



# ネットワーク アクセスに対する AAA 規則の設定

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」と発音）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、一般的な操作のコンフィギュレーション ガイドの“[Configuring AAA for System Administrators](#)” section on page 43-21 を参照してください。

この章は、次の項で構成されています。

- 「AAA のパフォーマンス」 (P.7-1)
- 「AAA ルールのライセンス要件」 (P.7-1)
- 「ガイドラインと制限事項」 (P.7-2)
- 「ネットワーク アクセス認証の設定」 (P.7-2)
- 「ネットワーク アクセス許可の設定」 (P.7-12)
- 「ネットワーク アクセスのアカウントिंगの設定」 (P.7-18)
- 「MAC アドレスによるトラフィックの認証と許可の免除」 (P.7-19)
- 「AAA ルールの機能履歴」 (P.7-21)

## AAA のパフォーマンス

ASA は「カットスルー プロキシ」を使用します。これにより、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。ASA カットスルー プロキシは、アプリケーション層で最初にユーザ確認を行い、続いて標準 AAA サーバまたはローカル データベースで認証します。ASA 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 ルールのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

## ガイドラインと制限事項

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

クラスタリングでは、この機能は、マスター ユニットでのみサポートされます。

## ネットワーク アクセス認証の設定

この項は、次の内容で構成されています。

- 「認証について」 (P.7-2)
- 「ネットワーク アクセス認証の設定」 (P.7-6)
- 「HTTP 認証および HTTPS 認証におけるリダイレクション方式のイネーブル化」 (P.7-7)
- 「Web クライアントのセキュアな認証のイネーブル化」 (P.7-8)
- 「での直接認証 ASA」 (P.7-9)
- 「認証プロキシに対する制限の設定」 (P.7-11)

## 認証について

ASA では、AAA サーバを使用するネットワーク アクセス認証を設定できます。この項は、次の内容で構成されています。

- 「一度だけの認証」 (P.7-3)
- 「認証確認を受けるために必要なアプリケーション」 (P.7-3)
- 「ASA の認証プロンプト」 (P.7-3)
- 「AAA プロンプトとアイデンティティ ファイアウォール」 (P.7-4)
- 「バックアップ認証方式としての AAA ルール」 (P.7-5)

- 「スタティック PAT および HTTP」 (P.7-6)

## 一度だけの認証

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、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインを参照してください)。たとえば、Telnet および FTP の認証を行うように ASA が設定されている場合、最初に Telnet 認証を受けたユーザは、その認証セッションが継続している限り、FTP 認証を受ける必要はありません。

## 認証確認を受けるために必要なアプリケーション

プロトコルまたはサービスへのネットワーク アクセス認証を要求するように ASA を設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。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、ASA は認証が必要な他のトラフィックを許可しません。

次のように、ASA が AAA 用にサポートしている認証ポートは固定値です。

- ポート 21 は FTP 用
- ポート 23 は Telnet 用
- ポート 80 は HTTP 用
- ポート 443 は HTTPS 用

## ASA の認証プロンプト

Telnet および FTP の場合、ASA は認証プロンプトを生成します。

HTTP の場合、ASA はデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。必要に応じて、ユーザ名とパスワードを入力するための内部 Web ページにユーザがリダイレクトされるように ASA を設定することができます (設定は、[Configuration] > [Firewall] > [AAA Rules] > [Advanced] > [AAA Rules Advanced Options] ダイアログボックスで行います。「[HTTP 認証および HTTPS 認証におけるリダイレクション方式のイネーブル化](#)」 (P.7-7) を参照してください)。

HTTPS の場合、ASA はカスタム ログイン画面を生成します。必要に応じて、ユーザ名とパスワードを入力するための内部 Web ページにユーザがリダイレクトされるように ASA を設定することもできます (設定は、[Configuration] > [Firewall] > [AAA Rules] > [Advanced] > [AAA Rules Advanced Options] ダイアログボックスで行います。「[HTTP 認証および HTTPS 認証におけるリダイレクション方式のイネーブル化](#)」 (P.7-7) を参照してください)。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザエクスペリエンスが提供されると同時に、Easy VPN でもファイアウォールモードでも、HTTP および HTTPS と同じユーザエクスペリエンスが提供されるためです。また、ASA での直接認証もサポートしています。

次の理由で、基本 HTTP 認証を引き続き使用しなければならない場合があります。

- ASA でリスニングポートを開きたくない。
- ルータ上で NAT を使用しており、ASA によって提供される Web ページのトランスレーショナルールを作成したくない。
- 基本 HTTP 認証の方がネットワークで有効に機能する見込みがある。

たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

正常に認証されると、ASA 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。基本 HTTP 認証を使用する際、宛先サーバで別のユーザ名およびパスワードの入力を必要とする場合は、仮想 HTTP を設定する必要があります ([Configuration] > [Firewall] > [Advanced Options] > [Virtual Access] ペインを参照)。



(注)

HTTP 認証を使用する場合、デフォルトでクリア テキストのユーザ名とパスワードがクライアントから ASA に送信されます。さらにこのユーザ名とパスワードは宛先 Web サーバにも送信されます。クレデンシャルの保護の詳細については、「Web クライアントのセキュアな認証のイネーブル化」(P.7-8) を参照してください。

