CHAPTER 19

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 AAA の設定」（P.40-5）を参照してください。

この章の内容は、次のとおりです。

AAA のパフォーマンス

セキュリティ アプライアンスは「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。セキュリティ アプライアンス 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。セキュリティ アプライアンス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

この項では、次のトピックについて取り上げます。

認証の概要

セキュリティ アプライアンスでは、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。この項では、次のトピックについて取り上げます。

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（タイムアウトの値については、『*Cisco Security Appliance 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 を認証するようにセキュリティ アプライアンスが設定されていて、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。

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セキュリティ アプライアンスを設定することは、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、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。

セキュリティ アプライアンスが 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

セキュリティ アプライアンスの認証プロンプト

Telnet および FTP の場合、セキュリティ アプライアンスは認証プロンプトを生成します。

HTTP の場合、セキュリティ アプライアンス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。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

HTTPS の場合、セキュリティ アプライアンスはカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

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、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。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、セキュリティ アプライアンス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 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

（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セキュリティ アプライアンスに送信されます。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.19-5）を参照してください。

FTP の場合、セキュリティ アプライアンス 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、セキュリティ アプライアンス 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@jchrichton
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 認証では、スタティック PAT が設定されている場合、セキュリティ アプライアンスは実際のポートをチェックします。セキュリティ アプライアンスは、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（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、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、セキュリティ アプライアンス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。セキュリティ アプライアンスが 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。

```
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は表示されません。代わりに、セキュリティ アプライアンスは 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.13-12）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.16-6）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。HTTP、HTTPS、Telnet、または FTP のいずれかの宛先ポートをアクセス リストに必ず含めます。これは、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、他のサービスがセキュリティ アプライアンスの通過を許可されないためです。

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、*interface_name* は **nameif** コマンドで指定したインターフェイスの名前、*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、『*Cisco Security Appliance Command Reference*』を参照してください。

ステップ 4　（任意）HTTP または HTTPS 接続に対する認証のリダイレクション方式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 authentication listener http[s] interface_name [port portnum]
redirect
```

引数 *interface_name* は、受信ポートをイネーブルにするインターフェイスです。

port *portnum* 引数で、セキュリティ アプライアンスが受信するポート番号を指定します。デフォルトは 80（HTTP）と 443（HTTPS）です。

このコマンドを HTTP と HTTPS について別々に入力します。

ステップ 5　（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、セキュリティ アプライアンスがいずれのユーザ 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、次のコマンドを使用します。

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

number は 1 ～ 16 の範囲で指定します。

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。

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
hostname(config)# aaa authentication listener http inside redirect
```

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
```

Web クライアントのセキュアな認証のイネーブル化

セキュリティ アプライアンス は、安全に HTTP 認証を行う方法を提供します。HTTP 認証を保護せずに、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セキュリティ アプライアンスに渡されます。**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 セキュリティ アプライアンス の間でユーザ名とパスワードを交換できます。

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、セキュリティ アプライアンスが 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、ユーザはセキュリティ アプライアンスにより元の HTTP URL にリダイレクトされます。

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

```
hostname(config)# aaa authentication secure-http-client
```

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。
- **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 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。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
```

セキュリティ アプライアンスでの直接認証

HTTP、HTTPS、Telnet、または FTP がセキュリティ アプライアンス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 を使用してセキュリティ アプライアンスの認証を直接受けることができます。

この項では、次のトピックについて取り上げます。

- 「HTTP と HTTPS による直接認証のイネーブル化」（P.19-6）
- 「Telnet による直接認証のイネーブル化」（P.19-6）

HTTP と HTTPS による直接認証のイネーブル化

「ネットワーク アクセス認証のイネーブル化」（P.19-3）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。基本 HTTP 認証を引き続き使用しながら、HTTP および HTTPS に対する直接認証をイネーブルにする場合は、次のコマンドを入力します。

```
hostname(config)# aaa authentication listener http[s] interface_name [port portnum]
```

interface_name 引数は、直接認証をイネーブルにするインターフェイスです。

port *portnum* 引数で、セキュリティ アプライアンスが受信するポート番号を指定します。デフォルトは 80（HTTP）と 443（HTTPS）です。

このコマンドを HTTP と HTTPS について別々に入力します。

インターフェイスの AAA をイネーブルにすると、次の URL でセキュリティ アプライアンス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
```

