CHAPTER 18

AAA ルールの設定

この章では、ネットワーク アクセスに対して AAA（トリプル エー）をイネーブルにする方法について説明します。

管理アクセスの AAA については、P.11-2 の「AAA Access」を参照してください。

この章には、次の項があります。

- AAA パフォーマンス（P.18-1）
- AAA Rules（P.18-2）
- ネットワーク アクセス認証の設定（P.18-5）
- ネットワーク アクセス認可の設定（P.18-9）
- アカウンティング ルールの追加および編集（P.18-15）
- MAC アドレスによるトラフィックの認証と認可の免除（P.18-17）
- Advanced AAA Configuration（P.18-18）

AAA パフォーマンス

FWSM は「カットスルー プロキシ」を使用します。この方法により、従来のプロキシ サーバと比較して、パフォーマンスが大幅に向上します。従来のプロキシ サーバは、OSI モデルのアプリケーション レイヤですべてのパケットを分析するため、プロキシ サーバのパフォーマンスに負担がかかります。FWSM カットスルー プロキシは、アプリケーション レイヤで最初にユーザ確認を行い、標準 AAA サーバまたはローカル データベースで認証します。FWSM はユーザを認証した後、セッション フローをシフトするため、セッション ステート情報を維持したまま、すべてのトラフィックが送信元と宛先の間で直接かつ迅速に流れます。

AAA Rules

Security Policy ペインには、ルールに示されたネットワーク セキュリティ ポリシーが表示されます。このペインには、AAA ルールのほか、他のルールのタブもあります。この項目では AAA ルールを説明します。AAA サービスの概要については、第 10 章「AAA サーバの設定」を参照してください。

AAA Rules タブを選択すると、MAC 免除ルールとともに、認証、認可、またはアカウンティング（AAA）ルールを定義できます。AAA は FWSM に、ユーザが誰か、ユーザが何を実行できるか、およびユーザが何を実行したかを知らせます。認証のみで使用することも、認可とともに使用することもできます。認可には常に認証が必要です。たとえば、内部ネットワークのサーバにアクセスする外部ユーザを認証する場合、認証だけで十分に対応します。ただし、特定のユーザがアクセスする内部サーバを制限する場合は、認可サーバを設定し、どのサーバとサービスにユーザがアクセスできるのかを指定することができます。

AAA には、ユーザ アクセスに対して、アクセスリスト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 DMZ ネットワークのサーバ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。登録したユーザだけがサーバに Telnet できるようにするには、AAA を設定して、認証または認可、あるいはその両方が行われたユーザだけが FWSM を通過できるようにします。サーバに独自の認証および認可がある場合、ユーザは 2 番目のユーザ名とパスワードのセットを入力します（FTP の場合、ユーザはアット マーク（@）で区切ったユーザ名とパスワードの両方を入力する必要があります）。

各 AAA ルールでは、一致トラフィックの次の特性が識別されます。

- 送信元および宛先ネットワーク
- アクション（認証、認可、またはアカウンティング。ルールでは、AAA から MAC アドレスを除外することもできます）
- AAA サーバ グループ
- サービス グループ（Telnet や FTP など）

前提条件

1. Configuration > Features > Properties > AAA Setup > AAA Server Groups ペインで、各ホストまたはサーバを定義します。
2. ローカル データベースにユーザを追加します（**Configuration > Features > Properties > Administration > User Accounts** を参照）。
3. ユーザが指定したネットワークにアクセスできることを確認します（必要に応じて「アクセス ルールの設定」を参照）。
4. AAA サーバを正しくセットアップします。

フィールド

- **Add**：新しい AAA ルールを追加します。ドロップダウン リストから、追加するルールのタイプを選択します。
- **Edit**：AAA ルールを編集します。
- **Delete**：AAA ルールを削除します。
- Move Up：ルールを上に移動します。ルールは、テーブルに表示されている順に査定されます。したがって、重複するルールがある場合、その順序が問題になります。
- Move Down：ルールを下に移動します。
- Cut：ルールを切り取ります。
- Copy：ルール パラメータをコピーします。Paste ボタンを使用すれば、新しいルールを同じパラメータで開始できます。

