ファイアウォール AAA ルールの管理

認証、許可、アカウンティング（AAA）ルールを使用すると、IP アドレスではなくユーザ権限に基づいて、ネットワーク リソースへのアクセスを制御できます。認証ルールを設定すると、ユーザは保護されたデバイスの背後にあるネットワークにアクセスしようとするたびに、ユーザ名とパスワードを入力する必要があります。認証後、ネットワーク アクセスがユーザに認可されていることを確認するために、さらにユーザアカウントのチェックを要求することもできます。最後に、アカウンティングルールを使用して、請求、セキュリティ、またはリソース割り当ての目的でアクセスを追跡できます。

AAA ルールの設定は複雑であり、AAA ルール ポリシー以外の設定も必要となります。ここでは、AAA ルールについて詳しく説明し、AAA ルール ポリシーの設定だけでなく関連ポリシーで設定する必要があるものに関する手順を示します。

AAA ルールについて

認証、許可、アカウンティング（AAA）ルールを使用すると、IP アドレスではなくユーザ権限に基づいて、ネットワーク リソースへのアクセスを制御できます。AAA ルールは、従来のアクセス ルールとは異なるタイプの制御を実現します。アクセス ルールでは、許可する IP アドレスとサービスを制御できますが、AAA ルールでは、各ユーザの ACL を設定して、ユーザの接続元 IP アドレスに関係なくユーザごとに認可を定義できます（これらのユーザ単位の ACL は、デバイスに定義される AAA ルールではなく、AAA サーバで設定します）。

AAA ルール ポリシーは、デバイスに向けられたトラフィックではなく、デバイスを通過するトラフィックに AAA ルールが適用されることが、他のデバイス プラットフォームの AAA ポリシーとは異なります。AAA ルールを使用すると、ネットワークへの着信とネットワークからの発信を制御できます。このことは、セキュリティ レベルの高いネットワーク セグメントでアクセスを慎重に制御する必要がある場合に役立ちます。AAA ルールは、請求、セキュリ

ティ、またはリソース割り当ての目的でユーザ単位のアカウンティング レコードを維持する必要がある場合にも役立ちます。

AAA ルール ポリシーでは、実際には3つの異なるタイプのルールを設定します。これらのルールの設定は、IOS デバイスの場合と ASA、PIX、および FWSM デバイスの場合で大きく異なります。IOS デバイスの場合、これらのポリシーではいわゆる認証プロキシ アドミッション コントロールを定義します。共有 AAA ルールを作成する場合は、これらのデバイス タイプに別々のルールを作成します。AAA ルールで設定できるルール タイプは次のとおりです。

- 認証ルール：認証ルールでは、基本的なユーザアクセスを制御します。認証ルールを設定した場合、ユーザは、ルールが定義されているデバイスを接続要求が通過するときにログインする必要があります。HTTP、HTTPS、FTP、または Telnet 接続に対して、ユーザにログインを強制できます。ASA、PIX、および FWSM デバイスの場合、その他のタイプのサービスを制御できますが、ユーザは、まずサポートされているいずれかのプロトコルを使用して認証を受ける必要があり、その後、他のタイプのトラフィックが許可されます。

デバイスがこれらのトラフィック タイプを認識できるのは、デフォルト ポート（FTP（21）、Telnet（23）、HTTP（80）、HTTPS（443））上だけです。これらのタイプのトラフィックを他のポートにマッピングすると、ユーザにプロンプトが表示されず、アクセスは失敗します。

- 認可ルール：認証以外に、追加の制御レベルを定義できます。認証では、ユーザが自身を識別することだけが必要となります。認証に成功すると、認可ルールは、AAA サーバにユーザが試行した接続を完了するのに十分な権限を持っているかどうかを問い合わせることができます。認可に失敗した場合、接続はドロップされます。
  - ASA、PIX、および FWSM デバイスの場合は、AAA ルール ポリシーで直接認可ルールを定義します。認証を必要としないトラフィックの認可が必要な場合、認証されていないトラフィックは常にドロップされます。認証に RADIUS サーバを使用する場合、認可は自動的に実行されるため、認可ルールは必要ありません。認可ルールを設定する場合は、TACACS+ サーバを使用する必要があります。
  - IOS デバイスの場合、認可を設定するには、[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA] ポリシーで認可サーバーグループを設定する必要があります。認可は、認証の対象となる、どのトラフィックに対しても実行されます。TACACS+ または RADIUS サーバを使用できます。
- アカウンティング：認証または認可を設定しない場合でも、アカウンティング ルールを定義できます。認証を設定すると、ユーザごとにアカウンティング レコードが作成されるため、接続を確立した特定のユーザを識別できます。ユーザ認証が実行されない場合、アカウンティング レコードは IP アドレスに基づきます。アカウンティングに TACACS+ または RADIUS サーバを使用できます。
  - ASA、PIX、および FWSM デバイスの場合は、AAA ルール ポリシーで直接アカウンティング ルールを定義します。TCP または UDP プロトコルに対してアカウンティングを実行できます。
  - IOS デバイスの場合、アカウンティングを設定するには、[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA] ポリシーでアカウンティング サーバー グ

ループを設定する必要があります。アカウンティングは、認証の対象となる、どのトラフィックに対しても実行されます。

ユーザの認証方法について

AAA ルールを作成して、ユーザがデバイスから接続を確立しようとしたときに認証を要求する場合、ユーザはクレデンシャル（ユーザ名とパスワード）を入力するよう要求されます。これらのクレデンシャルは、AAA サーバまたはデバイスに設定されているローカル データベースで定義されている必要があります。

ユーザに要求されるのは、HTTP、HTTPS、FTP、および Telnet 接続の場合だけです（認証を要求するようにこれらのプロトコルが設定されている場合）。また、ASA、PIX、およびFWSM デバイスの場合、他のプロトコルの認証を要求することもできます。ただし、その場合、ユーザにはプロンプトが表示されないため、認証を必要とする他のプロトコルの接続を完了するには、まずサポートされている 4 つのプロトコルのいずれかを試して認証に成功する必要があります。

ヒント　ASA、PIX、およびFWSMデバイスの場合、セキュリティアプライアンスからのHTTP、HTTPS、Telnet、またはFTPを許可せず、他のタイプのトラフィックを認証するには、対話型認証を使用するようにインターフェイスを設定して（**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** ポリシー）、ユーザーに HTTP または HTTPS を使用して直接セキュリティアプライアンスで認証を受けるように要求できます。この場合、ユーザーは、次のいずれかの URL を使用して他の接続を試行する前に、アプライアンスで認証されます。*interface_ip* はインターフェイスの IP アドレス、*port* はオプションのポート番号です（[対話型認証（Interactive Authentication）] テーブルのプロトコルにデフォルト以外のポートを指定する場合）：**http://***interface_ip* [**:***port*]**/netaccess/connstatus.html** または **https://***interface_ip* [**:***port*]**/netaccess/connstatus.html**。

デバイスから接続を試行すると、ユーザにはプロトコルに応じてプロンプトが表示されます。

- HTTP：ユーザにユーザ名とパスワードを入力するための Web ページが表示されます。このページは、認証に成功するまで繰り返し表示されます。ユーザが正しく認証されると、ユーザは元の宛先にリダイレクトされます。宛先サーバーにも独自の認証がある場合、ユーザーは別のユーザー名とパスワードを入力します。

ASA、PIX、および FWSM デバイスの場合、セキュリティ アプライアンスは、デフォルトでは基本HTTP認証を使用し、認証プロンプトを表示します。対話型認証を使用するようにインターフェイスを設定し、HTTP トラフィックのリダイレクトを指定すると、ユーザエクスペリエンスを向上できます。これにより、ユーザは認証のためにアプライアンス上でホスティングされている Web ページにリダイレクトされます。対話型認証を使用するようにインターフェイスを設定するには、**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** ポリシー（[AAA Firewall] 設定ページの [Advanced Setting] タブ（27 ページ）を参照）で [対話型認証（Interactive Authentication）] テーブルにインターフェイ

スを追加します。インターフェイスを追加するときに、HTTP およびリダイレクトのオプションを選択してください。

基本 HTTP 認証を継続して使用する例としては、セキュリティ アプライアンスでリスニング ポートを開きたくない場合、ルータで NAT を使用しているのでセキュリティ アプライアンスで処理する Web ページの変換ルールを作成したくない場合、および基本 HTTP 認証とネットワークとの相性がよい場合があります。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。

ただし、基本 HTTP 認証を使用する場合、認証を必要とする HTTP サーバにユーザがアクセスしようとすると、アプライアンスでの認証に使用されたものと同じユーザ名とパスワードが HTTP サーバに送信されます。したがって、ASA と HTTP サーバで同じユーザ名とパスワードが使用される場合を除き、HTTP サーバへのログインは失敗します。この問題を回避するには、ASA に仮想 HTTP サーバーを設定する必要があります。**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA ファイアウォール（AAA Firewall）]** ポリシーを使用して、仮想 HTTP サーバーを設定できます ([AAA Firewall] 設定ページの [Advanced Setting] タブ （27 ページ）を参照)。

