CHAPTER 17

# ネットワーク アクセスへの AAA の適用

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、「システム管理者用の AAA」（P.23-10）を参照してください。

この章では、次の内容について説明します。



## 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層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 のカットスルー プロキシは、最初にアプリケーション層でユーザを照合したあと、標準の Remote Authentication Dial-In User Service（RADIUS）、Terminal Access Controller Access Control System Plus（TACACS+）、またはローカル データベースを使用して認証を行います。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。

## ネットワーク アクセス認証の設定

ここでは、次の内容について説明します。

# 認証の概要

FWSM 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。ここでは、次の内容について説明します。



## One-Time 認証

所定の IP アドレスを持つユーザは、認証セッションの期限が切れるまで、すべてのルールおよびタイプについて認証を 1 回受けるだけで済みます。（タイムアウトの値については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』で **timeout uauth** コマンドを参照してください）。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、**timeout uauth** コマンドが非常に小さな値に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==」ストリングをキャッシュして、当該サイトへの後続の接続すべてに使用するためです。このストリングがクリアされるのは、ユーザが Web ブラウザのインスタンスをすべて終了し、再起動したときだけです。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に必要なアプリケーション

どのプロトコルまたはサービスへのネットワーク アクセスについても認証を課すように FWSM を設定することはできますが、ユーザは、HTTP、HTTPS、Telnet、または FTP のいずれかで認証を直接受けるだけで済みます。ユーザがこれらのサービスのいずれかで認証されると、FWSM は認証を必要とする別のトラフィックも許可します。

FWSM が AAA 用にサポートしている認証ポートは固定値です。

- FTP の場合はポート 21
- Telnet の場合はポート 23
- HTTP の場合はポート 80
- HTTPS の場合はポート 443

## FWSM 認証プロンプト

Telnet および FTP では、FWSM が認証プロンプトを生成します。正しく認証されると、FWSM によって元の宛先にリダイレクトされます。宛先サーバに独自の認証が設定されている場合には、別のユーザ名とパスワードを入力することになります。

HTTP の場合、ブラウザに備わっている基本 HTTP 認証を使用してログインします。HTTPS の場合、FWSM によってカスタム ログイン ウィンドウが生成されます。

（注）　**aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントから FWSM に送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することを推奨します。**aaa authentication secure-http-client** コマンドの詳細については、「Web クライアントのセキュアな認証のイネーブル化」（P.17-6）を参照してください。

FTP では、ユーザが FWSM のユーザ名に続けてアットマーク（@）を入力し、次に FTP ユーザ名を入力する（name1@name2）オプションがあります。パスワードを入力するとき、ユーザは FWSM のパスワードに続けてアットマーク（@）を入力し、次に FTP パスワードを入力します（password1@password2）。たとえば、次のテキストを入力します。

```
name> user1@user2
password> letmein@he110
```

この機能が役立つのは、複数のログインが必要になる、カスケードされたファイアウォールがある場合です。複数の名前とパスワードを区切るには、複数のアット マーク（@）を使用します。

## スタティック PAT と HTTP

HTTP 認証では、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。実際のポート 80 宛てのトラフィックを検出した場合、マッピング ポートが何番であるかにかかわらず、FWSM はその HTTP 接続を代行受信し、認証を強制します。

たとえば、外部 TCP ポート 889 が次のようにポート 80（www）に変換されていて、関係するすべてのアクセス リストでこのトラフィックが許可されているとします。

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

この場合、ユーザが 10.48.66.155 にポート 889 でアクセスしようとすると、FWSM がトラフィックを代行受信して HTTP 認証を強制します。FWSM が HTTP 接続を完了する前に、ユーザの Web ブラウザに 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 以外になっているとします。

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

この場合、ユーザには認証ページが表示されません。代わりに、FWSM 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。

## FWSM での直接認証

FWSM を経由する HTTP(S)、Telnet、または FTP 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には、仮想 Telnet、仮想 SSH、または仮想 HTTP を設定できます。この場合、ユーザが FWSM 上に設定された特定の IP アドレスに Telnet、SSH、または HTTP を使用して接続すると、FWSM にプロンプトが表示されます。**virtual telnet**、**virtual ssh**、または **virtual http** コマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