- Paste：コピーまたは切り取ったルール パラメータが入力済みの Add/Edit Rule ダイアログボックスが開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上にルールが追加されます。Paste ドロップダウン リストから Paste After 項目を選択すると、選択したルールの後にルールが追加されます。
- Find：表示をフィルタリングして、一致するルールのみを表示します。**Find** をクリックすると、Filter フィールドが表示されます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter ドロップダウン リスト：Interface、Source、Destination、Service、Action、または Rule Query の中からフィルタの基準を選択します。ルール クエリーは複数の基準の集合であり、保存して繰り返し使用できます。
  - Filter フィールド：Interface タイプの場合は、このフィールドがドロップダウン リストになります。リストでは、インターフェイス名または **All Interfaces** を選択できます。Action タイプの場合、ドロップダウン リストには Permit と Deny が表示されます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが表示されます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開き、アドレスを参照します。Service タイプには、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。IP アドレスを 1 つ手動で入力するか、**...** ボタンをクリックし、Browse Service Groups ダイアログボックスを開いて参照します。
  - Filter：フィルタリングを実行します。
  - Clear：Filter フィールドをクリアします。
  - Rule Query：名前付きルール クエリーを管理できる Rule Queries ダイアログボックスが開きます。
- Show Rule Flow Diagram：ルール テーブルの下に Rule Flow Diagram 領域を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクション（Authenticate または Do Not Authenticate など）を示しています。

次の説明では、AAA Rules テーブルのカラムをまとめています。これらのカラムの内容は、テーブル セルをダブルクリックすると編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムをソート キーとして、テーブルの内容がアルファベットの昇順で並べ替えられます。ルールを右クリックすると、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- **No**：ルールの評価順序を示します。
- **Enabled**：ルールがイネーブルになっているか、またはディセーブルになっているかを示します。
- **Action**：AAA ルールのタイプを指定します。
- **Source**：Destination カラムに一覧表示された IP アドレスにトラフィックが送信されたとき、AAA の対象となる IP アドレスを一覧表示します。
- **Destination**：Source カラムに一覧表示された IP アドレスからトラフィックが送信されたとき、AAA の対象となる IP アドレスを一覧表示します。
- **Service**：ルールで指定されるサービスまたはプロトコルを表示します。
- Action：Authenticate、Do Not Authenticate、Authorize、Do Not Authorize など、ルールで指定されたアクションを表示します。
- **Server Group**：AAA Server Group タグを指定します。AAA サーバ グループの設定は、Properties > AAA Setup > AAA Server Groups で行います。新しい AAA ルールを作成するには、サーバ グループがあり、その中に 1 つ以上のサーバが存在する必要があります。
- **Time**：このルールで有効な時間範囲の名前を指定します。
- **Description**：ルールの追加時に入力した説明です。

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
•	•	•	•	—

ネットワーク アクセス認証の設定

ここでは、次の項目について説明します。

- 認証の概要（P.18-5）
- 認証ルールの追加および編集（P.18-7）

認証の概要

FWSM では、AAA サーバを利用してネットワーク アクセス認証を設定します。ここでは、次の項目について説明します。

- ワンタイム認証（P.18-5）
- 認証チャレンジの受信が必要なアプリケーション（P.18-5）
- スタティック PAT および HTTP（P.18-6）
- FWSM での直接認証（P.18-6）

ワンタイム認証

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります（タイムアウト値については、「Timeouts」を参照）。たとえば、Telnet および FTP を認証するように FWSM が設定されていて、ユーザが正常に Telnet 認証を受けた場合、認証セッションが継続している限り、ユーザは FTP 認証を受ける必要はありません。

