定のトンネルグループに対して、クライアント アップデート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、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。

トンネルグループの WebVPN 接続パラメータ

次のアトリビュートは WebVPN 接続に固有です。

- AAA または証明書の認証方式。
- 適用するカスタマイゼーションの名前。カスタマイゼーションは、ログイン時にユーザに表示されるウィンドウの内容を決定します。カスタマイゼーション パラメータは、WebVPN 設定の一部として設定します。
- DNS サーバ グループ名。DNS サーバ グループは、DNS サーバ名、ドメイン名、ネーム サーバ、リトライ回数、および DNS サーバがトンネルグループに使用するタイムアウト値を指定します。
- 1 つ以上のグループ エイリアス。これらはサーバがトンネルグループを参照できる代替名です。ログイン時に、ユーザはドロップダウン メニューからグループ名を選択します。
- 1 つ以上のグループ URL。このパラメータを設定する場合、指定されている URL に加わるユーザは、ログイン時にグループを選択する必要はありません。
- デフォルトのグループポリシーとは異なる WebVPN ユーザ アクセス権を許可するグループポリシー。
- CIFS 名前解決に使用する NetBIOS ネーム サービス サーバ（nbns-server）の名前。

トンネルグループの設定

次の各項では、トンネルグループの内容とコンフィギュレーションについて説明します。

- デフォルトの IPSec リモートアクセス トンネルグループのコンフィギュレーション（P.26-6）
- トンネルグループの IPSec 一般パラメータの設定（P.26-6）
- IPSec リモートアクセス トンネルグループの設定（P.26-7）
- LAN-to-LAN トンネルグループの設定（P.26-12）
- WebVPN トンネルグループの設定（P.26-15）
- WebVPN ユーザ用のログイン ウィンドウのカスタマイズ（P.26-22）

デフォルト トンネルグループは変更可能です。また、3 つのトンネルグループ タイプの 1 つとして新しいトンネルグループを設定することもできます。トンネルグループのアトリビュートを明示的に設定しない場合、そのアトリビュートは、値をデフォルト トンネルグループから取得します。デフォルト トンネルグループのタイプは ipsec-ra 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 トンネルグループも含めて、すべてのトンネルグループ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。

デフォルトの IPSec リモートアクセス トンネルグループのコンフィギュレーション

デフォルトのリモートアクセス トンネルグループの内容は、次のとおりです。

```
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 authentication-server-group LOCAL
 no authorization-server-group
 no accounting-server-group
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 password-management password-expire-in-days 14
 no override-account-disable
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 300 retry 2
```

トンネルグループの IPSec 一般パラメータの設定

一般パラメータは、複数のトンネルグループ タイプにわたって共通です。IPSec リモートアクセスおよび WebVPN トンネルは、同じ一般パラメータの大部分を共有します。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な説明については、『*Cisco Security Appliance Command Reference*』を参照してください。次の各項では、IPSec リモートアクセス トンネルグループ、IPSec LAN-to-LAN トンネルグループ、および WebVPN トンネルグループの設定方法について説明します。

IPSec リモートアクセス トンネルグループの設定

ハードウェアまたはソフトウェア クライアントを使用して、リモート クライアントと中央サイトのセキュリティ アプライアンスとの間の接続をセットアップする場合は、IPSec リモートアクセス トンネルグループを使用します。IPSec リモートアクセス トンネルグループを設定するには、最初にトンネルグループ一般アトリビュートを設定してから、IPSec リモートアクセス アトリビュートを設定します。IPSec リモートアクセス VPN トンネルグループは、リモートアクセス IPSec クライアント接続にのみ適用されます。

IPSec リモートアクセス トンネルグループの名前とタイプの指定

トンネルグループを作成し、**tunnel-group** コマンドを入力してその名前とタイプを指定します。IPSec リモートアクセス トンネルの場合、タイプは ***ipsec-ra*** になります。

```
hostname(config)# tunnel-group tunnel_group_name type ipsec-ra
hostname(config)#
```

たとえば、TunnelGroup1 という名前の IPSec リモートアクセス トンネルグループを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup1 type ipsec-ra
hostname(config)#
```

IPSec リモートアクセス トンネルグループの一般アトリビュートの設定

トンネルグループの一般アトリビュートを設定または変更するには、次の手順でパラメータを指定します。

ステップ 1　一般アトリビュートを設定するには、tunnel-group general-attributes コマンドを入力して、トンネルグループの一般アトリビュート コンフィギュレーション モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

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

ステップ 2　認証サーバ グループがある場合、使用するグループの名前を指定します。指定した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、***LOCAL*** というキーワードを追加します。

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

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オプションで設定することができます。IPSec トンネルの終端位置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。次のコマンドは、test　という名前のインターフェイスで servergroup1 という名前のサーバを認証に使用するように、インターフェイス固有の認証を設定しています。

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

ステップ 3　認可サーバ グループがある場合、使用するグループの名前を指定します。この値を設定する場合、接続する認可データベースにユーザが存在する必要があります。

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

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

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

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

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

たとえば、次のコマンドは、comptroller という名前のアカウンティング サーバ グループ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)#
```

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

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

ステップ 6　DHCP サーバ（最大 10 サーバ）の名前または IP アドレス、および DHCP アドレス プール（最大 6 プール）の名前を指定します。デフォルトでは、DHCP サーバとアドレス プールは使用されません。

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

（注）　インターフェイス名は丸カッコで囲む必要があります。

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

ステップ 7　ユーザ名を AAA サーバに渡す前に、ユーザ名からグループまたは領域を除去するかどうかを指定します。デフォルトでは、グループ名も領域も除去されません。

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

領域は管理ドメインです。領域を除去すると、セキュリティ アプライアンスは、ユーザ名とグループ（ある場合）認証を使用します。グループを除去すると、セキュリティ アプライアンスは認証にユーザ名と領域（ある場合）を使用します。領域修飾子を削除するには **strip-realm** コマンドを入力し、認証時にユーザ名からグループ修飾子を削除するには strip-group コマンドを使用してします。両方の修飾子を削除すると、認証は *username* だけに基づいて実行されます。それ以外の場合は、*username@realm* または *username<delimiter> group* 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、**strip-realm** を指定する必要があります。

ステップ 8　オプションで、サーバが RADIUS、RADIUS with NT、または LDAP サーバである場合、パスワード管理をイネーブルにできます。この機能は、デフォルトでイネーブルになっていますが、現在のパスワードがまもなく有効期限切れになる場合にユーザに警告します。デフォルトでは、期限切れの 14 日前にユーザへの警告を開始します。

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

サーバが LDAP サーバの場合、期限切れが迫っていることをユーザに警告し始める有効期限までの日数（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）　トンネルグループの一般アトリビュート コンフィギュレーション モードで入力される **password-management** コマンドは、トンネルグループの ipsec アトリビュート モードで以前入力された非推奨の **radius-with-expiry** コマンドに置き換えられます。

このコマンドを設定する場合、セキュリティ アプライアンスはログイン時に、ユーザの現在のパスワードがまもなく期限切れになるか、または期限切れであることをリモート ユーザに通知します。その後セキュリティ アプライアンスは、パスワードを変更する機会をユーザに提供します。現在のパスワードの期限がまだ切れていない場合、ユーザは引き続きそのパスワードを使用してログインできます。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスはこのコマンドを無視します。

これはパスワードの期限切れまでの日数を変更するのではなく、まもなく期限切れになることをセキュリティ アプライアンスがユーザに警告し始めるまでの期限前の日数を変更すること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、日数も指定する必要があります。

日数を 0 にしてこのコマンドを指定すると、このコマンドはディセーブルになります。セキュリティ アプライアンスは、期限切れが迫っていることをユーザに通知しませんが、ユーザは期限が切れた後にパスワードを変更できます。

ステップ 9　オプションで、**override-account-disable** コマンドを入力して、AAA サーバから account-disabled インジケータを上書きする機能を設定します。

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

（注）　override-account-disable を許可すると、セキュリティ上のリスクが発生する可能性があります。

ステップ 10 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 つまたは複数のアトリビュートを指定します。このアトリビュートにより、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名として使用するかが指定されます。

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

たとえば、次のコマンドは、CN アトリビュートを認可用のユーザ名として使用することを指定しています。

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

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

ステップ 11 ユーザに接続を許可する前に、そのユーザ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-ipsec)# authorization-required
hostname(config-tunnel-ipsec)#
```

IPSec リモートアクセス トンネルグループの IPSec アトリビュートの設定

リモートアクセス トンネルグループに IPSec アトリビュートを設定するには、次の手順を実行します。次の説明では、すでに IPSec リモートアクセス トンネルグループが作成済みであると仮定しています。IPSec リモートアクセス トンネルグループには、IPSec LAN-to-LAN トンネルグループよりも多くのアトリビュートがあります。

ステップ 1 IPSec リモートアクセス トンネルグループのアトリビュートを指定するには、次のコマンドを入力してトンネルグループ ipsec アトリビュート モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

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

このコマンドによりトンネルグループ ipsec アトリビュート コンフィギュレーションモードに入ります。リモートアクセス トンネルグループの IPSec アトリビュートは、このモードで設定します。

たとえば、次のコマンドは、TG1 という名前のトンネルグループに関係するトンネルグループ ipsec アトリビュート 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 アトリビュート モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type ipsec-ra
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 IKE 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 リモートアクセス トンネルグループの IKE 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)# 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。

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)#
```

このアトリビュートは、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)# 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)# trust-point mytrustpoint
```

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。

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

threshold パラメータは、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で指定します（10 ～ 3600）。***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インターバルです（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。

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。

（注）　以前トンネルグループ ipsec-ra 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、推奨しません。トンネルグループ一般アトリビュート モードで入力される **password-management** コマンドが、これに代わります。

LAN-to-LAN トンネルグループの設定

IPSec LAN-to-LAN VPN トンネルグループは、LAN-to-LAN IPSec クライアント接続だけに適用されます。設定するパラメータの多くは IPSec リモートアクセス トンネルグループの場合と同じですが、LAN-to-LAN トンネルのほうがパラメータの数は少なくなっています。LAN-to-LAN トンネルグループを設定するには、この項の手順を実行します。

デフォルトの LAN-to-LAN トンネルグループのコンフィギュレーション

デフォルトの LAN-to-LAN トンネルグループの内容は、次のとおりです。

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

LAN-to-LAN トンネルグループのパラメータはリモートアクセス トンネルグループ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、値をデフォルトのトンネルグループから継承します。

LAN-to-LAN トンネルグループの名前とタイプの指定

トンネルグループ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 トンネルグループを作成するには、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 トンネルグループの一般アトリビュートの設定

トンネルグループの一般アトリビュートを設定するには、次の手順を実行します。

ステップ 1　general-attributes キーワードを指定して、トンネルグループ一般アトリビュート モードに入ります。

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

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

たとえば、docs という名前のトンネルグループの場合、次のコマンドを入力します。

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

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

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

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

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

ステップ 3　デフォルト グループポリシーの名前を指定します。

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

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

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

LAN-to-LAN IPSec アトリビュートの設定

IPSec アトリビュートを設定するには、次の手順を実行します。

ステップ 1　トンネルグループ IPSec アトリビュートを設定するには、IPSec アトリビュート キーワードとともに tunnel-group コマンドを入力して、トンネルグループ ipsec アトリビュート コンフィギュレーション モードに入ります。

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

たとえば、次のコマンドは、config-ipsec モードに入り、TG1 という名前のトンネルグループ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 アトリビュート 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 IKE 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)# pre-shared-key key
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、IPSec LAN-to-LAN トンネルグループの IKE 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)# 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)#
```

すべてのトンネルグループ タイプにこのアトリビュートを適用できます。

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)#
```

すべてのトンネルグループ タイプにこのアトリビュートを適用できます。

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で指定します（10 ～ 3600）。***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インターバルです（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。また、retry パラメータのデフォルト値は 2 です。

WebVPN トンネルグループの設定

WebVPN トンネルグループは、WebVPN 接続だけに適用されます。WebVPN トンネルグループのトンネルグループ一般アトリビュートは IPSec リモートアクセス トンネルグループの場合と同じですが、トンネルグループのタイプが webvpn であり、**strip-group** および **strip-realm** コマンドが適用されない点が異なります。WebVPN 固有のアトリビュートは個別に定義します。次の各項では、WebVPN トンネルグループの設定方法について説明します。

WebVPN トンネルグループの名前とタイプの指定

トンネルグループを作成し、グローバル コンフィギュレーション モードで **tunnel-group** コマンドを入力してその名前とタイプを指定します。IPSec リモートアクセス トンネルの場合、タイプは ***webvpn*** になります。

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

たとえば、TunnelGroup3 という名前の WebVPN トンネルグループを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup3 type webvpn
hostname(config)#
```

WebVPN トンネルグループの一般アトリビュートの設定

トンネルグループの一般アトリビュートを設定または変更するには、次の手順でパラメータを指定します。

ステップ 1　一般アトリビュートを設定するには、**tunnel-group general-attributes** コマンドを入力して、トンネルグループ一般アトリビュート コンフィギュレーション モードに入ります。プロンプトが次のように変化します。

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

以前の項で作成した TunnelGroup3 の一般アトリビュートを設定するには、次のコマンドを入力します。

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

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

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

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。次のコマンドは、test という名前のインターフェイスでサーバ servergroup1 を認証に使用するように、インターフェイス固有の認証を設定しています。

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

ステップ 3　オプションで、認可サーバ グループがある場合、使用するグループの名前を指定します。認可を使用しない場合は、ステップ 6 に進みます。この値を設定する場合、接続する認可データベースにユーザが存在する必要があります。