# ネットワーク アクセス認証のイネーブル化

ネットワーク アクセス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**　**aaa-server** コマンドを使用して、AAA サーバを指定します。すでに AAA サーバを指定してある場合は、次の手順に進みます。

AAA サーバの指定方法の詳細については、「AAA サーバ グループおよびサーバの識別」（P.11-9）を参照してください。

**ステップ 2**　**access-list** コマンドを使用して、認証するトラフィックの送信元アドレスと宛先アドレスを指定するアクセス リストを作成します。手順については、「拡張アクセス リストの追加」（P.13-6）を参照してください。

**許可** ACE は、一致したトラフィックを認証するようにマークします。一方、**拒否**エントリは、一致したトラフィックを認証から除外します。アクセス リストには HTTP(S)、Telnet、または FTP のいずれかの宛先ポートを必ず指定してください。ユーザは、FWSM 経由の他のサービスの許可を得る前に、これらのサービスのいずれかで認証される必要があるからです。

**ステップ 3**　認証を設定するには、次のコマンドを入力します。

```
hostname(config)# aaa authentication match acl_name interface_name server_group
```

*acl_name* は ステップ 2 で作成したアクセス リストの名前です。*interface_name* は **nameif** コマンドで指定されたインターフェイスの名前です。*server_group* は ステップ 1 で作成した AAA サーバ グループです。

**（注）**　もう 1 つの方法として、**aaa authentication include** コマンド（コマンド内でトラフィックを指定するコマンド）を使用することもできます。ただし、同一コンフィギュレーション内で両方の方法を使用することはできません。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

**ステップ 4**　（任意）ネットワーク アクセス認証にローカル データベースを使用していて、FWSM がいずれのユーザ アカウントに対しても、連続して失敗できるログイン試行回数を制限する場合、**aaa local authentication attempts max-fail** コマンドを使用します。次に例を示します。

```
hostname(config)# aaa local authentication attempts max-fail 7
```

**ヒント**　特定のユーザまたはすべてのユーザのロックアウト ステータスを解除するには、**clear aaa local user lockout** コマンドを使用します。

**ステップ 5**　（任意）ユーザ認証がタイムアウトになるか、**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、次のコマンドを入力して、アクティブなすべての接続を即座に強制終了できます。

```
hostname(config)# aaa authentication clear-conn interface_name source_ip source_mask
```

このコマンドを使用しないと、ユーザ認証セッションがタイムアウトになっても、アクティブな接続は終了しません。

たとえば、次のコマンドは、すべての内部 HTTP トラフィックおよび SMTP トラフィックを認証します。

```
hostname(config)# aaa-server AuthOutbound protocol tacacs+
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# access-list MAIL_AUTH extended permit tcp any any eq smtp
hostname(config)# access-list MAIL_AUTH extended permit tcp any any eq www
```

```
hostname(config)# aaa authentication match MAIL_AUTH inside AuthOutbound
```

次のコマンドは、外部インターフェイスから特定のサーバ（209.165.201.5）への Telnet トラフィックを認証します。

```
hostname(config)# aaa-server AuthInbound protocol tacacs+
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)# access-list TELNET_AUTH extended permit tcp any host 209.165.201.5 eq
telnet
hostname(config)# aaa authentication match TELNET_AUTH outside AuthInbound
```

# カスタム ログイン プロンプトの設定

デフォルトでは、FWSM でのユーザの認証時には、次のプロンプトが表示されます。

- HTTP の場合：`HTTP 認証`
- FTP の場合：`FTP 認証`
- Telnet の場合：プロンプトなし

ログイン プロンプトをカスタマイズして、ユーザが許可または拒否されたときにもプロンプトを表示できます。Windows Active Directory サーバと通信する RADIUS サーバを使用している場合、無効な証明書（ユーザ名またはパスワードが正しくない）またはパスワードの有効期限切れが原因でユーザが拒否されたときに拒否プロンプトを表示するようにカスタマイズできます。パスワードの有効期限が切れている場合、ユーザは新しいパスワードの入力を求められます。