HTTP 認証または HTTPS 認証では、タイムアウトが非常に短く設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」文字列をキャッシュして、後続の接続のすべてに使用するからです。この文字列がクリアされるのは、ユーザが Web ブラウザの すべてのインスタンス終了してブラウザを再起動したときのみです。キャッシュをフラッシュしても意味がありません。

認証チャレンジの受信が必要なアプリケーション

どのプロトコルやサービスへのネットワーク アクセスについても、認証を必要とするように FWSM を設定できますが、ユーザが直接認証を受けられるのは HTTP、HTTPS、Telnet、または FTP を使用する場合のみです。ユーザがこれらのサービスのいずれかの認証を受けないと、FWSM は認証が必要な他のトラフィックを許可しません。

FWSM が AAA 用にサポートしている認証ポートは、次のように固定されています。

- ポート 21（FTP の場合）
- ポート 23（Telnet の場合）
- ポート 80（HTTP の場合）
- ポート 443（HTTPS の場合）

Telnet および FTP の場合、FWSM は認証プロンプトを生成します。正常に認証されると、FWSM により元の宛先にリダイレクトされます。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。

HTTP の場合、ブラウザが提供する基本 HTTP 認証を使用してログインします。HTTPS の場合、FWSM は専用のログイン ウィンドウを生成します。

（注）　HTTP クライアント認証（「Advanced AAA Configuration」を参照）を使用せずに HTTP 認証を使用する場合、ユーザ名とパスワードはクリア テキストで宛先 Web サーバに送信され、AAA サーバには送信されません。たとえば、内部ユーザが外部の Web サーバにアクセスするときに認証すると、有効なユーザ名とパスワードが外部から判別可能になります。HTTP 認証をイネーブルにする場合は、必ずセキュアな HTTP クライアント認証を使用することをお勧めします。

FTP の場合、FWSM ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、FWSM パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> jamiec@patm
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

スタティック PAT および HTTP

HTTP 認証でスタティック PAT が設定されている場合、FWSM は実際のポートをチェックします。FWSM は、マッピング ポートにかかわらず、実際のポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、外部 TCP ポート 889 はポート 80（www）に変換され、すべての関連アクセスリストはトラフィックを許可するものとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask
255.255.255.255
```

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、FWSM はそのトラフィックを代行受信し、HTTP 認証を実行します。FWSM が HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

次の例のように、ローカル ポートが 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask
255.255.255.255
```

この場合、認証ページはユーザに表示されません。その代わりに、FWSM は、要求したサービスを使用するには認証を受ける必要があることを示すエラーメッセージを Web ブラウザに送信します。

FWSM での直接認証

FWSM で HTTP（S）、Telnet、または FTP は許可しないが、他のトラフィック タイプの認証する場合、仮想 Telnet、仮想 SSH、仮想 HTTP を設定できます。仮想 Telnet、SSH、HTTP では、ユーザが Telnet、SSH、または HTTP を使用して FWSM に設定された所定の IP アドレスに接続すると、FWSM はプロンプトを表示します。詳細については、P.11-13 の「Virtual Access」を参照してください。

認証ルールの追加および編集

このダイアログボックスでは、認証ルールを追加または編集できます。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Authenticate** または **Do not Authenticate** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- **Add Server/User**：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認証するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Destination：認証するトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Protocol and Service：認証するトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp、udp、ip、icmp、またはその他のいずれかのトラフィックのプロトコルを選択します。

  tcp または **udp** を選択した場合、次のフィールドが表示されます。

  - Source Port：認証するトラフィックの送信元ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、... ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

- Destination Port：認証するトラフィックの宛先ポートを設定します。

  Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

  Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、... ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

icmp を選択した場合、次のフィールドが表示されます。

- ICMP Type：ICMP タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
- ICMP Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、... ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

other を選択した場合、次のフィールドが表示されます。

- Protocol：IP プロトコル タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
- Protocol Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、... ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクション（Authenticate または Do Not Authenticate など）を示しています。

Options：このルールのオプションを設定します。

- **Time Range**：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- **Description**：このルールの説明を入力します。