ヒント HTTP 認証では、ユーザ名とパスワードがクリア テキストで送信されます。これを防ぐには、**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA ファイアウォール（AAA Firewall）]** ポリシーで [安全な HTTP 認証の使用（Use Secure HTTP Authentication）] オプションを選択します。このオプションを選択すると、クレデンシャルが暗号化されます。

- HTTPS：HTTPS の場合、ユーザ エクスペリエンスは HTTP の場合と同じです。つまり、認証に成功するまでユーザにプロンプトが表示され、ユーザは認証されると元の宛先にリダイレクトされます。

ASA、PIX、および FWSM デバイスの場合、セキュリティ アプライアンスは、カスタム ログイン画面を使用します。HTTP と同様に、対話型認証を使用するようにインターフェイスを設定できます。その場合、HTTPS 接続は HTTP 接続と同じ認証ページを使用します。HTTPS リダイレクト用に個別にインターフェイスを設定する必要があります。設定には**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA ファイアウォール（AAA Firewall）]** ポリシーを使用します。

IOS デバイスの場合、HTTPS 接続が認証されるのは、デバイス上で SSL をイネーブルにし、AAA ルールで HTTP 認証プロキシが必要とされている場合だけです。この設定については、IOS デバイスの AAA ルールの設定 （9 ページ）を参照してください。

- FTP：デバイスは、一度だけ認証を要求します。認証に失敗すると、ユーザは接続を再試行する必要があります。

プロンプトが表示されたら、ユーザはデバイス認証に必要なユーザ名、そのあとに続けてアット マーク（@）、FTP ユーザ名を入力できます（name1@name2）。パスワードについては、

デバイス認証パスワード、そのあとに続けてアットマーク（@）、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> asa1@partreqpassword> letmein@he110

IOSデバイスの場合は、この方法でデバイスとFTPの両方のクレデンシャルを入力する必要があります。ASA、PIX、およびFWSMデバイスの場合は、ファイアウォールが複数のログインを必要とするカスケード形式になっている場合に、この方法が役立ちます。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。

- Telnet：デバイスは、複数回認証を要求します。認証に数回失敗すると、ユーザは接続を再試行する必要があります。認証後、Telnet サーバはユーザ名とパスワードを要求します。**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** ポリシーを使用して、仮想 Telnet サーバーを設定できます ([AAA Firewall] 設定ページの [Advanced Setting] タブ （27 ページ）を参照)。

ASA、PIX、および FWSM デバイスの AAA ルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

ASA、PIX、またはFWSMデバイスのAAAルールを設定する場合は、デバイスからのHTTP、HTTPS、FTP、および Telnet 接続（デバイスへの接続ではない）の確立をどのユーザに許可するかを定義するポリシーを設定します。ネットワーク アクセス認証を完全に設定するには、AAA ルール ポリシーだけでなく、いくつかのポリシーを設定する必要があります。

次の手順では、ネットワークアクセス認証に対応した完全な認証、許可、アカウンティングのサポートを提供するために設定する必要があるすべてのポリシーについて説明します。不要な機能のオプションを設定する必要はありません。

関連項目

- AAA ルールについて （1 ページ）
- ユーザの認証方法について （3 ページ）
- 新しい共有ポリシーの作成
- ポリシー ビューにおけるポリシー割り当ての変更
- ポリシー ビューにおけるポリシー割り当ての変更
- ネットワーク/ホストオブジェクトについて
- インターフェイス ロール オブジェクトについて
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定
- AAA サーバおよびサーバ グループ オブジェクトについて

ステップ 1 次のいずれかを実行して、[AAA Rules] ページ （12 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）]>[AAAルール（AAA Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）]>[AAAルール（AAA Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （17 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールの編集を参照してください。

ステップ 3 ルールを設定します。次に、一般的に判断が必要となる重要な点を示します。フィールドを設定する方法の詳細については、[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （17 ページ）を参照してください。

- 認証（ユーザアイデンティティあり、またはなし）、許可、またはアカウンティングアクション：この規則に適用できるオプションを選択します。認証を選択した場合、ユーザはHTTP、HTTPS、FTP、または Telnet アクセスを試行するときにユーザ名とパスワードの入力を要求されます。認可は追加レベルであり、ユーザ認証後にAAAサーバをチェックして、ユーザにそのタイプのアクセスが認可されていることを確認します。アカウンティングは、AAAサーバに使用状況レコードを生成し、請求、セキュリティ、またはリソース割り当ての目的で使用できます。TCPまたはUDPトラフィックのアカウンティング情報を生成できます。

[認証（Authentication）] を選択すると、[ユーザアイデンティティ（User-Identity）] も選択できます（ASA 8.4(2+) のみ）。このオプションは、ASA がアイデンティティ ファイアウォール ドメイン マッピングで構成されている Active Directory サーバを使用して、ユーザを認証することを示します（Active Directory サーバおよびエージェントの識別を参照）。ユーザがドメイン名を入力すると、そのドメインに関連付けられた AD サーバーが照会されます。それ以外の場合は、デフォルトドメインに関連付けられた AD サーバーが照会されます。[User-Identity] を選択し、[Authorization] または [Accounting] を選択しなかった場合は、AAA サーバ グループを指定しないでください。

- 許可または拒否：識別されたトラフィックを AAA で制御するか（許可）、または AAA 制御から除外するか（拒否）どうか。拒否されたトラフィックは認証を要求されないので認証なしで通過できますが、アクセス ルールによってトラフィックがドロップされる場合があります。
- 送信元アドレスおよび宛先アドレス：トラフィックを生成したアドレスまたはその宛先にかかわらず、ルールを適用する場合は、送信元または宛先に「All-Addresses」を使用します。ルールがホストまたはネットワークに固有の場合は、アドレスまたはネットワーク/ホストオブジェクトを入力します。受け入れられるアドレス形式の詳細については、ポリシー定義中の IP アドレスの指定を参照してください。
- 送信元および宛先のセキュリティグループ（ASA 9.0+ のみ）：送信元および宛先アドレスに加えて、トラフィックのフィルタリングに使用される TrustSec セキュリティグループを指定できます。セキュ

リティグループの詳細については、ポリシーでのセキュリティグループの選択、TrustSec ベースのファイアウォールルールの設定、およびセキュリティ グループ オブジェクトの作成を参照してください。

- 送信元ユーザー（ASA 8.4.2 以降のみ）：Active Directory（AD）ユーザー名（NetBIOS_DOMAIN\username 形式）、ユーザーグループ（NetBIOS_DOMAIN\\user_group）、または名前とグループを定義するアイデンティティ ユーザー グループ オブジェクトを指定して、トラフィックの送信元をさらに定義できます。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。詳細については、アイデンティティ ベースのファイアウォール ルールの設定およびアイデンティティ ユーザ グループ オブジェクトの作成を参照してください。
- サービス：認証ルールと認可ルールのあらゆるサービスタイプを指定できます。ただし、ユーザ認証が要求されるのは、HTTP、HTTPS、FTP、および Telnet 接続の場合だけです。したがって、これらのサービス以外のサービスを指定した場合、ユーザは、まずこれらの接続のいずれかを試して認証（および認可アクションを含めた場合は認可）に成功する必要があります。その後、他のタイプの接続が許可されます。アカウンティング ルールについては、すべてのトラフィック タイプのアカウンティングを実行する場合、TCP または UDP サービス（あるいは単純に TCP と UDP 自体）を指定できます。
- AAA サーバ グループ：認証、許可、またはアカウンティングに使用する AAA サーバ グループ ポリシー オブジェクト。ルールでこれらのアクションを複数適用する場合は、選択したすべてのアクションがサーバ グループでサポートされている必要があります。たとえば、TACACS+ サーバだけが認可規則のサービスを提供でき（ただし、認証規則に RADIUS を使用すると、自動的に RADIUS 認可が含まれます）、TACACS+ および RADIUS サーバだけがアカウンティング サービスを提供できます。アクションごとに異なるサーバ グループを使用する場合は、異なるグループを必要とするアクション タイプごとに別のルールを定義します。
- インターフェイス：ルールを設定するインターフェイスまたはインターフェイス ロール。

ルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、ルールの移動とルール順序の重要性を参照してください。

ステップ 5 （デバイスビューまたはポリシービューで）[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA ファイアウォール（AAA Firewall）] を選択して [AAA Firewall] 設定ページの [Advanced Setting] タブ （27 ページ）を開きます。AAA ファイアウォールを設定します。

- HTTP 認証のルールを設定した場合は、[安全なHTTP認証の使用（Use Secure HTTP Authentication）] を選択する必要があります。これにより、HTTP 認証で入力したユーザ名とパスワードが暗号化されます。このオプションを選択しない場合は、クレデンシャルがクリア テキストで送信されるため、安全性が損なわれます。

ヒント このオプションを選択する場合は、[ユーザー認証のタイムアウト（user authentication timeout）] に 0 を設定（[プラットフォーム（Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）] ポリシーで **timeout uauth 0** を設定）しないでください。設定すると、ユーザーが繰り返し認証を要求され、ネットワーク機能が中断する可能性があります。

