CHAPTER 35

AAA への TACACS+ サーバの設定

この章では、AAA で使用する TACACS+ サーバの設定方法を説明します。次の項目を取り上げます。

- 「TACACS+ サーバについての情報」（P.35-1）
- 「TACACS+ サーバのライセンス要件」（P.35-2）
- 「注意事項と制約事項」（P.35-3）
- 「TACACS+ サーバの設定」（P.35-3）
- 「TACACS+ サーバによる認証および許可のテスト」（P.35-6）
- 「TACACS+ サーバのモニタリング」（P.35-7）
- 「TACACS+ サーバの機能履歴」（P.35-7）

TACACS+ サーバについての情報

ASA は、ASCII、PAP、CHAP、MS-CHAPv1 のプロトコルで TACACS+ サーバ認証をサポートします。

TACACS+ 属性の使用

ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの 2 種類の属性をサポートします。サーバとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注） TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

表 35-1 に、カットスルー プロキシ接続に対してサポートされている TACACS+ 許可応答属性の一覧を示します。表 35-2 に、サポートされている TACACS+ アカウンティング属性の一覧を示します。

表 35-1　サポートされる TACACS+ 許可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みの ACL を識別します。
idletime	認証済みユーザ セッションが終了する前に許可される非アクティブ時間（分）を示します。
timeout	認証済みユーザ セッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。

表 35-2　サポートされる TACACS+ アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。
bytes_out	この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行するコマンドを定義します（コマンド アカウンティングのみ）。
disc-cause	切断理由を特定する数字コードを示します（ストップ レコードのみ）。
elapsed_time	接続の経過時間（秒）を定義します（ストップ レコードのみ）。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求の場合はユーザの権限レベル、それ以外の場合は 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。
service	使用するサービスを指定します。コマンド アカウンティングだけは、常に「シェル」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザの名前を示します。

TACACS+ サーバのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。
- 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。
- ローカル データベースを使用してフォール バック サポートを設定する場合は、「フォールバック サポート」（P.33-2）と「グループ内の複数のサーバを使用したフォールバックの仕組み」（P.33-2）を参照してください。
- TACACS+ 認証または許可を使用する場合に ASA からのロック アウトを防止するには、「ロック アウトからの回復」（P.45-35）を参照してください。

TACACS+ サーバの設定

この項では、次のトピックについて取り上げます。

- 「TACACS+ サーバを設定するためのタスク フロー」（P.35-3）
- 「TACACS+ サーバ グループの設定」（P.35-4）
- 「グループへの TACACS+ サーバの追加」（P.35-4）
- 「認証プロンプトの追加」（P.35-5）

TACACS+ サーバを設定するためのタスク フロー

ステップ 1　TACACS+ サーバ グループを追加します。「TACACS+ サーバ グループの設定」（P.35-4）を参照してください。

ステップ 2　サーバ グループの場合は、グループにサーバを追加します。「グループへの TACACS+ サーバの追加」（P.35-4）を参照してください。

ステップ 3　（任意）AAA 認証チャレンジ プロセスの実行中にユーザに表示するテキストを指定します。「認証プロンプトの追加」（P.35-5）を参照してください。

TACACS+ サーバ グループの設定

認証、許可、アカウンティングに TACACS+ サーバを使用する場合は、まず TACACS+ サーバ グループを少なくとも 1 つ作成し、各グループに 1 台以上のサーバを追加する必要があります。TACACS+ サーバ グループは名前で識別されます。

TACACS+ サーバ グループを追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2　[AAA Server Groups] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[Server Group] フィールドで、グループの名前を入力します。

ステップ 4　[Protocol] ドロップダウン リストから、次のいずれかの TACACS+ サーバ タイプを選択します。

ステップ 5　[Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバに送信されます。

ステップ 6　[Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、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。

ステップ 7　[Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

[Dead Time] には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 8　[Max Failed Attempts] フィールドに、許容される試行の失敗回数を指定します。

