CHAPTER 13

AAA サーバとローカル データベースの設定

この章では、AAA（「トリプル エー」と発音）のサポート、および AAA サーバとローカル データベースの設定方法について説明します。

この章の内容は、次のとおりです。

AAA の概要

AAA によって、セキュリティ アプライアンスが、ユーザが誰か（認証）、ユーザが何を実行できるか（許可）、およびユーザが何を実行したか（アカウンティング）を判別することが可能になります。

AAA には、ユーザ アクセスに対して、アクセス リストだけを使用する場合よりもレベルの高い保護および制御機能が用意されています。たとえば、すべての外部ユーザが DMZ ネットワークのサーバ上の Telnet にアクセスできるようにするアクセス リストを作成できます。サーバへのアクセスを一部のユーザだけに限定する場合で、対象ユーザの IP アドレスが必ずしも明らかでないときには、AAA をイネーブルにして、認証または許可されたユーザだけに セキュリティ アプライアンス を通過させることができます （Telnet サーバもまた、認証を実行します。セキュリティ アプライアンスは、許可されないユーザがサーバにアクセスできないようにします）。

認証だけで使用することも、許可およびアカウンティングとともに使用することもできます。許可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および許可とともに使用することもできます。

この項では、次のトピックについて取り上げます。

認証の概要

認証では、有効な証明書（一般にはユーザ名とパスワード）を要求することによって、アクセスを制御します。次の項目を認証するように、セキュリティ アプライアンスを設定できます。

- セキュリティ アプライアンスへのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール
  - ASDM（HTTPS を使用）
  - VPN 管理アクセス
- **enable** コマンド
- ネットワーク アクセス
- VPN アクセス

許可の概要

許可では、ユーザを認証したあと、*各ユーザ*のアクセスを制御できます。次の項目を許可するように、セキュリティ アプライアンスを設定できます。

- 管理コマンド
- ネットワーク アクセス
- VPN アクセス

許可は、認証された個々のユーザが使用できるサービスおよびコマンドを制御します。許可をイネーブルにせずに認証だけを使用する場合、認証されたすべてのユーザに対し、サービスへのアクセスが一様に提供されます。

許可で提供される制御を必要とする場合は、広範な認証ルールを設定してから、詳細な許可を設定できます。たとえば、内部ユーザを認証して外部ネットワークの任意サーバにアクセスできるようにしたあと、外部サーバへのアクセスを制限して、特定のユーザだけが許可を使用してアクセスできるように設定することができます。

セキュリティ アプライアンスはユーザあたり最初の 16 件の許可要求をキャッシュするため、ユーザが現在の認証セッション中に同じサービスにアクセスした場合、セキュリティ アプライアンスは許可サーバに要求を再送信しません。

アカウンティングの概要

アカウンティングは、セキュリティ アプライアンスを通過するトラフィックを追跡して、ユーザ アクティビティを記録できるようにします。トラフィックの認証をイネーブルにすると、ユーザごとにトラフィックをアカウンティングできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウンティングできます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、セキュリティ アプライアンスを通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

AAA サーバおよびローカル データベースのサポート

セキュリティ アプライアンスは、さまざまな AAA サーバ タイプおよびセキュリティ アプライアンスに保存されているローカル データベースをサポートします。ここでは、各 AAA サーバ タイプおよびローカル データベースのサポートについて説明します。

ここでは、次の内容について説明します。

サポートの要約

表 13-1 に、各 AAA サービスのサポート状況の要約を AAA サーバ タイプ（ローカル データベースを含む）別に示します。特定の AAA サーバ タイプのサポートの詳細については、表に続く項目を参照してください。

表 13-1　AAA サポートの要約

AAA サービス	データベース タイプ							
	ローカル	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
認証								
VPN ユーザ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]
ファイアウォール セッション	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
管理者	Yes	Yes	Yes	Yes[2]	Yes	Yes	Yes	No
許可								
VPN ユーザ	Yes	Yes	No	No	No	No	Yes	No
ファイアウォール セッション	No	Yes[3]	Yes	No	No	No	No	No
管理者	Yes[4]	No	Yes	No	No	No	No	No
アカウンティング								
VPN 接続	No	Yes	Yes	No	No	No	No	No
ファイアウォール セッション	No	Yes	Yes	No	No	No	No	No
管理者	No	Yes[5]	Yes	No	No	No	No	No