- インターフェイス上の HTTP または HTTPS トラフィックの認証を設定した場合は、インターフェイスを [Interactive Authentication] テーブルに追加することを検討してください。インターフェイスで対話型

認証を使用できるようにすると、ユーザには改良された認可 Web ページ（HTTP と HTTPS の両方で同じページ）が表示されます。

[行の追加（Add Row）] をクリックして、インターフェイスをテーブルに追加します。インターフェイスで HTTP または HTTPS トラフィックを受信するか（両方のプロトコルを受信する場合はインターフェイスを 2 回追加します）、およびプロトコルのデフォルト ポート（それぞれ 80 と 443）を使用しない場合は受信するポートを選択します。[認証リクエストにネットワークユーザをリダイレクト（Redirect network users for authentication request）] を選択して、ネットワーク アクセス トラフィックに対して改良された認証プロンプトが表示されるようにします。このオプションを選択しない場合は、このデバイスにログインしようとするユーザにだけプロンプトが表示されます。

（注） 基本 HTTP 認証を継続して使用する例としては、セキュリティ アプライアンスでリスニング ポートを開きたくない場合、ルータで NAT を使用しているのでセキュリティ アプライアンスで処理する Web ページの変換ルールを作成したくない場合、および基本 HTTP 認証とネットワークとの相性がよい場合があります。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。

- FWSM デバイスの場合は、認証を必要とするように設定したプロトコルの認証チャレンジをディセーブルにすることもできます。インターフェイスを [Clear Connections] テーブルに追加して、認証がタイムアウトしたユーザのアクティブな接続をクリアし、ハングしないようにすることもできます。
- Media Access Control（MAC：メディア アクセス コントロール）アドレスに基づいて AAA ルールから一部のデバイスを免除する場合は、[MAC免除リスト（MAC Exempt List）] タブをクリックして [AAA Firewall] ページの [MAC-Exempt List] タブ （34 ページ）を開きます。免除リストの名前を入力し、[行の追加（Add Row）] ボタンをクリックします。次に [Firewall AAA MAC Exempt Setting] ダイアログボックス （36 ページ）に入力し、許可ルールを使用して MAC アドレスをテーブルに追加します。この操作は、信頼できるセキュア デバイスに対して実行できます。

エントリの順序は処理に影響を及ぼします。このため、より広範なエントリにも当てはまるエントリは、テーブル内で、広範なエントリよりも前に配置してください。デバイスは、リストを順番に処理し、最初に一致したものがホストに適用されます。MAC免除リスト内のエントリが処理される方法の詳細については、 [AAA Firewall] ページの [MAC-Exempt List] タブ （34 ページ）を参照してください。

ステップ 6 RADIUS サーバを使用して認証ルールを設定し、ユーザ ポリシーにユーザ単位の ACL 設定を含める場合は、インターフェイスに対してユーザ単位のダウンロード可能 ACL をイネーブルにします（RADIUS 認証には、承認チェックが自動的に含まれます。）ユーザごとの ACL の設定については、http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/access_fwaaa.htmlにある『*Cisco ASA 5500 Series Configuration Guide Using the CLI*』の RADIUS 認証の設定に関する情報を参照してください。

a) （デバイスビューまたはポリシービューで）[ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）] を選択して[Access Control Settings] ページを開きます。

b) インターフェイス テーブルの下にある [Add Row] ボタンをクリックし、[Firewall ACL Setting] ダイアログボックスで少なくとも次のオプションを入力または選択します。

- 認可を実行するインターフェイスまたはインターフェイス ロールを入力します。
- [ユーザ単位のダウンロード可能ACL（Per User Downloadable ACLs）] を選択します。

c) [OK] をクリックして変更を保存します。

IOS デバイスの AAA ルールの設定

IOS デバイスの AAA ルールを設定する場合は、認証プロキシ（AuthProxy）アドミッションコントロールポリシーを設定します。これらのポリシーでは、デバイスからの HTTP、HTTPS、FTP、および Telnet 接続（デバイスへの接続ではない）の確立をどのユーザに許可するかを定義します。認証プロキシを完全に設定するには、AAA ルール ポリシーだけでなく、いくつかのポリシーを設定する必要があります。

次の手順では、認可プロキシ用の完全な認証、許可、アカウンティングのサポートを提供するために設定する必要がある、すべてのポリシーについて説明します。不要な機能のオプションを設定する必要はありません。

関連項目

- AAA ルールについて （1 ページ）
- ユーザの認証方法について （3 ページ）
- 新しい共有ポリシーの作成
- ポリシー ビューにおけるポリシー割り当ての変更
- ネットワーク/ホストオブジェクトについて
- インターフェイス ロール オブジェクトについて
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定
- AAA サーバおよびサーバ グループ オブジェクトについて

ステップ 1 次のいずれかを実行して、[AAA Rules] ページ （12 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）] > [AAA ルール（AAA Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [AAAルール（AAA Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （17 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールの編集を参照してください。

ステップ 3 ルールを設定します。次に、一般的に判断が必要となる重要な点を示します。フィールドを設定する方法の詳細については、[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （17 ページ）を参照してください。

- **認証アクション**：このオプションを選択します。認証ルールは、IOS デバイスの AAA ルール ポリシーで設定できる唯一のルール タイプです。
- 許可または拒否：識別されたトラフィックを AAA で制御するか（許可）、または AAA 制御から除外するか（拒否）どうか。拒否されたトラフィックは認証を要求されないので認証なしで通過できますが、アクセス ルールによってトラフィックがドロップされる場合があります。
- 送信元アドレスおよび宛先アドレス：トラフィックを生成したアドレスまたはトラフィックの宛先にかかわらず、ルールを適用する場合は、送信元または宛先に「All-Addresses」を使用します。ルールがホストまたはネットワークに固有の場合は、アドレスまたはネットワーク/ホスト オブジェクトを入力します。受け入れられるアドレス形式の詳細については、ポリシー定義中の IP アドレスの指定を参照してください。
- 送信元および宛先セキュリティグループ（ASA 9.0 以降のみ）：送信元および宛先アドレスに加えてトラフィックのフィルタ処理に使用される TrustSec セキュリティグループを指定できます。セキュリティグループの詳細については、ポリシーでのセキュリティグループの選択、TrustSec ベースのファイアウォールルールの設定、およびセキュリティ グループ オブジェクトの作成を参照してください。
- 送信元ユーザー（ASA 8.4.2 以降のみ）：Active Directory（AD）ユーザー名（NetBIOS_DOMAIN\username 形式）、ユーザーグループ（NetBIOS_DOMAIN\\user_group）、または名前とグループを定義するアイデンティティ ユーザー グループ オブジェクトを指定して、トラフィックの送信元をさらに定義できます。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。詳細については、アイデンティティ ベースのファイアウォール ルールの設定およびアイデンティティ ユーザ グループ オブジェクトの作成を参照してください。
- サービス：認証ルールと認可ルールのサービスタイプを指定できます。ただし、ユーザー認証が要求されるのは、HTTP、HTTPS、FTP、および Telnet 接続の場合だけです。したがって、これらのサービス以外のサービスを指定した場合、ユーザは、まずこれらの接続のいずれかを試して認証（および認可アクションを含めた場合は認可）に成功する必要があります。その後、他のタイプの接続が許可されます。アカウンティング ルールについては、すべてのトラフィック タイプのアカウンティングを実行する場合、TCP または UDP サービス（あるいは単純に TCP と UDP 自体）を指定できます。
- インターフェイス：ルールを設定するインターフェイスまたはインターフェイス ロール。
- 認証プロキシをトリガーするサービス：ユーザ認証をトリガーするトラフィックのタイプ（HTTP、FTP、または Telnet）のチェックボックスをオンにします。自由に組み合わせて選択できます。HTTPS サポート用のプロキシをトリガーする場合は、[HTTP] を選択し、あとの手順で説明する HTTPS 設定を実行します。

ルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、ルールの移動とルール順序の重要性を参照してください。

ステップ 5 （デバイスビューまたはポリシービューで）[ファイアウォール（Firewall）]>[設定（Settings）]>[AuthProxy] を選択して [AAA] ページ （37 ページ）を開きます。認証プロキシを設定します。

- **認可サーバーグループ**：すべての認証ルールでユーザー認可も実行する場合は、認可を制御する TACACS+ または RADIUS サーバーを識別する AAA サーバー グループ ポリシー オブジェクトのリストを指定します。[LOCAL] を指定して、デバイスに定義されているユーザ データベースを使用することもできます。サーバ グループを指定しない場合は、認可が実行されません。

ヒント AAA サーバでユーザごとに ACL を設定して、各ユーザに適用する権限を定義する必要があります。認可を設定する場合は、サービスとして [auth-proxy] を指定し（service = auth-proxy など）、権限レベルを 15 にします。AAA サーバーを設定する方法と一般的な認証プロキシを設定する方法の詳細については、次の URL にある『Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T』の「Configuring the Authentication Proxy」を参照してください。http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_prxy_ps6441_TSD_Products_Configuration_Guide_Chapter.html