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
•	•	•	•	—

ネットワーク アクセス認可の設定

ユーザが所定の接続の認証を受けると、FWSM は認可を使用して、そのユーザのトラフィックをさらに制御できます。

ここでは、次の項目について説明します。

- TACACS+ 認可の設定（P.18-9）
- RADIUS 認可の設定（P.18-11）

TACACS+ 認可の設定

次のダイアログボックスでは、認証ルールを追加または編集できます。

TACACS+ でネットワーク アクセス認可を実行するように FWSM を設定できます。

認証ルールと認可ルールは互いに依存しませんが、認可ルールで一致した未認証トラフィックはすべて拒否されます。認可が成功するためには、ユーザは最初に FWSM で認証を受ける必要があります。所定の IP アドレスのユーザは、すべてのルールおよびタイプに対して一度だけ認証を受ければよいため、認証セッションが期限切れになっていなければ、トラフィックが認証文で一致した場合でも、認可が発生することがあります。

ユーザの認証が完了すると、FWSM は、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ルールに一致した場合、FWSM はユーザ名を TACACS+ サーバに送信します。TACACS+ サーバは FWSM に応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。FWSM は、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Authorize** または **Do not Authorize** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- **Add Server/User**：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認可するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Destination：認可するトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Protocol and Service：認可するトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp、udp、ip、icmp、またはその他のいずれかのトラフィックのプロトコルを選択します。

  tcp または **udp** を選択した場合、次のフィールドが表示されます。

  - Source Port：認可するトラフィックの送信元ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。
  - Destination Port：認可するトラフィックの宛先ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

  icmp を選択した場合、次のフィールドが表示されます。

  - ICMP Type：ICMP タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
  - ICMP Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

  other を選択した場合、次のフィールドが表示されます。

  - Protocol：IP プロトコル タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
  - Protocol Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクション（Authorize または Do Not Authorize など）を示しています。

Options：このルールのオプションを設定します。

- **Time Range**：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- **Description**：このルールの説明を入力します。

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
•	•	•	•	—

RADIUS 認可の設定

認証が成功すると、RADIUS プロトコルは RADIUS サーバによって送信される access-accept パケットでユーザ認可を返します。認証の設定の詳細については、P.18-5 の「ネットワーク アクセス認証の設定」を参照してください。

ネットワーク アクセスについてユーザを認証するように FWSM を設定すると、RADIUS 認可も暗黙的にイネーブルになっています。したがって、この項では、FWSM 上の RADIUS 認可の設定については取り上げません。ここでは、FWSM が RADIUS サーバから受信したアクセスリスト情報をどのように処理するかについて説明します。

アクセスリストを FWSM にダウンロードするように RADIUS サーバを設定できます。または、認証時にアクセスリスト名をダウンロードするようにも設定できます。ユーザは、ユーザ固有のアクセスリストで許可された操作だけを認可されます。

（注）　アクセス ルールを作成した場合、Per User Override オプションは、ユーザ固有のアクセスリストによる認可に対して次のような影響を与えますので注意してください。

- Per User Override オプションを使用しない場合、ユーザ セッションのトラフィックが、インターフェイス アクセスリストとユーザ固有のアクセスリストの両方によって許可される必要があります。
- Per User Override 機能を使用した場合、ユーザ固有のアクセスリストによって許可される内容が決まります。

詳細については、P.17-15 の「Advanced Access Rule Configuration」を参照してください。

ここでは、次の項目について説明します。

- ユーザごとの ACL をダウンロードするための RADIUS サーバの設定（P.18-12）
- ユーザごとの ACL 名をダウンロードするための RADIUS サーバの設定（P.18-14）

ユーザごとの ACL をダウンロードするための RADIUS サーバの設定

この項では、Cisco Secure ACS およびサードパーティ RADIUS サーバを設定する方法について説明します。次の項目を取り上げます。

- ダウンロード可能なアクセスリストに関する Cisco Secure ACS の設定（P.18-12）
- ダウンロード可能なアクセスリストに関する任意の RADIUS サーバの設定（P.18-13）

