CHAPTER 10

AAA サーバの設定

この章には、次の項があります。

AAA について

この章では、AAA について説明し、AAA サーバのサポートに関する情報、および ASDM における AAA の実装場所に関する情報について説明します。次の項目を取り上げます。

AAA の概要

AAA によって、FWSM が、ユーザが誰か（認証）、ユーザが何を実行できるか（認可）、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。認証のみで使用することも、認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。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングのみで使用することも、認証および認可とともに使用することもできます。

AAA には、ユーザ アクセスに対して、ACL のみ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内部インターフェイスのサーバ上の Telnet にアクセスできるようにする ACL を作成できます。一部のユーザのみがサーバにアクセスできるようにするが、そのユーザの IP アドレスを常に認識しているとは限らない場合、AAA を使用すると、認証済みまたは認可済み（あるいはその両方）のユーザのみが FWSM を介してアクセスすることが許可されるようにできます（Telnet サーバもまた、認証を実行します。FWSM は、認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）。

- **認証の概要**：認証では、ユーザ ID に基づいてアクセス権が許可されます。認証では、有効なユーザ クレデンシャルを要求してユーザ ID を確立します。このクレデンシャルは通常、ユーザ名とパスワードです。
- **認可の概要**：認可では、ユーザ認証後、ユーザごとにアクセスを制御します。認可では、各認証済みユーザが使用可能なサービスおよびコマンドを制御します。認可をイネーブルにしていない場合は、認証のみで、すべての認証済みユーザがサービスに同じようにアクセスできます。

  認可で提供される制御が必要な場合、広範な認証ルールを設定して、詳細な認可が設定できます。たとえば、外部ネットワーク上のサーバにアクセスする内部ユーザを認証して、特定のユーザがアクセスできる外部サーバを認可によって制限します。

  FWSM はユーザあたり最初の 16 個の認可要求をキャッシュするので、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、FWSM は認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、FWSM 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、そのセッションで FWSM を経由したバイト数、使用されたサービス、セッションの継続時間が含まれます。

AAA の準備

AAA サービスは、LOCAL データベース、または少なくとも 1 つの AAA サーバの使用に依存します。また、AAA サーバが提供するほとんどのサービスに対するフォールバックとして LOCAL データベースを使用することもできます。AAA を実装する前に LOCAL データベースを設定するとともに、AAA サーバ グループとサーバ群を設定する必要があります。

LOCAL データベースおよび AAA サーバの設定方法は、FWSM がサポートする AAA サービスによって異なります。AAA サーバを使用するかどうかに関係なく、管理アクセスをサポートするユーザ アカウントを使用して LOCAL データベースを設定する必要があります。これは、誤ってロックアウトされないためであると同時に、AAA サーバにアクセスできないときに、希望によりフォールバック方式を提供するためでもあります。詳細については、「LOCAL データベース」を参照してください。

表 10-1 では、AAA サーバ タイプごと、および LOCAL データベースごとの AAA サービスのサポートの要約を示しています。LOCAL データベースの管理は、Configuration > Properties > Device Administration > User Accounts ペインでユーザ プロファイルを設定して行います。AAA サーバ グループの確立は、Configuration > Properties > AAA Setup > AAA Server Groups ペインで行います。Configuration > Properties > AAA Setup > AAA Servers ペインで、個別の AAA サーバをサーバ グループに追加します。

表 10-1　AAA サポートの要約

	データベース タイプ						
AAA サービス	**ローカル**	**RADIUS**	**TACACS+**	**SDI**	**NT**	**Kerberos**	**LDAP**
認証							
VPN ユーザ[1]	あり	あり	あり	あり	あり	あり	なし
ファイアウォール セッション	あり	あり	あり	なし	なし	なし	なし
管理者	あり	あり	あり	なし	なし	なし	なし
認可							
VPN ユーザ [1]	あり	あり	なし	なし	なし	なし	あり
ファイアウォール セッション	なし	あり[2]	あり	なし	なし	なし	なし
管理者	あり[3]	なし	あり	なし	なし	なし	なし
アカウンティング							
VPN 接続 [1]	なし	あり	あり	なし	なし	なし	なし
ファイアウォール セッション	なし	あり	あり	なし	なし	なし	なし
管理者	なし	あり	あり	なし	なし	なし	なし