- **アカウンティング サーバー グループ**：すべての認証ルールでアカウンティングを実行する場合は、アカウンティングを実行する TACACS+ または RADIUS サーバーを識別する AAA サーバー グループ ポリシー オブジェクトのリストを指定します。サーバ グループを指定しない場合、アカウンティングは実行されません。アカウンティングを実行する場合は、必要に応じて次のオプションも設定します。
  - 複数のサーバーグループを指定する場合は、[アカウンティングにブロードキャストを使用（Use Broadcast for Accounting）] の選択を検討してください。このオプションを選択すると、アカウンティング レコードが各サーバ グループ内のプライマリ サーバに送信されます。
  - [アカウンティング通知（Accounting Notice）] オプションでは、サーバーにいつ通知するかを定義します。デフォルトでは、接続の開始時と終了時にサーバに通知されますが、終了通知だけを送信するか、またはまったく通知を送信しないかを選択できます。
- 各サービスの認証バナーをカスタマイズすることもできます。[Timeout] タブで、デフォルト アイドルと絶対セッション タイムアウトをグローバルに変更したり、インターフェイスごとに変更したりできます。

ステップ 6 [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA]（ポリシービューでは [ルータ プラットフォーム（Router Platform）] フォルダにあります）を選択して[AAA] ポリシー ページを開きます。[Authentication] タブで次のオプションを設定します。

- [デバイス ログイン認証の有効化（Enable Device Login Authentication）] を選択します。
- 認証を制御するサーバ グループのリスト（プライオリティ順）を入力します。通常は、AuthProxy ポリシーで使用されているのと同じ LDAP、RADIUS、または TACACS+ サーバーグループの少なくとも一部を使用します。ただし、このポリシーでは、デバイス ログイン制御も定義するため、他のサーバ グループの一部を含めることが必要にある場合があります。詳細については、[AAA] ページ - [Authentication] タブを参照してください。

ステップ 7 HTTP 接続で認証プロキシを使用し、HTTPS 接続でもそのプロキシを使用する場合は、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP]（ポリ

シービューでは [ルータプラットフォーム（Router Platform）] フォルダにあります）を選択して[HTTP] ポリシー ページを開きます。次のオプションを設定します。

- [HTTP の有効化（Enable HTTP）] と [SSL の有効化（Enable SSL）] を選択します（まだ選択されていない場合）。
- [AAA] タブで、デバイスへのログインアクセスの設定が適切であることを確認します。AAA を使用してデバイスからのアクセスを制御する場合は、デバイスへのアクセスにその AAA を使用できます。

[AAA Rules] ページ

[AAA Rules] ページを使用して、デバイスインターフェイスの AAA ルールを設定します。AAA ルールでは、ネットワーク アクセス制御（IOS デバイスの認証プロキシと呼ばれる）を設定します。これにより、ユーザはデバイスを通過するネットワーク接続を試行するときに認証が必要になります。認証されたトラフィックに、認可を受けることを要求することもできます（ユーザーが有効なユーザー名とパスワードを入力したあとで、AAA サーバーをチェックして、ユーザーにネットワークアクセスが許可されていることを確認します）。認証されていないトラフィックにもアカウンティングルールを設定して、請求、セキュリティ、およびリソース割り当ての目的で使用できる情報を提供することもできます。

（注） Cisco Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 AAA ルールを設定するための個別のポリシーとオブジェクトが「統合」されました。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスをどちらも使用できる一組の AAA ルールになりました（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更を参照してください）。ポリシービューでは、IPv4 および統合バージョンの AAA ポリシータイプが提供されています。さらに、既存の IPv4 ポリシーの変換に使用できるユーティリティが提供されています（IPv4 ルールから統合ルールへの変換を参照）。次の説明は、特に明記されている場合を除き、AAA ルールテーブルのすべてのバージョンに適用されます。IPv4 AAA ルール共有ポリシーを 9.0 以降のデバイスに割り当てると、それらのポリシーの統合バージョンをそのデバイスに割り当てることはできなくなります。同様に、統合 AAA ルール共有ポリシーを 9.0 以降のデバイスに割り当てると、それらの共有ポリシーの IPv4 バージョンをそのデバイスに割り当てることはできなくなります。そのデバイスは、共有ポリシーの [割り当て（Assignments）] タブの使用可能なデバイスのリストには含まれなくなります。

AAA ルールの設定は複雑であり、オペレーティングシステムによって大きく異なります。AAA ルールを設定する場合には、次の項をよく読んでください。

- AAA ルールについて （1 ページ）
- ユーザの認証方法について （3 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （5 ページ）

- IOS デバイスの AAA ルールの設定 （9 ページ）

ヒント　ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。

ナビゲーション パス

[AAA Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで [ファイアウォール（Firewall）] > [AAAルール（AAA Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [AAAルール（AAA Rules）] を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [AAAルール（AAA Rules）] を選択します。

関連項目

- ルールの追加および削除
- ルールの編集
- ルールの移動とルール順序の重要性
- セクションを使用したルール テーブルの編成
- ルール テーブルの使用
- テーブルのフィルタリング

フィールド リファレンス

表 1 : [AAA Rules] ページ

要素	説明
[すべての行を展開する（Expand all rows）]/[すべての行を折りたたむ（Collapse all rows）]	ルールテーブルのすべてのセクションを展開または折りたたむには、これらのボタンを使用します。 （注）　ボタンは、アクセスルールテーブルの上にある [フィルタ（Filter）] 領域の右上隅にあります。

要素	説明
[競合インジケータ（Conflict Indicator）] アイコン	競合を識別し、競合のタイプをすばやく視覚的に表現します。競合の種類や、この列から実行できるアクションなどの詳細については、自動競合検出についてを参照してください。
番号	順序が付けられたルール番号。
許可（Permit）	定義済みのトラフィックをルールの対象とするか（[Permit]）、またはルールを免除するか（[Deny]）。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。
ソース	このルールのトラフィック ソース。つまり、ネットワーク、セキュリティ グループ（ASA 9.0 以降のみ）、およびユーザーになります。複数のエントリは、テーブル セル内の個別の行に表示されます。
宛先	このルールの宛先。つまり、ネットワークおよびセキュリティ グループになります（ASA 9.0 以降のみ）。複数のエントリは、テーブル セル内の個別の行に表示されます。
サービス	ルールが適用されるトラフィックのプロトコルおよびポートを指定するサービスまたはサービス オブジェクト。複数のエントリは、テーブル セル内の個別の行に表示されます。サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。インターフェイス ロール オブジェクトについてを参照してください。

要素	説明
アクション	このルールで定義される AAA 制御のタイプ： • [Authenticate]：デバイスから接続を確立するユーザは、ユーザ名とパスワードで認証される必要があります。認証を必要とするプロトコルは、[Service] フィールド（ASA/PIX/FWSM デバイスの場合）または [AuthProxy] 方式（IOS デバイスの場合）で定義します。 • [Authorize]：認証済みユーザは、接続の確立が許可されていることを確認するために AAA サーバでもチェックされます（ASA/PIX/FWSM だけ）。 • [Account]：識別されたトラフィックのアカウンティング レコードが AAA サーバに送信されます（ASA/PIX/FWSM だけ）。 既存の AAA ルールの [アクション（Action）] セルを右クリックし、[アクションの編集（Edit Action）] を選択して、選択を変更できます。詳細については、[Edit AAA Option] ダイアログボックス （25 ページ）を参照してください。
[AAA方式（AAA Method）]（IOS） （ASA 9.0 以降のデバイスには表示されません）	このルールの認証方法：Web 認証プロキシ（認証プロキシ）、HTTP 基本認証、または Windows NT LAN Manager（NTLM）
AuthProxy	認証プロキシ方式を使用した認証を必要とするプロトコル。このことは、IOS デバイスにだけ適用されます。 既存の AAA ルールの [認証プロキシ（AuthProxy）] セルを右クリックし、[認証プロキシの編集（Edit AuthProxy）] を選択して、選択を変更できます。詳細については、[AuthProxy] ダイアログボックス （25 ページ）を参照してください。
Server Group	ルールで定義された認証、許可、またはアカウンティングのサポートを提供する AAA サーバ グループ。このグループは、ASA/PIX/FWSM デバイスの場合だけ使用されます。これらのルールで使用する IOS デバイスの AAA サーバの設定については、IOS デバイスの AAA ルールの設定 （9 ページ）を参照してください。 既存の AAA ルールの [サーバーグループ（Server Group）] セルを右クリックし、[サーバーグループの編集（Edit Server Group）] を選択して、選択を変更できます。詳細については、[Edit Server Group] ダイアログボックス （26 ページ）を参照してください。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
説明	ルールの説明（ある場合）。
[最後のチケット（Last Ticket(s)）]	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページを参照）。
ルールテーブルの下のページ要素	
クエリ	ポリシークエリを実行するには、このボタンをクリックします。実行すると、ルールを評価して、効果のないルールを特定できます。ポリシー クエリー レポートの生成を参照してください
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内のさまざまなタイプの項目を検索し、必要に応じてその項目を置換するには、このボタンをクリックします。ルールテーブルの項目の検索と置換を参照してください。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、ルールの移動とルール順序の重要性を参照してください。
[Add Row] ボタン	[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （17 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、ルールの追加および削除を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、ルールの編集を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