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

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

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

ステップ 4　ユーザに接続を許可する前に、そのユーザが正常に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-ipsec)# authorization-required
hostname(config-tunnel-ipsec)#
```

ステップ 5　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 つまたは複数のアトリビュートを指定します。このアトリビュートにより、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名として使用するかが指定されます。

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

たとえば、次のコマンドは、CN アトリビュートを認可用のユーザ名として使用することを指定しています。

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

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

ステップ 6　オプションで、アカウンティング サーバ グループがある場合、使用するグループの名前を指定します。アカウンティングを使用しない場合は、ステップ 7 に進みます。

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

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

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

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

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

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

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

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

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

（注）　インターフェイス名は丸カッコで囲む必要があります。

アドレス プールは、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して設定します。アドレス プールの設定については、第 27 章「VPN の IP アドレスの設定」を参照してください。

ステップ 9　オプションで、サーバが RADIUS、RADIUS with NT、または LDAP サーバである場合、パスワード管理をイネーブルまたはディセーブルにできます。この機能は、デフォルトでイネーブルになっていますが、現在のパスワードがまもなく有効期限切れになる場合にユーザに警告します。デフォルトでは、期限切れの 14 日前にユーザへの警告を開始します。

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

サーバが LDAP サーバの場合、期限切れが迫っていることをユーザに警告し始める有効期限までの日数を指定できます。

（注）　トンネルグループ一般アトリビュート コンフィギュレーション モードで入力される **password-management** コマンドは、トンネルグループ ipsec アトリビュート モードで以前入力された非推奨の **radius-with-expiry** コマンドに置き換えられます。

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

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

WebVPN トンネルグループの WebVPN アトリビュートの設定

WebVPN トンネルグループに固有のパラメータを設定するには、この項の手順を実行します。

ステップ 1　WebVPN トンネルグループのアトリビュートを指定するには、次のコマンドを入力してトンネルグループの webvpn アトリビュート モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

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

たとえば、sales という名前の WebVPN トンネルグループに webvpn アトリビュートを指定するには、次のコマンドを入力します。

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

ステップ 2　使用する認証方式 AAA、デジタル署名、またはその両方を指定するには、**authentication** コマンドを入力します。aaa または certificate あるいはその両方を、任意の順序で指定できます。

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

たとえば、AAA と証明書認証の両方を許可するには、次のコマンドを入力します。

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

ステップ 3　以前定義した Web ページ カスタマイゼーションを適用して、ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するには、customization コマンドを入力します。

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

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

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

カスタマイゼーション自体を WebVPN モードで設定します。

ステップ 4　セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NBNS サーバにクエリーを行います。WebVPN は、リモート システム上のファイルをアクセスまたは共有することを NetBIOS に要求します。WebVPN は、NetBIOS および CIFS プロトコルを使用して、リモート システム上のファイルをアクセスまたは共有します。コンピュータ名を使用して Windows コンピュータへのファイル共有接続を試みる場合、指定するファイル サーバは、ネットワーク上のリソースを識別する特定の NetBIOS 名に対応します。

セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NetBIOS ネーム サーバにクエリーを行います。WebVPN は、リモート システム上のファイルをアクセスまたは共有することを NetBIOS に要求します。

NBNS 機能を正常に動作させるには、少なくとも 1 つの NetBIOS サーバ（ホスト）を設定する必要があります。冗長性を確保するため、最大 3 つの NBNS サーバを設定できます。セキュリティ アプライアンスは、リストにある最初のサーバを NetBIOS/CIFS の名前解決に使用します。クエリーが失敗すると、次のサーバを使用します。

CIFS の名前解決に使用する NBNS（NetBIOS ネーム サービス）サーバの名前を指定するには **nbns-server** コマンドを使用します。サーバ エントリは最大 3 つまで入力できます。設定する最初のサーバはプライマリ サーバであり、その他のサーバは冗長性を確保するためのバックアップです。これが（単なる WINS サーバではなく）マスター ブラウザであるかどうかと、タイムアウト間隔、およびリトライ回数を指定することもできます。通常、WINS サーバまたはマスター ブラウザは、セキュリティ アプライアンスと同じネットワーク上にあるか、またはそのネットワークから到達可能です。リトライ回数より先にタイムアウト間隔を指定する必要があります。

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

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

```
hostname(config)# name 192.168.2.1 nbnsprimary
hostname(config-tunnel-webvpn)# nbns-server nbnsprimary master timeout 5 retry 3
hostname(config-tunnel-webvpn)# nbns-server 192.168.2.2 timeout 5 retry 3
hostname(config-tunnel-webvpn)#
```

タイムアウト間隔は 1 ～ 30 秒の範囲（デフォルトは 2）に、リトライ回数は 0 ～ 10 の範囲（デフォルトは 2）にすることができます。

トンネルグループの webvpn アトリビュート コンフィギュレーション モードの **nbns-server** コマンドは、webvpn コンフィギュレーション モードの非推奨のコマンドに置き換えられます。

ステップ 5　グループに代替の名前を指定するには、**group-alias** コマンドを使用します。グループ エイリアスを指定すると、ユーザがトンネルグループを参照できる代替名が 1 つ以上作成されます。ここで指定するグループ エイリアスは、ユーザのログイン ページでドロップダウン リストに表示されます。各グループには、それぞれ別個のコマンドで指定された複数のエイリアスを持つようにすることも、エイリアスを持たないようにすることもできます。この機能は、「Devtest」と「QA」のように、複数の通常名によって同じグループが認識される場合に便利です。

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

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

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

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

（注）　WebVPN トンネルグループ リストは、（ドロップダウン）グループ リストが表示されるようにイネーブルにしておく必要があります。

ステップ 6　グループに着信 URL または IP アドレスを指定するには、**group-url** コマンドを使用します。グループ URL または IP アドレスを指定すると、ユーザはログイン時にグループを選択する必要がなくなります。ユーザがログインするとき、セキュリティ アプライアンスは、ユーザの着信 URL またはアドレスを tunnel-group-policy テーブルで探します。URL またはアドレスが検出され、group-url がトンネルグループでイネーブルになっている場合、セキュリティ アプライアンスは、関連付けられているトンネルグループを自動的に選択して、ユーザ名フィールドとパスワード フィールドだけをログイン ウィンドウでユーザに提示します。これにより、ユーザ インターフェイスは簡略化され、さらにグループのリストがユーザに公開されないという利点が加わります。ユーザに表示されるログイン ウィンドウでは、そのトンネルグループに設定されたカスタマイゼーションが使用されます。

URL またはアドレスがディセーブルになっており、グループ エイリアスが設定されている場合、グループのドロップダウン リストも表示されるため、ユーザはグループを選択する必要があります。

グループに複数の URL またはアドレスを設定（あるいは設定しないことも）できます。各 URL またはアドレスは、個別にイネーブルまたはディセーブルにすることができます。指定した各 URL またはアドレスごとに別個の **group-url** コマンドを使用する必要があります。http または https プロトコルのいずれかを含む URL またはアドレス全体を指定する必要があります。

同じ URL またはアドレスを複数のグループに関連付けることはできません。セキュリティ アプライアンスは、トンネルグループの URL またはアドレスを受け入れる前に、URL またはアドレスが一意であることを確認します。

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

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

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

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

さらに詳細な例については、P.26-22 の「WebVPN ユーザ用のログイン ウィンドウのカスタマイズ」を参照してください。

ステップ 7　WebVPN トンネルグループに使用する DNS サーバを指定するには、**dns-group** コマンドを入力します。デフォルト値は DefaultDNS です。

```
hostname(config-tunnel-webvpn)# dns-group {hostname | ip_address}
hostname(config-tunnel-webvpn)#
```

dns-group コマンドは、ホスト名をトンネルグループの適切な DNS サーバに解決します。たとえば、server1 という名前の DNS サーバの使用を指定する場合、次のコマンドを入力します。

```
hostname(config)# name 10.10.10.1 server1
hostname(config-tunnel-webvpn)# dns-group server1
hostname(config-tunnel-webvpn)#
```

ステップ 8　（オプション）Cisco Secure Desktop Manager を使用してグループベース ポリシー アトリビュートを「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合、VPN 機能ポリシーを指定するには、**hic-fail-group-policy** コマンドを使用します。デフォルト値は DfltGrpPolicy です。

```
hostname(config-tunnel-webvpn)# hic-fail-group-policy name
hostname(config-tunnel-webvpn)#
```

Name は、WebVPN トンネルグループに作成されたグループポリシーの名前です。

このポリシーは、次の CSD クライアントのアクセス権を区別するための代替グループポリシーです。

- 「Use Failure Group-Policy」に設定されている CSD ロケーション エントリと一致するクライアント。
- 「Use Success Group-Policy, if criteria match」に設定された CSD ロケーション エントリと一致し、設定されているグループベース ポリシー基準と一致しないクライアント。詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。

次の例は、group2 という名前の代替グループポリシーを指定します。

```
hostname(config-tunnel-webvpn)# hic-fail-group-policy group2
hostname(config-tunnel-webvpn)#
```

（注） VPN 機能ポリシーを「Always use Success Group-Policy」に設定した場合、セキュリティ アプライアンスはこのアトリビュートを使用しません。

詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。

WebVPN ユーザ用のログイン ウィンドウのカスタマイズ

カスタマイゼーション プロファイルとトンネルグループの組み合せを使用して、さまざまなグループに異なるログイン ウィンドウをセットアップできます。たとえば、salesgui と呼ばれるカスタマイゼーション プロファイルを作成したとすれば、次の例で示すように、そのカスタマイゼーション プロファイルを使用する sales という名前の WebVPN トンネルグループを作成できます。

ステップ 1　webvpn モードで、WebVPN カスタマイゼーション（この場合は salesgui という名前）を定義して、デフォルトのロゴを mycompanylogo.gif に変更します。あらかじめ mycompanylogo.gif をセキュリティ アプライアンスのフラッシュ メモリにロードしてコンフィギュレーションを保存しておく必要があります。詳細については、WebVPN の章を参照してください。

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

ステップ 2　グローバル　コンフィギュレーション　モードで、ユーザ名をセットアップして、それを定義した WebVPN カスタマイゼーションに関連付けます。

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

ステップ 3　グローバル コンフィギュレーション モードで、sales という名前の WebVPN トンネルグループを作成します。

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

ステップ 4　このトンネルグループに salesgui カスタマイゼーションを使用することを指定します。

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

ステップ 5　セキュリティ アプライアンスへのログイン時にユーザがブラウザに入力するアドレスに、グループ URL を設定します。たとえば、セキュリティ アプライアンスの IP アドレスが 192.168.3.3 の場合、グループ URL を https://192.168.3.3 に設定します。

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

正常にログインするためにポート番号が必要になる場合は、コロンを前に付けてポート番号を含めます。セキュリティ アプライアンスは、この URL を sales トンネルグループにマップし、salesgui カスタマイゼーション プロファイルを、ユーザが https://192.168.3.3 にログインするときに表示されるログイン画面に適用します。

グループポリシー

この項では、グループポリシーとその設定方法について説明します。ここでは、次の項目について説明します。

- デフォルトのグループポリシー（P.26-24）
- グループポリシーの設定（P.26-26）

グループポリシーは、IPSec 接続用のユーザ関連のアトリビュート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 サーバ上に保存されます。トンネルグループは、トンネルの確立後、ユーザ接続の条件を設定するグループポリシーを使用します。グループポリシーを使用すると、アトリビュートのセット全体をユーザまたはユーザのグループに適用することができ、各ユーザに各アトリビュートを個別に指定する必要がなくなります。

ユーザにグループポリシーを割り当てたり、特定のユーザのグループポリシーを変更したりするには、グローバル コンフィギュレーション モードで **group-policy** コマンドを入力します。

セキュリティ アプライアンスには、デフォルトのグループポリシーが含まれています。変更は可能でも削除できないデフォルト グループポリシーだけではなく、環境に固有のグループポリシーを 1 つ以上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、セキュリティ アプライアンスの内部データベースに設定されます。外部グループは、RADIUS のような外部認証サーバに設定されます。グループポリシーには、次のアトリビュートがあります。

- ID
- サーバ定義
- クライアント ファイアウォールの設定
- トンネリング プロトコル
- IPSec の設定
- ハードウェア クライアントの設定
- フィルタ
- クライアント コンフィギュレーションの設定
- WebVPN の機能
- 接続の設定

デフォルトのグループポリシー

セキュリティ アプライアンスでは、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 グループポリシーは、DfltGrpPolicy という名前で必ずセキュリティ アプライアンス上に存在していますが、このデフォルト グループポリシーは、セキュリティ アプライアンスで使用するように設定しないと有効になりません。他のグループポリシーを設定する場合、明示的に指定しない任意のアトリビュートがその値をデフォルト グループポリシーから受け継ぎます。デフォルト グループポリシーを表示するには、次のコマンドを入力します。

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

デフォルト 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。コマンドのシンタックスは、`hostname(config)# group-policy DfltGrpPolicy {internal | external}` となっていますが、タイプを external に変更することはできません。

デフォルト グループポリシーの任意のアトリビュートを変更する場合は、次のように **group-policy attributes** コマンドを使用してアトリビュート モードに入り、その後、目的の任意のアトリビュート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）　アトリビュート モードは内部グループポリシーだけに適用されます。

セキュリティ アプライアンスが提供するデフォルトのグループポリシー DfltGrpPolicy は、次のとおりです。

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 wins-server none
 dns-server none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol IPSec
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 banner none
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 leap-bypass disable
 nem disable
 backup-servers keep-client-config
 client-firewall none
 client-access-rule none
 webvpn
  functions url-entry
  no html-content-filter
  no homepage
  no filter
  no url-list
  no port-forward
  port-forward-name value Application Access
```

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あらゆる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。グループポリシーを設定するには、次の項の手順を実行します。

外部グループポリシーの設定

外部グループポリシーは、指定した外部サーバからアトリビュート値を取得します。外部グループポリシーの場合は、セキュリティ アプライアンスがアトリビュートのクエリーを実行できる AAA サーバ グループを指定し、その外部 AAA サーバ グループからアトリビュートを取得するときに使用するパスワードを指定します。外部認証サーバを使用している場合、ユーザ名とグループ名は一意でなければならないことに留意してください。グループに名前を付ける場合、外部ユーザの名前と一致する名前を選択しないようにします。これとは逆に、外部ユーザに名前を割り当てる場合、外部グループの名前を選択しないようにします。

セキュリティ アプライアンスは、外部 LDAP または RADIUS サーバでのユーザ認可をサポートします。外部サーバを使用するようにセキュリティ アプライアンスを設定する前に、正しいセキュリティ アプライアンス認可アトリビュートでサーバを設定し、これらのアトリビュートのサブセットから個々のユーザに固有のアクセス権を割り当てる必要があります。付録 E「認可および認証用の外部サーバの設定」の手順に従って、外部サーバを設定します。

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、サーバ グループ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 タイプは RADIUS のみです。

たとえば、次のコマンドは、ExtRAD という名前の外部 RADIUS サーバからアトリビュートを取得する ExtGroup という名前の外部グループポリシーを作成し、アトリビュートを取得するときに使用するパスワードが newpassword パスワードであることを指定します。