FTP の場合、ASA 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、ASA 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> name1@name2
password> password1@password2
```

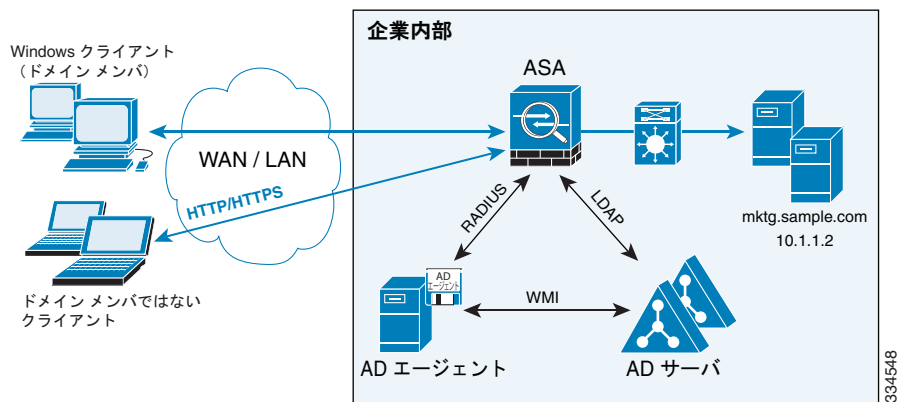
この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク (@) で区切ることができます。

## AAA プロンプトとアイデンティティ ファイアウォール

企業では、ユーザによっては、Web ポータル (カットスルー プロキシ) を使用した認証など、通常とは異なる認証メカニズムを使用してネットワークにログインする場合があります。たとえば、クライアントとして Mac や Linux を使用しているユーザは、Web ポータル (カットスルー プロキシ) にログインすることがあります。そのため、これらの認証方式がアイデンティティに基づくアクセス ポリシーと連携できるようにアイデンティティ ファイアウォールを設定する必要があります。

図 7-1 は、カットスルー プロキシ認証キャプティブ ポータルをサポートする展開方法を示しています。Active Directory サーバと AD エージェントはメイン サイトの LAN 上に配置されています。ただし、アイデンティティ ファイアウォールは、Active Directory ドメインに含まれないクライアントの認証をサポートするよう設定されています。

図 7-1 カットスルー プロキシ認証をサポートする展開



ASA は、Web ポータル (カットスルー プロキシ) 経由でログインするユーザを認証が行われる Active Directory ドメインに属するユーザと見なします。

ASA は、Web ポータル (カットスルー プロキシ) によってログインしたユーザを AD エージェントに報告し、AD エージェントがユーザ情報を登録されているすべての ASA デバイスに配布します。この場合は、アイデンティティ ファイアウォールは、Active Directory ドメインとユーザを関連付けることができます。具体的には、認証されたユーザのユーザ アイデンティティと IP アドレスのマッピングが、パケットを受信して認証する入力インターフェイスを含むすべての ASA コンテキストに転送されます。

ユーザは、HTTP/HTTPS、FTP、Telnet、または SSH を使用してログインできます。ユーザがこれらの認証方式でログインする場合は、次のガイドラインが適用されます。

- HTTP/HTTPS トラフィックの場合、認証されていないユーザには認証ウィンドウが表示されます。
- Telnet および FTP トラフィックの場合、ユーザはカットスルー プロキシ サーバ経由でログインし、さらに Telnet および FTP サーバにログインする必要があります。
- ユーザは、ログイン クレデンシャル (形式は domain\username) を入力するときに、Active Directory ドメインを指定できます。ASA は、指定されたドメインに関連付けられた AAA サーバグループを自動的に選択します。
- ユーザがログイン クレデンシャル (形式は domain\username) を入力するときに Active Directory ドメインを指定すると、ASA はドメインを解析し、それを使用して、アイデンティティ ファイアウォール用に設定された AAA サーバから認証サーバを選択します。AAA サーバには username だけが渡されます。
- ログイン クレデンシャルにバックスラッシュ (\) デリミタが含まれていない場合、ASA はドメインを解析せず、アイデンティティ ファイアウォールに設定されたデフォルト ドメインに対応する AAA サーバで認証が実行されます。
- デフォルト ドメインが設定されていない場合、またはそのデフォルト ドメインにサーバグループが設定されていない場合、ASA は認証を拒否します。
- ドメインが指定されない場合、ASA はアイデンティティ ファイアウォールに設定されたデフォルト ドメインの AAA サーバグループを選択します。

## バックアップ認証方式としての AAA ルール

認証ルール (「カットスルー プロキシ」とも呼ばれます) は、ユーザに基づいてネットワーク アクセスを制御します。この機能がアクセス ルールとアイデンティティ ファイアウォールに非常に似ているため、AAA ルールは、ユーザの AD ログインの期限が切れるか、有効なユーザが AD にまだログインしていない場合、認証のバックアップ方式として使用できます。たとえば、有効なログインのないユーザの場合、AAA ルールをトリガーできます。AAA ルールが有効なログインがないユーザに対してだけトリガーされるようにするには、拡張 ACL でアクセス ルールと AAA ルールに使用される特別なユーザ名 **None** (有効なログインのないユーザ) および **Any** (有効なログインを持つユーザ) を指定します。アクセス ルールでは、ユーザおよびグループのポリシーを通常どおりに設定しますが、**any any** を拒否する前にすべての **None** ユーザを許可するルールを含めます。これらのユーザが後で AAA ルールをトリガーできるように、これらのユーザを許可する必要があります。次に、**Any** ユーザ (これらのユーザは、AAA ルールの対象ではなく、アクセス ルールによってすでに処理されています) を照合せず、すべての **None** ユーザのみを照合する AAA ルールを設定して、**None** ユーザに対する AAA 認証をトリガーします。ユーザがカットスルー プロキシによって正常にログインした後、トラフィックは再び正常に流れます。

## スタティック PAT および HTTP

HTTP 認証では、スタティック PAT が設定されている場合、ASA は実際のポートをチェックします。ASA 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 が次のようにポート 80 に変換されていて、関係するすべての ACL でこのトラフィックが許可されているとします。

```
object network obj-192.168.123.10-01
  host 192.168.123.10
  nat (inside,outside) static 10.48.66.155 service tcp 80 889
```

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、ASA はそのトラフィックを代行受信して、HTTP 認証を実行します。ASA 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、ローカルポートがポート 80 ではないとします。