1. VPN は、管理接続のみで使用でき、ASDM で設定することはできません。
2. ファイアウォール セッションの場合、RADIUS 認可はユーザ固有の ACL でのみサポートされます。この ACL は RADIUS 認証応答で受信または指定されます。
3. ローカル コマンド認可は、特権レベルに限りサポートされます。

LOCAL データベース

FWSM 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。

- User Profiles：ユーザ プロファイルには、少なくともユーザ名が含まれています。通常、パスワードはオプションであっても、各ユーザ名に割り当てられます。また、ユーザ プロファイルでは、ユーザごとの VPN アクセス ポリシーも指定されます。ユーザ プロファイルは、Configuration > Properties > Device Administration > User Accounts ペインを使用して管理できます。
- Fallback Support：ローカル データベースは、コンソールに対するフォールバック方式として機能し、コマンド認可、VPN 認証および認可に対するパスワード認証をイネーブルにします。この動作は、FWSM 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。この対処により、透過フォールバックがサポートされます。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。

FWSM での AAA の実装

ここでは、次の項目について説明します。

デバイス管理のための AAA

次のような、FWSM へのすべての管理接続を認証できます。

- Telnet
- SSH
- ASDM
- VPN 管理アクセス

また、イネーブル モードを入力しようとしている管理者も認証できます。さらに、管理コマンドを認可できます。管理セッションのアカウンティング データ、およびアカウンティング サーバに送信された、セッション中に発行済みのコマンドのアカウンティング データを保持できます。

Configuration > Properties > Device Access > AAA Access ペインを使用して、AAA をデバイス管理用に設定できます。

ネットワーク アクセス用の AAA

Configuration > Security Policy > AAA Rules ペインを使用して、ファイアウォールを通過するトラフィックの認証、認可、アカウンティングのルールの設定ができます。作成するルールはアクセス ルールに類似していますが、定義したトラフィックの認証、認可、アカウンティングを実行するかどうかを指定する点、また、AAA サービス要求の処理に FWSM が使用する AAA サーバ グループを指定する点が異なります。

AAA のセットアップ

AAA Setup ペインでは、AAA サーバ グループ、AAA サーバ、および認証プロンプトを設定できます。ここでは、次の項目について説明します。

- AAA Server Groups
- AAA Servers
- Auth. Prompt

AAA Server Groups

AAA Server Groups ペインでは、FWSM が各グループに表示されたサーバとの通信に使用する AAA サーバ グループとプロトコルを設定できます。外部グループに個別のサーバを設定する必要があります。既存の AAA サーバ グループに AAA サーバを追加および設定するには、「AAA Servers」を参照してください。

シングルモードでは最大 15 のグループを、マルチモードでは最大 4 つのグループを指定できます。各グループには、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。ユーザがログインするとき、アクセスされるサーバは一度に 1 つだけです。指定したサーバから、応答があるまで順に 1 つずつアクセスしていきます。

AAA アカウンティングが有効になっている場合、同時アカウンティングを設定していない限り、アカウンティング情報が送られるのはアクティブ サーバに対してだけです。

AAA サービスの概要については、「AAA のセットアップ」を参照してください。

フィールド

（注）　AAA Server Groups テーブルで任意の行をダブルクリックすると、Edit AAA Server Group ダイアログボックスが開きます。このダイアログボックスでは、AAA Server Group パラメータを変更できます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには **Apply** をクリックする必要があります。