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

（注）　付録 E「認可および認証用の外部サーバの設定」で説明しているように、複数のベンダー固有のアトリビュート（VSA）を設定できます。RADIUS サーバが Class アトリビュート（#25）を返すように設定されている場合、セキュリティ アプライアンスは、そのアトリビュートを使用してグループ名を認証します。RADIUS サーバで、アトリビュートは OU=*groupname* の形式をとる必要があります。ここで *groupname* は、たとえば OU=Finance のように、セキュリティ アプライアンスで設定されているグループ名と同じです。

内部グループポリシーの設定

内部グループポリシーを設定するには、グループポリシーの名前とタイプを指定します。

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

デフォルトのタイプは ***internal*** です。

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、内部グループポリシーのアトリビュートをその既存のグループポリシーの値に初期設定することができます。

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

グループポリシー アトリビュートの設定

内部グループポリシーの場合は、特定のアトリビュート値を指定できます。最初に、グローバル コンフィギュレーション モードで **group-policy attributes** コマンドを入力して、グループポリシーのアトリビュート モードに入ります。

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

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。グループポリシー アトリビュート モードでは、指定したグループポリシーのアトリビュートと値のペアを設定することができます。グループポリシー アトリビュート モードで、デフォルト グループから継承しないアトリビュートと値のペアを明示的に設定します。このためのコマンドを、次の各項で説明します。

WINS サーバおよび DNS サーバの設定

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

ステップ 1　プライマリとセカンダリの WINS サーバを指定します。

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

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

wins-server コマンドを入力するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定し、その後 WINS サーバ y.y.y.y を設定すると、2 番目のコマンドで最初のコマンドが上書きされ、y.y.y.y が単独の WINS サーバになります。サーバを複数設定する場合も同様です。以前に設定したサーバを上書きせずに WINS サーバを追加するには、このコマンドを入力するときにすべての WINS サーバの IP アドレスを指定します。

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

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

ステップ 2　プライマリとセカンダリの DNS サーバを指定します。

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

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

dns-server コマンドを入力するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、その後 DNS サーバ y.y.y.y を設定すると、2 番目のコマンドで最初のコマンドが上書きされ、y.y.y.y が単独の DNS サーバになります。サーバを複数設定する場合も同様です。以前に設定したサーバを上書きせずに DNS サーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを指定します。

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 DNS サーバを設定する方法を示しています。

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

VPN 固有アトリビュートの設定

VPN アトリビュートの値を設定するアトリビュートを設定するには、この項の手順を実行します。これらのアトリビュートは、アクセス時間、許可される同時ログイン数、タイムアウト、VPN 接続に使用する ACL の名前、およびトンネル プロトコルを制御します。

ステップ 1　VPN アクセス時間を設定します。これには、グループポリシー コンフィギュレーション モードで **vpn-access-hours** コマンドを使用して、グループポリシーを設定済みの time-range ポリシーに関連付けます。

```
hostname(config-group-policy)# vpn-access-hours value {time-range | none}
```

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。

time-range 変数は、グローバル コンフィギュレーション モードで **time-range** コマンドを使用して定義されたアクセス時間のセットの名前です。次の例は、FirstGroup という名前のグループポリシーを 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)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours value 824
```

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-simultaneous-logins** コマンドを使用して、任意のユーザに許可される同時ログイン数を指定します。

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

デフォルト値は 3 です。値の範囲は 0 ～ 2147483647 の整数です。グループポリシーは、別のグループポリシーからこの値を継承することができます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。次の例は、FirstGroup という名前のグループポリシーで最大 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)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
hostname(config-group-policy)#
```

（注）　同時ログインの最大数の制限は非常に大きいですが、複数の同時ログインの許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼす恐れがあります。

ステップ 3　グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを入力して、ユーザ タイムアウト期間を設定します。

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

最小時間は 1 分で、最大時間は 35791394 分です。デフォルトは 30 分です。この期間中に接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

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

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

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

ステップ 4　グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用して、VPN 接続の最大時間を設定します。

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

最小時間は 1 分で、最大時間は 35791394 分です。デフォルト値はありません。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

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

次の例は、FirstGroup という名前のグループポリシーに 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)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

ステップ 5　グループポリシー モードで **vpn-filter** コマンドを使用して、VPN 接続に使用する ACL の名前を指定します（このアトリビュートはユーザ名モードでも設定できます。その場合、グループポリシー値はユーザ名のもとで設定された値に置き換えられます）。

```
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、アクセスリスト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、アクセスリストが拒否されます。

次の例は、FirstGroup という名前のグループポリシーに対して acl_vpn という名前のアクセスリストを呼び出すフィルタ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-filter acl_vpn
hostname(config-group-policy)#
```

ステップ 6　このグループポリシーの VPN トンネル タイプ（IPSec または WebVPN）を指定します。

```
hostname(config-group-policy)# vpn-tunnel-protocol {webvpn | IPSec}
hostname(config-group-policy)#
```

デフォルトは IPSec です。このアトリビュート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 vpn-tunnel-protocol [webvpn | IPSec]
hostname(config-group-policy)#
```

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、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**：HTTP 対応 Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは不要です。

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 トンネルで接続するユーザに対して、1 つ以上のトンネリング 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 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 IPSec
hostname(config-group-policy)#
```

セキュリティ アトリビュートの設定

この項のアトリビュートは、グループの特定のセキュリティ設定を指定します。

ステップ 1　グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **password-storage** コマンドを使用し、ユーザがログイン パスワードをクライアント システムに保存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。パスワード保存は、セキュアなサイトにあることがわかっているシステムでのみ、イネーブルにします。

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

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

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

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

次の例は、FirstGroup という名前のグループポリシ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)# 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。

```
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 アトリビュート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、値を別のグループポリシーから継承できます。

```
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ことにより、モデムで接続するリモート ダイヤルイン ユーザのデータ伝送レートが高くなる可能性があります。

注意　データ圧縮を使用すると、ユーザ セッションごとのメモリ要求と CPU 使用率が増加し、結果としてセキュリティ アプライアンス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するリモート ユーザについてのみイネーブルにすることを推奨します。モデム ユーザ専用のグループポリシーを設計して、そのようなユーザに対してのみ圧縮をイネーブルにしてください。

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 キーの再生成時にユーザが再認証を受ける必要があるかどうかを指定します。IKE キーが再生成される際の再認証をイネーブルにすると、セキュリティ アプライアンスは初回のフェーズ 1 PKE ネゴシエーションでユーザにユーザ名とパスワードの入力を求めるプロンプトを表示し、IKE キーの再生成が発生するたびに同様にユーザ認証のプロンプトを表示します。再認証によりセキュリティがより強固になります。

設定されているキーの再生成インターバルが短い場合、ユーザは繰り返し認可要求を受けるため、不便を感じる場合があります。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の再生成インターバルを確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを入力して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータのキロバイト単位のライフタイムを表示します。IKE キーが再生成される際のユーザの再認証をディセーブルにするには、**disable** キーワードを入力します。IKE キーが再生成される際の再認証は、デフォルトで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、このコマンドの **no** 形式を入力して、re-xauth アトリビュートを実行コンフィギュレーションから削除します。

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

（注）　接続先にユーザが存在しない場合、再認証は失敗します。

ステップ 4　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** コマンドを使用することにより、トンネルグループだけを介してアクセスするようにリモート ユーザを制限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、セキュリティ アプライアンスがユーザの接続に関して要求する既存のトンネルグループの名前を指定します。group-lock は、VPN クライアントで設定されたグループが、そのユーザが割り当てられているトンネルグループと同じかどうかをチェックすることによって、ユーザを制限します。同じでない場合、セキュリティ アプライアンスはそのユーザによる接続を禁

止します。group-lock を設定しない場合、セキュリティ アプライアンスは割り当てられているグループを考慮せずに、ユーザを認証します。グループ ロックはデフォルトでディセーブルになっています。

group-lock アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別の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。

ステップ 5　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)#
```

完全転送秘密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。

完全転送秘密アトリビュート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)#
```

バナー メッセージの設定

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

（注）　バナー内の復帰改行は、2 文字として数えられます。

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

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

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

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

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

IPSec-UDP アトリビュートの設定

IPSec over UDP（IPSec through NAT と呼ばれることもあります）を使用すると、Cisco VPN クライアントまたはハードウェア クライアントは、NAT を実行しているセキュリティ アプライアンスに UDP 経由で接続することができます。この機能はデフォルトで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にのみ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。セキュリティ アプライアンスは、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、システムのパフォーマンスがわずかに低下する場合があります。

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、**ipsec-udp** コマンドに **enable** キーワードを指定します。

```
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、次のように **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 のアトリビュート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、IPSec over UDP の値を別のグループポリシーから継承できます。

また、IPSec over UDP を使用するように Cisco VPN クライアントを設定しておく必要があります（Cisco VPN クライアントは、デフォルトで IPSec over UDP を使用するように設定されています）。VPN 3002 では、IPSec over UDP を使用するためのコンフィギュレーションは必要ありません。

次の例は、FirstGroup という名前のグループポリシーに IPSec over UDP を設定する方法を示しています。

```
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、セキュリティ アプライアンスは設定されたポートでリスンし、他のフィルタ規則で 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、IPSec over UDP のポート値を別のグループポリシーから継承できます。

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

次の例は、FirstGroup という名前のグループポリシーの IPSec UDP ポートをポート 4025 に設定する方法を示しています。

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

スプリット トンネリング アトリビュートの設定

スプリット トンネリングを使用すると、リモートアクセス IPSec クライアントは、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリア テキスト形式でネットワーク インターフェイスに誘導したりすることができます。スプリット トンネリングがイネーブルになっている場合、IPSec トンネルの相手側を宛先としないパケットを暗号化する必要はありません。このようなパケットはトンネル上を復号化された状態で送信され、その後、最終的な宛先にルーティングされます。このコマンドは、このスプリット トンネリング ポリシーを特定のネットワークに適用します。

スプリット トンネリング ポリシーの設定

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規則を設定します。

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

デフォルトでは、すべてのトラフィックがトンネリングされます。スプリット トンネリング ポリシーを設定するには、グループポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを入力します。***split-tunnel-policy*** アトリビュート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、スプリット トンネリングの値を別のグループポリシーから継承できます。

トラフィックがクリア テキストで送信されるネットワークのリストは、**excludespecified** キーワードで定義します。この機能は、トンネル経由で企業ネットワークに接続しながら、プリンタなどのローカル ネットワーク デバイスにアクセスするリモート ユーザにとって便利です。このオプションは、Cisco VPN クライアントに対してのみ適用されます。

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

tunnelspecified キーワードでは、指定されたネットワークとの間のすべてのトラフィックがトンネリングされます。このオプションにより、スプリット トンネリングはイネーブルになります。このオプションでは、トンネリングするアドレスのネットワーク リストを作成することができます。これ以外のすべてのアドレスに対するデータは、クリア テキストで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

（注） スプリット　トンネリングは主としてトラフィック管理機能であり、セキュリティ機能ではありません。最大限のセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

次の例は、FirstGroup という名前のグループポリシーで、指定されたネットワークのトンネリングに関してだけ、スプリット トンネリング ポリシ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)# split-tunnel-policy tunnelspecified
```

スプリット トンネリング用ネットワーク リストの作成

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

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

スプリット トンネリングのネットワーク リストは、トラフィックをトンネル経由で送信する必要のあるネットワークと、トンネリングが不要なネットワークを区別します。セキュリティ アプライアンスは、ネットワーク リストに基づいてスプリット トンネリングを実行するかどうかを決定します。ネットワーク リストは、プライベート ネットワーク上のアドレスのリストで構成された ACL です。標準タイプの ACL のみが許可されます。

value *access-list name* パラメータは、トンネリングを実行する、または実行しないネットワークを列挙したアクセスリストを指定します。

none キーワードは、スプリット トンネリング用のネットワーク リストが存在しないことを示し、セキュリティ アプライアンス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 トンネリングのネットワーク リストが存在しない場合、ユーザはデフォルトまたは指定されたグループポリシー内に存在するネットワーク リストを継承します。ユーザがこのようなネットワーク リストを継承しないようにするには、**split-tunnel-network-list none** コマンドを入力します。

次の例は、FirstGroup という名前のグループポリシーに FirstList という名前のネットワーク リス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)# split-tunnel-network-list FirstList
```

トンネリング用ドメイン アトリビュートの設定

トンネリングされたパケットのデフォルトのドメイン名またはスプリット トンネルを介して解決されるドメインのリストを指定できます。次の各項では、これらのドメインの設定方法について説明します。

トンネリングされたパケットのデフォルト ドメイン名の設定

セキュリティ アプライアンスは、ドメイン フィールドが省略される DNS クエリーにドメインを追加するために、IPSec クライアントにデフォルトのドメイン名を渡します。デフォルトのドメイン名が存在しない場合、ユーザはデフォルト グループポリシーのドメイン名を継承します。グループポリシーのユーザにデフォルトの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、そのグループのデフォルト ドメイン名を示します。デフォルト ドメイン名が存在しないことを示すには、***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** キーワードとともに **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。

次の例は、FirstGroup という名前のグループポリシーに FirstDomain というデフォルト ドメイン名を設定する方法を示しています。

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

スプリット トンネリング用ドメインのリストの定義

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

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

すべてのスプリット トンネリング ドメイン リストを削除するには、引数を指定せずに **no split-dns** コマンドを入力します。これにより、**none** キーワードとともに **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* は、セキュリティ アプライアンスがスプリット 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。このコマンドのシンタックスは次のとおりです。

```
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、文字列全体で 255 文字を超えることはできません。英数字、ハイフン（-）、およびピリオド（.）のみを使用できます。デフォルトのドメイン名がトンネルを介して解決される場合、その名前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
```

VPN ハードウェア クライアント用アトリビュートの設定

この項にあるコマンドは、セキュア ユニット認証とユーザ認証をイネーブルまたはディセーブルにし、VPN ハードウェア クライアントのユーザ認証のタイムアウト値を設定します。また、これらのコマンドを使用すると、Cisco IP Phone と LEAP パケットが個々のユーザ認証をバイパスでき、ネットワーク拡張モードを使用するハードウェア クライアントが接続できるようになります。

