CHAPTER 15

# ネットワーク アクセスへの AAA の適用

この章では、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）（[トリプル A］と発音）をネットワーク アクセスに対してイネーブルにする方法を説明します。

管理アクセスの AAA の詳細については、「システム管理者用の AAA」（p.21-13）を参照してください。

この章で説明する内容は、次のとおりです。



## AAA パフォーマンス

FWSM では、「カットスルー プロキシ」を採用することによって、従来のプロキシ サーバに比べてパフォーマンスが著しく改善されています。従来のプロキシ サーバは、Open Systems Interconnection（OSI; 開放型システム間相互接続）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ので、パフォーマンスが損なわれます。FWSM のカットスルー プロキシは、最初にアプリケーション レイヤ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 でユーザが認証されてからセッション フローに移行するので、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伝送され、セッション ステート情報も保持されます。

# ネットワーク アクセスの認証の設定

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 サーバを使用したネットワーク アクセス認証を設定できます。

特定の IP アドレスのユーザに必要な認証は、認証セッションがタイムアウトになるまでは、すべてのルールとタイプに対して 1 回だけです（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*』の **timeout uauth** コマンドを参照してください）。たとえば、FWSM に Telnet と FTP の認証を設定した場合、ユーザは最初に Telnet の認証に成功すれば、そのセッションの継続中は FTP の認証を受ける必要はありません。

任意のプロトコルまたはサービスについてネットワーク アクセスの認証を必要とするよう FWSM を設定できますが、HTTP、Telnet、または FTP に限り、認証を直接設定できます。FWSM が認証を必要とする他のトラフィックを許可する前に、ユーザはまず、これらのサービスのいずれかで認証される必要があります。

FWSM を経由する HTTP、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 を設定できます。この場合、ユーザが FWSM 上に設定された指定の IP アドレスに Telnet 接続すると、FWSM に Telnet プロンプトが表示されます。**virtual telnet** 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。

Telnet、HTTP、FTP の場合、FWSM によって認証プロンプトが生成されます。宛先サーバに独自の認証が設定されている場合には、ユーザは別途ユーザ名とパスワードを入力することになります。

（注）　**aaa authentication secure-http-client** コマンドを使用せずに HTTP 認証を行うと、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、外部の Web サーバにアクセスする内部ユーザを認証する場合、外部の者は誰でも有効なユーザ名とパスワードを学習できます。HTTP 認証をイネーブルにするときは、**aaa authentication secure-http-client** コマンドを使用することを推奨します。

FTP の場合、FWSM のユーザ名のあとにアットマーク（@）を入力し、続けて FTP ユーザ名を入力できます（name1@name2）。パスワードの場合も、FWSM のパスワードのあとにアットマーク（@）を入力し、さらに FTP パスワードを入力します（password1@password2）。次に、例を示します。

```
name> terryc@jchrichton
password> letmein@he110
```

この機能は、ファイアウォールをカスケード接続して設定し、複数のログインが必要となる場合に便利です。複数の名前とパスワードを、複数のアットマーク（@）で区切ることができます。

## 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手順は、次のとおりです。

**ステップ 1**　**aaa-server** コマンドを使用して、AAA サーバを識別します。すでに AAA サーバを識別している場合、次の手順を行います。

AAA サーバの識別の詳細については、「AAA サーバ グループおよびサーバの識別」（p.14-13）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、認証したいトラフィックの送信元アドレスおよび宛先アドレスを識別するアクセス 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.10-7）を参照してください。

**permit** Access Control Entry（ACE; アクセス制御エントリ）は一致するトラフィックを認証し、**deny** エントリは一致するトラフィックの認証を拒否します。アクセス リストには HTTP、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/contexta(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）**　**aaa authentication include** コマンド（コマンド内でトラフィックを識別する）を使用することもできます。ただし、同じ設定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/contexta(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 ステータスをクリアするには、**clear aaa local user lockout** コマンドを使用します。