**（注）** ログイン プロンプトをカスタマイズすると、FWSM でユーザ パスワード用に MSCHAPv2 が使用されるようになります。この機能をイネーブルにする前に、RADIUS サーバとバックエンド データベースに MSCHAPv2 との互換性があることを確認してください。

ログイン プロンプトをカスタマイズする手順は、次のとおりです。

**ステップ 1**　ログイン プロンプトをカスタマイズするには、次のコマンドを入力します。

```
hostname(config)# auth-prompt prompt text
```

*text* には、最大 235 文字の英数字文字列または最大 31 単語を使用できます。最初に到達した方の制限が適用されます。特殊文字、スペース、および句読点を使用できます。疑問符を入力するか、または Enter キーを押すと、ストリングが終了します。（疑問符はストリングに含まれます）。

**ステップ 2**　ユーザが許可されたときにテキストを表示するには、次のコマンドを入力します。

```
hostname(config)# auth-prompt accept text
```

**ステップ 3**　ユーザが拒否されたときにテキストを表示するには、次のコマンドを入力します。

```
hostname(config)# auth-prompt reject text
```

**invalid-credentials** または **reject expired-pwd** キーワードを指定せずに **reject** キーワードを入力すると、無効な証明書またはパスワードの有効期限切れが原因で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。無効な証明書またはパスワードの有効期限切れが原因の拒否に対しては、

**invalid-credentials** または **reject expired-pwd** キーワードに設定したプロンプトが表示されます。無効な証明書またはパスワードの有効期限切れに対してプロンプトを設定しなかった場合、すべての状況で汎用の拒否プロンプトが表示されます。

**ステップ 4**　無効な証明書が原因でユーザが拒否されたときにテキストを表示するには、次のコマンドを入力します。

```
hostname(config)# auth-prompt reject invalid-credentials text
```

**ステップ 5**　パスワードの有効期限切れが原因でユーザが拒否されたときにテキストを表示するには、次のコマンドを入力します。

```
hostname(config)# auth-prompt reject expired-pwd text
```

このプロンプトは、RADIUS サーバでユーザ名およびパスワード用に Windows Active Directory サーバを使用している場合にだけ使用されます。ユーザに新しいパスワードの入力を求めるには、**expired-pwd** キーワードを使用してプロンプトを設定する必要があります。

---

次に、認証プロンプトを「Please enter your username and password」というストリングに設定する例を示します。

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

このストリングがコンフィギュレーションに追加されると、ユーザには次のように表示されます。

```
Please enter your username and password
User Name:
Password:
```