セキュア ユニット認証の設定

セキュア ユニット認証は、VPN ハードウェア クライアントがトンネルを開始するたびにユーザ名とパスワードを使用して認証されるようにすることにより、セキュリティを強化します。この機能がイネーブルの場合、ハードウェア クライアントはユーザ名とパスワードを保存しません。セキュア ユニット認証はデフォルトでディセーブルになっています。

（注）　この機能がイネーブルの場合、VPN　トンネルを起動するには、ユーザがユーザ名とパスワードを入力する必要があります。

セキュア ユニット認証では、ハードウェア クライアントが使用するトンネルグループに対して認証サーバ グループが設定されている必要があります。プライマリ セキュリティ アプライアンスでセキュア ユニット認証を使用する必要がある場合は、すべてのバックアップ サーバにも必ず同じ設定を行ってください。

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

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

セキュア ユニット認証をディセーブルにするには、**disable** キーワードを入力します。セキュア ユニット認証のアトリビュート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、セキュア ユニット認証の値を別のグループポリシーから継承できます。

次の例は、FirstGroup という名前のグループポリシーでセキュア 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
```

ユーザ認証の設定

ユーザ認証はデフォルトでディセーブルになっています。ユーザ認証がイネーブルの場合、ハードウェア クライアントの背後の個々のユーザは、トンネルを介してネットワークにアクセスするために認証を受ける必要があります。個々のユーザは、設定した認証サーバの順序に従って認証されます。

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

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

ユーザ認証をディセーブルにするには、**disable** キーワードを入力します。ユーザ認証アトリビュート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、ユーザ認証の値を別のグループポリシーから継承できます。

プライマリ セキュリティ アプライアンスでユーザ認証を使用する必要がある場合は、すべてのバックアップ サーバにも必ず同じ設定を行ってください。

次の例は、FirstGroup という名前のグループポリシーでユーザ認証をイネーブルにする方法を示しています。

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

アイドル タイムアウトの設定

グループポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを入力して、ハードウェア クライアントの背後の個々のユーザにアイドル タイムアウトを設定します。アイドル タイムアウト期間中にハードウェア クライアントの背後のユーザによる通信アクティビティがない場合、セキュリティ アプライアンスはそのクライアントのアクセスを終了します。

```
hostname(config-group-policy)# user-authentication-idle-timeout {minutes | none}
hostname(config-group-policy)# no user-authentication-idle-timeout
```

（注）　**user-authentication-idle-timeout** コマンドで終了されるのは、VPN トンネルを経由したクライアントのアクセスだけであり、VPN トンネル自体は終了されません。

minutes パラメータには、アイドル タイムアウト期間の長さを分単位で指定します。最小値は 1 分、デフォルト値は 30 分、最大値は 35791394 分です。

アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、アイドル タイムアウト値を別のグループポリシーから継承できます。

アイドル タイムアウト値を継承しないようにするには、**none** キーワードを指定して **user-authentication-idle-timeout** コマンドを入力します。このコマンドにより、アイドル タイムアウトにヌル値が設定されます。この設定によってアイドル タイムアウトが拒否され、デフォルトまたは指定されたグループポリシーからユーザ認証のアイドル タイムアウト値が継承されなくなります。

次の例は、FirstGroup という名前のグループポリシーに 45 分の アイドル タイムアウト値を設定する方法を示しています。

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

IP Phone Bypass の設定

Cisco IP Phone は、ハードウェア クライアントの背後の個々のユーザ認証をバイパスさせることができます。IP Phone Bypass をイネーブルにするには、グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-phone-bypass** コマンドを入力します。IP Phone Bypass を使用すると、ハードウェア クライアントの背後の IP Phone はユーザ認証プロセスを実行しなくても接続が可能になります。IP Phone Bypass は、デフォルトでディセーブルになっています。イネーブルの場合、セキュア ユニット認証は有効なままになります。

IP Phone Bypass をディセーブルにするには、**disable** キーワードを入力します。IP Phone Bypass アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、IP Phone Bypass の値を別のグループポリシーから継承できます。

```
hostname(config-group-policy)# ip-phone-bypass {enable | disable}
hostname(config-group-policy)# no ip-phone-bypass
```

LEAP Bypass の設定

LEAP Bypass がイネーブルの場合、VPN 3002 ハードウェア クライアントの背後の無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過します。このアクションにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立し、その後、ユーザ単位で再度認証を実行することができます。LEAP Bypass は、デフォルトでディセーブルになっています。

シスコの無線アクセス ポイントからの LEAP パケットが個々のユーザ認証をバイパスできるようにするには、グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **leap-bypass** コマンドを入力します。LEAP Bypass をディセーブルにするには、**disable** キーワードを入力します。LEAP Bypass のアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、LEAP Bypass の値を別のグループポリシーから継承できます。

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

（注）　IEEE 802.1X は、有線および無線ネットワークにおける認証規格です。この規格では、クライアントと認証サーバの間で強力な相互認証を実現し、ユーザ単位およびセッション単位のダイナミックな無線暗号化秘密（WEP）キーの使用を可能にして、スタティックな WEP キーの場合に介在する面倒な管理作業やセキュリティ上の問題を軽減することができます。

シスコシステムズは、Cisco LEAP と呼ばれる 802.1X 無線認証タイプを開発しました。LEAP（Lightweight Extensible Authentication Protocol）は、無線クライアントと RADIUS サーバの間の接続における相互認証を実装します。パスワードなど、認証に使用されるクレデンシャルは、無線メディア上で送信される前に必ず暗号化されます。

Cisco LEAP では、無線クライアントを RADIUS サーバに対して認証します。RADIUS アカウンティング サービスは提供されません。

対話的なハードウェア クライアント認証をイネーブルにしている場合、この機能は意図したように動作しません。

注意　認証されていないトラフィックがトンネルを通過できるようにすると、ネットワークにセキュリティ リスクを招く恐れがあります。

次の例は、FirstGroup という名前のグループポリシーに LEAP Bypass を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

ネットワーク拡張モードのイネーブル化

ネットワーク拡張モードを使用すると、ハードウェア クライアントは、VPN トンネル経由でリモート プライベート ネットワークに 1 つのルーティング可能なネットワークを提供することができます。ハードウェア クライアントの背後のプライベート ネットワークからセキュリティ アプライアンスの背後のネットワークへのすべてのトラフィックは、IPSec でカプセル化されます。PAT は適用されません。したがって、セキュリティ アプライアンスの背後のデバイスは、トンネル経由でのみハードウェア クライアントの背後にあるプライベート ネットワーク上のデバイスに直接アクセスでき、逆方向の場合も同様にトンネル経由の場合にのみ可能になります。トンネルは、ハードウェア クライアントから開始する必要がありますが、トンネルの確立後はどちらの側からデータ交換を開始してもかまいません。

グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **nem** コマンドを入力し、ハードウェア クライアントの ネットワーク拡張モードをイネーブルにします。

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

NEM をディセーブルにするには、**disable** キーワードを入力します。この NEM のアトリビュート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、値を別のグループポリシーから継承できます。

次の例は、FirstGroup という名前のグループポリシーに NEM を設定する方法を示しています。

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

バックアップ サーバ アトリビュートの設定

バックアップ サーバを設定します（使用する予定がある場合）。IPSec バックアップ サーバを使用すると、VPN クライアントはプライマリ セキュリティ アプライアンスが使用不可の場合も接続が可能になります。バックアップ サーバを設定すると、セキュリティ アプライアンスは、IPSec トンネルを確立するときにクライアントにサーバ リストを渡します。バックアップ サーバは、クライアントまたはプライマリ セキュリティ アプライアンスにその設定を行うまでは存在しません。

バックアップ サーバは、クライアントまたはプライマリ セキュリティ アプライアンスのいずれかに設定します。セキュリティ アプライアンスにバックアップ サーバを設定すると、セキュリティ アプライアンスはバックアップ サーバ ポリシーをグループ内のクライアントに配信し、クライアントにバックアップ サーバ リストが設定されている場合はそのリストを置き換えます。

（注） ホスト名を使用している場合は、バックアップ用の DNS サーバおよび WINS サーバを、プライマリの DNS サーバおよび WINS サーバと異なる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 経由でそのハードウェア クライアントから DNS および WINS の情報を取得している場合に、プライマリ サーバへの接続が失われると、バックアップ サーバに別の DNS および WINS の情報があっても、クライアントは DHCP リースの期限が満了するまではアップデートされなくなります。また、ホスト名を使用している場合に DNS サーバ が使用不可になると、大幅な遅延が発生する恐れがあります。

バックアップ サーバを設定するには、グループポリシー コンフィギュレーション モードで **backup-servers** コマンドを入力します。

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

バックアップ サーバを削除するには、バックアップ サーバを指定してこのコマンドの **no** 形式を入力します。backup-servers アトリビュートを実行コンフィギュレーションから削除し、backup-servers の値を他のグループポリシーから継承できるようにするには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

clear-client-config キーワードは、クライアントでバックアップ サーバを使用しないことを指定します。セキュリティ アプライアンスはヌルのサーバ リストを配信します。

keep-client-config キーワードは、セキュリティ アプライアンスがバックアップ サーバ情報をクライアントに送信しないことを指定します。クライアントは、そのクライアントのサーバ リストを使用します（設定されている場合）。これがデフォルトです。

server1 server 2.... server10 パラメータ リストは、プライマリ セキュリティ アプライアンスが使用不可の場合に VPN クライアントが使用するサーバを、プライオリティ順にスペースで区切ったリストです。このリストには、サーバを IP アドレスまたはホスト名で指定します。このリストの長さは 500 文字までで、格納できるエントリは 10 個までです。

次の例は、FirstGroup という名前のグループポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップ サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

ファイアウォール ポリシーの設定

*ファイアウォール*は、データの個々の着信パケットと発信パケットをそれぞれ検査して、パケットを許可するかドロップするかどうか決定することにより、コンピュータをインターネットから分離して保護します。ファイアウォールは、グループのリモート ユーザがスプリット トンネリングを設定してある場合、セキュリティの向上をもたらします。この場合、ファイアウォールは、インターネットまたはユーザのローカル LAN を経由する侵入からユーザの PC を保護することで、企業ネットワークを保護します。VPN クライアントを使用してセキュリティ アプライアンスに接続しているリモート ユーザは、適切なファイアウォール オプションを選択できます。

グループポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用して、セキュリティ アプライアンスが 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** キーワードとともに **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 ポリシーが存在しない場合、ユーザはデフォルトまたはその他のグループポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがこのようなファイアウォール ポリシーを継承しないようにするには、**none** キーワードを指定して **client-firewall** コマンドを入力します。

Add or Edit Group Policy ウィンドウ、Client Firewall タブでは、追加または変更するグループポリシーに対して VPN クライアントのファイアウォール設定を指定できます。

（注）　これらのファイアウォール機能を使用できるのは、Microsoft Windows を実行する VPN クライアントだけです。現在、ハードウェア クライアントまたは他の（Windows 以外の）ソフトウェア クライアントでは、これらの機能は使用できません。

最初のシナリオでは、リモート ユーザの PC 上にパーソナル ファイアウォールがインストールされています。VPN クライアントは、ローカル ファイアウォールで定義されているファイアウォール ポリシーを適用し、そのファイアウォールが実行されていることを確認するために監視します。ファイアウォールの実行が停止すると、VPN クライアントはセキュリティ アプライアンスへの通信をドロップします（このファイアウ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監視するからです。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てセキュリティ アプライアンスへの接続が終了したことを認識します）。ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合もありますが、この方法を使用すれば、ユーザは各自の設定をカスタマイズできます。

第 2 のシナリオでは、VPN クライアント PC のパーソナル ファイアウォールに中央集中型ファイアウォール ポリシーを適用することが選択されることがあります。一般的な例としては、スプリット トンネリングを使用してグループのリモート PC へのインターネット トラフィックをブロックすることがあげられます。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。セキュリティ アプライアンスでは、VPN クライアントに適用するトラフィック管理規則のセットを作成し、これらの規則をフィルタに関連付けて、そのフィルタをファイアウォール ポリシーに指定します。セキュリティ アプライアンスは、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。

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。このコマンドに設定できるインスタンスは 1 つだけです。この一連のコマンドの後に記載された表 26-1 で、これらのコマンドのシンタックス要素について説明します。

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]
```

ZoneLabs ファイアウォール

```
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 26-1　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ように指定します。セキュリティ アプライアンス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。セキュリティ アプライアンスは、確認のために「Are You There?」という質問を行い、応答がない場合はトンネルを切断します。
cisco-integrated	Cisco 統合ファイアウォール 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です。
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 ポリシーが存在しないことを示します。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 タイプを示します。
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 タイプを示します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。

表 26-1　client-firewall コマンドのキーワードと変数（続き）

パラメータ	説明
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 ベンダーを指定します。
zonelabs-zonealarm	Zone Labs ZoneAlarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs ZoneAlarm 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 ZoneAlarm Pro ファイアウォール タイプを指定します。

次の例は、FirstGroup という名前のグループポリシーで、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方法を示しています。

```
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 アクセス規則の設定

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、セキュリティ アプライアンスを介して 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規則を指定します。次のガイドラインに従って規則を作成します。

- 規則を定義しない場合、セキュリティ アプライアンスはすべての接続タイプを許可します。
- クライアントがどの規則にも一致しない場合、セキュリティ アプライアンスは接続を拒否します。拒否規則を定義する場合は、許可規則も 1 つ以上定義しないと、セキュリティ アプライアンス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。各規則で複数回入力することができます。たとえば、**client-access rule 3 deny type * version 3.*** では、バージョン 3.x のソフトウェア リリースを実行しているすべてのクライアント タイプを拒否する、プライオリティ 3 のクライアント アクセス規則が作成されます。
- グループポリシーごとに最大 25 の規則を作成できます。
- 規則のセット全体で 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。

規則を削除するには、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
```

すべての規則を削除するには、引数を指定せずに **no client-access-rule** コマンドを入力します。これにより、**none** キーワードとともに **client-access-rule** コマンドを発行して作成したヌル規則があればそれも含めて、設定済みのすべての規則が削除されます。

デフォルトでは、アクセス規則はありません。クライアント アクセス規則が存在しない場合、ユーザはデフォルト グループポリシー内に存在する規則を継承します。

ユーザがクライアント アクセス規則を継承しないようにするには、**none** キーワードを指定して **client-access-rule** コマンドを入力します。このコマンドの結果、すべてのタイプとバージョンのクライアントが接続できるようになります。

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type type
version {version | none}

hostname(config-group-policy)# no client-access rule [priority {permit | deny} type
type version version]
```