次に、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する例を示します。

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

次に、外部インターフェイスから特定サーバ（209.165.201.5）への Telnet トラフィックを認証する例を示します。

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

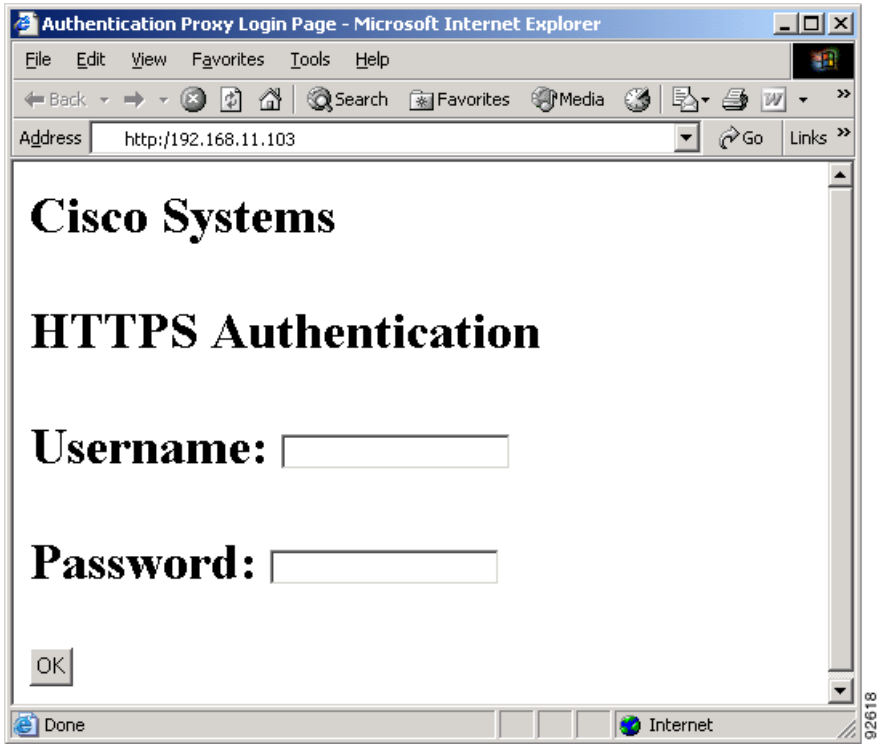
## Web クライアントのセキュア認証のイネーブル化

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 認証を設定した 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 15-1 に示す Authentication Proxy Login ページが FWSM によって表示されます。

**図 15-1　Authentication Proxy Login 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。このコマンドの詳細な構文については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。**auth-prompt** コマンドを使用してテキストを指定しない場合、このフィールドは空白になります。

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）のページが表示され、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）のページが表示されます。

セキュア Web クライアントの認証には次の制限があります。

- 最大 16 の同時 HTTPS 認証セッションがサポートされます。最大 16 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** が設定されている（**uauth timeout** が 0 に設定されている）場合、HTTPS 認証は機能しないことがあります。HTTPS 認証後、ブラウザが Web ページをロードするために複数の TCP 接続を開始した場合、最初の接続は許可されますが、以降の接続に対しては認証が発生します。その結果、正しいユーザ名とパスワードを入力しても、認証ページが継続的に表示されることになります。この問題を回避するには、**timeout uauth 0:0:1** コマンドを使用して、**uauth timeout** を 1 秒に設定してください。ただし、ウィンドウが 1 秒間オープンしているため、同じ送信元 IP アドレスからアクセスする未認証のユーザが、ファイアウォールを通過する可能性があります。

- HTTPS 認証は SSL ポート 443 で実行されるので、ポート 443 で HTTP クライアントから HTTP サーバ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 に Web トラフィック用のスタティック PAT を設定する場合には、SSL ポートにもスタティック PAT を設定する必要があります。次の例では、1 行めで 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 行めを追加して、HTTPS 認証設定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場合では、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** 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.15-3）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チャレンジのディセーブル化

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。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場合は、**aaa authentication** コマンドを使用できます。

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

特定のプロトコルの認証照合をディセーブルにした場合、そのプロトコルを使用するトラフィックは、以前に認証されたセッションに属している場合にのみ、許可されます。この認証は、認証照合がイネーブルであるプロトコルを使用したトラフィックによって実行されます。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。ユーザが、認証照合がイネーブルであるプロトコル（HTTP など）を使用してセッションを確立する場合、FTP トラフィックは許可されます。

# ネットワーク アクセスの許可の設定

特定の接続についてユーザが認証されると、FWSM はユーザからのトラフィックをさらに制御する許可を使用できます。

次の内容について説明します。



## TACACS+ 許可の設定

TACACS+ を使用したネットワーク アクセス許可を実行するよう FWSM を設定することができます。許可ルールと一致する必要のあるアクセス リストを指定することで、許可するトラフィックを識別します。または、許可ルール内で直接、トラフィックを識別します。

**ヒント**　許可するトラフィックを、アクセス リストを使用して識別すると、入力しなければならない許可コマンドの数を大幅に減らすことができます。これにより、許可ルールに指定できる送信元と宛先のサブネットおよびサービスは 1 つだけですが、アクセス リストには複数のエントリを指定できます。

認証および許可ステートメントは独立していますが、認証されないトラフィックが許可ステートメントと一致しても拒否されます。許可されるには、ユーザはまず、FWSM で認証される必要があります。特定の IP アドレスのユーザに必要な認証は、認証セッションがタイムアウトになるまでは、すべてのルールとタイプに対して 1 回だけなので、トラフィックが許可ステートメントと一致すれば許可できます。