1. HTTP Form プロトコルでは、WebVPN ユーザに限って、シングル サインオン認証がサポートされます。

2. SDI は、HTTP 管理アクセスについてはサポートされません。
3. ファイアウォール セッションの場合、RADIUS 許可はユーザ固有のアクセス リストでだけサポートされます。このアクセス リストは RADIUS 認証応答で受信または指定されます。
4. ローカル コマンド許可は、特権レベルに限りサポートされます。
5. コマンド アカウンティングは、TACACS+ でのみ使用できます。

RADIUS サーバのサポート

セキュリティ アプライアンス は RADIUS サーバをサポートします。

ここでは、次の内容について説明します。

認証方法

セキュリティ アプライアンスは、RADIUS で次の認証方法をサポートします。

- PAP：すべての接続タイプの場合。
- CHAP：L2TP-over-IPSec の場合。
- MS-CHAPv1：L2TP-over-IPSec の場合。
- MS-CHAPv2：L2TP-over-IPSec 用、およびパスワード管理機能がイネーブルの場合は通常の IPSec リモート アクセス接続用。

属性のサポート

セキュリティ アプライアンスは、次の RADIUS 属性のセットをサポートします。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウンティング属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- RADIUS ベンダー ID 9 によって識別される Cisco IOS VSA
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

RADIUS 許可機能

セキュリティ アプライアンスでは RADIUS サーバを使用して、ダイナミック アクセス リストまたはユーザごとのアクセス リスト名を使用するネットワーク アクセスに対して、ユーザ許可を実行できます。ダイナミック アクセス リストを実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能なアクセス リスト、またはアクセス リスト名がセキュリティ アプライアンスに送信されます。所定のサービスへのアクセスがアクセス リストによって許可または拒否されます。認証セッションの有効期限が切れると、セキュリティ アプライアンスによってアクセス リストが削除されます。

TACACS+ サーバのサポート

セキュリティ アプライアンスは、ASCII、PAP、CHAP、および MS-CHAPv1 で TACACS+ 認証をサポートします。

SDI サーバのサポート

RSA SecureID サーバは、SDI サーバとも呼ばれます。

ここでは、次の内容について説明します。

SDI バージョンのサポート

セキュリティ アプライアンスでは、SDI バージョン 5.0 および 6.0 がサポートされています。SDI は、SDI プライマリ サーバおよび SDI レプリカ サーバの概念を使用します。各プライマリおよびそのレプリカは、シングル ノード秘密ファイルを共有します。そのノード秘密ファイルの名前は、.sdi が付加された ACE/ サーバ IP アドレスの 16 進数値に基づきます。

セキュリティ アプライアンスに設定するバージョン 5.0 または 6.0 SDI サーバは、プライマリでも、レプリカのいずれか 1 つでもかまいません。ユーザ認証のための SDI エージェントによるサーバの選択方法の詳細については、「SDI プライマリ サーバとレプリカ サーバ」（P.13-5）を参照してください。

2 ステップ認証プロセス

SDI バージョン 5.0 および 6.0 は 2 ステップのプロセスを使用して、侵入者が RSA SecurID 認証要求から情報をキャプチャし、この情報を使用して別のサーバに認証を証明しないように防止します。エージェントはまず、SecurID サーバにロック要求を送信してから、ユーザ認証要求を送信します。サーバはユーザ名をロックして、別の（レプリカ）サーバがユーザ名を受信できないようにします。そのため、同じユーザが同じ認証サーバを同時に使用して、2 台の セキュリティ アプライアンス に認証することができなくなります。ユーザ名のロックに成功すると、セキュリティ アプライアンスはパスコードを送信します。

SDI プライマリ サーバとレプリカ サーバ

セキュリティ アプライアンスは、最初のユーザが設定済みサーバ（プライマリでもレプリカでもかまいません）に認証を証明するときに、サーバ リストを取得します。次に、セキュリティ アプライアンスはリスト上の各サーバにプライオリティを割り当て、その後のサーバ選択では、この割り当てられたプライオリティのサーバから無作為に抽出します。最もプライオリティの高いサーバが選択される可能性が高くなります。

NT サーバのサポート

セキュリティ アプライアンスは、NTLM バージョン 1（集合的に NT サーバと呼びます）をサポートしている Microsoft Windows サーバ オペレーティング システムをサポートします。