表 26-2 で、これらのコマンドのキーワードとパラメータの意味を説明します。

表 26-2　client-access rule コマンドのキーワードと変数

パラメータ	説明
deny	特定のタイプまたはバージョン（あるいはその両方）のデバイスの接続を拒否します。
none	クライアント アクセス規則を許可しません。client-access-rule をヌル値に設定して、制限を拒否します。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値を継承しないようにします。
permit	特定のタイプまたはバージョン（あるいはその両方）のデバイスの接続を許可します。
priority	規則のプライオリティを決定します。最小の整数値を持つ規則の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またはバージョン（あるいはその両方）に一致し、最小の整数値を持つ規則が適用されます。それよりもプライオリティの低い規則は、セキュリティ アプライアンスでは無視されます。
type *type*	デバイス タイプを、「VPN 3002」などの自由形式の文字列で指定します。文字列は、**show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。
version *version*	デバイスのバージョンを、「7.0」などの自由形式の文字列で指定します。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。

次の例は、FirstGroup という名前のグループポリシーにクライアント アクセス規則を作成する方法を示しています。これらの規則は、バージョン 4.x のソフトウェアを実行する Cisco VPN クライアントを許可し、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、クライアントが接続時にセキュリティ アプライアンスに送信する固定値と一致している必要があります。

グループポリシーの WebVPN アトリビュートの設定

WebVPN によってユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェア クライアントもハードウェア クライアントも必要ありません。WebVPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。WebVPN は SSL およびその後継である TLS1 を使用して、リモートユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。WebVPN は、デフォルトではディセーブルになっています。

特定の内部グループポリシー用の WebVPN コンフィギュレーションをカスタマイズできます。

（注）グローバル コンフィギュレーション モードで webvpn モードを入力することによって、WebVPN のグローバル設定を構成できます。この項で説明する webvpn モード（グループポリシー コンフィギュレーション モードから入る webvpn モード）を使用すると、特定のグループポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

グループポリシーの webvpn コンフィギュレーション モードでは、すべての機能の設定を継承するか、または次のパラメータをカスタマイズするかどうかを指定できます。各パラメータについては、後述のステップで説明します。

- functions
- customizations
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server（single-signon server）
- auto-signon
- deny message
- SSL VPN Client（SVC）
- keep-alive ignore

多くの場合、WebVPN の設定の一部として WebVPN アトリビュートを定義した後、グループポリシーの webvpn アトリビュートを設定するときにこれらの定義を特定のグループに適用します。グループポリシーの コンフィギュレーション モードで **webvpn** コマンドを使用して、グループポリシーの webvpn コンフィギュレーション モードに入ります。グループポリシー用の webvpn コマンドは、ファイル、MAPI プロキシ、URL、および TCP アプリケーションへの WebVPN 経由のアクセスを定義します。フィルタリングする ACL とトラフィックの種類も特定します。WebVPN は、デフォルトではディセーブルになっています。WebVPN アトリビュートの設定の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』および『*Cisco Security Appliance Command Reference*』を参照してください。

グループポリシーの webvpn コンフィギュレーション モードで入力されたすべてのコマンドを削除するには、このコマンドの **no** 形式を入力します。これらの webvpn コマンドは、設定を行ったユーザ名またはグループポリシーに対して適用されます。

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

電子メール プロキシを使用するために WebVPN を設定する必要はありません。

次の例は、FirstGroup という名前のグループポリシーの webvpn コンフィギュレーション モードに入る方法を示しています。

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

グループポリシーの WebVPN 機能アトリビュートの設定

イネーブルにする WebVPN 機能を設定します。グループポリシーに対して、WebVPN を使用した、ファイル アクセスとファイル ブラウジング、HTTP プロキシ、MAPI プロキシ、および URL エントリを設定するには、webvpn モードで **functions** コマンドを入力します。これらの機能は、デフォルトではディセーブルです。

```
hostname(config-group-webvpn)# functions {auto-download | citrix | file-access |
file-browsing | file-entry | filter | http-proxy | mapi | none | port-forward |
url-entry}
```

設定した機能を削除するには、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ます。機能の値を継承しないようにするには、**functions none** コマンドを入力します。

functions none コマンドを発行して作成したヌル値を含めて、設定済みのすべての機能を削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-webvpn)# no functions [auto-download | citrix | file-access |
file-browsing | file-entry | filter | http-proxy | mapi | none | port-forward |
url-entry]
```

このコマンドで使用するキーワードの意味を、表 26-3 で説明します。

表 26-3　functions コマンドのキーワード

キーワード	意味
auto-download	ポート転送アプレットを自動的にダウンロードします。
citrix	Citrix をイネーブルにします。
file-access	ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルにすると、WebVPN ホーム ページにサーバ リストのファイル サーバが表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイル サーバとファイル共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ユーザがファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。
filter	webtype アクセスリストを適用します。

表 26-3　functions コマンドのキーワード（続き）

キーワード	意味
http-proxy	HTTP アプレット プロキシのクライアントへの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、Flash など、適切なマングリングを妨げる技術に対して有用です。セキュリティ アプライアンスの使用を継続しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ コンフィギュレーションを自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、実質的にすべてのクライアント サイド技術をサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。
mapi	Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。
none	すべての WebVPN の **functions** にヌルを設定します。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機能を継承しないようにします。
port-forward	ポート転送をイネーブルにします。
url-entry	ユーザの URL エントリをイネーブルまたはディセーブルにします。イネーブルにしても、セキュリティ アプライアンスは設定されている URL またはネットワーク ACL で、URL を制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは、WebVPN ユーザがホーム ページの URL にのみアクセスできるように制限します。

次の例は、FirstGroup という名前のグループポリシーに対して、ファイル アクセス、ファイル ブラウジング、および MAPI プロキシを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions file-access file-browsing MAPI
hostname(config-group-webvpn)#
```

カスタマイゼーションの適用

カスタマイゼーションは、ログイン時にユーザに表示されるウィンドウの内容を決定します。カスタマイゼーション パラメータは、WebVPN 設定の一部として指定します。以前定義した Web ページ カスタマイゼーションを適用して、ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するには、ユーザ名の webvpn コンフィギュレーション モードで customization コマンドを入力します。

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

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

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

「拒否」メッセージの指定

Web VPN に正しくログインしたリモート ユーザに送信されるメッセージを指定できます。リモート ユーザが VPN 特権を持たない場合は、グループポリシーの webvpn コンフィギュレーション モードで **deny-message** コマンドを入力すると、リモート ユーザに送信されるメッセージを指定できます。

```
hostname(config-group-webvpn)# deny-message value "message"
hostname(config-group-webvpn)# no deny-message value "message"
hostname(config-group-webvpn)# deny-message none
```

no deny-message value コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

no deny-message none コマンドは、トンネルグループのポリシー コンフィギュレーションからアトリビュートを削除します。このポリシーはアトリビュート値を継承します。

メッセージには、最長で特殊文字、スペース、および句読点を含めて英数字 491 文字を使用できますが、囲みの引用符はカウントされません。ログイン時には、リモート ユーザのブラウザにテキストが表示されます。**deny-message value** コマンドに文字列を入力しているときは、コマンドがラップしても入力を続けてください。

デフォルトの拒否メッセージは、「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.」です。

次の例の最初のコマンドは、Group2 という名前の内部グループポリシーを作成します。後続のコマンドは、そのポリシーに関連付けられている webvpn 拒否メッセージが含まれたアトリビュートを変更します。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK.
However, you have not been granted rights to use the VPN features. Contact your
administrator for more information."
hostname(config-group-webvpn)
```

グループポリシーの WebVPN フィルタ アトリビュートの設定

webvpn モードで **html-content-filter** コマンドを使用して、このグループポリシーの WebVPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするかどうかを指定します。HTML フィルタリングは、デフォルトでディセーブルです。

コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**none** キーワードとともに **html-content-filter** コマンドを発行して作成したヌル値を含めて、すべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。HTML コンテンツ フィルタを継承しないようにするには、**none** キーワードを指定して **html-content-filter** コマンドを入力します。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

```
hostname(config-group-webvpn)# html-content-filter {java | images | scripts | cookies
| none}

hostname(config-group-webvpn)# no html-content-filter [java | images | scripts |
cookies | none]
```

このコマンドで使用するキーワードの意味を、表 26-4 で説明します。

表 26-4　filter コマンドのキーワード

キーワード	意味
cookies	イメージからクッキーを削除して、アドバタイズメント フィルタリングを制限し、プライバシーを保持します。
images	イメージへの参照を削除します（<IMG> タグを削除）。
java	Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> の各タグを削除）。
none	フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
scripts	スクリプトへの参照を削除します（<SCRIPT> タグを削除）。

次の例は、FirstGroup という名前のグループポリシーに、Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
hostname(config-group-webvpn)#
```

ユーザ ホームページの指定

グループポリシーの webvpn コンフィギュレーション モードで **homepage** コマンドを使用して、このグループのユーザのログイン時に表示される Web ページの URL を指定します。デフォルトのホーム ページはありません。

homepage none コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。ホーム ページを継承しないようにするには、**homepage none** コマンドを入力します。

none キーワードは、WebVPN ホームページがないことを示します。これにより、ヌル値が設定されてホーム ページが拒否され、ホーム ページが継承されなくなります。

キーワード ***value*** の後ろの *url-string* 変数で、ホームページの URL を指定します。文字列の先頭は、http:// または https:// にする必要があります。

```
hostname(config-group-webvpn)# homepage {value url-string | none}
hostname(config-group-webvpn)# no homepage
hostname(config-group-webvpn)#
```

自動サインオンの設定

auto-signon コマンドは、WebVPN ユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のために WebVPN ログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の auto-signon コマンドを入力でき、コマンドは入力順序に従って処理されます（先に入力されたコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名はグループに優先し、グループはグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、使用する認証の対象範囲によって異なります。

特定のサーバへの特定のユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URI を指定してこのコマンドの **no** 形式を使用します。すべてのサーバへの認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、値をグループポリシーから継承できます。

次の例では、webvpn コンフィギュレーション モードで入力し、基本認証を使用して、10.1.1.0 から 10.1.1.255 の範囲の IP アドレスを持つサーバへの anyuser という名前のユーザの自動サインオンを設定します。

次の例では、基本認証または NTLM 認証を使用して、Web VPN ユーザの ExamplePolicy グループに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
hostname(config-group-webvpn)#
```

次の例では、基本認証または NTLM 認証を使用して、Web VPN ユーザの ExamplePolicy2 グループに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
all
hostname(config-group-webvpn)#
```

WebVPN 接続に使用するアクセスリストの指定

webvpn モードで **filter** コマンドを使用して、このグループポリシーまたはユーザ名で WebVPN 接続に使用するアクセスリストの名前を指定します。**filter** コマンドを入力して指定するまで、WebVPN アクセスリストは適用されません。

filter none コマンドを発行して作成したヌル値を含めて、アクセスリストを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

filter コマンドを入力して指定するまで、WebVPN アクセスリストは適用されません。

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

```
hostname(config-group-webvpn)# filter {value ACLname | none}
hostname(config-group-webvpn)# no filter
```

none キーワードは、**webvpntype** アクセスリストがないことを示します。これにより、ヌル値が設定されてアクセスリストが拒否され、別のグループポリシーからアクセスリストが継承されなくなります。

キーワード ***value*** の後ろの *ACLname* 文字列で、すでに設定されているアクセスリストの名前を指定します。

（注）　***functions*** コマンドでは、***filter*** を選択しておく必要があります。WebVPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次の例は、FirstGroup という名前のグループポリシーに対して *acl_in* という名前のアクセスリストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
hostname(config-group-webvpn)#
```

URL リストの適用

グループポリシーの WebVPN ホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して 1 つ以上の名前付きリストを作成する必要があります。特定のグループポリシーに WebVPN サーバと URL のリストを適用して、特定のグループポリシーのリストにある URL にアクセスできるようにするには、グループポリシーの webvpn コンフィギュレーションモードに入って、**url-list** コマンドを実行する際に、作成するリストの名前を使用します。デフォルトの URL リストはありません。

url-list none コマンドを使用して作成したヌル値を含めて、リストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。URL リストを継承しないようにするには、**url-list none** コマンドを入力します。コマンドを 2 回使用すると、先行する設定値が上書きされます。

```
hostname(config-group-webvpn)# url-list {value name | none} [index]
hostname(config-group-webvpn)# no url-list
```

表 26-5 に、**url-list** コマンドのパラメータと意味を示します。

表 26-5　url-list コマンドのキーワードと変数

パラメータ	意味
index	ホームページでの表示優先順位を示します。
none	URL リストにヌル値を設定します。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リストを継承しないようにします。
value *name*	事前に設定されている URL のリストの名前を指定します。そのようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

次の例では、FirstGroup という名前のグループポリシーに FirstGroupURLs という名前の URL リストを設定し、これがホームページに表示される最初の URL リストになるように指定します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
hostname(config-group-webvpn)#
```

グループポリシーの WebVPN アプリケーション アクセス のイネーブル化

このユーザの WebVPN アプリケーション アクセスをイネーブルにするには、グループポリシーの webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート転送は、デフォルトではディセーブルになっています。

グループポリシーの webvpn コンフィギュレーション モードで **port-forward** コマンドを入力し、アプリケーション アクセスをイネーブルにする前に、WebVPN 接続でユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力し、このリストを定義します。

port-forward none コマンドを発行して作成したヌル値を含めて、コンフィギュレーションからポート転送アトリビュートを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、リストを別のグループポリシーから継承できます。ポート転送リストを継承しないようにするには、***none*** キーワードを指定して **port-forward** コマンドを入力します。***none*** キーワードは、フィルタリングが実行されないことを示します。これにより、ヌル値が設定されてフィルタリングが拒否され、フィルタリング値が継承されなくなります。

このコマンドのシンタックスは次のとおりです。

```
hostname(config-group-webvpn)# port-forward {value listname | none}
hostname(config-group-webvpn)# no port-forward
```

キーワード ***value*** の後ろの *listname* 文字列で、WebVPN ユーザがアクセスできるアプリケーションのリストを指定します。webvpn コンフィギュレーション モードで port-forward コマンドを入力し、このリストを定義します。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