ユーザの認証後、FWSM はトラフィックが許可ルールに一致しているかどうかを検証します。トラフィックが許可ステートメントに一致すると、FWSM から TACACS+ サーバにユーザ名が送信されます。TACACS+ サーバは、ユーザの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の応答を FWSM に戻します。FWSM は応答における許可ルールを強化します。

ユーザのネットワーク アクセス許可の設定の詳細については、TACACS+ サーバのマニュアルを参照してください。

TACACS+ 許可を設定する手順は、次のとおりです。

**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.15-3）を参照してください。すでに認証をイネーブルにしている場合は、次の手順を行います。

**ステップ 2**　**access-list** コマンドを使用して、許可するトラフィックの送信元アドレスおよび宛先アドレスを識別するアクセス 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.10-7）を参照してください。

**permit** ACE は一致するトラフィックを許可し、**deny** エントリは一致するトラフィックの許可を拒否します。許可の一致に使用するアクセス リストには、認証の一致に使用するアクセス リストのルールと同じか、またはそのサブセットを含んでいる必要があります。

（注）　認証を設定して、認証されるトラフィックをすべて許可する場合、**aaa authentication match** コマンドを使用して作成した同じアクセス リストを使用できます。

**ステップ 3**　許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/contexta(config)# aaa authorization 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、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。

（注）　**aaa authorization include** コマンド（コマンド内でトラフィックを識別する）を使用することもできますが、同じ設定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。

次に、内部 Telnet トラフィックを認証し、許可する例を示します。209.165.201.5 以外のサーバへの Telnet トラフィックは認証されるだけですが、209.165.201.5 へのトラフィックには許可が必要です。

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

## 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 アクセスの認証の設定」（p.15-2）を参照してください。

ネットワークにアクセスするユーザを認証するよう FWSM を設定した場合、RADIUS 許可を暗黙でイネーブルにできますが、ここでは FWSM 上で RADIUS 許可を設定する詳細については説明しません。FWSM が RADIUS サーバから受信したアクセス リスト情報を処理する方法について説明します。

RADIUS サーバを設定し、認証時に FWSM にアクセス リストまたはアクセス リスト名をダウンロードできます。ユーザに実行できるのは、ユーザ指定のアクセス 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** キーワードは、ユーザ指定のアクセス リストによる許可に与える以下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 リストとユーザ指定のアクセス リスト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、ユーザ指定のアクセス 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 エントリ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.15-9）
- RADIUS サーバからユーザごとの ACL 名をダウンロードする設定（p.15-11）

## RADIUS サーバからユーザごとの ACL をダウンロードする設定

ここでは、Cisco Secure ACS RADIUS サーバまたはサードパーティ製の RADIUS サーバの設定手順について説明します。内容は次のとおりです。

- Cisco Secure ACS RADIUS サーバでのダウンロード可能なアクセス リストの設定（p.15-9）
- RADIUS サーバでのダウンロード可能なアクセス リストの設定（p.15-10）

### Cisco Secure ACS RADIUS サーバでのダウンロード可能なアクセス リストの設定

Cisco Secure ACS に共有プロファイル コンポーネントとしてダウンロード可能なアクセス リストを設定し、グループまたは個人ユーザにアクセス リストを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 リストの作成、およびユーザへの対応付けに関する詳細については、Cisco Secure ACS のバージョンに対応するユーザ マニュアルを参照してください。

FWSM にダウンロードしたアクセス リストは、次の名前になります。

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

*acl_name* 引数は Cisco Secure ACS で定義された名前です（前の例では、acs_ten_acl）。*number* は Cisco Secure ACS によって生成された固有のバージョン ID です。

FWSM にダウンロードしたアクセス リストには、次の行が含まれます。

```
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
```

### RADIUS サーバでのダウンロード可能なアクセス リストの設定

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 にユーザ固有のアクセス 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**

次のテキストに置換されます。

**ip:inacl#***nnn***=**

*nnn* 引数は、FWSM に設定するコマンド ステートメントの順序を表す 0 ～ 999,999,999 の範囲の数値です。このパラメータを省略すると、シーケンス値は 0 になり、cisco-av-pair RADIUS VSA 内の ACE の順序が使用されます。

次に、RADIUS サーバで cisco-av-pair VSA 用に設定する必要があるアクセス リスト定義の例を示します。

```
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 リストのユーザ別の設定については、RADIUS サーバのマニュアルを参照してください。

FWSM にダウンロードしたアクセス リスト名は、次の形式になります。