```
object network obj-192.168.123.10-02
  host 192.168.123.10
  nat (inside,outside) static 10.48.66.155 service tcp 111 889
```

この場合、ユーザには認証ページは表示されません。代わりに、ASA は Web ブラウザにエラーメッセージを送信して、要求されたサービスを使用する前にユーザが認証を受ける必要があることを通知します。

## ネットワーク アクセス認証の設定

ネットワーク アクセス認証を設定するには、次の手順を実行します。

**ステップ 1** [Configuration] > [Firewall] > [AAA Rules] ペインから、[Add] > [Add Authentication Rule] を選択します。

[Add Authentication Rule] ダイアログボックスが表示されます。

**ステップ 2** [Interface] ドロップダウン リストから、ルールを適用するためのインターフェイスを選択します。



### ヒント

[Action] フィールドで、実装内容に応じて、次のいずれかをクリックします。

- **Authenticate**
- **Do not Authenticate**

**ステップ 3** [AAA Server Group] ドロップダウン リストから、サーバグループを選択します。AAA サーバをサーバグループに追加する場合は、[Add Server] をクリックします。

AAA サーバグループとして [LOCAL] を選択した場合は、[Add User] をクリックして新しいユーザを追加することも可能です。詳細については、一般的な操作のコンフィギュレーションガイドの [“Adding a User Account to the Local Database” section on page 31-4](#) を参照してください。

**ステップ 4** [Source] フィールドで、送信元 IP アドレスを入力するか、省略符号 ([...]) ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

**ステップ 5** [Destination] フィールドで、宛先 IP アドレスを入力するか、省略符号 ([...]) ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

- ステップ 6** [Service] フィールドで、宛先サービスの IP サービス名または IP サービス番号を入力するか、省略符号 ([...]) をクリックしてサービスを選択します。
- ステップ 7** (任意) [Description] フィールドに説明を入力します。
- ステップ 8** (任意) [More Options] をクリックすると、必要に応じて次のような処理を実行できます。
- TCP または UDP 用の送信元サービスを指定する場合は、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。
  - 宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。
  - ルールを非アクティブにするには、[Enable Rule] チェックボックスをオフにします。  
これにより、ルールを削除しないまま無効にできます。
  - ルールの適用期間を設定する場合は、[Time Range] ドロップダウン リストから、既存の時間範囲を選択します。時間範囲を新規に追加する場合は、省略符号 ([...]) ボタンをクリックします。詳細については、一般的な操作のコンフィギュレーション ガイドの [“Configuring Time Ranges” section on page 15-26](#) を参照してください。
- ステップ 9** [OK] をクリックします。  
[Add Authentication Rule] ダイアログボックスが閉じ、ルールが [AAA Rules] テーブルに表示されます。
- ステップ 10** [Apply] をクリックします。  
変更内容が実行コンフィギュレーションに保存されます。

---

認証の詳細については、「[認証について](#)」(P.7-2) を参照してください。

## HTTP 認証および HTTPS 認証におけるリダイレクション方式のイネーブル化

認証にリダイレクション方式を使用すると、HTTP リスニング ポートまたは HTTPS リスニング ポートで、ネットワーク ユーザを認証できます。リスニング ポートをイネーブルにすると、ASA により直接接続に関する認証ページが表示され、さらにリダイレクションをイネーブルにすると、スルー トラフィックに関する認証ページが表示されます。この方式では、認証クレデンシヤルが続けて宛先サーバに送信されないようにします。リダイレクション方式と基本方式を比較した詳細については、「[ASA の認証プロンプト](#)」(P.7-3) を参照してください。

AAA リスナーをイネーブルにするには、次の手順を実行します。

- 
- ステップ 1** [Configuration] > [Firewall] > [AAA Rules] ペインから、[Advanced] をクリックします。  
[AAA Rules Advanced Options] ダイアログボックスが表示されます。
- ステップ 2** [Interactive Authentication] で、[Add] をクリックします。  
[Add Interactive Authentication Entry] ダイアログボックスが表示されます。
- ステップ 3** [Protocol] で、[HTTP] または [HTTPS] を選択します。HTTP と HTTPS の両方に対してリダイレクションをイネーブルにすることもできます。その場合は、上記の操作を繰り返し行い、それぞれに対して個別にルールを作成します。
- ステップ 4** [Interface] ドロップダウン リストから、リスナーをイネーブルにするインターフェイスを選択します。
- ステップ 5** [Port] ドロップダウン リストで、ポートを選択するか、またはポート番号を入力します。

これは、ASA が直接トラフィックまたはリダイレクトされたトラフィックをリッスンするポートです。デフォルトは 80 (HTTP) および 443 (HTTPS) です。任意のポート番号を使用して同じ機能を保持できますが、直接認証ユーザがそのポート番号を認識している必要があります。これは、リダイレクトされたトラフィックは正しいポート番号に自動的に送信されますが、直接認証するユーザは、ポート番号を手動で指定する必要があるためです。

**ステップ 6** (任意) [Redirect network users for authentication request] チェックボックスをオンにします。

このオプションを使用すると、ASA により表示される認証 Web ページにスルー トラフィックがリダイレクトされます。このオプションを使用しない場合は、ASA のインターフェイスに転送されるトラフィックに限り、認証 Web ページにアクセスできます。



**(注)** また、リダイレクト オプションをイネーブルにすると、インターフェイス IP アドレスを変換するインターフェイスおよびリスナーとして使用されるポートに対し、スタティック PAT は設定できません。スタティック PAT を設定した場合、NAT は正常に実行されますが、認証は失敗します。

**ステップ 7** [OK] をクリックし、もう一度 [OK] をクリックして、[AAA Rules Advanced Options] ダイアログボックスを閉じます。

**ステップ 8** [Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。

## Web クライアントのセキュアな認証のイネーブル化

HTTP 認証を使用する場合、デフォルトでユーザ名とパスワードがクリア テキストでクライアントから ASA に送信されます。さらにこのユーザ名とパスワードは宛先 Web サーバにも送信されます。

ASA では、HTTP 認証の保護のために次のような方式を用意しています。

- HTTP に対してリダイレクション方式の認証をイネーブルにする：「[HTTP 認証および HTTPS 認証におけるリダイレクション方式のイネーブル化](#)」(P.7-7) を参照してください。この方式では、認証クレデンシャルがその後続けて宛先サーバに送信されないようにします。リダイレクション方式と基本方式を比較した詳細については、「[ASA の認証プロンプト](#)」(P.7-3) を参照してください。
- 仮想 HTTP をイネーブルにする：仮想 HTTP では、ASA での認証と HTTP サーバでの認証を個別に行うことができます。HTTP サーバが 2 次認証を必要としない場合でも、このコマンドにより基本認証クレデンシャルは HTTP GET 要求から除去されます。詳細については、「[仮想サーバによる HTTP 接続および HTTPS 接続の認証](#)」(P.7-9) を参照してください。
- Web クライアントと ASA の間の HTTPS によるユーザ名とパスワードの交換をイネーブルにする：Web クライアントと ASA との間の HTTPS によるユーザ名とパスワードの交換をイネーブルにするには、次の手順を実行します。
  - a. [Configuration] > [Firewall] > [AAA Rules] ペインから、[Advanced] をクリックします。[AAA Rules Advanced Options] ダイアログボックスが表示されます。
  - b. [Secure HTTP] で、[Enable Secure HTTP] をクリックします。
  - c. [OK] をクリックし、もう一度 [OK] をクリックして、[AAA Rules Advanced Options] ダイアログボックスを閉じます。
  - d. [Apply] をクリックします。



これは ASA と宛先サーバの間だけでなく、クライアントと ASA の間のクレデンシャルを保護する唯一の方式です。この方式だけを使用することも、または他の方式のいずれかと組み合わせてセキュリティを最大限にすることもできます。

この機能をイネーブルにすると、ユーザが HTTP の使用時に認証を必要とする場合は、ASA が HTTP ユーザを HTTPS プロンプトにリダイレクトします。正常に認証されると、ユーザは ASA により元の HTTP URL にリダイレクトされます。

セキュアな Web クライアント認証では、次の制限事項があります。

- 同時に行うことができる HTTPS 認証セッションは、最大 16 個です。16 個の HTTPS 認証プロセスがすべて実行されている場合、認証を必要とする新しい接続は失敗します。
- ユーザ認証のタイムアウト時間が無制限に設定されていると、HTTPS 認証は実行されない場合があります。HTTPS 認証を受けた後、ブラウザが複数の TCP 接続を開始して Web ページのロードを試みると、最初の接続はそのまま許可されますが、後続の接続に対しては認証が発生します。その結果、ユーザが認証ページに正しいユーザ名とパスワードを毎回入力しても、繰り返し認証ページが表示されます。このような動作を回避するには、ユーザ認証のタイムアウト時間を 1 秒に設定します ([Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインを参照)。ただし、この回避策では、同じ送信元 IP アドレスからアクセスした認証されていないユーザがファイアウォールを通過できる期間が 1 秒間発生します。

HTTPS 認証は SSL ポート 443 上で実行されるため、HTTP クライアントから HTTP サーバへのトラフィックをポート 443 でブロックするというアクセスルールは設定しないようにしてください。また、ポート 80 上の Web トラフィックに対してスタティック PAT を設定する場合は、SSL ポートに対してもスタティック PAT を設定する必要があります。

## での直接認証 ASA

HTTP、HTTPS、Telnet、または FTP が ASA を通過することを許可せずに、他のタイプのトラフィックを認証する場合は、HTTP、HTTPS、または Telnet を使用して ASA の認証を直接受けることができます。

この項は、次の内容で構成されています。

- 「[仮想サーバによる HTTP 接続および HTTPS 接続の認証](#)」 (P.7-9)
- 「[仮想サーバによる Telnet 接続の認証](#)」 (P.7-11)

## 仮想サーバによる HTTP 接続および HTTPS 接続の認証

「[ネットワーク アクセス認証の設定](#)」 (P.7-6) に示す HTTP および HTTPS 認証のリダイレクト方式をイネーブルにした場合は、直接認証も自動的にイネーブルになります。

ASA で HTTP 認証を使用する場合（「[ネットワーク アクセス認証の設定](#)」 (P.7-6) を参照）、ASA では、基本 HTTP 認証がデフォルトで使用されます。

この認証方式は、ASA によって、ASA 自身が生成した Web ページに HTTP 接続がリダイレクトされるように変更できます（手順については、「[HTTP 認証および HTTPS 認証におけるリダイレクション方式のイネーブル化](#)」 (P.7-7) を参照してください）。

ただし、基本 HTTP 認証を引き続き使用する場合、HTTP 認証をカスケードするには仮想 HTTP サーバが必要になることがあります。

ASA のみでなく宛先 HTTP サーバでも認証が必要な場合は、仮想 HTTP を使用すると、ASA (AAA サーバ経由) での認証と HTTP サーバでの認証を個別に行うことができます。仮想 HTTP を使用しない場合は、ASA での認証に使用したものと同一ユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。AAA サーバと HTTP サーバでユーザ名とパスワードが異なる場合、HTTP 認証は失敗します。

この機能を使用すると、AAA 認証を必要とする HTTP 接続がすべて、ASA 上の仮想 HTTP サーバにリダイレクトされます。ASA により、AAA サーバのユーザ名とパスワードの入力を求めるプロンプトが表示されます。AAA サーバがユーザを認証すると、ASA は HTTP 接続を元のサーバにリダイレクトして戻しますが、AAA サーバのユーザ名とパスワードは含めません。HTTP パケットにユーザ名とパスワードが含まれていないため、HTTP サーバによりユーザに HTTP サーバのユーザ名とパスワードの入力を求めるプロンプトが別途表示されます。

着信ユーザ (セキュリティの低い方から高い方へ向かう) については、送信元インターフェイスに適用されるアクセス ルールに、宛先インターフェイスとして仮想 HTTP アドレスを追加する必要もあります。さらに、NAT が必要ない場合であっても、仮想 HTTP IP アドレスに対するスタティック NAT ルールを追加する必要があります。通常は、アイデンティティ NAT ルールが使用されます (アドレスをそれ自身に変換)。

発信ユーザについては、トラフィックに明示的な許可がありますが、内部インターフェイスにアクセス ルールを適用する場合は、必ず仮想 HTTP アドレスへのアクセスを許可する必要があります。スタティック NAT ルールは必要ありません。



(注)

仮想 HTTP を使用する場合、ユーザ認証のタイムアウト時間を 0 秒に設定することは避けてください。このような設定を行うと、実際の Web サーバに HTTP 接続できなくなります。「[グローバル タイムアウトの設定](#)」(P.21-9) を参照してください。

インターフェイスの AAA をイネーブルにすると、次の URL で ASA の直接認証を受けることができます。