右クリックメニュー

右クリックメニューも使用できます。このメニューから、上記の機能の多くにアクセスできます。表示されるオプションは、右クリックした場所によって異なります。

- テーブル内のルールを右クリックすると、右クリックした特定のテーブルセルに関連した編集機能がオプションに含められる場合があります。たとえば、[サーバーグループ（Server

Group）] セルを右クリックすると、コマンド「Edit Server Group」が含められます。詳細については、ルールの編集を参照してください。

- [ルールの結合（Combine Rules）] オプションも右クリックメニューに含まれています。詳細については、ルールの結合を参照してください。

[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス

[Add AAA Rules]/[Edit AAA Rules] ダイアログボックスを使用して、AAA ルールを追加および編集します。AAA ルールの設定は、このダイアログボックスに単に入力するよりも複雑であり、オペレーティング システムによって大きく異なります。AAA ルールを設定する場合には、次の項をよく読んでください。

- AAA ルールについて （1 ページ）
- ユーザの認証方法について （3 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （5 ページ）
- IOS デバイスの AAA ルールの設定 （9 ページ）

ナビゲーション パス

[AAA Rules] ページ （12 ページ）から、[行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ルールの追加および削除
- ルールの編集

フィールド リファレンス

表 2 : [Add AAA Rules]/[Edit AAA Rules] ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	ルールをイネーブルにするかどうか。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。ディセーブルなルールには、ルール テーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。

要素	説明
Action（[Permit]/[Deny]）	定義済みのトラフィックがルールの対象となるか（[Permit]）、またはルールが免除されるか（[Deny]）。 たとえば、HTTP サービスを使用した宛先への 10.100.10.0/24 ネットワークに認証拒否ルールを作成した場合、このネットワーク上のユーザは HTTP 要求時にデバイスでの認証を要求されません。

要素	説明
ソース	

要素	説明

	このルールのトラフィックソースを提供します。ネットワーク、セキュリティグループ、およびユーザーになります。次の 1 つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。
	• ネットワーク – さまざまなネットワーク、ホスト、およびインターフェイスの定義を、個別に、またはオブジェクトとして指定できます。インターフェイス オブジェクトを送信元として選択した場合、ダイアログボックスにタブが表示され、ホスト/ネットワークとインターフェイスが区別されます。
	
	「All-Address」オブジェクトは、ルールを特定のホスト、ネットワーク、またはインターフェイスに制限しません。これらのアドレスは、ホストまたはネットワーク、ネットワーク/ホスト オブジェクト、インターフェイス、またはインターフェイス ロールの IPv4 または IPv6 アドレスです。
	（注） 完全修飾ドメイン名（FQDN）は、FQDN ネットワーク/ホスト オブジェクトまたは FQDN オブジェクトを含むグループオブジェクトを提供することによってのみ指定できます。FQDN を直接入力することはできません。
	これらの定義の詳細については、ネットワーク/ホストオブジェクトについて、ポリシー定義中の IP アドレスの指定、およびインターフェイス ロール オブジェクトについてを参照してください。
	• セキュリティグループ（ASA 9.0 以降）– ルールについて、1 つ以上のソースセキュリティグループの名前またはタグ番号を入力するか選択します（存在する場合）。セキュリティグループの詳細については、ポリシーでのセキュリティグループの選択、TrustSec ベースのファイアウォールルールの設定、およびセキュリティ グループ オブジェクトの作成を参照してください。
	• ユーザー：ルールについて、Active Directory（AD）ユーザー名、ユーザーグループ、またはアイデンティティ ユーザー グループ オブジェクトを入力するか選択します（存在する場合）。次のものを組み合わせて入力できます。
	  • 個別のユーザ名：NetBIOS_DOMAIN\username
	  • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group
	  • アイデンティティ ユーザ グループ オブジェクト名。
	
	詳細については、以下を参照してください。
	• ポリシーでのアイデンティティ ユーザの選択

要素	説明
	• アイデンティティ ベースのファイアウォール ルールの設定 • アイデンティティ ユーザ グループ オブジェクトの作成 （注） これらのフィールドのいずれかに、項目をカンマで区切って複数の値を入力します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックです。
宛先	このルールのトラフィックの宛先を指定します。ネットワークまたはセキュリティグループにすることができます。送信元と同様に、ネットワークおよびセキュリティグループ（ASA 9.0 以降）タイプの 1 つ以上の宛先について、値またはオブジェクト名を入力するかオブジェクトを選択できます。
サービス	動作対象のトラフィックタイプを定義するサービス。サービスオブジェクトおよびサービスタイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力するか選択できます。 項目をカンマで区切って複数の値を入力します。 サービスタイプは、デバイスタイプに基づいて慎重に選択することが重要です。 • IOS デバイスの場合、ダイアログボックスの下部で、認可プロキシのチェックボックスを使用して選択したプロトコルだけが AAA 制御に使用されるため、IP をプロトコルとして使用できます。 • ASA、PIX、およびFWSMデバイスの場合、どのタイプのトラフィックにも認証を強制できますが、セキュリティアプライアンスでプロンプトが表示されるのは、HTTP/HTTPS、FTP、および Telnet トラフィックの場合だけです。これらのサービス以外のサービスを指定した場合、ユーザは、これらのサービスのいずれかを試して認証に成功するまではアプライアンスから接続を確立できません。 アカウンティングのルールだけの場合は、レコードを作成する TCP または UDP プロトコルを指定できます。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。 （注） PIX 6.3 および FWSM デバイスには問題があるため、送信元ポートを使用してサービスを指定した場合、トラフィックは認証されません。そのため、これらのデバイス タイプのルールから CLI が生成される場合、送信元ポートは無視されます。

要素	説明
インターフェイス	ユーザの認証、許可、またはアカウンティングを実行するインターフェイスを識別するインターフェイスまたはインターフェイス ロール。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか新しいインターフェイス ロール オブジェクトを作成します。 ASA および PIX デバイス上の認証ルールの場合、[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA ファイアウォール（AAA Firewall）] ポリシーを使用して、このインターフェイスによる HTTP/HTTPS トラフィックの認証方法を変更できます。インターフェイスを HTTP/HTTPS リスニング ポートとして設定すると、認証のユーザ エクスペリエンスを向上できます。詳細については、ユーザの認証方法について （3 ページ）および [AAA Firewall] 設定ページの [Advanced Setting] タブ （27 ページ）を参照してください。
説明	オプションで入力するルールの説明（最大 1024 文字）。
[認証アクション（Authentication Action）]、[許可アクション（Authorization Action）]、および [アカウンティングアクション（Accounting Action）] チェックボックスでは、デバイスに生成されるルールのタイプを定義します。タイプごとに異なるコマンドセットが生成されますが、複数のオプションを選択すると、このダイアログボックスの他の選択肢は、選択したすべてのアクションでサポートされる選択肢に制限されます。 既存の AAA ルールの [アクション（Action）] セルを右クリックし、[アクションの編集（Edit Action）] を選択して、選択を変更できます。詳細については、[Edit AAA Option] ダイアログボックス （25 ページ）を参照してください。	

要素	説明
認証アクション（Authentication Action） ユーザーアイデンティティ（User-Identity）	• [認証（Authentication）]：ユーザーはデバイスから接続を確立するためにユーザー名とパスワードを入力する必要があります。ASA、PIX、およびFWSMデバイスの場合、[Services]フィールドに入力した情報によって、認証を必要とするプロトコルが決まりますが、プロンプトが表示されるのは、HTTP、HTTPS、FTP、およびTelnet接続の場合だけです。IOSデバイスの場合、いずれのプロトコルが認証を必要とするかは、ダイアログボックスの下部で選択した認可プロキシのチェックボックスに基づきます。 • User-Identity（ASA 8.4(2+) のみ）：ASA デバイスでは、[Authentication Action] を選択した場合、[User-Identity] も選択できます。このオプションは、デバイスが、AAA ルールの AAA サーバーグループ設定の代わりに、アイデンティティ オプション ポリシーで定義されたアイデンティティ ファイアウォール ドメインマッピングを使用してユーザーを認証する必要があることを示します。ユーザーがドメイン名を入力すると、そのドメインに関連付けられた AD サーバーが照会されます。それ以外の場合は、デフォルトドメインに関連付けられたADサーバーが照会されます。Active Directory サーバおよびエージェントの識別を参照してください。
Authorization Action（PIX/ASA/FWSM）	[Authorization]：認証に成功すると、ユーザが要求した接続の確立を許可されているかどうかを確認するためにAAAサーバもチェックされます。認証ルールにRADIUSサーバを指定した場合は、認可ルールを設定しなくても認可が実行されます。TACACS+ サーバを使用している場合は、認可ルールを別途作成する必要があります。
Accounting Action（PIX/ASA/FWSM）	[Accounting]：アカウンティング レコードが [Services] フィールドで指定された TCP および UDP プロトコルの TACACS+ または RADIUS サーバに送信されます。認証も設定する場合、これらのレコードはユーザ単位です。認証を設定しない場合はIPアドレスに基づきます。IOSデバイスの場合、アカウンティングは、AAA ルールではなく [ファイアウォール（Firewall）]>[設定（Settings）]>[ScanSafe Web セキュリティ（ScanSafe Web Security）] ポリシーで設定され、認証プロキシに選択したプロトコルにだけ適用されます。