ダウンロード可能なアクセスリストに関する Cisco Secure ACS の設定

Cisco Secure ACS 上のダウンロード可能なアクセスリストを共有プロファイル コンポーネントとして設定し、そのアクセスリストをグループまたは個々のユーザに割り当てることができます。

アクセスリスト定義は、次のプレフィックスがない点を除いて拡張 **access-list** コマンドに類似する、1 つまたは複数の FWSM コマンドで構成されます。

access-list *acl_name* **extended**

Cisco Secure ACS バージョン 3.3 上のダウンロード可能なアクセスリスト定義の例を次に示します。

```
+-------------------------------------------+
| Shared profile Components                 |
|                                           |
|      Downloadable IP ACLs Content         |
|                                           |
| Name:    acs_ten_acl                      |
|                                           |
|      ACL Definitions                      |
|                                           |
| permit tcp any host 10.0.0.254            |
| permit udp any host 10.0.0.254            |
| permit icmp any host 10.0.0.254           |
| permit tcp any host 10.0.0.253            |
| permit udp any host 10.0.0.253            |
| permit icmp any host 10.0.0.253           |
| permit tcp any host 10.0.0.252            |
| permit udp any host 10.0.0.252            |
| permit icmp any host 10.0.0.252           |
| permit ip any any                         |
+-------------------------------------------+
```

ダウンロード可能なアクセスリストを作成する方法、およびそれらをユーザと関連付ける方法の詳細については、ご使用のバージョンの Cisco Secure ACS のマニュアルを参照してください。

FWSM 上では、ダウンロードされたアクセスリストの名前は次のようになります。

```
#ACSACL#-ip-acl_name-number
```

acl_name 引数は Cisco Secure ACS で定義された名前（上記の例では acs_ten_acl）、*number* は Cisco Secure ACS が生成した一意のバージョン ID です。

FWSM 上にダウンロードされたアクセスリストは、次の行で構成されます。

```
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit ip any any
```

ダウンロード可能なアクセスリストに関する任意の RADIUS サーバの設定

ユーザ固有のアクセスリストを Cisco IOS RADIUS cisco-av-pair VSA（VSA 番号 1）で FWSM に送信するように Cisco IOS RADIUS VSA をサポートする任意の RADIUS サーバを設定できます。Cisco IOS RADIUS VSA は、RADIUS ベンダー ID 9 で識別されます。

cisco-av-pair VSA で、**access-list extended** コマンドと類似する 1 つまたは複数の ACE を設定します。ただし、次のコマンド プレフィックスを置き換える必要があります。

access-list *acl_name* **extended**

次のテキストに置き換えます。

ip:inacl#nnn**=**

nnn 引数は、0 ～ 999999999 の番号で、FWSM 上に設定するコマンド文の順序を指定します。このパラメータを省略すると、順番は 0 となり、cisco-av-pair RADIUS VSA 内部の ACE の順序が使用されます。

RADIUS サーバ上の cisco-av-pair VSA に対して設定されている必要のあるアクセスリスト定義の例を次に示します。

```
ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#99=deny tcp any any
ip:inacl#2=permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#100=deny udp any any
ip:inacl#3=permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```

cisco-av-pair アトリビュートで送信されるアクセスリストをユーザごとに一意にする方法については、ご使用の RADIUS サーバのマニュアルを参照してください。

FWSM 上では、ダウンロードされたアクセスリストの名前は次の形式になります。

AAA-user-*username*

username 引数は、認証を受けるユーザの名前です。

FWSM 上にダウンロードされたアクセスリストは、次の行で構成されます。RADIUS サーバ上で指定された番号に基づいた順序になっています。