Telnet による直接認証のイネーブル化

Telnet による直接認証をイネーブルにするには、仮想 Telnet サーバを設定します。仮想 Telnet を設定した場合、ユーザはセキュリティ アプライアンス上で設定された所定の IP アドレスに Telnet で接続し、セキュリティ アプライアンスが Telnet プロンプトを表示します。仮想 Telnet サーバを設定するには、次のコマンドを入力します。

```
hostname(config)# virtual telnet ip_address
```

ip_address 引数には、仮想 Telnet サーバの IP アドレスを設定します。このアドレスは必ず、セキュリティ アプライアンス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、外部にアクセスするときに内部アドレスに NAT を実行し、仮想 Telnet サーバに外部からアクセスする場合は、仮想 Telnet サーバ アドレスにグローバル NAT アドレスの 1 つを使用します。

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、セキュリティ アプライアンスは許可を使用して、ユーザからのトラフィックをさらに制御できます。

この項では、次のトピックについて取り上げます。

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、セキュリティ アプライアンスを設定できます。許可ルールが一致する必要のあるアクセス リストを指定することにより、許可するトラフィックを指定します。または、許可ルール自体で直接、トラフィックを指定することもできます。

ヒント　アクセス リストを使用して許可するトラフィックを指定すると、入力する必要のある許可コマンドの数を大幅に少なくすることができます。これは、入力した各許可規則では、送信元と宛先のサブネットとサービスを 1 つだけ指定できるのに対して、アクセス リストには多数のエントリを含めることができるためです。

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。ユーザが許可を受けるには、まずセキュリティ アプライアンスに認証される必要があります。所定の IP アドレスのユーザは、すべての規則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、許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、セキュリティ アプライアンスは、一致するトラフィックの許可ルールをチェックします。トラフィックが許可ステートメントに一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバはセキュリティ アプライアンスに応答し、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。セキュリティ アプライアンスは、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 アクセス認証のイネーブル化」（P.19-3）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　**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.16-6）を参照してください。

許可 ACE は、一致したトラフィックを許可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許可から除外します。許可の照合に使用するアクセス リストには、認証の照合に使用するアクセス リストの規則と同じ規則またはその一部が含まれている必要があります。

（注）　認証を設定済みで、なおかつ認証されたトラフィックをすべて許可する場合、**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　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(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、*interface_name* は **nameif** コマンドまたはデフォルトで指定したインターフェイスの名前、*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）　もう 1 つの方法として、**aaa authorization 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、『*Cisco Security Appliance 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し、許可します。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許可が必要です。

```
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-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 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.19-1）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セキュリティ アプライアンスを設定すると、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、セキュリティ アプライアンス上の RADIUS 許可の設定については取り上げません。ここでは、セキュリティ アプライアンスが 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 リストをセキュリティ アプライアンス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許可されます。

（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は、**per-user-override** キーワードが、ユーザ固有のアクセス リストによる許可に対して次のように影響を与えることに注意してください。

- **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** キーワードを使用した場合、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定されます。

詳細については、『*Cisco Security Appliance Command Reference*』の **access-group** コマンドの項を参照してください。

この項では、次のトピックについて取り上げます。

- 「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.19-9）
- 「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.19-13）

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アクセス リストの機能と Cisco Secure ACS について」（P.19-9）
- 「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.19-11）
- 「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.19-12）
- 「ダウンロード可能なアクセス リスト内のワイルドカード ネットマスク表現の変換」（P.19-13）

ダウンロード可能なアクセス リストの機能と Cisco Secure ACS について

ダウンロード可能なアクセス リストは、Cisco Secure ACS を使用して各サーバに適切なアクセス リスト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。

- 無制限のアクセス リスト サイズ：ダウンロード可能なアクセス リストは、完全なアクセス リストを Cisco Secure ACS からセキュリティ アプライアンス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。
- アクセス リスト管理の簡素化および集中化：ダウンロード可能なアクセス リストにより、一度記述したアクセス リスト 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、多数のセキュリティ アプライアンス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アクセス リスト 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、アクセス リストのサイズを問わず有用です。

セキュリティ アプライアンスは、ダウンロード可能なアクセス リストを Cisco Secure ACS から次のプロセスで受信します。

1. セキュリティ アプライアンスがユーザ 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アクセス リスト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アクセス リスト 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アクセス リストの内部名です。この名前は、Cisco Secure ACS 管理者がアクセス リストに割り当てた名前とアクセス リストが最後に変更された日時の組み合わせです。

3. セキュリティ アプライアンスはダウンロード可能なアクセス リストの名前を検査し、以前にその名前のダウンロード可能なアクセス リストを受信したことがあるかどうかを判別します。
   - セキュリティ アプライアンスが以前にその名前のダウンロード可能なアクセス リストを受信したことがある場合は、Cisco Secure ACS との通信は完了し、セキュリティ アプライアンスはアクセス リストをユーザ セッションに適用します。ダウンロード可能なアクセス リスト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アクセス リストの名前が一致するということは、セキュリティ アプライアンスはダウンロード可能なアクセス リストの最新バージョンを持っていることになります。
   - セキュリティ アプライアンスが以前にその名前のダウンロード可能なアクセス リストを受信したことがない場合は、そのアクセス リストの古いバージョンを持っているか、そのアクセス リストのどのバージョンもダウンロードしたことがないことになります。いずれの場合でも、セキュリティ アプライアンスは、ダウンロード可能なアクセス リスト名を 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、セキュリティ アプライアンスは Message-Authenticator 属性（IETF RADIUS 属性 80）で要求に署名します。
4. ダウンロード可能なアクセス リスト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アクセス リスト名がネットワーク 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。
5. 要求されたアクセス リストの長さが約 4 KB 未満の場合、Cisco Secure ACS はそのアクセス リストを含めた access-accept メッセージで応答します。メッセージには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アクセス リストの最大サイズは 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アクセス リストを cisco-av-pair RADIUS VSA で送信します。アクセス リストは、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
   ```