また、FWSM で認証試行が許可または拒否されたときにそれぞれ表示するメッセージを指定することもできます。次に例を示します。

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

無効な証明書、パスワードの有効期限切れ、および不明な拒否理由に関する拒否メッセージを設定するには、次のコマンドを入力します。

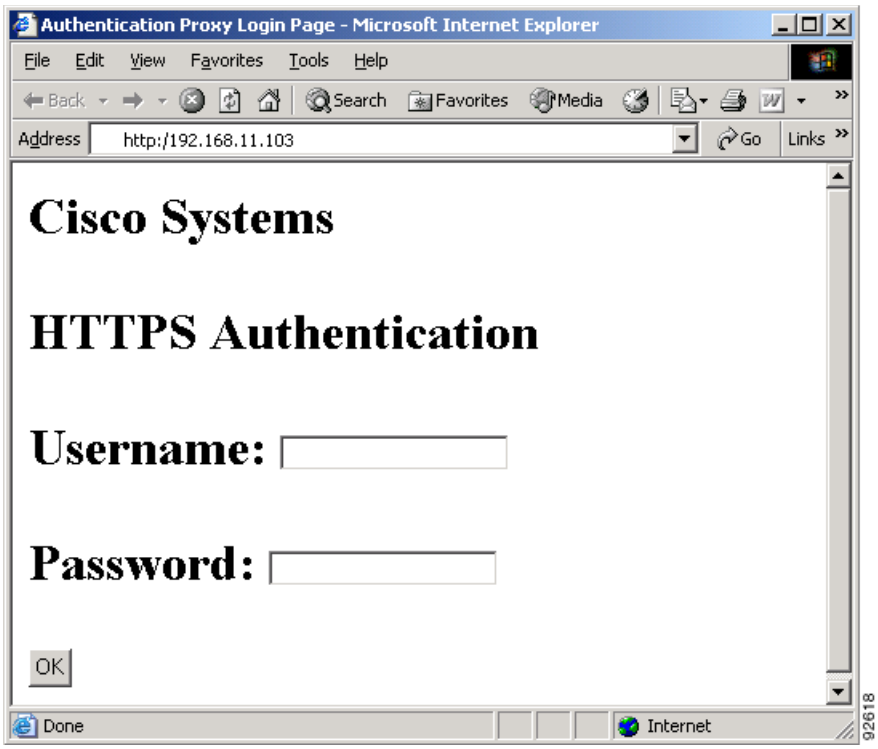
```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt reject invalid-credentials Incorrect username or password
hostname(config)# auth-prompt reject expired-pwd Your password is expired. Reset your
password and try again.
```

# Web クライアントのセキュアな認証のイネーブル化

FWSM は、安全に HTTP 認証を行う方法を提供します。HTTP 認証を保護しないと、FWSM に提供されたユーザ名とパスワードは宛先 Web サーバに転送されます。**aaa authentication secure-http-client** コマンドを使用すると、Web クライアントおよび HTTPS 設定を適用した FWSM の間でユーザ名とパスワードを交換できます。HTTPS により伝送が暗号化され、ユーザ名とパスワードが HTTP によって外部 Web サーバに転送されるのを回避します。

この機能をイネーブルにした場合、認証を必要とする Web ページにユーザがアクセスすると、図 17-1 に示す [Authentication Proxy Login] ページが FWSM によって表示されます。

図 17-1　認証プロキシの HTML ログイン ページ




（注）　この画面に表示されている Cisco Systems のテキスト フィールドは、**auth-prompt** コマンドを使用して変更できます。「カスタム ログイン プロンプトの設定」（P.17-5）を参照してください。

有効なユーザ名とパスワードを入力すると、[Authentication Successful]（認証成功）ページが表示され、自動的に終了します。ユーザ名とパスワードが無効の場合には、[Authentication Failed]（認証失敗）ページが表示されます。

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。

- 最大 128 の同時 HTTPS 認証セッションがサポートされます。最大 128 の HTTPS 認証プロセスが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。
- **uauth timeout 0** が設定されると（**uauth timeout** が 0 に設定される）、HTTPS 認証は機能しない場合があります。HTTPS 認証後にブラウザによって複数の TCP 接続が開始されて Web ページがロードされると、最初の接続は通過を許可されますが、後続の接続では認証がトリガーされます。その結果、正しいユーザ名とパスワードを毎回入力しても、認証ページが繰り返しユーザに表示されます。この状況を回避するには、**timeout uauth 0:0:1** コマンドで **uauth timeout** を 1 秒に設定します。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 で行われるため、HTTP クライアントから HTTP サーバ ポート 443 へのトラフィックをブロックするように、**access-list** コマンド ステートメントを設定しないでください。また、ポート 80 での 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。次の例では、1 行目で Web トラフィックに対してスタティック PAT を設定しているため、2 行目を追加して、HTTPS 認証コンフィギュレーションをサポートする必要があります。

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
```

```
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

- **aaa authentication secure-http-client** が設定されていない場合、HTTP ユーザには、ブラウザが生成するポップアップ ウィンドウが表示されます。**aaa authentication secure-http-client** が設定されている場合、ブラウザのフォームがロードされると、ユーザ名とパスワードが収集されます。また、ユーザの入力したパスワードが誤っていると、ユーザは再入力を求められます。Web サーバと認証サーバがそれぞれ別のホスト上にある場合、正常な認証処理を実行するには **virtual http** コマンドを使用します。