（注）　NT サーバでは、ユーザ パスワードの最大長は 14 文字です。15 文字めからは切り捨てられます。これは、NTLM バージョン 1 の制限です。

Kerberos サーバのサポート

セキュリティ アプライアンスは、3DES、DES、および RC4 暗号タイプをサポートしています。

（注）　セキュリティ アプライアンスは、トンネル ネゴシエーション中のユーザ パスワードの変更はサポートしていません。この状況が意図せずに発生することを回避するために、セキュリティ アプライアンスに接続するユーザの Kerberos/Active Directory サーバでのパスワード期限切れをディセーブルにします。

単純な Kerberos サーバ コンフィギュレーションの例については、例 13-2 を参照してください。

LDAP サーバのサポート

この項では、ユーザ認証と VPN 許可にセキュリティ アプライアンスを利用する LDAP ディレクトリの使用方法について説明します。この項では、次のトピックについて取り上げます。

- 「LDAP による認証」（P.13-6）
- 「VPN のための LDAP での許可」（P.13-7）
- 「LDAP 属性のマッピング」（P.13-8）

LDAP による認証または許可をセットアップする設定手順の例については、付録 E「許可および認証用の外部サーバの設定」を参照してください。

LDAP による認証

認証中、セキュリティ アプライアンスは、ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーン テキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバに対する認証を行います。デフォルトで、セキュリティ アプライアンスは、通常はユーザ名とパスワードである認証パラメータを LDAP サーバにプレーン テキストで渡します。SASL とプレーン テキストのいずれを使用する場合でも、**ldap-over-ssl** コマンドを使用して、SSL でセキュリティ アプライアンスと LDAP サーバの間の通信を保護できます。

（注）　SASL を設定しない場合、SSL で LDAP 通信を保護することを強くお勧めします。『*Cisco Security Appliance Command Reference*』の **ldap-over-ssl** コマンドを参照してください。

ユーザ LDAP 認証が成功すると、LDAP サーバは認証されたユーザの属性を返します。VPN 認証では、通常これらの属性には、VPN セッションに適用される許可データが含まれます。したがって、LDAP を使用すると、認証と許可が 1 つのステップで行われます。

SASL を使用した LDAP 認証の保護

セキュリティ アプライアンスでは、次の SASL メカニズムをサポートしています。次に、強度の低い順番に示します。

- Digest-MD5：セキュリティ アプライアンスは、ユーザ名とパスワードから計算した MD5 値を使用して LDAP サーバに応答します。
- Kerberos：セキュリティ アプライアンスは、Generic Security Services Application Programming Interface（GSSAPI; 汎用セキュリティ サービス API）Kerberos メカニズムを使用して、ユーザ名と領域を送信することで LDAP サーバに応答します。

これらの SASL メカニズムの任意の組み合わせをサポートするように、セキュリティ アプライアンスと LDAP サーバを設定できます。その場合、セキュリティ アプライアンスでは、サーバ上に設定されている SASL メカニズムのリストが取得され、セキュリティ アプライアンスとサーバの双方に設定されている最も強力なメカニズムが、認証メカニズムとして設定されます。たとえば、LDAP サーバとセキュリティ アプライアンスの両方がこれら両方のメカニズムをサポートしている場合、セキュリティ アプライアンスは、より強力な方の Kerberos メカニズムを選択します。

次の例では、ldap_dir_1 という名前の LDAP ディレクトリ サーバに対する認証に digest-MD5 SASL メカニズムを使用し、SSL で保護された接続で通信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)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

LDAP サーバ タイプの設定

セキュリティ アプライアンスは LDAP バージョン 3 をサポートします。現在のリリースでは、Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory とだけ互換性があります。後続のリリースでは、セキュリティ アプライアンスは、その他の OpenLDAP サーバをサポートするようになります。

デフォルトでセキュリティ アプライアンスは、Microsoft または Sun LDAP ディレクトリ サーバに接続されているかどうかを自動検出します。ただし、自動検出により LDAP サーバのタイプが特定できなくても、そのサーバが、Microsoft または Sun サーバのいずれであるかがわかっている場合は、そのサーバ タイプを手動で設定できます。次の例では、LDAP ディレクトリ サーバ ldap_dir_1 を Sun Microsystems タイプに設定します。