```
http://interface_ip[:port]/netaccess/connstatus.html
https://interface_ip[:port]/netaccess/connstatus.html
```

HTTP サーバとは別に ASA の仮想サーバでユーザを認証できるようにするには、次の手順を実行します。

- 
- ステップ 1** [Configuration] > [Firewall] > [Advanced] > [Virtual Access] > [Virtual HTTP Server] 領域で、[Enable] チェックボックスをオンにします。
- ステップ 2** [Virtual HTTP Server] フィールドで、仮想 HTTP サーバの IP アドレスを追加します。  
このアドレスは必ず、ASA にルーティングされる未使用のアドレスにしてください。たとえば、外部サーバにアクセスするとき内部アドレス用の NAT を実行し、仮想 HTTP サーバへの外部アクセスを可能にする場合は、仮想 HTTP サーバのアドレスとして、グローバル NAT アドレスをいずれか 1 つ使用できます。
- ステップ 3** (任意) リダイレクションが自動的には行われないテキストベースのブラウザを使用している場合は、[Display redirection warning] チェックボックスをオンにします。これにより、HTTP 接続がリダイレクトされる際に、ユーザにそのことを通知するためのアラートがイネーブルになります。
- ステップ 4** [Apply] をクリックします。  
仮想サーバが追加され、変更内容が実行コンフィギュレーションに保存されます。
-

## 仮想サーバによる Telnet 接続の認証

任意のプロトコルまたはサービスを対象としたネットワーク アクセス認証を設定することが可能ですが、「ネットワーク アクセス認証の設定」(P.7-6)を参照)、HTTP、Telnet、または FTP のみを使用して直接認証を行うこともできます。ユーザがまずこれらのサービスのいずれかで認証を受けておかないと、他のサービスは通過を許可されません。HTTP、Telnet、または FTP トラフィックの ASA の通過を許可せず、その他のタイプのトラフィックを認証する場合は、ASA 上で設定された所定の IP アドレスにユーザが Telnet で接続し、ASA によって Telnet プロンプトが表示されるように、仮想 Telnet を設定できます。

認証が済んでいないユーザが仮想 Telnet IP アドレスに接続すると、ユーザはユーザ名とパスワードを求められ、その後 AAA サーバにより認証されます。ユーザが認証されると、「Authentication Successful」というメッセージが表示されます。これで、ユーザは認証が必要な他のサービスにアクセスできます。

着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス ルールに、宛先インターフェイスとして仮想 Telnet アドレスを追加する必要もあります。さらに、NAT が不要な場合でも、仮想 Telnet IP アドレスに対するスタティック NAT ルールを追加する必要があります。通常は、アイデンティティ NAT ルールが使用されます（アドレスをそれ自身に変換）。

発信ユーザについては、トラフィックに明示的な許可がありますが、内部インターフェイスにアクセスルールを適用する場合は、必ず仮想 Telnet アドレスへのアクセスを許可する必要があります。スタティック NAT ルールは必要ありません。

ASA からログアウトするには、仮想 Telnet IP アドレスに再接続します。ログアウトするように求められます。

Telnet を使用した直接認証をイネーブルにするには、次の手順を実行します。

- 
- ステップ 1** [Configuration] > [Firewall] > [Advanced] > [Virtual Access] > [Virtual Telnet Server] 領域で、[Enable] チェックボックスをオンにします。
- ステップ 2** [Virtual Telnet Server] フィールドで、仮想 Telnet サーバの IP アドレスを入力します。
- このアドレスは必ず、ASA にルーティングされる未使用のアドレスにしてください。たとえば、外部サーバにアクセスするときに内部アドレス用の NAT を実行し、仮想 HTTP サーバへの外部アクセスを可能にする場合は、仮想 HTTP サーバのアドレスとして、グローバル NAT アドレスをいずれか 1 つ使用できます。
- ステップ 3** [Apply] をクリックします。
- 仮想サーバが追加され、変更内容が実行コンフィギュレーションに保存されます。
- 

## 認証プロキシに対する制限の設定

ユーザごとの最大同時プロキシ接続数を設定することにより、ユーザ認証のセッション制限を手動で設定できます。

プロキシに対する制限を設定するには、次の手順を実行します。

- 
- ステップ 1** [Configuration] > [Firewall] > [AAA Rules] を選択し、[Advanced] をクリックします。
- [AAA Rules Advanced Options] ダイアログボックスが表示されます。

- ステップ 2** [Proxy Limit] 領域で、[Enable Proxy Limit] チェックボックスをオンにします。
- ステップ 3** [Proxy Limit] フィールドに、ユーザごとの同時プロキシ接続数として、1 から 128 の間の数を入力します。
- ステップ 4** [OK] をクリックして、[Apply] をクリックします。  
変更内容が実行コンフィギュレーションに保存されます。
- 

## ネットワーク アクセス許可の設定

ユーザが所定の接続のための認証を受けると、ASA は許可を使用して、ユーザからのトラフィックをさらに制御できます。

この項は、次の内容で構成されています。

- 「TACACS+ 許可の設定」(P.7-12)
- 「RADIUS 許可の設定」(P.7-13)

## TACACS+ 許可の設定

TACACS+ でネットワーク アクセス許可を実行するように、ASA を設定できます。認証ステートメントと許可ステートメントは互いに独立しています。ただし、認証されていないトラフィックは、許可ルールに一致した場合でも拒否されます。許可は次のように実行されます。

1. ユーザは最初に ASA 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ルールで一致した場合でも、許可が発生することがあります。
2. ユーザの認証が完了すると、ASA は、一致するトラフィックの許可ルールをチェックします。
3. トラフィックが許可ルールに一致した場合は、ASA によりユーザ名が TACACS+ サーバに送信されます。
4. TACACS+ サーバは ASA 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。
5. ASA は、その応答内の許可ルールを実施します。

ユーザに対するネットワーク アクセス許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。

TACACS+ 許可を設定するには、次の手順を実行します。

---

- ステップ 1** 認証をイネーブルにします。詳細については、「[ネットワーク アクセス認証の設定](#)」(P.7-6) を参照してください。すでに認証をイネーブルにしてある場合は、次の手順に進みます。
- ステップ 2** [Configuration] > [Firewall] > [AAA Rules] ペインから、Add] > [Add Authorization Rule] を選択します。  
[Add Authorization Rule] ダイアログボックスが表示されます。
- ステップ 3** [Interface] ドロップダウン リストから、ルールを適用するためのインターフェイスを選択します。
- ステップ 4** [Action] フィールドで、実装内容に応じて、次のいずれかをクリックします。

- **Authorize**
- **Do not Authorize**

- ステップ 5** [AAA Server Group] ドロップダウン リストから、サーバ グループを選択します。AAA サーバをサーバ グループに追加する場合は、[Add Server] をクリックします。
- サポートされているのは TACACS+ サーバだけです。
- ステップ 6** [Source] フィールドで、送信元 IP アドレスを入力するか、省略符号 ([...]) ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。
- ステップ 7** [Destination] フィールドで、宛先 IP アドレスを入力するか、省略符号 ([...]) ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。
- ステップ 8** [Service] フィールドで、宛先サービスの IP サービス名または IP サービス番号を入力するか、省略符号 ([...]) をクリックしてサービスを選択します。
- ステップ 9** (任意) [Description] フィールドに説明を入力します。
- ステップ 10** (任意) [More Options] をクリックすると、必要に応じて次のような処理を実行できます。
- TCP または UDP 用の送信元サービスを指定する場合は、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。
  - 宛先サービスと送信元サービスは同じである必要があります。[Source Service] フィールドに [Destination Service] フィールドの内容をコピー アンド ペーストします。
  - ルールを非アクティブにするには、[Enable Rule] チェックボックスをオフにします。
- これにより、ルールを削除しないまま無効にできます。
- ルールの適用期間を設定する場合は、[Time Range] ドロップダウン リストから、既存の時間範囲を選択します。時間範囲を新規に追加する場合は、省略符号 ([...]) ボタンをクリックします。詳細については、一般的な操作のコンフィギュレーション ガイドの [“Configuring Time Ranges” section on page 15-26](#) を参照してください。
- ステップ 11** [OK] をクリックします。
- [Add Authorization Rule] ダイアログボックスが閉じ、ルールが [AAA Rules] テーブルに表示されます。
- ステップ 12** [Apply] をクリックします。
- 変更内容が実行コンフィギュレーションに保存されます。

## RADIUS 許可の設定

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` メッセージでユーザ許可を返します。認証の設定の詳細については、「[ネットワーク アクセス認証の設定 \(P.7-6\)](#)」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 ASA を設定すると、RADIUS 許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、ASA 上の RADIUS 許可の設定については取り上げません。ここでは、ASA が RADIUS サーバから受信した ACL 情報をどのように処理するかについて説明します。

ACL を ASA 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 ACL 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 ACL で許可された操作だけを許可されます。



(注)

[Per User Override Setting] をイネーブルにした場合 ([Configuration] > [Firewall] > [Access Rules] > [Advanced] > [Access Rules Advanced Options] ダイアログボックスを参照)、ユーザ固有のアクセスリストによる許可について、per-user-override 機能の次の効果に注意が必要です。

- per-user-override 機能を使用しない場合、ユーザセッションのトラフィックは、インターフェイス ACL とユーザ固有の ACL 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 ACL によって許可される内容が決定されます。

この項は、次の内容で構成されています。

- 「ダウンロード可能なアクセス コントロール リスト (ACL) を送信するための RADIUS サーバの設定」(P.7-14)
- 「ユーザごとのアクセス コントロール リスト名をダウンロードするための RADIUS サーバの設定」(P.7-18)

## ダウンロード可能なアクセス コントロール リスト (ACL) を送信するための RADIUS サーバの設定

この項では、Cisco Secure Access Control Server (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 ACL の機能と Cisco Secure ACS について」(P.7-14)
- 「ダウンロード可能な ACL に関する Cisco Secure ACS の設定」(P.7-16)
- 「ダウンロード可能な ACL に関する任意の RADIUS サーバの設定」(P.7-17)
- 「ダウンロード可能な ACL 内のワイルドカード ネットマスク表現の変換」(P.7-17)

### ダウンロード可能な ACL の機能と Cisco Secure ACS について

ダウンロード可能な ACL は、Cisco Secure ACS を使用して各サーバに適切な ACL を提供する場合に最もスケーラブルな方法です。次の機能があります。

- 無制限 ACL のサイズ: ダウンロード可能な ACL は、完全な ACL を Cisco Secure ACS から ASA に転送するために必要な数の RADIUS パケットを使用して送信されます。
- ACL 管理の簡素化および集中化: ダウンロード可能な ACL により、一度記述した ACL セットを多数のユーザ プロファイルまたはグループ プロファイルに適用することや、多数の ASA に配布することができます。

この方法は、複数の Cisco Secure ACS ユーザまたはグループに適用する非常に大きい ACL セットがある場合に最適ですが、Cisco Secure ACS ユーザおよびグループの管理を簡素化できることから、ACL のサイズを問わず有用です。

ASA は、ダウンロード可能な ACL を Cisco Secure ACS から次のプロセスで受信します。

1. ASA がユーザセッションのための RADIUS 認証要求パケットを送信します。
2. Cisco Secure ACS がそのユーザを正常に認証した場合、Cisco Secure ACS は、該当するダウンロード可能な ACL の内部名が含まれた RADIUS access-accept メッセージを返します。Cisco IOS cisco-av-pair RADIUS VSA (ベンダー 9、属性 1) には、ダウンロード可能な ACL セットを特定する次の AV のペアが含まれています。