要素	説明
AAA Server Group（PIX、ASA、FWSM）	ルールで定義されるトラフィックの認証、許可、またはアカウンティングを提供する AAA サーバを定義する AAA サーバ グループ ポリシー オブジェクト。ポリシーオブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストから名前を選択するか、新しいオブジェクトを作成します。 ルールに定義されているすべてのアクションを実行できるサーバのタイプを選択する必要があります。たとえば、（デバイスに定義されている）ローカル データベースでは、認可サービスを提供できません。認証に RADIUS サーバを使用する場合、認可サービスは自動的に提供されますが、RADIUS サーバを使用する認可ルールは定義できません。 同じ送信元/宛先ペアに対する異なるアクションに対して、複数のサーバグループを混在させて使用できます。このことを行うには、認証、許可、アカウンティングアクションを用途に応じて組み合わせ、個別のルールを作成します。AAA サーバ グループ オブジェクトの詳細については、AAA サーバおよびサーバ グループ オブジェクトについてを参照してください。 **ヒント** • [Authenticate] アクションと [User-Identity] を選択し、[Authorization] または [Accounting] アクションを選択しなかった場合、ここで指定したサーバは無視されます。検証時の警告を防止するため、サーバは選択しないでください。 • IOS デバイスの AAA サーバ グループは、他のポリシーで定義されます。設定の詳細については、 IOS デバイスの AAA ルールの設定（9 ページ）を参照してください。 • 既存の AAA ルールの [サーバーグループ（Server Group）] セルを右クリックし、[サーバーグループの編集（Edit Server Group）] を選択して、選択を変更できます。詳細については、[Edit Server Group] ダイアログボックス （26 ページ）を参照してください。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
Method (IOS) （ASA 9.0 以降のデバイスでは表示されません）	認証プロキシ、HTTP Basic、または NTLM を選択します。 認証プロキシを選択する場合、次のオプションを使用できます。 • HTTP • FTP • Telnet 認証プロキシを使用して認証を強制するプロトコルを指定します。HTTP を選択した場合は、デバイスで SSL をイネーブルにして、HTTPS 認証プロキシを設定することもできます。詳細については、IOS デバイスの AAA ルールの設定 （9 ページ）を参照してください。 既存の AAA ルールの [認証プロキシ（AuthProxy）] セルを右クリックし、[認証プロキシの編集（Edit AuthProxy）] を選択して、選択を変更できます。詳細については、IOS デバイスの AAA ルールの設定 （9 ページ）を参照してください。

[Edit AAA Option] ダイアログボックス

[AAAオプションの編集（Edit AAA Option）] ダイアログボックスを使用して、ルールが認証（ユーザ ID あり、またはなし）、許可、またはアカウンティングのうち、いずれのアクションを実行するかを選択します。認可ルールとアカウンティングルールは、ASA、PIX、および FWSM デバイスでだけ機能します。これらのオプションの詳細については、次の項の関連する説明を参照してください。

- [Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （17 ページ）
- AAA ルールについて （1 ページ）

ナビゲーション パス

（[AAA Rules] ページ （12 ページ）で）AAA ルール内の [アクション（Action）] セルを右クリックし、[AAAの編集（Edit AAA）] を選択します。

[AuthProxy] ダイアログボックス

[AuthProxy] ダイアログボックスを使用して、AAA ルール内の認可プロキシ設定を編集します。IOS デバイスの場合、認証プロキシを使用して認証を強制するプロトコル（HTTP、FTP、または Telnet）を選択します。HTTP を選択した場合は、デバイスで SSL をイネーブルにして、HTTPS 認証プロキシを設定することもできます。詳細については、IOS デバイスの AAA ルールの設定 （9 ページ）を参照してください。

ナビゲーション パス

（[AAA Rules] ページ （12 ページ）で）AAA ルール内の [AuthProxy] セルを右クリックし、[AuthProxyの編集（Edit AuthProxy）] を選択します。

[Edit Server Group] ダイアログボックス

[Edit Server Group] ダイアログボックスを使用して、AAA ルールで使用する AAA サーバ グループを編集します。AAA サーバ グループは、ルールで定義されたトラフィックの認証、許可、またはアカウンティングを提供する AAA サーバを提供します。ポリシーオブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストから名前を選択するか、または新しいオブジェクトを作成します。AAA サーバ グループ オブジェクトの詳細については、AAA サーバおよびサーバ グループ オブジェクトについてを参照してください。

ルールに定義されているすべてのアクションを実行できるサーバのタイプを選択する必要があります。たとえば、（デバイスに定義されている）ローカルデータベースでは、認可サービスを提供できません。認証に RADIUS サーバを使用する場合、認可サービスは自動的に提供されますが、RADIUS サーバを使用する認可ルールは定義できません。[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （17 ページ）とは異なり、このダイアログボックスでは選択内容は検証されません。

（注） この設定は、ASA、PIX、および FWSM デバイスにだけ適用されます。IOS デバイスの AAA サーバ グループは、他のポリシーで定義されます。設定の詳細については、IOS デバイスの AAA ルールの設定 （9 ページ）を参照してください。

ナビゲーション パス

（[AAA Rules] ページ （12 ページ）で）AAA ルール内の [サーバーグループ（Server Group）] セルを右クリックし、[サーバーグループの編集（Edit Server Group）] を選択します。

AAA ファイアウォール設定ポリシー

AAA ファイアウォール設定ポリシーの設定は、AAA ルールの動作に影響を及ぼします。

ここでは、次の内容について説明します。

- [AAA Firewall] 設定ページの [Advanced Setting] タブ （27 ページ）
- [AAA Firewall] ページの [MAC-Exempt List] タブ （34 ページ）
- [AAA] ページ （37 ページ）

[AAA Firewall] 設定ページの [Advanced Setting] タブ

AAA ファイアウォール設定ポリシーを使用して、AAA ルール ポリシーの動作を改良するためのオプション設定を指定します。ここでは、[Advanced Setting] タブで使用できる設定について説明します。[MAC Exempt List] タブの詳細については、[AAA Firewall] 設定ページの [Advanced Setting] タブ （27 ページ）を参照してください。

ナビゲーション パス

[AAA Firewall] 設定ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）ASA、PIX、または FWSM デバイスを選択し、**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** を選択します。必要に応じて [詳細設定（Advanced Setting）] タブを選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** の順に選択します。新しいポリシーを作成するか既存のポリシーを選択し、必要に応じて [詳細設定（Advanced Setting）] タブを選択します。
- （マップビュー）ASA、PIX、または FWSM デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [AAAファイアウォール（AAA Firewall）]** を選択し、必要に応じて [詳細設定（Advanced Setting）] タブを選択します。

関連項目

- AAA ルールについて （1 ページ）
- ユーザの認証方法について （3 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （5 ページ）

フィールド リファレンス

表 *3 : [AAA Firewall]* 設定ページの *[Advanced Setting]* タブ

要素	説明
Use Secure HTTP Authentication	セキュリティ アプライアンスを通過する HTTP 要求を行うユーザが、まず SSL（HTTPS）を使用してセキュリティ アプライアンスで認証される必要があるかどうか。ユーザはユーザ名とパスワードの入力を要求されます。 セキュアな HTTP 認証を使用すると、HTTP ベースの Web 要求にセキュリティ アプライアンスの通過を許可する前に、セキュリティ アプライアンスに対するユーザ認証を安全な方法で実行できます。これは HTTP カットスルー プロキシ認証とも呼ばれます。 このオプションを選択する場合は、アクセス ルールによって HTTPS トラフィック（ポート 443）がブロックされないこと、および PAT 設定にもポート 443 が含まれていることを確認してください。また、許可される同時認証の最大数は 16 であり、ユーザー認証のタイムアウトに 0 を設定（**[プラットフォーム（Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）]** ポリシーで **timeout uauth 0** を設定）すると、ユーザーが繰り返し認証を要求され、ネットワーク機能が中断することに注意してください。 **ヒント** このオプションを選択しない場合、HTTP 認証では、ユーザ名とパスワードがクリア テキストで送信されます。
Enable Proxy Limit Maximum Concurrent Proxy Limit per User	プロキシ接続を許可するかどうか。プロキシをイネーブルにする場合は、ユーザごとに許可するプロキシ接続の数に制限を設定する必要があります（1 ～ 128）。デバイスのデフォルトは 16 ですが、数を指定する必要があります。