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# server-type sun
hostname(config-aaa-server-host)#
```

（注）

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

VPN のための LDAP での許可

VPN アクセスのためのユーザ LDAP 認証が成功すると、セキュリティ アプライアンスは、LDAP 属性を返す LDAP サーバのクエリーを実行します。通常これらの属性には、VPN セッションに適用される許可データが含まれます。したがって、LDAP を使用すると、認証と許可が 1 つのステップで行われます。

ただし、場合によっては、許可メカニズムとは別の異なる許可を LDAP ディレクトリ サーバから取得する必要があります。たとえば、認証に SDI または証明書サーバを使用している場合、許可情報は返されません。この場合、ユーザ許可では、認証の成功後に LDAP ディレクトリのクエリーを実行するため、認証と許可は 2 つのステップで行われます。

LDAP を使用する VPN ユーザ許可を設定するには、最初に AAA サーバ グループとトンネル グループを作成する必要があります。次に、**tunnel-group general-attributes** コマンドを使用して、サーバとトンネル グループを関連付けます。特定の要件で使用できる許可関連のコマンドとオプションは他にもありますが、次の例では、LDAP でのユーザ許可をイネーブルにする基本のコマンドを示します。この例では、remote-1 という名前の IPSec リモート アクセス トンネル グループを作成し、以前作成した許可のための ldap_dir_1 AAA サーバに、その新しいトンネル グループを割り当てます。

```
hostname(config)# tunnel-group remote-1 type ipsec-ra
hostname(config)# tunnel-group remote-1 general-attributes
hostname(config-general)# authorization-server-group ldap_dir_1
hostname(config-general)#
```

この基本設定作業が完了したら、ディレクトリ パスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 許可パラメータを次のように設定できます。

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# ldap-login-dn obscurepassword
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

詳細については、『*Cisco Security Appliance Command Reference*』の LDAP コマンドを参照してください。

LDAP 属性のマッピング

既存の LDAP ディレクトリにセキュリティ アプライアンスを導入する場合、その LDAP 属性の名前および値は、既存のものとは異なる場合があります。既存のユーザ定義の属性の名前および値を、セキュリティ アプライアンスと互換性のあるシスコの属性の名前と値にマッピングする LDAP 属性マップを作成する必要があります。次に、ユーザは、必要に応じてこれらの属性マップを LDAP サーバにバインドしたり、削除したりできます。また、属性マップを表示または消去することもできます。

（注） 属性マッピング機能を適切に使用するには、シスコの LDAP 属性の名前と値およびユーザ定義の属性の名前と値を理解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 モードで入力された次のコマンドは、att_map_1 という名前の空の LDAP 属性マップ テーブルを作成します。

```
hostname(config)# ldap attribute-map att_map_1
hostname(config-ldap-attribute-map)#
```

次のコマンドは、ユーザ定義の属性名 department を、シスコの属性名 cVPN3000-IETF-Radius-Class にマッピングします。2 つ目のコマンドは、ユーザ定義の属性値 Engineering を、ユーザ定義の属性 department とシスコ定義の属性値 group1 にマッピングします。

```
hostname(config)# ldap attribute-map att_map_1
hostname(config-ldap-attribute-map)# map-name department cVPN3000-IETF-Radius-Class
hostname(config-ldap-attribute-map)# map-value department Engineering group1
hostname(config-ldap-attribute-map)#
```

次のコマンドは、属性マップ att_map_1 を、LDAP サーバ ldap_dir_1 にバインドします。

```
hostname(config)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# ldap-attribute-map att_map_1
hostname(config-aaa-server-host)#
```

（注）　属性マップを作成するためのコマンド（**ldap attribute-map**）と、それを LDAP サーバにバインドするためのコマンド（**ldap-attribute-map**）は、ハイフン 1 つとモードが異なります。

次のコマンドは、実行コンフィギュレーション内のすべての LDAP 属性マップを表示または消去します。

```
hostname# show running-config all ldap attribute-map
hostname(config)# clear configuration ldap attribute-map
hostname(config)#
```

頻繁にマッピングされるシスコの LDAP 属性の名前と、一般にマッピングされるユーザ定義の属性のタイプは次のとおりです。

cVPN3000-IETF-Radius-Class — Department or user group
cVPN3000-IETF-Radius-Filter-Id — Access control list
cVPN3000-IETF-Radius-Framed-IP-Address — A static IP address
cVPN3000-IPSec-Banner1 — A organization title
cVPN3000-Tunneling-Protocols — Allow or deny dial-in

シスコの LDAP 属性の名前と値のリストについては、付録 E「許可および認証用の外部サーバの設定」を参照してください。または、次の例のように ldap-attribute-map モードで「?」と入力すれば、シスコの LDAP 属性名の完全なリストを表示することもできます。

```
hostname(config)# ldap attribute-map att_map_1
hostname(config-ldap-attribute-map)# map-name att_map_1 ?

ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
    :
    :
  cVPN3000-X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

HTTP Form による Web VPN の SSO サポート

セキュリティ アプライアンスでは、WebVPN ユーザのシングル サインオン（SSO）認証に限って HTTP Form プロトコルを使用できます。シングル サインオンのサポートによって、WebVPN ユーザはユーザ名とパスワードを 1 回だけ入力して、複数の保護されているサービスおよび Web サーバにアクセスできます。セキュリティ アプライアンス上で実行されている WebVPN サーバは、認証サーバにアクセスするユーザのプロキシとして機能します。ユーザがログインすると、SSO 認証要求（ユーザ名とパスワードを含む）が WebVPN サーバから認証サーバに HTTPS を使用して送信されます。サーバによって認証要求が承認されると、SSO 認証クッキーが WebVPN サーバに返されます。セキュリティ アプライアンスは、ユーザの代わりにこのクッキーを保持し、ユーザの認証にこのクッキーを使用して、SSO サーバで保護されているドメイン内の Web サイトの安全を守ります。

WebVPN 管理者は、SSO の設定に対して、HTTP Form プロトコルのほかにも、基本 HTTP 認証プロトコルや NTLM 認証プロトコル（**auto-signon** コマンド）、あるいは Computer Associates eTrust SiteMinder SSL サーバ（旧 Netegrity SiteMinder）を選択できます。HTTP Form、**auto-signon** または SiteMinder を使用した SSO の設定の詳細については、「WebVPN の設定」の章を参照してください。

ローカル データベースのサポート

セキュリティ アプライアンスは、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。

ここでは、次の内容について説明します。

- 「ユーザ プロファイル」（P.13-10）
- 「フォールバック サポート」（P.13-10）

ユーザ プロファイル

ユーザ プロファイルには、少なくともユーザ名が含まれます。通常、パスワードはオプションですが、各ユーザ名にパスワードが割り当てられます。

username attributes コマンドによって、ユーザ名モードを開始できます。このモードでは、別の情報を特定のユーザ プロファイルに追加できます。追加可能な情報には、VPN 関連属性（VPN セッション タイムアウト値など）が含まれます。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、セキュリティ アプライアンスから誤ってロックアウトされないようにすることを意図しています。

フォールバック サポートを必要とするユーザでは、ローカル データベース内のユーザ名とパスワードと AAA サーバ内のユーザ名とパスワードを一致させることをお勧めします。これにより、トランスペアレント フォールバック サポートが提供されます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用することは、指定するべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- **コンソールおよびイネーブル パスワードの認証**：**aaa authentication console** コマンドを使用する場合、AAA サーバ グループ タグのあとに **LOCAL** キーワードを追加できます。すべてのグループのサーバが利用できない場合、セキュリティ アプライアンス は、ローカル データベースを使用して管理アクセスを認証します。これにもイネーブル パスワードの認証を含めることができます。
- **コマンドの許可**：**aaa authorization command** コマンドを使用する場合、AAA サーバ グループ タグのあとに **LOCAL** キーワードを追加できます。すべてのグループの TACACS+ サーバが利用できない場合、ローカル データベースを使用して、イネーブル レベルに基づいてコマンドを許可します。
- **VPN 認証および許可**：VPN サービスを正常にサポートするはずの AAA サーバを利用できない場合、VPN 認証および許可がサポートされ、セキュリティ アプライアンス へのリモート アクセスがイネーブルになります。**authentication-server-group** コマンド（トンネルグループ一般属性モードで使用可能）を使用すると、トンネル グループの属性を設定するときに、**LOCAL** キーワードが指定できます。管理者の VPN クライアントが、ローカル データベースへのフォールバックに設定されたトンネル グループを指定する場合、AAA サーバ グループを利用できなくても、ローカル データベースに必要な属性が設定されていれば、VPN トンネルを確立できます。