カラムの先頭をクリックすると、そのカラムの内容に従って、テーブルの行が英数字順に並び替わります。

- Server Group：選択したサーバ グループのシンボリック名を指定します。
- Protocol：グループのサーバがサポートする AAA プロトコルが一覧表示されます。
- Accounting Mode：同時モード アカウンティングまたはシングルモード アカウンティングを選択します。シングルモードでは、FWSM はアカウンティング データを 1 つのサーバにのみ送信します。同時モードでは、FWSM はアカウンティング データをグループ内のすべてのサーバに送信します。
- Reactivation Mode：障害が発生したサーバを再アクティブ化する方法を Depletion または Timed 再アクティブ化モードから指定します。Depletion モードでは、障害が発生したサーバは、グループ内のサーバのすべてが非アクティブになった場合にのみ再アクティブ化されます。Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。
- Dead Time：グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度アクティブにするまでの経過時間を分数で指定します。このパラメータは、Depletion モードでのみ適用されます。
- Max Failed Attempts：応答のないサーバを非アクティブと宣言する前に許可される接続試行失敗の回数を指定します。

- Add：Add AAA Server Group ダイアログボックスが表示されます。
- Edit：Edit AAA Server Group ダイアログボックスを表示します。ただし、サーバ グループとして LOCAL を選択した場合は、Edit AAA Local Server Group ダイアログボックスを表示します。
- Delete：現在選択しているサーバ グループ エントリをサーバ グループ テーブルから削除します。確認されず、やり直しもできません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit AAA Server Group

Add/Edit AAA Server Group ダイアログボックスは、AAA Server Group ペインで **Add** または **Edit** ボタンをクリックしたときに表示されます。これによって、AAA サーバ グループを追加または変更できます。結果は AAA Server テーブルに表示されます。

フィールド

- Server Group：サーバ グループの名前を指定します。
- Protocol : グループのサーバでサポートされているプロトコルを指定します。サポートされているプロトコルは次のとおりです。
  - RADIUS
  - TACACS+
  - NT Domain
  - SDI
  - Kerberos
  - LDAP
- Accounting Mode：同時モード アカウンティングまたはシングルモード アカウンティングを選択します。
  - Single：FWSM は、アカウンティング データをサーバ 1 つだけに送信します。
  - Simultaneous：FWSM は、アカウンティング データをグループ内のすべてのサーバに送信します。
- Reactivation Mode：障害が発生したサーバを再アクティブ化する方法を Depletion または Timed 再アクティブ化モードから指定します。
  - Depletion：障害が発生したサーバは、グループ内のサーバのすべてが非アクティブになった場合にのみ再アクティブ化されます。
  - Timed：30 秒のダウン タイムの後、障害が発生したサーバは再アクティブ化されます。
- Dead Time：グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度アクティブにするまでの経過時間を分数で指定します。このボックスは、Timed モードでは使用できません。
- Max Failed Attempts：応答がないサーバを非アクティブと宣言するまでに許可される接続試行失敗の回数（1 ～ 5）を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Edit AAA Local Server Group

Edit AAA Local Server Group ダイアログボックスでは、ローカル ユーザ ロックアウトをイネーブルにしたり、ログイン試行の最大失敗回数を設定したりすることができます。ユーザがロックアウトされた場合、正常にログインするには、管理者がロックアウト状態をクリアしておく必要があります。

フィールド

- Enable Local User Lockout：設定された認証試行の最大失敗回数を超えたユーザのロックアウトと、そのユーザのアクセス拒否をイネーブルにします。
- Maximum Attempts：ユーザをロックアウトし、そのユーザのアクセスを拒否する前に許可するログイン試行の最大失敗回数を指定します。この制限は、認証に LOCAL データベースが使用されているときのみ適用されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

AAA Servers

AAA Servers ペインでは、既存の AAA サーバ グループに AAA サーバを追加および設定できます。サーバ グループを設定するには、「AAA Server Groups」を参照してください。このサーバには、RADIUS、TACACS+、NT、SDI、Kerberos、または LDAP サーバを指定できます。

AAA サービスの概要については、「AAA のセットアップ」を参照してください。

フィールド

- Server Group (Protocol)：サーバ グループが使用するサーバ グループ名と AAA プロトコルを指定します。
- Interface：認証サーバが常駐するネットワーク インターフェイスを指定します。
- Server IP Address：AAA サーバの IP アドレスを指定します。
- Timeout：タイムアウト間隔を秒数で指定します。この時間に達すると、FWSM はプライマリ AAA サーバに対する要求の送信を放棄します。スタンバイ AAA サーバがある場合、FWSM はバックアップ サーバに要求を送信します。
- Add：新しい AAA サーバをリストに追加します。
- Edit：すでにリストに存在する AAA サーバのパラメータを変更します。
- Delete：AAA サーバをリストから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit AAA Server