```
ACS: CiscoSecure-Defined-ACL=acl-set-name
```

`acl-set-name` はダウンロード可能な ACL の内部名です。この名前は、Cisco Secure ACS 管理者が ACL に割り当てた名前と ACL が最後に変更された日時の組み合わせです。

- ASA はダウンロード可能な ACL の名前を検査し、以前にその名前のダウンロード可能な ACL を受信したことがあるかどうかを判別します。

- ASA が以前にその名前のダウンロード可能な ACL を受信したことがある場合は、Cisco Secure ACS との通信は完了し、ASA は ACL をユーザセッションに適用します。ダウンロード可能な ACL の名前には最後に変更された日時が含まれているため、Cisco Secure ACS から送信された名前と、以前にダウンロードした ACL の名前が一致するという事は、ASA はダウンロード可能な ACL の最新バージョンを持っていることとなります。

- ASA が以前にその名前のダウンロード可能な ACL を受信したことがない場合は、その ACL の古いバージョンを持っているか、その ACL のどのバージョンもダウンロードしたことがないこととなります。いずれの場合でも、ASA は、ダウンロード可能な ACL 名を RADIUS 要求内のユーザ名として使用し、ヌルパスワード属性とともに RADIUS 認証要求を発行します。cisco-av-pair RADIUS VSA では、この要求に次の属性と値のペアも含まれます。