ローカル データベースの設定

ここでは、ローカル データベース内のユーザの管理方法について説明します。ローカル データベースは、CLI アクセス認証、特権モード認証、コマンド許可、ネットワーク アクセス認証、および VPN 認証および許可に使用できます。ローカル データベースはネットワーク アクセス許可には使用できません。ローカル データベースはアカウンティングをサポートしません。

マルチコンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して個々のログインを指定できます。しかし、システム実行スペースでは **aaa** コマンドは設定できません。

注意　CLI へのアクセスが許可され、イネーブル モードの使用が許可されないユーザをローカル データベースに追加する場合は、コマンド許可をイネーブルにします（「ローカル コマンド許可の設定」（P.40-8）を参照）。コマンド許可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権モード（およびすべてのコマンド）にアクセスできます。別の方法としては、RADIUS または TACACS+ 認証を使用してユーザが **login** コマンドを使用できないように設定するか、またはすべてのローカル ユーザをレベル 1 に設定してから、システム イネーブル パスワードを使用して特権モードにアクセスできるユーザを制御します。

ローカル データベースにユーザ アカウントを定義するには、次の手順を実行します。

ステップ 1　ユーザ アカウントを作成します。そのためには、次のコマンドを入力します。

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

オプションは次のとおりです。

- *username*：4 ～ 64 文字の長さの文字列を指定します。
- **password** *password*：3 ～ 16 文字の長さの文字列を指定します。
- **mschap**：パスワードを入力後に unicode に変換し、MD4 を使用してハッシュすることを指定します。このキーワードは、ユーザを MSCHAPv1 または MSCHAPv2 を使用して認証する場合に使用します。
- **privilege** *level*：新しいユーザ アカウントに割り当てるイネーブル レベル（0 ～ 15）を指定します。デフォルトは 2 です。この特権レベルは、コマンド許可で使用されます。
- **nopassword**：パスワードを使用しないユーザ アカウントを作成します。

通常、**encrypted** および **nt-encrypted** キーワードは表示専用です。**username** コマンド内のパスワードを定義すると、セキュリティ アプライアンスはセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドは実際のパスワードを表示しません。このコマンドは暗号化されたパスワードを表示し、次に **encrypted** または **nt-encrypted** キーワード（**mschap** を指定する場合）を表示します。たとえば、「test」というパスワードを入力した場合、**show running-config** コマンドの表示は次のようになります。

```
username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted
```

実際に CLI で **encrypted** または **nt-encrypted** キーワードを入力するのは、ある設定を他のセキュリティ アプライアンスにカット アンド ペーストして、同じパスワードを使用している場合だけです。

ステップ 2　VPN 属性を持ったローカル ユーザ アカウントを設定する手順は、次のとおりです。

a.　次のコマンドを入力します。

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

username attributes コマンドを入力すると、ユーザ名モードが開始されます。このモードで利用できるコマンドは、次のとおりです。

- **group-lock**
- **password-storage**
- **vpn-access-hours**
- **vpn-filter**
- **vpn-framed-ip-address**
- **vpn-group-policy**
- **vpn-idle-timeout**
- **vpn-session-timeout**
- **vpn-simultaneous-logins**
- **vpn-tunnel-protocol**
- **webvpn**

このコマンドを必要に応じて使用して、ユーザ プロファイルを設定してください。これらのコマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

b. ユーザ プロファイルの設定を終了する場合、**exit** を入力してコンフィギュレーション モードに戻ります。

次に、admin ユーザのアカウントにイネーブル レベル 15 を割り当てる例を示します。

```
hostname(config)# username admin password passw0rd privilege 15
```

次のコマンドは、パスワードを指定しないユーザ アカウントを作成します。

```
hostname(config)# username bcham34 nopassword
```

次のコマンドはパスワードのあるユーザ アカウントを作成し、username モードを開始し、2 ～ 3 の VPN 属性を指定します。

```
hostname(config)# username rwilliams password gOgeOus
hostname(config)# username rwilliams attributes
hostname(config-username)# vpn-tunnel-protocol IPSec
hostname(config-username)# vpn-simultaneous-logins 6
hostname(config-username)# exit
```

AAA サーバ グループおよびサーバの識別

認証、許可、またはアカウンティングに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。各サーバ グループは、Kerberos、LDAP、NT、RADIUS、SDI、または TACACS+ というサーバの 1 つのタイプ専用となります。