   属性と値のペア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
   ```
6. 要求されたアクセス リストの長さが約 4 KB を超える場合、Cisco Secure ACS は、上記の形式のアクセス リストの一部が含まれた 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。

セキュリティ アプライアンスはアクセス リスト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アクセス リスト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。

これは、Cisco Secure ACS がアクセス リストの最後の部分を access-accept メッセージで送信するまで続行されます。

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

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（「拡張アクセス リストの追加」（P.16-6）を参照）に類似する、1 つ以上のセキュリティ アプライアンス 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 のガイドを参照してください。

セキュリティ アプライアンス上では、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。

セキュリティ アプライアンス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-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（ベンダー 9、属性 1）でセキュリティ アプライアンスに送信するように、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（「拡張アクセス リストの追加」（P.16-6）を参照）と類似する 1 つ以上の 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、セキュリティ アプライアンス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。

セキュリティ アプライアンス上では、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。

セキュリティ アプライアンス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」はセキュリティ アプライアンスによって作成されたハッシュ値で、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。

ダウンロード可能なアクセス リスト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アクセス リストを Cisco VPN 3000 シリーズ コンセントレータおよびセキュリティ アプライアンスに提供する場合は、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セキュリティ アプライアンスを設定する必要がある場合があります。これは、Cisco VPN 3000 シリーズ コンセントレータはワイルドカード ネットマスク表現をサポートしますが、セキュリティ アプライアンス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アクセス リスト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セキュリティ アプライアンスを設定することで、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アクセス リストのコンフィギュレーションを変更することなく、Cisco VPN 3000 シリーズ コンセントレータ用に記述されたダウンロード可能なアクセス リストをセキュリティ アプライアンスで使用できます。

アクセス リスト ネットマスク変換は、**acl-netmask-convert** コマンドを使用してサーバごとに設定できます。このコマンドは AAA サーバ コンフィギュレーション モードで使用できます。RADIUS サーバの設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.13-12）を参照してください。**acl-netmask-convert** コマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

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、セキュリティ アプライアンス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。

セキュリティ アプライアンス 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.16-6）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

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過する任意の 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。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、セキュリティ アプライアンス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セキュリティ アプライアンスを設定する場合は、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.19-3）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セキュリティ アプライアンスを設定する場合は、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.16-6）を参照してください。

許可 ACE は、一致したトラフィックを許可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許可から除外します。

（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、『*Cisco Security Appliance 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、許可、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許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許可の免除

セキュリティ アプライアンスは、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、セキュリティ アプライアンス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。

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　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。一連の MAC アドレスをグループ化するには、同じ ID 値で必要な回数の **mac-list** コマンドを入力します。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 リストを作成できますが、一度に使用できるのは 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 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 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、認証および許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。

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

```
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
```

次の例では、00a0.c95d.02b2 以外の MAC アドレス グループの認証をバイパスします。00a0.c95d.02b2 は permit ステートメントとも一致するため、permit ステートメントよりも前に deny ステートメントを入力します。permit ステートメントが前にある場合、deny ステートメントとは一致しません。

```
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
```