Web クライアントのセキュアな認証をイネーブルにする手順は、次のとおりです。

**ステップ 1**　HTTP 認証をイネーブルにします。認証のイネーブル化の詳細については、「ネットワーク アクセス認証のイネーブル化」（P.17-3）を参照してください。

**ステップ 2**　Web クライアントのセキュアな認証をイネーブルにするには、次のコマンドを入力します。

```
aaa authentication secure-http-client
```

**（注）**　**aaa authentication secure-http-client** コマンドの使用は、HTTP 認証のイネーブル化に依存しません。あとで HTTP 認証をイネーブルにしたときに、セキュア Web クライアント認証によってユーザ名とパスワードが保護されているようにするには、HTTP 認証をイネーブルにする前にこのコマンドを入力します。

# プロトコル単位の認証照合のディセーブル化

FWSM がユーザに対し、ユーザ名とパスワードの照合を行うかどうかを設定できます。デフォルトでは、AAA ルールが新しいセッションでトラフィックの認証を強化し、トラフィックのプロトコルが FTP、Telnet、HTTP、または HTTPS である場合、FWSM はユーザに指示を出します。場合によっては、次のコマンドを使用して、1 つまたは複数のプロトコルの認証照合をディセーブルにすることがあります。

```
hostname(config)# aaa authentication protocol challenge disable
```

たとえば、FTP を使用して新しい接続のためのユーザ名とパスワードの照合をディセーブルにするには、次のコマンドを入力します。

```
hostname(config)# aaa authentication ftp challenge disable
```

特定のプロトコルの認証チャレンジをディセーブルにすると、そのプロトコルを使用しているトラフィックは、以前に認証されたセッションに属している場合にだけ、許可されます。この認証は、認証チャレンジがイネーブルのままになっているプロトコルを使用するトラフィックによって完了できます。たとえば、FTP の認証照合をディセーブルにすると、トラフィックが許可ルールに指定されている場合、FWSM は FTP を使用する新しいセッションを拒否します。認証チャレンジがイネーブルになっているプロトコル（HTTP など）を使用してユーザがセッションを確立した場合、FTP トラフィックは許可されます。

# ネットワーク アクセス認証の設定

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

ここでは、次の内容について説明します。



## TACACS+ 認可の設定

FWSM では、TACACS+ を使用してネットワーク アクセス認可を実行するように設定できます。

ユーザが認証されると、FWSM は認可ルールをチェックして、一致するトラフィックがあるかどうかを調べます。トラフィックが認可ステートメントに一致した場合、FWSM はユーザ名を TACACS+ サーバに送信します。TACACS+ サーバは、ユーザ プロファイルに基づいて、必要な情報を FWSM に戻します。この情報は、FWSM でそのトラフィックのユーザ指定のダイナミック アクセス リストとして扱われます。

（注）　**access-group** コマンドを使用してアクセス リストをインターフェイスに適用した場合、**per-user-override** キーワードがダイナミック アクセス リストによる許可に与える、次の影響について注意してください。

- **per-user-override** キーワードを使用しない場合、ユーザ セッションのトラフィックは、インターフェイス アクセス リストとダイナミック 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** キーワードを使用する場合、ダイナミック アクセス リストが許可の内容を判別します。

詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **access-group** コマンドの項を参照してください。

認証ステートメントと認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、認可ステートメントに一致した場合でも拒否されます。ユーザが認可を受けるには、まず FWSM に認証される必要があります。

（注）　認証と許可で扱うトラフィックは同じものを使用することを推奨します。許可ステートメントを認証ステートメントより制限的にすると、FWSM でのダイナミック アクセス リストの使用方法に起因して、一部の接続が予期せず拒否されます。ユーザが最初に認証されたときに、その接続が認証ステートメントとは一致し、許可ステートメントとは一致しなかった場合、（uauth セッションが存在しているかぎり）許可ステートメントと一致するそれ以降の接続は拒否されます。逆に、最初の接続が許可ステートメントと一致した場合、認証ステートメントとは一致し、許可ステートメントとは一致しないそれ以降の接続は拒否されます。したがって、認証と許可の設定は同一にする必要があります。