セキュリティ アプライアンス は、グループ内の最初のサーバと通信します。最初のサーバが使用できない場合、セキュリティ アプライアンス はグループ内の次のサーバ（設定されている場合）と通信します。グループ内のすべてのサーバが使用できない場合、セキュリティ アプライアンスは、ローカル

データベースがフォールバック方式として設定されていると、ローカル データベースに接続しようとします（管理認証および許可限定）。フォールバック方式として設定されていない場合、セキュリティ アプライアンスは引き続き AAA サーバにアクセスしようとします。

サーバ グループを作成して、AAA サーバを追加するには、次の手順を実行します。

ステップ 1　作成する必要のある AAA サーバ グループについて、次の手順を実行します。

a. サーバ グループ名とプロトコルを指定します。そのためには、次のコマンドを入力します。

```
hostname(config)# aaa-server server_group protocol {kerberos | ldap | nt | radius |
sdi | tacacs+}
```

たとえば、RADIUS を使用してネットワーク アクセスを認証し、TACACS+ を使用して CLI アクセスを認証するには、RADIUS サーバ用に 1 つ、TACACS+ サーバ用に 1 つというように、最低 2 つのサーバ グループを作成する必要があります。

最大 15 のシングルモード サーバ グループまたは 4 つのマルチモード サーバ グループを指定できます。各サーバ グループには、シングルモードで最大 16 台、マルチモードで最大 4 台のサーバを含めることができます。

aaa-server protocol コマンドを入力する場合は、グループ モードに移行します。

b. 次のサーバに移行する前に、グループ内の 1 つの AAA サーバに送信する要求の最大数を指定するには、次のコマンドを入力します。

```
hostname(config-aaa-server-group)# max-failed-attempts number
```

number の範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカル データベースを使用してフォールバック方式を設定し（管理アクセスだけの場合は、「システム管理者用 AAA の設定」（P.40-5）および「TACACS+ コマンド許可の設定」（P.40-11）を参照してフォールバック メカニズムを設定）、グループ内のすべてのサーバが応答できなかった場合、グループは非応答と見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続いたら、ただちにフォールバック方式が使用されます。応答不可の時間をデフォルト以外に変更する場合は、次の **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、セキュリティ アプライアンスは引き続きグループ内のサーバにアクセスしようとします。

c. グループ内の障害の発生したサーバが再度アクティブ化される方法（再アクティブ化ポリシー）を指定する場合は、次のコマンドを入力します。

```
hostname(config-aaa-server-group)# # reactivation-mode {depletion [deadtime minutes] |
timed}
```

depletion キーワードは、グループ内のすべてのサーバが非アクティブになった後に限り、障害の発生したサーバを再度アクティブ化します。

deadtime *minutes* 引数は、グループ内の最後のサーバをディセーブルにしてから、次にすべてのサーバを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デフォルトは 10 分です。

timed キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。

d. グループのすべてのサーバにアカウンティング メッセージを送信する場合（RADIUS または TACACS+ だけ）、次のコマンドを入力します。

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

アクティブ サーバだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

ステップ 2　ネットワーク上の各 AAA サーバについて、次の手順を実行します。

a. サーバを、所属する AAA サーバ グループを含めて、指定します。そのためには、次のコマンドを入力します。

```
hostname(config)# aaa-server server_group (interface_name) host server_ip
```

aaa-server host コマンドを入力する場合、ホスト モードに移行します。

b. 必要に応じて、ホスト モード コマンドを使用して、さらに AAA サーバを設定します。

ホスト モードでのコマンドは、すべての AAA サーバ タイプに適用されるわけではありません。表 13-2 に、使用できるコマンド、適用されるサーバ タイプ、新しい AAA サーバ定義にコマンドのデフォルト値があるかどうかを示します。指定したサーバ タイプにコマンドを適用でき、デフォルト値がない（「—」で表示）場合、次のコマンドを使用して値を指定します。これらのコマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