要素	説明
仮想HTTPの有効化（Enable Virtual HTTP）	仮想 HTTP サーバーを設定するかどうかを指定します。この機能を使用すると、AAA 認証を必要とするすべての HTTP 接続が、ASA 上の仮想 HTTP サーバーにリダイレクトされます。ASA により、AAA サーバーのユーザー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 サーバーがユーザーを認証すると、ASA は HTTP 接続を元のサーバーにリダイレクトして戻しますが、AAA サーバーのユーザー名とパスワードは含めません。HTTP パケットにユーザー名とパスワードが含まれていないため、HTTP サーバーによりユーザーに HTTP サーバーのユーザー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。詳細については、ユーザの認証方法について （3 ページ）を参照してください。 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。 仮想 HTTP サーバーを設定するには、次の手順を実行します。 **1.** [仮想HTTPの有効化（Enable Virtual HTTP）] チェックボックスをオンにします。 **2.** IP アドレスを入力するか、または仮想 HTTP サーバーを表すネットワーク/ホストオブジェクトを選択します。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。 **3.** （任意）リダイレクションが自動的に実行さ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、[警告（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。

要素	説明
仮想Telnetの有効化（Enable Virtual Telnet）	仮想 Telnet サーバーを設定するかどうかを指定します。 認証が済んでいないユーザーが仮想 Telnet IP アドレスに接続すると、ユーザーはユーザー名とパスワードを求められ、その後 AAA サーバーにより認証されます。ユーザーが認証されると、「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。 仮想 Telnet サーバーを設定するには、次の手順を実行します。 **1.** [仮想Telnetの有効化（Enable Virtual Telnet）] チェックボックスをオンにします。 **2.** IP アドレスを入力するか、または仮想 Telnet サーバーを表すネットワーク/ホストオブジェクトを選択します。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、外部サーバー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 Telnet サーバーへの外部アクセスを可能にする場合は、仮想 Telnet サーバーのアドレスとして、グローバル NAT アドレスの 1 つを使用できます。

要素	説明
[Interactive Authentication] テーブル（ASA/PIX 7.2.2+）	このテーブルを使用して、認証対象の HTTP または HTTPS トラフィックを受信するインターフェイスを指定します。AAA ルールがこのテーブルで指定されたインターフェイスにおけるこれらのプロトコルの認証を必要とする場合、ユーザには、アプライアンスで使用されるデフォルトの認証ページではなく、改良された認証 Web ページが表示されます。これらのページは、デバイスへの直接接続の認証にも使用されます。 • インターフェイスをテーブルに追加するには、[行の追加（Add Row）] ボタンをクリックし、[Interactive Authentication Configuration] ダイアログボックス （32 ページ）に入力します。 • 設定を編集するには、設定を選択して [行の編集（Edit Row）] ボタンをクリックします。 • 設定を削除するには、設定を選択して [行の削除（Delete Row）] ボタンをクリックします。
Disable FTP Authentication Challenge Disable HTTP Authentication Challenge Disable HTTPS Authentication Challenge Disable Telnet Authentication Challenge （すべて FWSM 3.x+ だけ）	示されているプロトコルの認証チャレンジをディセーブルにするかどうか。デフォルトでは、AAA ルールが新しいセッションにおけるトラフィックの認証を強制し、トラフィックのプロトコルが FTP、Telnet、HTTP、または HTTPS の場合に、FWSM はユーザにユーザ名とパスワードの入力を要求します。 これらのプロトコルの 1 つ以上に対して認証チャレンジをディセーブルにすることが必要になる場合もあります。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 の認証チャレンジをディセーブルにすると、トラフィックが認証 AAA ルールに含まれている場合に、FWSM では FTP を使用した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。

要素	説明
Clear Connections When Uauth Timer Expires table （FWSM 3.2+ だけ）	このテーブルを使用して、ユーザー認証がタイムアウトするか、または **clear uauth** コマンドで認証セッションをクリア後すぐにアクティブな接続を強制的に終了するインターフェイスと送信元アドレスを指定します。（ユーザー認証のタイムアウトは、**[プラットフォーム（Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）]** ポリシーで定義します）。このテーブルにインターフェイスと送信元アドレスのペアがない場合、ユーザー認証セッションが期限切れになっても、アクティブなセッションは終了しません。 • インターフェイスと送信元アドレスのペアを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Clear Connection Configuration] ダイアログボックス （33 ページ）に入力します。 • 設定を編集するには、設定を選択して [行の編集（Edit Row）] ボタンをクリックします。 • 設定を削除するには、設定を選択して [行の削除（Delete Row）] ボタンをクリックします。

[Interactive Authentication Configuration] ダイアログボックス

[Interactive Authentication Configuration] ダイアログボックスを使用して、HTTP または HTTPS トラフィックを受信してネットワーク ユーザを認証するようにインターフェイスを設定します。リスニング ポートで使用される認証 Web ページでは、これらのプロトコルに使用されるデフォルトの認証ページと比べてユーザエクスペリエンスが向上します。認証ページは、デバイスへの直接接続に使用されます。また、リダイレクション オプションを選択し、かつ、AAA ルール ポリシーで HTTP/HTTPS ネットワーク アクセス認証が必要とされている場合、認証ページはスルー トラフィックにも使用されます。詳細については、 ユーザの認証方法について （3 ページ）を参照してください。

ナビゲーション パス

[AAA Firewall] 設定ページの [Advanced Setting] タブ （27 ページ）に移動し、双方向認証テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- AAA ルールについて （1 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （5 ページ）

フィールド リファレンス

表 4 : *[Interactive Authentication Configuration]* ダイアログボックス

要素	説明
プロトコル	受信するプロトコル（[HTTP] または [HTTPS]）。インターフェイスで両方のプロトコルを受信する場合は、インターフェイスをテーブルに 2 回追加します。
インターフェイス	受信者をイネーブルにするインターフェイスまたはインターフェイスロール。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。
[ポート（Port）]	デフォルト ポート（80（HTTP）および 443（HTTPS））を使用しない場合に、セキュリティ アプライアンスがこのプロトコルを受信するポート番号。
Redirect network users for authentication request	デバイスから要求しているユーザを、セキュリティ アプライアンスが提供する認証 Web ページにリダイレクトするかどうか。このオプションを選択しない場合、インターフェイスに向けられたトラフィックに対してだけ改良された認証 Web ページが表示されます。

[Clear Connection Configuration] ダイアログボックス

[接続設定のクリア（Clear Connection Configuration）] ダイアログボックスを使用して、ユーザー認証がタイムアウトするか、または **clear uauth** コマンドで認証セッションをクリア後すぐにアクティブな接続を閉じる送信元アドレスを指定します。これらのセッションをクリアするインターフェイスを指定する必要があります。これらの設定は、FWSM 3.2+デバイスだけに使用されます。

ユーザー認証のタイムアウトは、**[プラットフォーム（Platform）]>[セキュリティ（Security）]>[タイムアウト（Timeouts）]** ポリシーで定義します。

ナビゲーション パス

[AAA Firewall] 設定ページの [Advanced Setting] タブ （27 ページ）に移動し、[Uauthタイマーの終了時に接続をクリア（Clear Connections When Uauth Timer Expires）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の項目を選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 5 : [Clear Connection Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	設定を行うインターフェイスまたはインターフェイス ロール。名前を入力します。または [選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択するか、または新しいロールを作成します。複数のエントリを指定する場合は、カンマで区切ります。
送信元 IP アドレス/ネットマスク	ユーザ認証のタイマーが切れるとすぐに接続をクリアするホストまたはネットワーク アドレス。リストには、ホスト IP アドレス、ネットワーク アドレス、アドレス範囲、またはネットワーク/ホスト オブジェクトを含めることができます。複数のアドレスを指定する場合は、カンマで区切ります。アドレスを入力する方法の詳細については、ポリシー定義中の IP アドレスの指定を参照してください。

[AAA Firewall] ページの [MAC-Exempt List] タブ

ASA、PIX、および FWSM 3.x+ デバイスの場合、[AAA Firewall] 設定ポリシーの [MAC Exempt List] タブを使用して、認証と認可を免除するホストを指定します。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上で発信される TCP トラフィックを認証し、特定のサーバからの認証されていない TCP 接続を許可する場合は、そのサーバの 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ます。

マスクを使用して、MACアドレスのグループのルールを作成できます。たとえば、MACアドレスが 0003.e3 で始まるすべての Cisco IP Phone を免除する場合は、マスク ffff.ff00.0000 を使用して 0003.e300.0000 の許可ルールを作成します（マスクの f はアドレス内の対応する数と一致し、0 はすべてと一致します）。

拒否ルールが必要になるのは、MACアドレスのグループを許可し、許可されたグループ内に、認証と認可を使用する必要があるいくつかのアドレスがある場合だけです。拒否ルールはトラフィックを禁止しません。ホストに通常の認証と認可を要求するだけです。たとえば、00a0.c95d で始まる MAC アドレスを持つすべてのホストを許可し、00a0.c95d.0282 に認証と認可の使用を強制する場合は、次のルールを順番に入力します。