Add/Edit AAA Server ダイアログボックスでは、新しい AAA サーバを既存のグループに追加したり、または既存の AAA サーバのパラメータを変更したりします。

フィールド

（注）　最初の 4 つのフィールドは、すべてのサーバ タイプに共通です。コンテンツ領域は、各サーバ タイプに固有です。

- Server Group：Configuration > Properties > AAA Setup > AAA Server Groups で設定されているとおりに、サーバ グループの名前を指定します。
- Interface Name：サーバが常駐するネットワーク インターフェイスを指定します。
- Server IP Address：AAA サーバの IP アドレスを指定します。
- Timeout：タイムアウト間隔を秒数で指定します。この時間に達すると、FWSM はプライマリ AAA サーバに対する要求の送信を放棄します。スタンバイ AAA サーバがある場合、FWSM はバックアップ サーバに要求を送信します。
- RADIUS Parameters：RADIUS サーバの使用に必要なパラメータを指定します。選択したサーバ グループが RADIUS を使用するときにのみ、この領域が表示されます。
  - Retry Interval：サーバにクエリーを送信しても応答がないときに、接続を再試行する前に待機する秒数を指定します。最小時間は 1 秒です。デフォルト時間は 10 秒です。最大時間は 10 秒です。
  - Server Authentication Port：ユーザ認証に使用するサーバ ポートを指定します。デフォルト ポートは 1645 です。

（注）　最新の RFC では、RADIUS を UDP ポート番号 1812 に設定すべきだとしているので、このデフォルトは 1812 への変更が必要になる場合があります。

  - Server Accounting Port：ユーザ アカウンティングに使用するサーバ ポートを指定します。デフォルト ポートは 1646 です。
  - Server Secret Key：暗号化に使用する、たとえば C8z077f のようなサーバ秘密鍵（「共有秘密情報」とも呼ばれます）を指定します。この秘密鍵では、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。FWSM は、サーバ秘密鍵を使用して、RADIUS サーバに対する認証を行います。ここで設定したサーバ秘密鍵は、RADIUS サーバで設定されたサーバ秘密鍵と一致する必要があります。RADIUS サーバのサーバ秘密鍵がわからない場合は、RADIUS サーバの管理者に問い合せてください。最大フィールド長は、64 文字です。

- Confirm Server Secret Key：正確であることを確認するため、サーバの秘密鍵を再度入力する必要があります。この秘密鍵では、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。
- Common Password：RADIUS 認可サーバで使用するための共通パスワードを指定します。パスワードは、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。RADIUS サーバを認可ではなく認証に使用するよう定義する場合は、共通パスワードを設定しないでください。

  RADIUS 認可サーバでは、接続しようとする各ユーザのパスワードとユーザ名が必要です。パスワードはここに入力します。RADIUS 認可サーバの管理者は、このパスワードを FWSM 経由でサーバに接続する各ユーザ認可に関連付けて RADIUS サーバを設定する必要があります。この情報は、必ず RADIUS サーバの管理者に提供してください。この FWSM 経由で RADIUS 認可サーバにアクセスするすべてのユーザの共通パスワードを入力します。

  このフィールドを空白のままにすると、各ユーザのユーザ名がパスワードになります。たとえば、ユーザ名「jsmith」であるユーザの場合、「jsmith」と入力されます。セキュリティ上の予防措置として、RADIUS 認可サーバを絶対に認証に使用しないでください。共通パスワードを使用したり、パスワードとしてユーザ名を使用したりすることは、ユーザごとに強力なパスワードを使用するのに比べてはるかにセキュリティが低くなります。

（注）　RADIUS プロトコルではパスワード フィールドが必須であり、RADIUS サーバによっても要求されますが、ユーザはパスワードを知る必要がありません。

- Confirm Common Password：正確であることを確認するため、共通パスワードを再度入力する必要があります。パスワードは、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。