表 13-2　ホスト モード コマンド、サーバ タイプ、およびデフォルト

コマンド	適用可能な AAA サーバ タイプ	デフォルト値
accounting-port	RADIUS	1646
acl-netmask-convert	RADIUS	標準
authentication-port	RADIUS	1645
kerberos-realm	Kerberos	—
key	RADIUS	—
	TACACS+	—
ldap-attribute-map	LDAP	—
ldap-base-dn	LDAP	—
ldap-login-dn	LDAP	—
ldap-login-password	LDAP	—
ldap-naming-attribute	LDAP	—
ldap-over-ssl	LDAP	—
ldap-scope	LDAP	—
nt-auth-domain-controller	NT	—
radius-common-pw	RADIUS	—
retry-interval	Kerberos	10 秒
	RADIUS	10 秒
	SDI	10 秒
sasl-mechanism	LDAP	—
server-port	Kerberos	88
	LDAP	389
	NT	139
	SDI	5500
	TACACS+	49
server-type	LDAP	auto-discovery
timeout	All	10 秒

例 13-1 に、1 つのプライマリ サーバと 1 つのバックアップ サーバを持つ 1 つの TACACS+ グループ、単一のサーバを持つ 1 つの RADIUS グループ、および 1 つの NT ドメイン サーバを追加するコマンドを示します。

例 13-1　複数の AAA サーバ グループおよびサーバ

```
hostname(config)# aaa-server AuthInbound protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 2
hostname(config-aaa-server-group)# reactivation-mode depletion deadtime 20
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
```

```
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.2
hostname(config-aaa-server-host)# key TACPlusUauthKey2
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthOutbound protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key RadUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server NTAuth protocol nt
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server NTAuth (inside) host 10.1.1.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)# exit
```

例 13-2 に、watchdogs という名前の Kerberos AAA サーバ グループを設定し、そのグループに AAA サーバを追加して、そのサーバの Kerberos 領域を定義するコマンドを示します。例 13-2 では、リトライ インターバルと Kerberos サーバがリスンするポートを定義していないため、セキュリティ アプライアンスは、これら 2 つのサーバ固有のパラメータにデフォルト値を使用します。表 13-2 に、すべての AAA サーバ ホスト モード コマンドのデフォルト値を示します。

（注）　Kerberos 領域名では数字と大文字だけを使用します。セキュリティ アプライアンスは領域名に小文字を受け入れますが、小文字を大文字に変換しません。大文字だけを使用してください。

例 13-2　Kerberos サーバ グループおよびサーバ

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

証明書とユーザ ログイン クレデンシャルの使用

この項では、認証と許可に証明書およびユーザ ログイン クレデンシャル（ユーザ名とパスワード）を使用する、さまざまな方法について説明します。これは、IPSec および WebVPN の両方に適用されます。

すべての場合において、LDAP 許可では、パスワードをクレデンシャルとして使用しません。RADIUS 許可では、すべてのユーザの共通パスワードまたはユーザ名のいずれかを、パスワードとして使用します。

ユーザ ログイン クレデンシャルの使用

認証および許可のデフォルトの方法では、ユーザ ログイン クレデンシャルを使用します。

- 認証
  - 認証サーバ グループ設定によってイネーブルにされます。
  - ユーザ名とパスワードをクレデンシャルとして使用します。
- 許可
  - 許可サーバ グループ設定によってイネーブルにされます。

- ユーザ名をクレデンシャルとして使用します。

証明書の使用

ユーザ デジタル証明書が設定されている場合、セキュリティ アプライアンスは最初に証明書を検証します。ただし、証明書の DN を認証用のユーザ名として使用しません。

認証と許可の両方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、ユーザの認証と許可の両方にユーザ ログイン クレデンシャルを使用します。

- 認証
  - 認証サーバ グループ設定によってイネーブルにされます。
  - ユーザ名とパスワードをクレデンシャルとして使用します。
- 許可
  - 許可サーバ グループ設定によってイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

認証がディセーブルで許可がイネーブルになっている場合、セキュリティ アプライアンスは許可にプライマリ DN フィールドを使用します。

- 認証
  - 認証サーバ グループ設定によってディセーブル（None に設定）になります。
  - クレデンシャルは使用されません。
- 許可
  - 許可サーバ グループ設定によってイネーブルにされます。
  - 証明書のプライマリ DN フィールドのユーザ名の値をクレデンシャルとして使用します。

（注） 証明書にプライマリ DN フィールドが存在しない場合、セキュリティ アプライアンスはセカンダリ DN フィールドの値を許可要求のユーザ名として使用します。

次の Subject DN フィールドと値が含まれるユーザ証明書を例に挙げます。

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com.
```

プライマリ DN = EA（電子メール アドレス）およびセカンダリ DN = CN（一般名）の場合、許可要求で使われるユーザ名は anyuser@example.com になります。