次の例は、FirstGroup という名前の内部グループポリシーに *ports1* というポート転送リストを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
hostname(config-group-webvpn)#
```

ポート転送表示名の設定

グループポリシーの webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用して、特定のユーザまたはグループポリシーでエンド ユーザへの TCP ポート転送を識別する表示名を設定します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するには、コマンドの **no** 形式を入力します。**no** オプションは、デフォルト名の Application Access を復元します。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。このコマンドのシンタックスは次のとおりです。

```
hostname(config-group-webvpn)# port-forward-name {value name | none}
hostname(config-group-webvpn)# no port-forward-name
```

次の例は、*FirstGroup* という名前の内部グループポリシーに Remote Access TCP Applications という名前を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
hostname(config-group-webvpn)#
```

セッション タイマー更新のために無視する最大オブジェクト サイズの設定

ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回線が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定したサイズ以下のすべてのメッセージをキープアライブ メッセージと見なし、セッション タイマーの更新時にトラフィックと見なさないようセキュリティ アプライアンスに指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

トランザクションごとに無視する HTTP/HTTPS トラフィックの上限を指定するには、グループポリシー アトリビュートの webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

The **no** form of the command removes this specification from the configuration:

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

SSO サーバの指定

WebVPN だけに使用できるシングル サインオンのサポートを使用すると、ユーザはユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。**sso-server value** コマンドをグループポリシーの webvpn モードで入力すると、SSO サーバをグループポリシーに割り当てることができます。

SSO サーバをグループポリシーに割り当てるには、グループポリシーの webvpn コンフィギュレーション モードで **sso-server value** コマンドを入力します。このコマンドは、コンフィギュレーションに CA SiteMinder コマンドが含まれていることを必要とします。

```
hostname(config-group-webvpn)# sso-server value server_name
hostname(config-group-webvpn)#
```

この割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。デフォルト ポリシーを継承しないようにするには、**sso-server none** コマンドを入力します。

```
hostname(config-group-webvpn)# sso-server {value server_name | none}
hostname(config-group-webvpn)# [no] sso-server value server_name
```

SSO サーバに割り当てられているデフォルト ポリシーは DfltGrpPolicy です。

次の例では、グループポリシー「my-sso-grp-pol」を作成して、「example」という名前の SSO サーバに割り当てます。

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

SVC の設定

SSL VPN Client（SVC）は、ネットワーク管理者がリモート コンピュータに IPSec VPN をインストールして設定しなくても、リモート ユーザが IPSec VPN クライアントの利点を活用できる VPN トンネリング テクノロジーです。SVC は、リモート コンピュータの既存の SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVC セッションを確立するには、リモート ユーザはセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスをブラウザに入力します。ブラウザはそのインターフェイスに接続して WebVPN のログイン画面を表示します。ユーザがログインと認証を完了し、ユーザが SVC を*必要としていることをセキュリティ アプライアンスが確認すると、セキュリティ アプライアンスは* SVC をリモート コンピュータにダウンロードします。セキュリティ アプライアンスが、SVC を使用する*オプション*がユーザにあると確認した場合、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをユーザ画面に表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC は自動的にインストールと設定を実行します。接続が切断されると（設定に応じて）、SVC はリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

セキュリティ アプライアンスは、さまざまなリモート コンピュータのオペレーティング システム用に、複数の独自の SVC イメージをキャッシュ メモリ内に備えている場合もあります。ユーザが接続を試みると、セキュリティ アプライアンスは、イメージとオペレーティング システムが一致するまで引き続きこれらのイメージの部分をリモート コンピュータにダウンロードできます。一致した時点で、SVC 全体をダウンロードします。接続のセットアップ時間を短縮するため、ダウンロードされる最初のイメージが、最もよく遭遇するリモート コンピュータのオペレーティング システムになるように SVC イメージの順序を指定できます。SVC のインストールと使用の詳細については、第 31 章「SSL VPN クライアントの設定」を参照してください。

第 31 章「SSL VPN クライアントの設定」に示すように、SVC をイネーブルにした後は、特定のグループの SVC 機能をイネーブルまたは必須にできます。この機能は、デフォルトでディセーブルになっています。SVC をイネーブルまたは必須にすると、この項で説明している一連の svc コマンドをイネーブルにできます。SVC とその関連する svc コマンドをイネーブルにするには、グループポリシーの webvpn コンフィギュレーション モードで次の手順を実行します。

ステップ 1　セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードできるようにするには、**svc enable** コマンドを入力します。このコマンドは、デフォルトではディセーブルになっています。セキュリティ アプライアンスは SVC ファイルをダウンロードしません。このコンフィギュレーションから **svc enable** コマンドを削除するには、このコマンドの ***no*** 形式を使用します。

```
hostname(config-group-webvpn)# svc {none | enable | required}
hostname(config-group-webvpn)#
```

（注）　**no svc enable** コマンドを入力しても、アクティブな SVC セッションは終了しません。

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

ステップ 2　SVC 接続経由で特定のグループについて HTTP データの圧縮をイネーブルにするには、svc compression コマンドを入力します。SVC 圧縮は、デフォルトで ***deflate***（イネーブル）に設定されています。特定のグループの圧縮をディセーブルにするには、***none*** キーワードを使用します。svc compression コマンドを削除して値が継承されるようにするには、このコマンドの ***no*** 形式を使用します。

```
hostname(config-group-webvpn)# svc compression {deflate | none}
hostname(config-group-webvpn)#
```

次の例では、sales という名前のグループポリシーの SVC 圧縮をディセーブルにします。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
hostname(config-group-webvpn)#
```

ステップ 3　セキュリティ アプライアンスで dead-peer-detection（DPD）をイネーブルにして、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定するには、**svc dpd-interval** コマンドを使用します。このコンフィギュレーションから **svc dpd-interval** コマンドを削除するには、このコマンドの ***no*** 形式を使用します。このグループの SVC DPD をディセーブルにするには、***none*** キーワードを使用します。

```
hostname(config-group-webvpn)# svc dpd-interval {[gateway {seconds | none}] | [client
{seconds | none}]}
hostname(config-group-webvpn)#
```

DPD チェックは、デフォルトでディセーブルになっています。

ゲートウェイは、セキュリティ アプライアンスのことです。セキュリティ アプライアンスが DPD テストを実行する頻度を、30 ～ 3600 秒（1 時間）の範囲で指定できます。***none*** を指定すると、セキュリティ アプライアンスが実行する DPD テストはディセーブルになります。

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

次の例では、sales という名前の既存のグループポリシーについて、セキュリティ アプライアンス（ゲートウェイ）によって実行される DPD の頻度を 3000 秒に設定し、クライアントによって実行される DPD の頻度を 1000 秒に設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dpd-interval gateway 3000
hostname(config-group-webvpn)# svc dpd-interval client 1000
hostname(config-group-webvpn)#
```

ステップ 4　接続のアイドル状態を維持できる時間をデバイスが制限している場合でも、プロキシ、ファイアウォール、または NAT デバイスを通じて SVC 接続のオープン状態を維持するように、キープアライブ メッセージの頻度を調整できます（*seconds* で指定）。

頻度を調整することで、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベースの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、SVC が切断して再接続をしないようにできます。

リモート コンピュータ上の SVC がキープアライブ メッセージをセキュリティ アプライアンスに送信する頻度（15 ～ 600 秒）を設定するには、**svc keepalive** コマンドを使用します。コンフィギュレーションからこのコマンドを削除して値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# svc keepalive {none | seconds}
hostname(config-group-webvpn)# no svc keepalive {none | seconds}
hostname(config-group-webvpn)#
```

SVC キープアライブは、デフォルトでディセーブルになっています。キーワード ***none*** を使用すると SVC キープアライブ メッセージがディセーブルになります。

次の例では、SVC 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)# svc keepalive 300
hostname(config-group-webvpn)#
```

ステップ 5　SVC がリモート コンピュータに永続的にインストールされた状態を保つには、***installed*** キーワードを指定して **svc keep-installer** コマンドを使用します。コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# svc keep-installer {installed | none}
hostname(config-group-webvpn)# no svc keep-installer {installed | none}
hostname(config-group-webvpn)#
```

デフォルトでは、SVC の永続的インストールがディセーブルになっています。SVC セッションの終わりに、SVC はリモートコンピュータからアンインストールされます。

次の例では、このグループのリモート コンピュータの SVC インストール状態を維持す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)# svc keep-installer installed
hostname(config-group-webvpn)#
```

ステップ 6　SVC が SVC セッションでキーの再生成を実行できるようにするには、**svc rekey** コマンドを使用します。キーの再生成をディセーブルにして、コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# svc rekey {method {ssl | new-tunnel} | time minutes |
none}}
hostname(config-group-webvpn)# no svc rekey {method {ssl | new-tunnel} | time minutes
| none}}
hostname(config-group-webvpn)#
```

SVC キーの再生成は、デフォルトでディセーブルになっています。

方式を new-tunnel に指定すると、SVC キーの再生成中に SVC が新しいトンネルを確立することが指定されます。方式を none に指定すると、SVC キーの再生成はディセーブルになります。方式を ssl に指定すると、SSL の再ネゴシエーションは SVC キーの再生成中に行われます。方式を指定する代わりに、セッションの開始からキーの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。

次の例で示すように、コマンドが ***no*** 形式の場合は、必要なのは最小限だけです。

```
hostname(config-username-webvpn)# no svc rekey method
hostname(config-username-webvpn)#
```

ただし、方式を new-tunnel に指定する場合は、次のようになります。

```
hostname(config-username-webvpn)# no svc rekey method new-tunnel
hostname(config-username-webvpn)#
```

しかし、現在の方式は ssl であり、値が一致しないためにコマンドは失敗します。

次の例では、キーの再生成中に SVC が SSL と再ネゴシエートするように設定し、キーの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ます。

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

ユーザ アトリビュートの設定

この項では、ユーザ アトリビュートとその設定方法について説明します。ここでは、次の項目について説明します。

- ユーザ名のコンフィギュレーションの表示（P.26-60）
- 特定ユーザのアトリビュートの設定（P.26-61）

デフォルトでは、ユーザは、割り当てられているグループポリシーからすべてのユーザ アトリビュートを継承します。また、セキュリティ アプライアンスでは、ユーザ レベルで個別にアトリビュートを割り当て、そのユーザに適用されるグループポリシーの値を上書きすることができます。たとえば、すべてのユーザに営業時間内のアクセスを許可し、特定のユーザに 24 時間のアクセスを許可するグループポリシーを指定することができます。

ユーザ名のコンフィギュレーションの表示

すべてのユーザ名のコンフィギュレーションを、グループポリシーから継承したデフォルト値も含めて表示するには、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#
```

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リストに表示されます。この例では、ユーザ名は testuser と ppurkm です。継承した値も含めて、これらの設定済みのユーザのコンフィギュレーションは、次のとおりです。

```
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
username testuser attributes
 vpn-group-policy testing
 vpn-access-hours value averylongtime
 vpn-simultaneous-logins 4
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter value tunneled
 no vpn-framed-ip-address
 group-lock value test
 webvpn
  no functions
  html-content-filter java images scripts cookies
  no homepage
  no filter
  no url-list
  no port-forward
  no port-forward-name

username ppurkm password vt/qqEzfgfrXXya4 encrypted privilege 2
username ppurkm attributes
 no vpn-group-policy
 vpn-tunnel-protocol webvpn
 no vpn-framed-ip-address
 webvpn
  functions url-entry file-access file-entry file-browsing
  no html-content-filter
  no homepage
  no filter
  no url-list
  no port-forward
  no port-forward-name
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
username newuser nopassword privilege 15
```

特定ユーザのアトリビュートの設定

特定のユーザを設定するには、**username** コマンドを使用してユーザ名モードに入り、ユーザにパスワード（パスワードなしも可）とアトリビュートを割り当てます。指定しなかったすべてのアトリビュートは、グループポリシーから継承されます。

内部ユーザ認証データベースは、**username** コマンドを使用して入力されたユーザで構成されています。**login** コマンドは、このデータベースを認証に使用します。セキュリティ アプライアンスのデータベースにユーザを追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、このコマンドの **no** 形式を使用して削除するユーザ名を指定します。すべてのユーザ名を削除するには、ユーザ名を指定せずに **clear configure username** コマンドを使用します。

ユーザのパスワードと特権レベルの設定

ユーザにパスワードと特権レベルを割り当てるには、**username** コマンドを入力します。***nopassword*** キーワードを入力して、そのユーザにパスワードが不要であることを指定することもできます。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、そのユーザの特権レベルを設定できます。特権レベルの範囲は 0（最低）～ 15 です。一般に、システム管理者は最高の特権レベルを持ちます。デフォルトのレベルは 2 です。

```
hostname(config)# username name {nopassword | password password [encrypted]}
[privilege priv_level]}
```

```
hostname(config)# no username [name]
```

表 26-6 で、このコマンドで使用するキーワードと変数の意味を説明します。

表 26-6　username コマンドのキーワードと変数

キーワード / 変数	意味
encrypted	パスワードの暗号化を指定します。
name	ユーザの名前を指定します。
nopassword	このユーザにパスワードが不要であることを指定します。
password *password*	このユーザにパスワードが存在することを示し、パスワードを指定します。
privilege *priv_level*	このユーザの特権レベルを設定します。範囲は 0 ～ 15 です。この数値が低いほど、コマンドの使用やセキュリティ アプライアンス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する VPN ユーザにはアトリビュートやグループポリシーは関連付けられません。すべての値を明示的に設定する必要があります。

次の例は、暗号化されたパスワードが pw_12345678 で、特権レベルが 12 の anyuser という名前のユーザを設定する方法を示しています。

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege 12
hostname(config)#
```

ユーザ アトリビュートの設定

ユーザのパスワード（存在する場合）と特権レベルの設定後は、その他のアトリビュートを設定します。これらは任意の順序で設定できます。任意のアトリビュートと値のペアを削除するには、該当コマンドの ***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、ユーザ名モードに入ります。

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

プロンプトが変化し、新しいモードになったことが示されます。これでアトリビュートを設定できます。

VPN ユーザ アトリビュートの設定

VPN ユーザ アトリビュートは、次の項で説明するように、VPN 接続に固有の値を設定します。

継承の設定

ユーザが、それまでにユーザ レベルで設定されていないアトリビュートの値をグループポリシーから継承するようにできます。このユーザがアトリビュートを継承するグループポリシーの名前を指定するには、**vpn-group-policy** コマンドを入力します。デフォルトでは、VPN ユーザにはグループポリシーが関連付けられていません。

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

ユーザ名モードで使用できるアトリビュートの場合、ユーザ名モードでアトリビュートを設定すると、特定のユーザに関してグループポリシーにおけるそのアトリビュートの値を上書きできます。

次の例は、anyuser という名前のユーザが FirstGroup という名前のグループポリシーのアトリビュートを使用するように設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

アクセス時間の設定

設定済みの time-range ポリシーの名前を指定して、このユーザがシステムへのアクセスを許可される時間を関連付けます。

このアトリビュート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、time-range の値を別のグループポリシーから継承できます。値を継承しないようにするには、**vpn-access-hours none** コマンドを入力します。デフォルトでは、アクセスは無制限です。