```
AAA:service=ip-admission
AAA:event=acl-download
```

これに加えて、ASA は Message-Authenticator 属性 (IETF RADIUS 属性 80) で要求に署名します。

- ダウンロード可能な ACL の名前が含まれているユーザ名属性を持つ RADIUS 認証要求を受信すると、Cisco Secure ACS は Message-Authenticator 属性をチェックして要求を認証します。Message-Authenticator 属性がない場合、または正しくない場合、Cisco Secure ACS はその要求を無視します。Message-Authenticator 属性の存在により、ダウンロード可能な ACL 名がネットワーク アクセスの不正取得に悪用されることが防止されます。Message-Authenticator 属性とその使用方法は、RFC 2869 「RADIUS Extensions」で定義されています。この文書は、<http://www.ietf.org> で入手できます。
- 要求された ACL の長さが約 4 KB 未満の場合、Cisco Secure ACS はその ACL を含めた `access-accept` メッセージで応答します。メッセージの一部に他の必須属性を含める必要があるので、1 つの `access-accept` メッセージに収まる ACL の最大サイズは 4 KB よりわずかに小さくなります。

Cisco Secure ACS はダウンロード可能な ACL を cisco-av-pair RADIUS VSA で送信します。ACL は、一連の属性と値のペアという形式をとります。各ペアには ACE が 1 つ含まれ、シリアル番号が付けられます。