```
access-list  AAA-user-bcham34-79AD4A08 permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 deny tcp any any
access-list  AAA-user-bcham34-79AD4A08 deny udp any any
```

ダウンロードされたアクセスリストの「access-list」という単語と名前の間には、2 個のスペースがあります。これらのスペースにより、ダウンロードされたアクセスリストとローカルのアクセスリストが区別されます。この例では、「79AD4A08」は FWSM が作成したハッシュ値で、RADIUS サーバ上でアクセスリスト定義がいつ変更されたかを判別するために役立ちます。

ユーザごとの ACL 名をダウンロードするための RADIUS サーバの設定

ユーザ認証時に、FWSM で作成済みのアクセスリストの名前を RADIUS サーバからダウンロードするには、IETF RADIUS filter-id アトリビュート（アトリビュート番号 11）を次のように設定します。

filter-id=*acl_name*

（注）　Cisco Secure ACS では、filter-id アトリビュートの値は、HTML インターフェイスのボックスで、**filter-id=** を省略し、*acl_name* だけを入力して指定します。

filter-id アトリビュートの値をユーザごとに一意にする方法については、ご使用の RADIUS サーバのマニュアルを参照してください。

ネットワーク アクセスのアカウンティングの設定

ここでは、次の項目について説明します。

- アカウンティング ルールの追加および編集（P.18-15）

アカウンティング ルールの追加および編集

FWSM は、FWSM を通過する任意の TCP トラフィックまたは UDP トラフィックに関するアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。そのトラフィックが認証されていない場合、AAA サーバは IP アドレスでアカウンティング情報を保持できます。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。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Account** または **Do not Account** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- **Add Server/User**：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認証するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Destination：アカウンティングするトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

Interface IP を選択した場合、次のフィールドが表示されます。

- Interface：ドロップダウン リストからインターフェイスを選択します。

Protocol and Service：アカウンティングするトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp または udp の、いずれかのトラフィックのプロトコルを選択します。
  - Source Port：アカウンティングするトラフィックの送信元ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。
  - Destination Port：アカウンティングするトラフィックの宛先ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクション（Account または Do Not Account など）を示しています。

Options：このルールのオプションを設定します。

- **Time Range**：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- **Description**：このルールの説明を入力します。

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
•	•	•	•	—

MAC アドレスによるトラフィックの認証と認可の免除

ここでは、次の項目について説明します。

• MAC 免除ルールの追加および編集（P.18-17）

MAC 免除ルールの追加および編集

FWSM は、特定の MAC アドレスからのトラフィックの認証および認可を免除できます。

たとえば、FWSM が特定のネットワークから発信される TCP トラフィックを認証しても、特定のサーバからの未認証の TCP 接続を許可する場合に、MAC 免除ルールを使用すると、このルールが指定したサーバからのすべてのトラフィックに対して認証および認可が免除されます。

ベスト マッチ シナリオと異なり、パケットは照合する最初のエントリを使用するので、エントリの順番が重要になります。許可エントリがあり、そのエントリにより許可されたアドレスを拒否する場合は、許可エントリの前に拒否エントリを入力してください。

フィールド

- Action：**MAC Exempt** または **No MAC Exempt** を選択します。MAC Exempt オプションでは、認証または認可する必要なく MAC アドレスからのトラフィックを許可します。No MAC Exempt オプションでは、認証または認可を免除しない MAC アドレスを指定します。ffff.ffff.0000 などの MAC アドレス マスクを使用して MAC アドレスの範囲を許可する場合、拒否エントリを追加する必要があります。また、その範囲で認証および認可されるように MAC アドレスを強制します。