- TACACS+ Parameters：TACACS+ サーバの使用に必要なパラメータを指定します。選択したサーバ グループが TACACS+ を使用するときにのみ、この領域が表示されます。
  - Server Port：使用するサーバ ポートを指定します。
  - Server Secret Key：暗号化に使用するサーバ秘密鍵を指定します。この秘密鍵では、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。
  - Confirm Server Secret Key：正確であることを確認するため、サーバの秘密鍵を再度入力する必要があります。この秘密鍵では、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。
- SDI Parameters：SDI サーバの使用に必要なパラメータを指定します。選択したサーバ グループが SDI を使用するときにのみ、この領域が表示されます。
  - Server Port：使用するサーバ ポートを指定します。
  - Retry Interval：接続を再試行する前に待機する秒数を指定します。
  - SDI Version：このサーバで実行している SDI ソフトウェアのバージョンを、SDI バージョン 5.0 以降、または SDI バージョン 5.0 以前のバージョンで指定します。
- Kerberos Parameters：Kerberos サーバの使用に必要なパラメータを指定します。選択したサーバ グループが Kerberos を使用するときにのみ、この領域が表示されます。
  - Server Port：使用するサーバ ポートを指定します。
  - Retry Interval：接続を再試行する前に待機する秒数を指定します。タイムアウト時間の経過後、サーバへのクエリー送信の再試行回数を入力します。再試行回数の入力を行った後でも応答がない場合、FWSM はこのサーバを操作不能であると宣言し、リスト内にある次の Kerberos および Active Directory サーバを使用します。最小リトライ数は 0、デフォルトのリトライ数は 2、最大リトライ数は 10 です。
  - Kerberos Realm：使用する Kerberos 領域の名前（USDOMAIN.EXAMPLE.COM など）を指定します。最大長は 64 文字です。サーバ タイプが Windows 2000、Windows XP、Windows.NET の場合、領域名はすべて大文字で入力する必要があります。この名前は入力するとき、IP アドレスを Server IP Address ボックスに入力したサーバの領域名に一致している必要があります。

- LDAP Parameters：LDAP サーバの使用に必要なパラメータを指定します。選択したサーバ グループが LDAP を使用するときにのみ、この領域が表示されます。
  - Server Port：使用するサーバ ポートを指定します。サーバにアクセスするための TCP ポート番号を入力します。
  - Base DN：ベース DN を指定します。認可要求を受信したときに、サーバが検索を開始する LDAP 階層の位置を入力します。たとえば、`OU=people, dc=cisco, dc=com` となります。
  - Scope：サーバが認可要求を受け取ったときに行う、LDAP 階層での検索範囲を指定します。オプションは One Level（ベース DN の下にある 1 レベルのみを検索します。このオプションは、時間がかかりません）および All Levels（ベース DN の下にあるすべてのレベルを検索します。つまり、サブツリー階層全体を検索します。このオプションは、多少時間がかかります）です。
  - Naming Attribute(s)：LDAP サーバのエントリを一意に識別する Relative Distinguished Name アトリビュートを指定します。共通の名前付きアトリビュートは、Common Name（cn）と User ID（uid）です。
  - Login DN：ログイン DN を指定します。一部の LDAP サーバ（Microsoft Active Directory サーバなど）は、FWSM に対し、他のあらゆる LDAP 操作の要求を受け入れる前に、認証済みバインディングを介してハンドシェイクを確立することを要求します。FWSM は、ユーザの認証要求に Login DN フィールドを付加することにより、自身が認証バインディングされていることを示します。Login DN フィールドは、FWSM の認証特性を定義します。これらの特性は、管理者の権限が与えられているユーザの特性に対応します。FWSM の認証済みバインディングのディレクトリ オブジェクト名を入力します。たとえば、cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com となります。匿名アクセスの場合は、このフィールドをブランクのままにしておきます。
  - Login Password：ログイン パスワードを指定します。入力した文字はアスタリスクに置き換えられます。
  - Confirm Login Password：前のパラメータで指定したログイン パスワードと同じでなければなりません。
- NT Domain Parameters：NT サーバの使用に必要なパラメータを指定します。選択したサーバ グループが NT Domain サーバ グループの場合にのみ、この領域が表示されます。
  - Server Port：サーバにアクセスするための TCP ポート番号を指定します。デフォルト ポート番号は 139 です。
  - NT Domain Controller：このサーバの NT プライマリ ドメイン コントローラのホスト名（PDC01 など）を指定します。ホスト名の最大長は 15 文字です。この名前を入力するとき、Authentication Server Address に入力したサーバのホスト名に一致している必要があります。名前が正しくないと、認証が失敗します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Auth. Prompt