```
hostname(config-username)# vpn-access-hours value {time-range | none}
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

次の例は、anyuser という名前のユーザを 824 と呼ばれる time-range ポリシーに関連付ける方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

最大同時ログイン数の設定

このユーザに許可される同時ログインの最大数を指定します。範囲は 0 ～ 2147483647 です。デフォルトの同時ログイン数は 3 です。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)#
```

（注） 同時ログインに最大数の制限はありませんが、複数の同時ログインの許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼす恐れがあります。

次の例は、anyuser という名前のユーザに最大 4 つの同時ログインを許可する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

アイドル タイムアウトの設定

アイドル タイムアウト期間を分単位で指定するか、***none*** を入力してアイドル タイムアウトをディセーブルにします。この期間中に接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

範囲は 1 ～ 35791394 分です。デフォルトは 30 分です。無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**none** キーワードを指定して **vpn-idle-timeout** コマンドを入力します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-idle-timeout {minutes | none}
hostname(config-username)# no vpn-idle-timeout
hostname(config-username)#
```

次の例は、anyuser という名前のユーザに 30 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)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout 30
hostname(config-username)#
```

最大接続時間の設定

ユーザの最大接続時間を分単位で指定するか、***none*** を入力して無制限の接続時間を許可し、このアトリビュートの値を継承しないようにします。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

範囲は 1 ～ 35791394 分です。デフォルトのタイムアウトはありません。無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**none**　キーワードを指定して **vpn-session-timeout** コマンドを入力します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-session-timeout {minutes | none}
hostname(config-username)# no vpn-session-timeout
hostname(config-username)#
```

次の例は、anyuser という名前のユーザに 180 分の VPN セッション タイムアウトを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

ACL フィルタの適用

VPN 接続用のフィルタとして使用する、事前に設定されたユーザ固有の ACL の名前を指定します。アクセスリストを拒否し、グループポリシーからアクセス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 **vpn-filter** コマンドを入力します。**vpn-filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。このコマンドには、デフォルトの動作や値はありません。

ACL を設定して、このユーザについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを使用して、これらの 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）　***functions*** コマンドには、***filter*** を選択しておく必要があります。WebVPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次の例は、anyuser という名前のユーザに対して acl_vpn という名前のアクセスリストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

IP アドレスとネットマスクの指定

特定のユーザに割り当てる IP アドレスとネットマスクを指定します。IP アドレスを削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)
```

次の例は、anyuser という名前のユーザに IP アドレス 10.92.166.7 を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)
```

前の手順で指定した IP アドレスに使用するネットワーク マスクを指定します。
no vpn-framed-ip-address コマンドを使用した場合は、ネットワーク マスクを指定しないでください。サブネット マスクを削除するには、このコマンドの **no** 形式を入力します。デフォルトの動作や値はありません。

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

次の例は、anyuser という名前のユーザに、サブネット マスク 255.255.255. 254 を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

トンネル プロトコルの指定

このユーザが使用できる VPN トンネル タイプ（IPSec または WebVPN）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。このアトリビュート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、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 :** HTTP 対応 Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは不要です。

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 トンネルで接続するユーザに対して、1 つ以上のトンネリング モードを設定する必要があります。

次の例は、anyuser という名前のユーザに WebVPN および IPSec トンネリング モードを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPSec
hostname(config-username)
```

リモート ユーザ アクセスの制限

value キーワードを指定して **group-lock** アトリビュートを設定することにより、指定した既存のトンネルグループだけを介してアクセスするようにリモート ユーザを制限します。group-lock は、VPN クライアントで設定されたグループが、そのユーザが割り当てられているトンネルグループと同じかどうかをチェックすることによって、ユーザを制限します。同じでない場合、セキュリティ アプライアンスはそのユーザによる接続を禁止します。group-lock を設定しない場合、セキュリティ アプライアンスは割り当てられているグループを考慮せずに、ユーザを認証します。

group-lock アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値をグループポリシーから継承できます。group-lock をディセーブルにし、デフォルトまたは指定されたグループポリシーから group-lock の値を継承しないようにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。

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

次の例は、anyuser という名前のユーザにグループ ロックを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel group name
hostname(config-username)
```

ソフトウェア クライアント ユーザのパスワード保存のイネーブル化

ユーザがログイン パスワードをクライアント システム上に保存するかどうかを指定します。パスワード保存は、デフォルトでディセーブルになっています。パスワード保存は、セキュアなサイトにあることがわかっているシステムでだけ、イネーブルにします。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを入力します。password-storage アトリビュート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、対話的なハードウェア クライアント認証やハードウェア クライアントの個別ユーザ認証では動作しません。

次の例は、anyuser という名前のユーザでパスワード保存をイネーブルにする方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
hostname(config-username)
```

特定ユーザの WebVPN の設定

次の各項では、特定のユーザの WebVPN 設定をカスタマイズする方法について説明します。ユーザ名のコンフィギュレーション モードで **webvpn** コマンドを使用して、ユーザ名の webvpn コンフィギュレーション モードに入ります。WebVPN によってユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェア クライアントもハードウェア クライアントも必要ありません。WebVPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。WebVPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされて

いる内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ユーザ名の webvpn コンフィギュレーション モード コマンドは、ファイル、MAPI プロキシ、URL、および TCP アプリケーションへの WebVPN 経由のアクセスを定義します。フィルタリングする ACL とトラフィックの種類も特定します。WebVPN は、デフォルトではディセーブルになっています。これらの **webvpn** コマンドは、設定を行ったユーザ名に適用されます。プロンプトが変化して、ユーザ名の webvpn コンフィギュレーション モードに入ったことがわかります。

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

ユーザ名の webvpn コンフィギュレーション モードで入力されたすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username)# no webvpn
hostname(config-username)#
```

電子メール プロキシを使用するために WebVPN を設定する必要はありません。

（注）グローバル コンフィギュレーション モードで webvpn モードを入力することによって、WebVPN のグローバル設定を構成できます。この項で説明した、ユーザ名モードから入ったユーザ名の webvpn コンフィギュレーション モードを使用すると、特定のユーザの WebVPN コンフィギュレーションをカスタマイズできます。

ユーザ名の webvpn コンフィギュレーション モードでは、次のパラメータをカスタマイズできます。各パラメータについては、後述のステップで説明します。

- functions
- customizations
- deny message
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server（single-signon server）
- auto-signon
- SSL VPN Client（SVC）
- keep-alive ignore

次の例は、ユーザ名 anyuser のアトリビュートのユーザ名の webvpn コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

イネーブルにする WebVPN 機能の設定

このユーザに対して、WebVPN を使用した、WebVPN 機能のファイル アクセスとファイル ブラウジング、HTTP プロキシ、MAPI プロキシ、および URL エントリを設定するには、ユーザ名の webvpn コンフィギュレーション モードで **functions** コマンドを入力します。設定した機能を削除するには、このコマンドの **no** 形式を入力します。これらの機能は、デフォルトではディセーブルです。

functions none コマンドを発行して作成したヌル値を含めて、設定済みのすべての機能を削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。機能の値を継承しないようにするには、**functions none** コマンドを入力します。

```
hostname(config-username-webvpn)# functions {auto-download | citrix | file-access |
file-browsing | file-entry | filter | http-proxy | mapi | none | port-forward |
url-entry}
```

```
hostname(config-username-webvpn)# no functions [auto-download | citrix | file-access |
file-browsing | file-entry | filter | http-proxy | mapi | none | port-forward |
url-entry]
```

表 26-7 で、このコマンドで使用するキーワードの意味を次の表で説明します。

表 26-7　functions コマンドのキーワード

キーワード	意味
auto-download	ポート転送アプレットを自動的にダウンロードします。
citrix	Citrix をイネーブルにします。
file-access	ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルにすると、WebVPN ホーム ページにサーバ リストのファイル サーバが表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイル サーバとファイル共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ユーザがファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。
filter	webtype アクセスリストを適用します。
http-proxy	HTTP アプレット プロキシのクライアントへの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、Flash など、適切なマングリングを妨げる技術に対して有用です。セキュリティ アプライアンスの使用を継続しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ コンフィギュレーションを自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、実質的にすべてのクライアント サイド技術をサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。
mapi	Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。
none	すべての WebVPN の **functions** にヌルを設定します。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機能を継承しないようにします。

表 26-7　functions コマンドのキーワード（続き）

キーワード	意味
port-forward	ポート転送をイネーブルにします。
url-entry	ユーザの URL エントリをイネーブルまたはディセーブルにします。イネーブルにしても、セキュリティ アプライアンスは設定されている URL またはネットワーク ACL で、URL を制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは、WebVPN ユーザがホーム ページの URL にのみアクセスできるように制限します。

このコマンドで使用するキーワードは、次のとおりです。

- **file-access：**ファイル　アクセスをイネーブルまたはディセーブルにします。イネーブルにすると、WebVPN ホーム ページにサーバ リストのファイル サーバが表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
- **file-browsing：**ファイル サーバとファイル共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。
- **file-entry：**ユーザがファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。
- **http-proxy：**HTTP アプレット プロキシのクライアントへの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、Flash など、適切なマングリングを妨げる技術に対して有用です。セキュリティ アプライアンスの使用を継続しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ コンフィギュレーションを自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、実質的にすべてのクライアント サイド技術をサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。
- **mapi：**Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。
- **none：**すべての WebVPN の **functions** にヌルを設定します。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機能を継承しないようにします。
- **url-entry：**ユーザの URL エントリをイネーブルまたはディセーブルにします。イネーブルにしても、セキュリティ アプライアンスは設定されている URL またはネットワーク ACL で、URL を制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは、WebVPN ユーザがホーム ページの URL にのみアクセスできるように制限します。

次の例は、anyuser という名前のユーザに対して、ファイル アクセス、ファイル ブラウジング、HTTP プロキシ、および MAPI プロキシを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# functions file-access file-browsing MAPI
hostname(config-username-webvpn)#
```

HTML からフィルタリングするコンテンツとオブジェクトの指定

このユーザの WebVPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするには、ユーザ名の webvpn コンフィギュレーション モードで **html-content-filter** コマンドを入力します。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**html-content-filter none** コマンドを発行して作成したヌル値を含めて、設定済みのすべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。HTML コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを入力します。HTML フィルタリングは、デフォルトでディセーブルです。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

```
hostname(config-username-webvpn)# html-content-filter {java | images | scripts |
cookies | none}

hostname(config-username-webvpn)# no html-content-filter [java | images | scripts |
cookies | none]
```

このコマンドで使用するキーワードは、次のとおりです。

- **cookies :** イメージからクッキーを削除して、アドバタイズメント フィルタリングを制限し、プライバシーを保持します。
- **images :** イメージへの参照を削除します（<IMG> タグを削除）。
- **java :** Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> の各タグを削除）。
- **none :** フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
- **scripts** : スクリプトへの参照を削除します（<SCRIPT> タグを削除）。

次の例は、anyuser という名前のユーザに、Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# html-content-filter java cookies images
hostname(config-username-webvpn)#
```

ユーザ ホームページの指定

この WebVPN ユーザのログイン時に表示される Web ページの URL を指定するには、ユーザ名の webvpn コンフィギュレーション モードで **homepage** コマンドを入力します。**homepage none** コマンドを発行して作成したヌル値を含めて、設定されているホーム ページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。ホーム ページを継承しないようにするには、**homepage none** コマンドを入力します。

none キーワードは、WebVPN ホームページがないことを示します。これにより、ヌル値が設定されてホーム ページが拒否され、ホーム ページが継承されなくなります。

キーワード ***value*** の後ろの *url-string* 変数で、ホームページの URL を指定します。文字列の先頭は、http:// または https:// にする必要があります。

デフォルトのホーム ページはありません。

```
hostname(config-username-webvpn)# homepage {value url-string | none}
hostname(config-username-webvpn)# no homepage
hostname(config-username-webvpn)#
```

次の例は、anyuser 」という名前のユーザのホームページとして www.example.com を指定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# homepage value www.example.com
hostname(config-username-webvpn)#
```

カスタマイゼーションの適用

カスタマイゼーションは、ログイン時にユーザに表示されるウィンドウの内容を決定します。カスタマイゼーション パラメータは、WebVPN 設定の一部として設定します。以前定義した Web ページ カスタマイゼーションを適用して、ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するには、ユーザ名の webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-username-webvpn)# customization customization_name
hostname(config-username-webvpn)#
```

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

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

「拒否」メッセージの指定

ユーザ名の webvpn コンフィギュレーション モードで **deny-message** コマンドを入力すると、WebVPN に正常なログインが可能でも VPN 特権を持たないリモート ユーザに送信されるメッセージを指定できます。

```
hostname(config-username-webvpn)# deny-message value "message"
hostname(config-username-webvpn)# no deny-message value "message"
hostname(config-username-webvpn)# deny-message none
```

no deny-message value コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

no deny-message none コマンドは、トンネルグループ ポリシー コンフィギュレーションからアトリビュートを削除します。ポリシーはアトリビュート値を継承します。

メッセージは、特殊文字、スペース、および句読点を含む、英数字最大 491 文字の長さにできますが、囲みの引用符はカウントされません。テキストは、ログイン時にリモート ユーザのブラウザに表示されます。**deny-message value** コマンドに文字列を入力しているときは、たとえコマンドがラップしても入力を続けます。