ユーザに対してネットワーク アクセス認可を設定する方法については、TACACS+ サーバのマニュアルを参照してください。

TACACS+ 認可を設定するには、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 アクセス認証のイネーブル化」（P.17-3）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**　認可をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# aaa authorization match acl_name interface_name server_group
```

*acl_name* は認証用に作成したアクセス リストの名前です。*interface_name* は **nameif** コマンドで指定されたインターフェイスの名前、またはデフォルトのインターフェイスの名前です。*server_group* は認証をイネーブルにしたときに作成した AAA サーバ グループです。

次のコマンドは、内部 Telnet トラフィックを認証し、認可します。

```
hostname(config)# access-list TELNET_AUTH extended permit tcp any any eq telnet
hostname(config)# aaa-server AuthOutbound protocol tacacs+
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa authentication match TELNET_AUTH inside AuthOutbound
hostname(config)# aaa authorization match TELNET_AUTH inside AuthOutbound
```

# 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たアクセス許可パケットにユーザ許可を戻します。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.17-1）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。FWSM が RADIUS サーバから受信したユーザ指定のダイナミック アクセス リスト情報を処理する方法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。ユーザが実行できるのは、ダイナミック アクセス リストで許可された内容だけです。

**（注）**　**access-group** コマンドを使用してアクセス リストをインターフェイスに適用した場合、**per-user-override** キーワードがダイナミック アクセス リストによる許可に与える、次の影響について注意してください。

- **per-user-override** キーワードを使用しない場合、ユーザ セッションのトラフィックは、インターフェイス アクセス リストとダイナミック 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** キーワードを使用する場合、ダイナミック アクセス リストが許可の内容を判別します。

詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **access-group** コマンドの項を参照してください。

ここでは、次の内容について説明します。

- 「RADIUS サーバからユーザごとの ACL をダウンロードする設定」（P.17-11）

- 「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.17-13）

## RADIUS サーバからユーザごとの ACL をダウンロードする設定

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アクセス リストに関する Cisco Secure ACS の設定」（P.17-11）
- 「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.17-12）

### 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 リストの定義には、拡張 **access-list** コマンドと同様の 1 つまたは複数の FWSM コマンドを設定します。ただし、次のプレフィクスは不要です。

**access-list** *acl_name* **extended**

次に、Cisco Secure ACS バージョン 3.3 でダウンロード可能なアクセス リストの例を示します。

```
+---------------------------------------------+
| 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 のガイド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 が生成した固有のバージョン 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

Cisco IOS RADIUS VSA をサポートする RADIUS サーバを、Cisco IOS RADIUS cisco-av-pair VSA（VSA 番号 1）の FWSM にダイナミック アクセス リストを送信するよう設定します。Cisco IOS RADIUS VSA は、RADIUS ベンダー ID 9 で識別されます。

cisco-av-pair VSA では、**access-list extended** コマンドと同様の 1 つまたは複数の ACE を設定してください。ただし、次のコマンド プレフィクスは、

**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 属性で送信されるアクセス リスト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。

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。

```
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、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 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。

FWSM でのアクセス リストの作成手順については、「拡張アクセス リストの追加」（P.13-6）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

FWSM は、FWSM を通過するすべての TCP または UDP トラフィックについてのアカウンティング情報を、RADIUS または TACACS+ サーバに送信できます。そのトラフィックが認証済みの場合、AAA サーバはユーザ名によってアカウンティング情報を保持できます。こ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守できます。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、FWSM 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。

アカウンティ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ティング データを提供するように FWSM 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 アクセス認証のイネーブル化」（P.17-3）を参照してください。IP アドレスごとのアカウンティング データを提供するように FWSM 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**　**access-list** コマンドを使用して、アカウンティング対象のトラフィックの送信元アドレスと宛先アドレスを指定するアクセス リストを作成します。手順については、「拡張アクセス リストの追加」（P.13-6）を参照してください。

**許可** ACE によって、一致するトラフィックが認可にマーク付けされる一方で、**拒否**エントリによって一致するトラフィックが認可から除外されます。

（注）　認証が設定済みで、なおかつ認証されたすべてのトラフィックのアカウンティング データが必要な場合、**aaa authentication match** コマンドで使用するために作成したアクセス リストと同じアクセス リストを使用できます。

**ステップ 3**　アカウンティングをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# aaa accounting match acl_name interface_name server_group
```