Auth. Prompt ペインでは、AAA 認証チャレンジ プロセス中にユーザに対して表示されるテキストを指定できます。TACACS+ または RADIUS サーバからユーザ認証が要求されたとき、FWSM を経由した HTTP、HTTPS、FTP、Telnet アクセスの AAA チャレンジ テキストを指定できます。このテキストは、主に表面的なものを整えることを目的としていて、ログイン時にユーザに対して表示される、ユーザ名とパスワード プロンプトの上に表示されます。

AAA サーバがユーザを認証する場合、指定されていれば、FWSM はユーザ承認テキストをユーザに対して表示します。それ以外の場合、指定されていればユーザ拒否テキストを表示します。拒否の原因が無効なクレデンシャル（正しくないユーザ名など）や、パスワードの期限切れである場合、ユーザ拒否テキストではなく、無効なクレデンシャル テキストまたは期限切れのパスワード テキストが表示されます。

（注）　Microsoft Internet Explorer では、認証プロンプトに最大 37 文字まで表示されます。Netscape Navigator では、認証プロンプトに最大 120 文字まで、Telnet および FTP では最大 235 文字まで表示されます。

フィールド

- Prompt：FWSM を経由したユーザ セッションに対して、AAA チャレンジ テキストの表示をイネーブルにします。
  - Prompt：235 文字までの英数字または 31 ワードまでの文字列を指定します。いずれかの最大値に達したときに制限されます。特殊文字は使用できませんが、スペースと句読点は使用できます。文字列を終了するには、疑問符を入力するか **Enter** キーを押します（Enter キーを押すと文字列に疑問符が表示されます）。
- Messages：ユーザが承認または拒否されたときに表示するメッセージを設定します。235 文字までの英数字または 31 ワードまでの文字列を指定します。いずれかの最大値に達したときに制限されます。特殊文字は使用できませんが、スペースと句読点は使用できます。文字列を終了するには、疑問符を入力するか **Enter** キーを押します（Enter キーを押すと文字列に疑問符が表示されます）。
  - User Accepted：ユーザ認証が承認されたときに表示するテキストを設定します。
  - User Rejected：ユーザ認証が拒否されたときに表示するテキストを設定します。無効なクレデンシャルまたは期限切れのパスワードが原因ではないすべての拒否に対して、この汎用プロンプトが表示されます。無効なクレデンシャルまたは期限切れのパスワードが原因の拒否に対しては、Invalid Credensials または Password Expired オプションで設定したプロンプトが表示されます。無効なクレデンシャルまたは期限切れのパスワードにプロンプトを設定していないと、すべての場合に汎用拒否プロンプトが表示されます。
  - Invalid Credentials：正しくないユーザ名またはパスワードなど、無効なクレデンシャルが原因でユーザ認証が拒否されたときに表示するテキストを設定します。
  - Password Expired：期限切れのパスワードが原因でユーザ認証が拒否されたときに表示するテキストを設定します。このプロンプトは、RADIUS サーバがユーザ名とパスワードに Windows Active Directory サーバを使用している場合にのみ使用されます。新しいパスワードの入力を求めるユーザに対して、このオプションを使用してプロンプトを設定する必要があります。

（注）　このペインのフィールドはすべてオプションです。認証プロンプトを指定していない場合、FTP ユーザには `FTP authentication` が、HTTP ユーザには `HTTP Authentication` が表示され、Telnet ユーザにはチャレンジ テキストが表示されません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—