```
ip:inacl#1=ACE-1
ip:inacl#2=ACE-2
.
.
ip:inacl#n=ACE-n

ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```

- 要求された ACL の長さが約 4 KB を超える場合、Cisco Secure ACS は、上記の形式の ACL の一部が含まれた `access-challenge` メッセージで応答します。メッセージには、State 属性 (IETF RADIUS 属性 24) も含まれています。State 属性には、Cisco Secure ACS がダウンロードの進捗を追跡するために使用する制御データが含まれています。Cisco Secure ACS は、RADIUS メッセージの最大サイズ以内で可能な限り多数の完全な属性と値のペアを cisco-av-pair RADIUS VSA に含めます。

ASA は ACL の一部を受信すると、それを保存し、新しい `access-request` メッセージで応答します。これには、ダウンロード可能な ACL を求める最初の要求と同じ属性と、`access-challenge` メッセージで受信した State 属性のコピーが含まれています。

このプロセスは、Cisco Secure ACS が ACL の最後の部分を `access-accept` メッセージで送信するまで繰り返されます。

### ダウンロード可能な ACL に関する Cisco Secure ACS の設定

Cisco Secure ACS 上のダウンロード可能な ACL を共有プロファイル コンポーネントとして設定し、その ACL 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。

ACL 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（コマンドリファレンスを参照）に類似する、1 つまたは複数の ASA の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 ACL 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 ACL 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 のガイドを参照してください。

ASA 上では、ダウンロードされた ACL 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 が生成した固有のバージョン ID です。

ASA 上にダウンロードされた ACL は、次の行で構成されます。

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



## ダウンロード可能な ACL に関する任意の RADIUS サーバの設定

ユーザ固有の ACL を Cisco IOS RADIUS cisco-av-pair VSA (ベンダー 9、属性 1) で ASA 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-av-pair VSA で、**access-list extended** コマンド (コマンドリファレンスを参照) 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、ASA 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せん。

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 ACL 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 属性で送信される ACL をユーザごとに固有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。

ASA 上では、ダウンロードされた ACL の名前は次のようになります。

```
AAA-user-username
```

*username* 引数は、認証を受けるユーザの名前です。

ASA 上にダウンロードされた ACL 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 ACL 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 ACL とローカルの ACL が区別されます。この例では、「79AD4A08」は ASA によって作成されたハッシュ値で、RADIUS サーバ上で ACL 定義がいつ変更されたかを判別するために役立ちます。

## ダウンロード可能な ACL 内のワイルドカード ネットマスク表現の変換

RADIUS サーバを使用して、ダウンロード可能な ACL を Cisco VPN 3000 Series Concentrator および ASA に提供する場合は、ワイルドカード ネットマスク表現を標準のネットマスク表現に変換するように ASA を設定しなければならない場合があります。これは、Cisco VPN 3000 Series Concentrator はワイルドカード ネットマスク表現をサポートしますが、ASA は標準のネットマスク表現しかサポートしないためです。これらの違いは、RADIUS サーバ上のダウンロード可能な ACL を設定する方法に影響しますが、ワイルドカード ネットマスク表現を変換するように ASA を設定することで、その影響を

最小限に抑えることができます。ワイルドカード ネットマスク 表現の変換により、RADIUS サーバ上のダウンロード可能な ACL のコンフィギュレーションを変更することなく、Cisco VPN 3000 Series Concentrator 用に記述されたダウンロード可能な ACL を ASA で使用できます。

アクセス リストのネットマスク変換は、サーバごとに設定します。設定は、サーバをサーバグループへ追加する際に、[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [AAA Server Groups] 領域で行います。

## ユーザごとのアクセス コントロール リスト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、ASA で作成済みの ACL の名前を RADIUS サーバからダウンロードするには、IETF RADIUS filter-id 属性（属性番号 11）を次のように設定します。

```
filter-id=acl_name
```



(注) Cisco Secure ACS では、filter-id 属性の値は、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 属性の値をユーザごとに固有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。

ASA 上で ACL を作成するには、一般的な操作のコンフィギュレーション ガイドの [Chapter 20, “Using the ACL Manager,”](#) を参照してください。