**（注）** もう 1 つの方法として、**aaa accounting include** コマンド（コマンド内でトラフィックを指定するコマンド）を使用することもできます。ただし、同一コンフィギュレーション内で両方の方法を使用することはできません。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

次のコマンドは、内部 Telnet トラフィックを認証、認可、アカウンティングします。209.165.201.5 以外のサーバに向かう Telnet トラフィックは認証だけを受けますが、209.165.201.5 に向かうトラフィックには認可およびアカウンティングが必要です。

```
hostname(config)# aaa-server AuthOutbound protocol tacacs+
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# access-list TELNET_AUTH extended permit tcp any any eq telnet
hostname(config)# access-list SERVER_AUTH extended permit tcp any host 209.165.201.5 eq
telnet
hostname(config)# aaa authentication match TELNET_AUTH inside AuthOutbound
hostname(config)# aaa authorization match SERVER_AUTH inside AuthOutbound
hostname(config)# aaa accounting match SERVER_AUTH inside AuthOutbound
```

# MAC アドレスによるトラフィックの認証と認可の免除

FWSM では、特定の MAC アドレスからのトラフィックを認証または許可の対象から除外できます。この機能は、認証プロンプトに応答できない IP 電話などのデバイスを免除する場合に特に便利です。

**（注）** この機能では、through-the-box 接続の MAC アドレスのリストだけが除外されます。Telnet から FWSM への接続などについては、デバイスの MAC アドレスが指定されていても、認証または許可は除外されません。

除外対象の MAC アドレスを識別する手順は、次のとおりです。

**ステップ 1**　MAC リストを設定するには、次のコマンドを入力します。

```
hostname(config)# mac-list id {deny | permit} mac macmask
```

*id* 引数は、MAC リストに割り当てる 16 進数です。

MAC アドレスを除外するには、**permit** キーワードを使用します。MAC アドレスを認証および許可の対象にするには、**deny** キーワードを使用します。

MAC アドレスのセットをグループ化するには、**mac-list** コマンドを同じ ID 値で必要な回数だけ入力します。AAA 免除に使用できる MAC リストは 1 つだけなので、MAC リストには免除するすべての MAC アドレスを含めてください。複数の MAC アドレス リストを作成できますが、使用できるのは一度に 1 つだけです。

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** エントリを指定している場合に、その **permit** エントリで許可されるアドレスを拒否するには、その **permit** エントリの前に **deny** エントリを入力します。

*mac* 引数には、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。

*macmask* 引数には、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 MAC アドレスと正確に照合されます。ffff.ffff.0000 は、最初の 8 桁とのみ照合されます。

**ステップ 2**　特定の MAC リストで指定されている MAC アドレスのトラフィックに対して免除するには、次のコマンドを入力します。

```
hostname(config)# aaa mac-exempt match id
```

*id* は、認証および認可を免除するトラフィックの MAC アドレスが含まれている MAC リストを指定する文字列です。**aaa mac-exempt** コマンドのインスタンスを 1 つだけ入力できます。

---

次に、1 つの MAC アドレスについての認証をバイパスする例を示します。

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

次のエントリでは、ハードウェア ID が 0003.E3 であるすべての Cisco IP Phone について、認証をバイパスします。

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

次に、00a0.c95d.02b2 を除き、MAC アドレス グループの認証をバイパスする例を示します。00a0.c95d.02b2 は **permit** ステートメントにも一致するため、**permit** ステートメントの前に **deny** ステートメントを入力してください。そうしないと、**deny** ステートメントが照合されなくなります。

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```