```
AAA-user-username
```

*username* 引数 は、認証されるユーザの名前です。

FWSM にダウンロードしたアクセス リストには、次の行が含まれます。順序が、RADIUS サーバ上の番号に基づいていることに注意してください。

```
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
```

ダウンロードしたアクセス リストでは、access-list と名前の間に 2 つのスペースが挿入されます。これらのスペースにより、ダウンロードしたアクセス リストとローカル アクセス リストを区別できます。この例での 79AD4A08 は、RADIUS サーバ上でアクセス リスト定義が変更されたときを判別するため、FWSM によって生成されたハッシュ値です。

## RADIUS サーバからユーザごとの ACL 名をダウンロードする設定

ユーザ認証時に、FWSM ですでに作成されているアクセス リストの名前を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 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指定され、**filter-id=** は省略され *acl_name* のみ入力します。

filter-id アトリビュート値のユーザ別の設定については、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.10-7）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 では、FWSM を通過する任意の TCP/UDP トラフィックについて、RADIUS サーバまたは TACACS+ サーバにアカウンティング情報を送信できます。トラフィックが認証されている場合は、AAA サーバでユーザ名ごとにアカウンティング情報を保持できます。トラフィックが認証されていない場合、AAA サーバで IP アドレスごとに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および終了時、ユーザ名、セッション中に FWSM を通過したバイト数、使用されたサービス、および各セッションの長さが含まれます。

アカウンティングを設定する手順は、次のとおりです。

**ステップ 1**　FWSM にユーザごとにアカウンティング データを提供させる場合、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.15-3）を参照してください。FWSM に IP アドレスごとにアカウンティング データを提供させる場合、認証をイネーブルにする必要はなく、次の手順を続行します。

**ステップ 2**　**access-list** コマンドを使用して、アカウント対象のトラフィックの送信元アドレスおよび宛先アドレスを識別するアクセス 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.10-7）を参照してください。

**permit** ACE は一致するトラフィックを許可し、**deny** エントリは一致するトラフィックの許可を拒否します。

**（注）**　認証を設定して、認証されるすべてのトラフィックのデータをアカウントする場合、**aaa authentication match** コマンドを使用して作成した同じアクセス 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/contexta(config)# aaa accounting match acl_name interface_name server_group
```

**（注）**　**aaa accounting include** コマンド（コマンド内でトラフィックを識別する）を使用することもできますが、同じ設定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。

次に、内部 Telnet トラフィックの AAA を設定する例を示します。209.165.201.5 以外のサーバへの Telnet トラフィックは認証されるだけですが、209.165.201.5 へのトラフィックには許可およびアカウンティングが必要です。

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

# MAC アドレスを使用した認証および許可からのトラフィックの除外

FWSM は、特定の MAC アドレスのトラフィックを認証および許可の対象から除外できます。

たとえば、FWSM は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ますが、特定のサーバから未認証の TCP 接続を許可したい場合、**mac-list** コマンドを使用してサーバの MAC アドレスからのトラフィックを許可するルールを作成してから、**aaa mac-exempt** コマンドを使用して MAC リストによって指定されたサーバのトラフィックを認証および許可の対象から除外します。

逆に、認証したにもかかわらず特定のコンピュータからのトラフィックは許可したくない場合、そのコンピュータの **mac-list** コマンドの MAC アドレスを使用できます。この事例の **aaa mac-exempt** コマンドを使用すると、このコンピュータからのトラフィックは許可ルールによって許可されても、アクセスを拒否されます。

MAC アドレスを使用して、認証および許可からトラフィックを除外する手順は、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/contexta(config)# mac-list id {deny | permit} mac macmask
```

*id* は MAC リストに付けたアルファベットの文字列です。*mac* は許可または拒否するトラフィックのコンピュータの MAC アドレスです。*macmask* は MAC アドレス マスクです。**mac-list** 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。

**ステップ 2**　特定の MAC リストで指定された MAC アドレスのトラフィックを除外するには、次のコマンドを入力します。

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

*id* は MAC アドレスを含んだ MAC リストを識別する文字列です。このトラフィックは、認証および許可の対象から除外する必要があります。

次のコマンドは、それぞれ 1 個の MAC アドレスで構成された 2 つの MAC リストを作成します。MAC リストの 1 つは MAC アドレスのトラフィックを許可し、もう 1 つは拒否します。最後の 2 つのコマンドを使用すると、FWSM が 2 つのリスト内の MAC アドレスから発信されるトラフィックを認証および許可から除外するように設定します。

```
hostname/contexta(config)# mac-list adc permit 00a0.cp5d.0282 ffff.ffff.ffff
hostname/contexta(config)# mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
hostname/contexta(config)# aaa mac-exempt match adc
hostname/contexta(config)# aaa mac-exempt match ac
```