- MAC Address：12 桁の 16 進数の形式（nnnn.nnnn.nnnn）で送信元の MAC アドレスを指定します。
- MAC Mask：照合に使用される MAC アドレスの一部を指定します。たとえば、ffff.ffff.ffff は完全に MAC アドレスと一致します。ffff.ffff.0000 は最初の 8 桁だけ一致します。

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
•	•	•	•	—

Advanced AAA Configuration

セキュアな HTTP 機能および Proxy Limit 機能をイネーブルまたはディセーブルにします。このダイアログボックスは、Configuration > Features > Security Policy ペインで Advanced をクリックすると表示されます。

フィールド

- **Secure HTTP**：Secure HTTP（HTTPS）をイネーブルにするか、ディセーブルにするかを指定します。
  - **Enable Secure HTTP**：ブラウザなどの HTTP クライアントがセキュアな HTTP（HTTPS）を使用する場合、FWSM で認証が必要です。このオプションがイネーブルでなければ FWSM は HTTP を使用します。パスワードはクリア テキストになります。

（注） Enable Secure HTTP のチェックボックスをオンにしても、AAA ルールに HTTP 認証が設定されていない場合、このオプションは機能しません。

- **Proxy Limit**：Proxy Limit パラメータを指定します。
  - **Enable Proxy Limit**：ユーザごとに許可される同時プロキシ接続の数を制限します。最大接続数は 128 です。この機能をイネーブルにしない場合、制限なしになります。
  - **Proxy Limit**：許可されるプロキシ同時接続数を指定します。指定できる値は 1 ～ 128、デフォルトは 16 です。
- Authentication Challenge：FWSM でユーザにユーザ名とパスワードを求めて、認証確認を行うかどうかを設定できます。新しいセッションのトラフィックでは認証を行うという AAA ルールが設定され、トラフィックのプロトコルが FTP または、Telnet、HTTP、HTTPS の場合、FWSM でプロンプトがデフォルトでユーザに表示されます。場合によって、上記のプロトコルのどれかで認証確認を不要にすることもあり得ます。

  あるプロトコルの認証確認をディセーブルにした場合は、そのプロトコルのトラフィックが認証済みのセッションに属していない限り許可されません。この認証は、認証確認がイネーブル状態のプロトコルを使用したトラフィックで実行できます。たとえば、FTP の認証確認をディセーブルにすると、トラフィックが認証ルールの対象になっている場合 FTP で開始したセッションは FWSM で拒否されます。認証確認がイネーブルになっているプロトコル（HTTP など）でセッションを確立すると、FTP のトラフィックは許可されます。
  - FTP：チェックボックスをオフにすると、FTP の認証確認がディセーブルになります。
  - HTTP：チェックボックスをオフにすると、HTTP の認証確認がディセーブルになります。
  - HTTPS：チェックボックスをオフにすると、HTTPS の認証確認がディセーブルになります。
  - Telnet：チェックボックスをオフにすると、Telnet の認証確認がディセーブルになります。
- Expired Connections：ユーザ認証でタイムアウトになったとき、または **clear uauth** コマンドを使用して認証セッションをクリアした場合、どのような IP アドレスであってもアクティブな接続をすぐに強制終了するには、このテーブルに IP アドレスを追加します。この機能を使用しない場合、ユーザの認証セッションが失効してもアクティブ接続は終了しません。接続の終了理由がこのオプションによる場合は、システム ログ メッセージ 109036 が表示されます。
  - Interface：ソース IP アドレスに接続するインターフェイス名です。
  - IP Address：ソース IP アドレスです。
  - Mask：サブネット マスクです。
  - Add：接続終了対象になる IP アドレスを追加します。
  - Edit：IP アドレスを編集します。
  - Delete：IP アドレスを削除します。

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
•	•	•	•	—

クリア接続の追加および編集

ユーザ認証でタイムアウトになったとき、または **clear uauth** コマンドを使用して認証セッションをクリアした場合、どのような IP アドレスであってもアクティブな接続をすぐに強制終了するには、このテーブルに IP アドレスを追加します。この機能を使用しない場合、ユーザの認証セッションが失効してもアクティブ接続は終了しません。接続の終了理由がこのオプションによる場合は、システム ログ メッセージ 109036 が表示されます。

フィールド

- Interface Name：ソース IP アドレスに接続するインターフェイス名を設定します。
- IP Address：ソース IP アドレスを設定します。
- Mask：サブネット マスクを設定します。

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
•	•	•	•	—