## ネットワーク アクセスのアカウントिंगの設定

ASA は、ASA を通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウントング情報を 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トング情報を保持できます。トラフィックが認証済みでない場合、AAA サーバは IP アドレスによってアカウントング情報を保持できます。ASA アカウントング情報には、セッションの開始時刻と終了時刻、ユーザ名、そのセッションでを經由したバイト数、使用されたサービス、各セッションの継続時間が含まれます。

アカウントングを設定するには、次の手順を実行します。

- ステップ 1** ユーザごとのアカウントング データを提供するように ASA を設定する場合は、認証をイネーブルにする必要があります。詳細については、「[ネットワーク アクセス認証の設定](#)」(P.7-6) を参照してください。IP アドレスごとのアカウントング データを提供するように ASA を設定する場合は、認証をイネーブルにする必要はありません。次のステップに進みます。
- ステップ 2** [Configuration] > [Firewall] > [AAA Rules] ペインから、[Add] > [Add Accounting Rule] を選択します。  
[Add Accounting Rule] ダイアログボックスが表示されます。
- ステップ 3** [Interface] ドロップダウン リストから、ルールを適用するためのインターフェイスを選択します。
- ステップ 4** [Action] フィールドで、実装内容に応じて、次のいずれかをクリックします。
  - **Account**
  - **Do not Account**

- ステップ 5** [AAA Server Group] ドロップダウン リストから、サーバ グループを選択します。AAA サーバをサーバ グループに追加する場合は、[Add Server] をクリックします。
- ステップ 6** [Source] フィールドで、送信元 IP アドレスを入力するか、省略符号 ([...]) をクリックして ASDM にすでに定義されている IP アドレスを選択します。
- ステップ 7** [Destination] フィールドで、宛先 IP アドレスを入力するか、省略符号 ([...]) ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。
- ステップ 8** [Service] フィールドで、宛先サービスの IP サービス名または IP サービス番号を入力するか、省略符号 ([...]) をクリックしてサービスを選択します。
- ステップ 9** (任意) [Description] フィールドに説明を入力します。
- ステップ 10** (任意) [More Options] をクリックすると、必要に応じて次のような処理を実行できます。
- TCP または UDP 用の送信元サービスを指定する場合は、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。
  - 宛先サービスと送信元サービスは同じである必要があります。[Source Service] フィールドに [Destination Service] フィールドの内容をコピー アンド ペーストします。
  - ルールを非アクティブにするには、[Enable Rule] チェックボックスをオフにします。  
これにより、ルールを削除しないまま無効にできます。
  - ルールの適用期間を設定する場合は、[Time Range] ドロップダウン リストから、既存の時間範囲を選択します。時間範囲を新規に追加する場合は、省略符号 ([...]) ボタンをクリックします。詳細については、一般的な操作のコンフィギュレーション ガイドの [“Configuring Time Ranges” section on page 15-26](#) を参照してください。
- ステップ 11** [OK] をクリックします。  
[Add Accounting Rule] ダイアログボックスが閉じ、ルールが [AAA Rules] テーブルに表示されます。
- ステップ 12** [Apply] をクリックします。  
変更内容が実行コンフィギュレーションに保存されます。

AAA には、ユーザ アクセスに対して、ACL 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、DMZ ネットワーク上のサーバの Telnet に対するすべての Outside ユーザのアクセスを許可する ACL を作成することができます。一部のユーザだけがサーバにアクセスできるようにする際に、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、認証済みまたは許可済みのユーザだけに ASA を介した接続を許可することができます (Telnet サーバもまた、認証を実行します。ASA 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)。

## MAC アドレスによるトラフィックの認証と許可の免除

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

たとえば、ASA 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、特定のサーバからの未認証の TCP 接続は許可する場合、MAC 免除規則を使用すると、この規則で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許可が免除されます。この機能は、認証プロンプトに回答できない IP 電話などのデバイスを免除する場合に特に便利です。

パケットが最適に一致するエントリではなく最初に一致するエントリを使用するため、エントリの順序が重要になります。permit エントリがあり、その permit エントリで許可されているアドレスを拒否する場合は、permit エントリよりも前に deny エントリを入力してください。

MAC アドレスを使用してトラフィックの認証および許可を免除するには、次の手順を実行します。

- 
- ステップ 1** [Configuration] > [Firewall] > [AAA Rules] ペインで、[Add] > [Add MAC Exempt Rule] を選択します。
- [Add MAC Exempt Rule] ダイアログボックスが表示されます。
- ステップ 2** [Action] ドロップダウン リストから、実装内容に応じて、次のいずれかのオプションをクリックします。
- **MAC Exempt**
  - **No MAC Exempt**
- [MAC Exempt] オプションを選択すると、特定の MAC アドレスから発信されたトラフィックを、認証および許可を行うことなく許可できます。[No MAC Exempt] オプションを選択すると、認証および許可を免除しない MAC アドレスを指定できます。ffff.ffff.0000 などの MAC アドレス マスクを使用してある範囲の MAC アドレスを許可し、その範囲内のある MAC アドレスを認証および許可の対象にする場合は、拒否エントリの追加が必要になることがあります。
- ステップ 3** [MAC Address] フィールドに、送信元の MAC アドレスを 12 桁の 16 進数の形式 (nnnn.nnnn.nnnn) で指定します。
- ステップ 4** [MAC Mask] フィールドに、MAC アドレスの中で照合に使用される部分を指定します。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。
- ステップ 5** [OK] をクリックします。
- [Add MAC Exempt Rule] ダイアログボックスが閉じ、ルールが [AAA Rules] テーブルに表示されません。
- ステップ 6** [Apply] をクリックします。
- 変更内容が実行コンフィギュレーションに保存されます。
-

## AAA ルールの機能履歴

表 7-1 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 7-1 AAA ルールの機能履歴

機能名	プラットフォーム リリース	機能情報
AAA ルール	7.0(1)	AAA ルールでは、ネットワーク アクセスで AAA をイネーブルに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] > [Firewall] > [AAA Rules] [Configuration] > [Firewall] > [Advanced] > [Virtual Access]
カットスルー プロキシを使用した認証	9.0(1)	アイデンティティ ファイアウォール機能とともに AAA ルールを使用して認証できます。