デフォルトの拒否メッセージは、「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.」です。

次の例の最初のコマンドは、ユーザ名モードに入り、anyuser という名前のユーザにアトリビュートを設定します。後続のコマンドは、ユーザ名の webvpn コンフィギュレーション モードに入り、そのユーザに関連付けられている拒否メッセージを変更します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# deny-message value "Your login credentials are OK.
However, you have not been granted rights to use the VPN features. Contact your
administrator for more information."
hostname(config-username-webvpn)
```

WebVPN 接続に使用するアクセスリストの指定

このユーザの WebVPN 接続に使用するアクセスリストの名前を指定するには、ユーザ名の webvpn コンフィギュレーション モードで **filter** コマンドを入力します。**filter none** コマンドを発行して作成したヌル値を含めて、アクセスリストを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

filter コマンドを入力して指定するまで、WebVPN アクセスリストは適用されません。

ACL を設定して、このユーザについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを入力して、これらの ACL を WebVPN トラフィックに適用します。

```
hostname(config-username-webvpn)# filter {value ACLname | none}
hostname(config-username-webvpn)# no filter
hostname(config-username-webvpn)#
```

none キーワードは、**webvpntype** アクセスリストがないことを示します。これにより、ヌル値が設定されてアクセスリストが拒否され、別のグループポリシーからアクセスリストが継承されなくなります。

キーワード ***value*** の後ろの *ACLname* 文字列で、すでに設定されているアクセスリストの名前を指定します。

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

次の例は、anyuser という名前のユーザに対して *acl_in* という名前のアクセスリストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# filter acl_in
hostname(config-username-webvpn)#
```

URL リストの適用

ユーザの WebVPN ホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して 1 つ以上の名前付きリストを作成する必要があります。特定のユーザに WebVPN サーバと URL のリストを適用するには、ユーザ名の webvpn コンフィギュレーション モードで **url-list** コマンドを入力します。

url-list none コマンドを使用して作成したヌル値を含めて、リストを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。URL リストを継承しないようにするには、**url-list none** コマンドを入力します。

```
hostname(config-username-webvpn)# url-list {listname displayname url | none}
hostname(config-username-webvpn)# no url-list
```

このコマンドで使用するキーワードと変数は、次のとおりです。

- *displayname*：URL の名前を指定します。この名前は、WebVPN のエンドユーザ インターフェイスに表示されます。
- *listname*：URL をグループ化する名前を指定します。
- **none**：URL のリストが存在しないことを示します。ヌル値を設定して、URL リストを拒否します。URL リストの値を継承しないようにします。
- *url*：WebVPN ユーザがアクセスできる URL を指定します。

デフォルトの URL リストはありません。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

次の例は、anyuser という名前のユーザに AnyuserURLs という URL リストを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# url-list value AnyuserURLs
hostname(config-username-webvpn)#
```

WebVPN アプリケーション アクセスのイネーブル化

このユーザの WebVPN アプリケーション アクセスをイネーブルにするには、ユーザ名の webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート転送は、デフォルトではディセーブルになっています。

port-forward none コマンドを発行して作成したヌル値を含めて、コンフィギュレーションからポート転送アトリビュートを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、リストをグループポリシーから継承できます。フィルタリングを拒否してポート転送リストを継承しないようにするには、***none*** キーワードを指定して **port-forward** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward {value listname | none}
hostname(config-username-webvpn)# no port-forward
hostname(config-username-webvpn)#
```

キーワード ***value*** の後ろの *listname* 文字列で、WebVPN ユーザがアクセスできるアプリケーションのリストを指定します。コンフィギュレーション モードで **port-forward** コマンドを入力し、このリストを定義します。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

ユーザ名の webvpn コンフィギュレーション モードで **port-forward** コマンドを入力し、アプリケーション アクセスをイネーブルにする前に、WebVPN 接続でユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力し、このリストを定義します。

次の例は、ports1 というポート転送リストを設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward value ports1
hostname(config-username-webvpn)#
```

ポート転送表示名の設定

ユーザ名の webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用して、特定のユーザでエンド ユーザへの TCP ポート転送を識別する表示名を設定します。
port-forward-name none コマンドを使用して作成したヌル値を含めて、表示名を削除するには、コマンドの **no** 形式を入力します。**no** オプションは、デフォルト名の Application Access を復元します。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward-name {value name | none}
hostname(config-username-webvpn)# no port-forward-name
```

次の例は、ポート転送名 test を設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward-name value test
hostname(config-username-webvpn)#
```

セッション タイマー更新のために無視する最大オブジェクト サイズの設定

デットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回線が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定したサイズ以下のすべてのメッセージをキープアライブ メッセージと見なし、セッション タイマーの更新時にトラフィックと見なさないようセキュリティ アプライアンスに指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

無視する HTTP/HTTPS トラフィックの上限をトランザクションごとに指定するには、グループポリシー アトリビュート webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

このコマンドの **no** 形式を使用すると、コンフィギュレーションから指定を削除します。

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

自動サインオンの設定

NTLM、基本 HTTP 認証、またはその両方を使用する内部サーバに、特定の WebVPN ユーザの WebVPN ログイン クレデンシャルを自動的に渡すには、ユーザ名の webvpn コンフィギュレーション モードで **auto-signon** コマンドを入力します。

auto-signon コマンドは、WebVPN ユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のために WebVPN ログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の auto-signon コマンドを入力でき、コマンドは入力順序に従って処理されます（先に入力されたコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名がグループに優先し、グループがグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、望ましい認証の範囲によって異なります。

特定のサーバへの特定のユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URI を指定してこのコマンドの **no** 形式を使用します。すべてのサーバへの認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、値をグループポリシーから継承できます。

次の例では、基本認証または NTLM 認証を使用して、anyuser という名前の Web VPN ユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow uri https://*.example.com/*
auth-type all
```

次の例では、基本認証または NTLM 認証を使用して、anyuser という名前の Web VPN ユーザに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type all
hostname(config-username-webvpn)#
```

SSO サーバの指定

WebVPN だけに使用できるシングル サインオンのサポートを使用すると、ユーザはユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。**sso-server value** コマンドをユーザ名の webvpn モードで入力すると、SSO サーバをユーザに割り当てることができます。

SSO サーバをユーザに割り当てるには、ユーザ名の webvpn コンフィギュレーション モードで **sso-server value** コマンドを入力します。このコマンドでは、コンフィギュレーションに CA SiteMinder コマンドが含まれている必要があります。

```
hostname(config-username-webvpn)# sso-server value server_name
hostname(config-username-webvpn)#
```

この割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。デフォルト ポリシーを継承しないようにするには、**sso-server none** コマンドを入力します。

```
hostname(config-username-webvpn)# sso-server {value server_name | none}
hostname(config-username-webvpn)# [no] sso-server value server_name
```

SSO サーバに割り当てられているデフォルト ポリシーは DfltGrpPolicy です。

次の例では、example という名前の SSO サーバを anyuser という名前のユーザに割り当てます。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value example
hostname(config-username-webvpn)#
```

SVC の設定

SSL VPN Client（SVC）は、ネットワーク管理者がリモート コンピュータに IPSec VPN をインストールして設定しなくても、リモート ユーザが IPSec VPN クライアントの利点を活用できる VPN トンネリング テクノロジーです。SVC では、リモート コンピュータにすでにある SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVC セッションを確立するには、リモート ユーザはセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスをブラウザに入力します。ブラウザはそのインターフェイスに接続して WebVPN のログイン画面を表示します。ユーザがログインと認証を完了し、ユーザが SVC を*必要としていることをセキュリティ アプライアンスが確認すると、セキュリティ アプライアンスは* SVC をリモート コンピュータにダウンロードします。セキュリティ アプライアンスが、SVC を使用する*オプション*がユーザにあると確認した場合、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをユーザ画面に表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC は自動的にインストールと設定を実行します。接続が切断されると（設定に応じて）、SVC はリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

セキュリティ アプライアンスは、さまざまなリモート コンピュータのオペレーティング システム用に、複数の独自の SVC イメージをキャッシュ メモリ内に備えている場合もあります。ユーザが接続を試みると、セキュリティ アプライアンスは、イメージとオペレーティング システムが一致するまで引き続きこれらのイメージの部分をリモート コンピュータにダウンロードできます。一致した時点で、SVC 全体をダウンロードします。接続のセットアップ時間を短縮するため、ダウンロードされる最初のイメージが、最もよく遭遇するリモート コンピュータのオペレーティング システムになるように SVC イメージの順序を指定できます。SVC のインストールと使用の詳細については、第 31 章「SSL VPN クライアントの設定」を参照してください。

第 31 章「SSL VPN クライアントの設定」に示すように、SVC をイネーブルにした後は、特定のグループの SVC 機能をイネーブルまたは必須にできます。この機能は、デフォルトでディセーブルになっています。SVC をイネーブルまたは必須にすると、この項で説明している一連の svc コマンドをイネーブルにできます。SVC とその関連する svc コマンドをイネーブルにするには、ユーザ名の webvpn コンフィギュレーション モードで次の手順を実行します。

ステップ 1　セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードできるようにするには、**svc enable** コマンドを入力します。このコマンドは、デフォルトではディセーブルになっています。セキュリティ アプライアンスは SVC ファイルをダウンロードしません。このコンフィギュレーションから **svc enable** コマンドを削除するには、このコマンドの ***no*** 形式を使用します。

```
hostname(config-username-webvpn)# svc {none | enable | required}
hostname(config-username-webvpn)#
```

（注）　**no svc enable** コマンドを入力しても、アクティブな SVC セッションは終了しません。

```
hostname(config)# username sales attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# svc enable
hostname(config-username-webvpn)#
```

ステップ 2　SVC 接続経由で特定のユーザについて HTTP データの圧縮をイネーブルにするには、svc compression コマンドを入力します。SVC 圧縮は、デフォルトで ***deflate***（イネーブル）に設定されています。特定のユーザの圧縮をディセーブルにするには、***none*** キーワードを使用します。svc compression コマンドを削除して値が継承されるようにするには、このコマンドの ***no*** 形式を使用します。

```
hostname(config-username-webvpn)# svc compression {deflate | none}
hostname(config-username-webvpn)#
```

次の例では、sales という名前のユーザ SVC 圧縮をディセーブルにします。

```
hostname(config)# username sales attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# svc compression none
hostname(config-username-webvpn)#
```

ステップ 3　セキュリティ アプライアンスで dead-peer-detection（DPD）をイネーブルにして、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定するには、**svc dpd-interval** コマンドを使用します。このコンフィギュレーションから **svc dpd-interval** コマンドを削除するには、このコマンドの ***no*** 形式を使用します。このユーザの SVC DPD をディセーブルにするには、***none*** キーワードを使用します。

```
hostname(config-username-webvpn)# svc dpd-interval {[gateway {seconds | none}] |
[client {seconds | none}]}
hostname(config-username-webvpn)#
```

DPD チェックは、デフォルトでディセーブルになっています。

ゲートウェイは、セキュリティ アプライアンスのことです。セキュリティ アプライアンスが DPD テストを実行する頻度を、30 ～ 3600 秒（1 時間）の範囲で指定できます。***none*** を指定すると、セキュリティ アプライアンスが実行する DPD テストはディセーブルになります。

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

次の例では、sales という名前の既存のユーザについて、セキュリティ アプライアンス（ゲートウェイ）によって実行される DPD の頻度を 3000 秒に設定し、クライアントによって実行される DPD の頻度を 1000 秒に設定しています。

```
hostname(config)# username sales attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# svc dpd-interval gateway 3000
hostname(config-username-webvpn)# svc dpd-interval client 1000
hostname(config-username-webvpn)#
```

ステップ 4　接続のアイドル状態を維持できる時間をデバイスが制限している場合でも、プロキシ、ファイアウォール、または NAT デバイスを通じて SVC 接続のオープン状態を維持するように、キープアライブ メッセージの頻度を調整できます（*seconds* で指定）。

頻度を調整することで、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベースの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、SVC が切断して再接続をしないようにできます。

リモート コンピュータ上の SVC がキープアライブ メッセージをセキュリティ アプライアンスに送信する頻度（15 ～ 600 秒）を設定するには、**svc keepalive** コマンドを使用します。コンフィギュレーションからこのコマンドを削除して値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# svc keepalive {none | seconds}
hostname(config-username-webvpn)# no svc keepalive {none | seconds}
hostname(config-username-webvpn)#
```

SVC キープアライブは、デフォルトでディセーブルになっています。キーワード ***none*** を使用すると SVC キープアライブ メッセージがディセーブルになります。

次の例では、ユーザは、SVC 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-username-webvpn)# svc keepalive 300
hostname(config-username-webvpn)#
```

ステップ 5　SVC がリモート コンピュータに永続的にインストールされた状態を保つには、***installed*** キーワードを指定して **svc keep-installer** コマンドを使用します。コマンドをこのコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# svc keep-installer {installed | none}
hostname(config-username-webvpn)# no svc keep-installer {installed | none}
hostname(config-username-webvpn)#
```

デフォルトでは、SVC の常時インストールがディセーブルになっています。SVC セッションの終わりに、SVC はリモートコンピュータからアンインストールされます。

次の例では、このユーザのリモート コンピュータの SVC インストール状態を維持す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-username-webvpn)# svc keep-installer installed
hostname(config-username-webvpn)#
```

ステップ 6　SVC が SVC セッションでキーの再生成を実行できるようにするには、**svc rekey** コマンドを使用します。

```
hostname(config-username-webvpn)# svc rekey {method {ssl | new-tunnel} | time minutes
| none}}
```

キーの再生成をディセーブルにして、コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# no svc rekey [method {ssl | new-tunnel} | time
minutes | none}]
hostname(config-username-webvpn)#
```

SVC キーの再生成は、デフォルトで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 SVC が新しいトンネルを確立することが指定されます。method を none に指定すると、SVC キーの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 SVC キーの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の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。

コマンドの ***no*** 形式の場合は、必要最小限の指定をします。適正な例は、次のとおりです。

```
hostname(config-username-webvpn)# no svc rekey method
hostname(config-username-webvpn)#
```

ただし、method を次のように new-tunnel に指定し、

```
hostname(config-username-webvpn)# no svc rekey method new-tunnel
hostname(config-username-webvpn)#
```

現在の method が ssl である場合、値が一致しないためにコマンドは失敗します。

次の例では、ユーザは、キーの再生成中に SVC が SSL と再ネゴシエートするように設定し、キーの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ます。

```
hostname(config-username-webvpn)# svc rekey method ssl
hostname(config-username-webvpn)# svc rekey time 30
hostname(config-username-webvpn)#
```