このオプションで設定するのは、応答の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の失敗回数です。

ステップ 9　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバ グループが [AAA Server Groups] テーブルに追加されます。

ステップ 10　[AAA Server Groups] ダイアログボックスの [Apply] をクリックして、変更内容を実行コンフィギュレーションに保存します。

グループへの TACACS+ サーバの追加

TACACS+ サーバをグループに追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域で、サーバを追加するサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] 領域の [Servers]（下部ペイン）で、[Add] をクリックします。

サーバ グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[Interface Name] ドロップダウン リストから、認証サーバが常駐するインターフェイスの名前を選択します。

ステップ 4　[Server Name] フィールドまたは [IP Address] フィールドに、グループに追加するサーバの名前または IP アドレスを入力します。

ステップ 5　[Timeout] フィールドで、タイムアウト値を入力します。デフォルト値をそのまま使用することもできます。[Timeout] フィールドには、バックアップ サーバへ要求を送信した ASA が、プライマリ サーバからの応答を待機する時間を秒単位で指定します。

ステップ 6　サーバ ポートを指定します。サーバ ポートは、ポート番号 139、または ASA によって TACACS+ サーバとの通信に使用される TCP ポートの番号です。

ステップ 7　サーバ秘密キーを指定します。ASA で TACACS+ サーバを認証する際に使用される共有秘密キーを指定します。ここで設定したサーバ秘密キーは、TACACS+ サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーが不明の場合は、TACACS+ サーバの管理者に問い合わせてください。最大フィールド長は、64 文字です。

ステップ 8　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバ グループに追加されます。

ステップ 9　[AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

AAA 認証チャレンジ プロセスの実行中にユーザに表示するテキストを指定できます。TACACS+ サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

認証プロンプトを指定しない場合、TACACS+ サーバでの認証時にユーザに対して表示される内容は次のようになります。

接続タイプ	デフォルトのプロンプト
FTP	FTP authentication
HTTP	HTTP authentication
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt] の順に選択します。

ステップ 2　ログイン時にユーザ名とパスワード プロンプトの上に表示するメッセージとして追加するテキストを、[Prompt] フィールドに入力します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	認証プロンプトの文字数制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

ステップ 3　[Messages] 領域の [User accepted message] フィールドおよび [User rejected message] フィールドにそれぞれメッセージを入力します。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証試行が AAA サーバにより受け入れられた、または拒否されたことを示すさまざまな状態のプロンプトを表示できます。

これらのメッセージ テキストをそれぞれ指定した場合、ASA では、AAA サーバにより認証されたユーザに対してはユーザ承認メッセージ テキストが表示され、認証されなかったユーザに対しては ASA によりユーザ拒否メッセージ テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。ユーザ承認メッセージ テキストおよびユーザ拒否メッセージ テキストは表示されません。

ステップ 4　[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

TACACS+ サーバによる認証および許可のテスト

ASA が TACACS+ サーバに接続して、ユーザを認証または承認できるかどうかを決定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [AAA Server Groups] テーブルで、サーバが含まれるサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] テーブルの [Servers] から、テストするサーバをクリックします。

テーブル内の該当する行が選択されます。

ステップ 3　[Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4　実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5　[Username] フィールドにユーザ名を入力します。

ステップ 6　認証をテストする場合は、そのユーザ名に対応するパスワードを [Password] フィールドに入力します。

ステップ 7　[OK] をクリックします。

認証または許可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

TACACS+ サーバのモニタリング

TACACS+ サーバをモニタするには、次のペインを参照してください。

パス	目的
[Monitoring] > [Properties] > [AAA Servers]	設定した TACACS+ サーバの統計情報を表示します。
[Monitoring] > [Properties] > [AAA Servers]	TACACS+ サーバ実行コンフィグレーションを表示します。

TACACS+ サーバの機能履歴

表 35-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 35-3　TACACS+ サーバの機能履歴

機能名	プラットフォーム リリース	機能情報
TACACS+ サーバ	7.0(1)	AAA に TACACS+ サーバを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]。