1. Deny 00a0.c95d.0282 ffff.ffff.ffff
2. Permit 00a0.c95d.0000 ffff.ffff.0000

ポリシーをデバイスに展開すると、**mac-list** および **aaa mac-exempt** コマンドを使用してこれらのエントリが設定されます。

ヒント MAC 免除リストで最初に一致したものが処理されます。このため、エントリの順序が重要となります。MAC アドレスのグループを許可し、その一部を拒否する場合は、許可ルールの前に拒否ルールを配置する必要があります。ただし、Security Manager では、MAC 免除ルールを順序付けることはできません。ルールは示されている順に実装されます。テーブルをソートすると、ポリシーが変更されます。エントリが相互に依存していない場合、このことは重要ではありません。依存している場合は、行を正しい順序で入力してください。

ナビゲーション パス

[MAC Exempt List] タブにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）ASA、PIX、または FWSM デバイスを選択し、[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）] を選択します。[MAC-Exemptリスト（MAC-Exempt List）] タブを選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）] の順に選択します。新しいポリシーを作成するか既存のポリシーを選択し、[MAC-Exemptリスト（MAC-Exempt List）] タブを選択します。
- （マップビュー）ASA、PIX、または FWSM デバイスを右クリックし、[ファイアウォール設定の編集（Edit Firewall Settings）] > [AAAファイアウォール（AAA Firewall）] を選択し、次に [MAC-Exemptリスト（MAC-Exempt List）] タブを選択します。

関連項目

- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （5 ページ）
- テーブルのフィルタリング

フィールド リファレンス

表 *6 : [AAA Firewall]* 設定ページの *[MAC-Exempt List]* タブ

要素	説明
MAC-Exempt List Name	MAC 免除リストの名前。

要素	説明
[MAC Exempt List] テーブル	実装する MAC 免除ルール。テーブルに MAC アドレスとマスク（16 進数）、およびそれらを許可するか（認証と認可を免除するか）または拒否するか（標準の認証と認可を強制するか）が表示されます。エントリはデバイスはによって順番に処理され、最適な一致ではなく、最初に一致するものが使用されます。 • 免除ルールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Firewall AAA MAC Exempt Setting] ダイアログボックス （36 ページ）に入力します。 • 免除ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • 免除ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Firewall AAA MAC Exempt Setting] ダイアログボックス

[Firewall AAA MAC Exempt Setting] ダイアログボックスを使用して、[MAC Exempt List] テーブルの免除エントリを追加および編集します。セキュリティアプライアンスは、許可された MAC アドレスに関連付けられているホストの認証と認可をスキップします。

ナビゲーション パス

[AAA Firewall] ページの [MAC-Exempt List] タブ （34 ページ）に移動し、[MAC免除リスト（MAC Exempt List ）] テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の項目を選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 7: [Firewall AAA MAC Exempt Setting] ダイアログボックス

要素	説明
操作	指定した MAC アドレスを使用するホストに対して実行するアクション： • [Permit]：ホストの認証と認可を免除します。 • [Deny]：ホストに認証と認可を強制します。
MAC アドレス	標準的な 12 桁の 16 進形式のホストの MAC アドレス（00a0.cp5d.0282 など）。完全な MAC アドレスまたはアドレスの一部を入力できます。 アドレスの一部を入力する場合、照合しない桁には 0 を入力できます。

要素	説明
MAC Mask	MAC アドレスに適用するマスク。f は数と正確に一致し、0 はその位置の任意の数と一致します。 • アドレスの完全一致を指定するには、ffff.ffff.ffff を入力します。 • アドレス パターンを照合するには、任意の文字を照合する桁に 0 を入力します。たとえば、ffff.ffff.0000 は、最初の 8 桁が同じであるすべてのアドレスと一致します。

[AAA] ページ

AAA ファイアウォール設定プロキシを使用して、認証プロキシに使用するサーバーやバナーを指定したり、デフォルト以外のタイムアウト値を設定したりします。IOS デバイスの認証プロキシは、ユーザが IOS デバイスから HTTP、Telnet、または FTP 接続を確立しようとするときにユーザにログインと認証を強制するサービスです。ここでの設定は、AAA ルールと組み合わせて機能します。AuthProxy 設定は、AAA ルールでこれらのサービスのいずれかにユーザ認証が必要とされている場合にだけ適用されます。

このポリシーの設定が **[ファイアウォール（Firewall）] > [AAAルール（AAA Rules）]** ポリシーと矛盾していないことを確認してください。さらに、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA]** ポリシーを使用して、ユーザーアクセスの認証に使用する AAA サーバーグループを定義する必要があります。このポリシーでは、許可およびアカウンティングのサーバーグループだけを定義します。HTTPS アクセスにも許可プロキシを使用する場合は、AAA ルールポリシーで HTTP 許可プロキシをイネーブルにするだけでなく、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP]** ポリシーで SSL をイネーブルにし、AAA を設定する必要があります。

ヒント AAA サーバでユーザごとに ACL を設定して、各ユーザに適用する権限を定義する必要があります。許可を設定する場合は、サービスとして [AAA] を指定し（service = AAA など）、権限レベルを 15 にします。AAA サーバーを設定する方法と一般的な認証プロキシを設定する方法の詳細については、次の URL にある『Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T』の「Configuring the Authentication Proxy」を参照してください。
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_proxy_ps6441_TSD_Products_Configuration_Guide_Chapter.html

ナビゲーション パス

[AAA] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで **[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [AAA]** を選択します。

関連項目

- AAA ルールについて （1 ページ）
- ユーザの認証方法について （3 ページ）
- IOS デバイスの AAA ルールの設定 （9 ページ）

フィールド リファレンス

表 *8 : AAA* ファイアウォール設定ポリシー

要素	説明
仮想 IP アドレス（Virtual IP Address）	仮想 IP アドレスは、IOS HTTP 認証とクライアント間の通信でのみ使用します。システムを正常に動作させるには、仮想 IP アドレスを設定する必要がありますが（0.0.0.0 は設定できません）、ネットワーク上の他のデバイスに同じアドレスを使用することはできません。1.1.1.1 など、割り当てられず、使用もされないゲートウェイ IP アドレスを使って設定する必要があります。
[General] タブ	
Authorization Server Groups	ユーザー単位の許可制御を提供する、LDAP、TACACS+ または RADIUS サーバーを識別する AAA サーバー グループ ポリシー オブジェクト。デバイスに定義されている LOCAL ユーザ データベースを使用することもできます。 サーバーグループオブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。グループをプライオリティ順に配置してください。認可は、最初のグループを使用して試行され、そのグループが使用できない場合は、その次のグループが使用されます。

要素	説明
Accounting Server Groups Use Broadcast for Accounting	アカウンティング サービスを提供する、LDAP、TACACS+、またはRADIUS サーバを識別する AAA サーバ グループ ポリシー オブジェクト。アカウンティングでは、請求、セキュリティ、またはリソース割り当ての目的でユーザ単位の使用情報を収集します。サーバーグループオブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 グループをプライオリティ順に配置してください。ブロードキャストオプションを選択しない場合、アカウンティングは、最初のグループを使用して試行され、そのグループが使用できない場合は、その次のグループが使用されます。 [アカウンティングにブロードキャストを使用（Use Broadcast for Accounting）]を選択した場合、アカウンティングレコードが各グループ内の最初のサーバーに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。
Accounting Notice	アカウンティング サーバ グループに送信されるアカウンティング通知のタイプ。 • [Start-stop]：ユーザ プロセスの開始時に開始アカウンティング通知を送信し、プロセスの終了時に終了アカウンティング通知を送信します。start アカウンティングレコードはバックグラウンドで送信されます。要求されたユーザ プロセスは、開始アカウンティング通知をアカウンティング サーバから受信したかどうかにかかわらず開始されます。 • [Stop-only]：要求されたユーザ プロセスの終了時に終了アカウンティング通知を送信します。 • [None]：アカウンティング レコードは送信されません。
HTTP Banner FTP Banner Telnet Banner	ユーザが指定サービスの認証を要求されたときに、認証プロキシページに表示されるバナー。 • [Disable Banner Text]：バナーは表示されません。 • [デフォルトのバナーテキストを使用（Use Default Banner Text）]：デフォルトのバナー「Cisco Systems, *router hostname* Authentication」が表示されます。 • [Use Custom Banner Text]：ユーザに表示されるテキストを入力します。
Use HTTP banner from File URL	HTTP 接続の認証に独自の Web ページを使用するかどうか。独自の HTTP バナーの URL を入力します。 HTTP バナー テキストと URL の両方を設定した場合は、URL バナーが優先されます。ただし、バナー テキストもデバイスに設定されます。

要素	説明
[Advanced] タブ	
Global Inactivity Time	セッションにユーザアクティビティがない場合に、ユーザの認証プロキシが保持される時間の長さ（分単位）。このタイマーが期限切れになると、動的なユーザ アクセス コントロール リスト（ACL）に従ってユーザ セッションがクリアされるので、ユーザは再度認証を受ける必要があります。有効な範囲は 1 ～ 2,147,483,647 です。デフォルトは 60 分です。 このタイムアウト値が**[ファイアウォール（Firewall）]>[設定（Settings）]>[インスペクション（Inspection）]**ポリシーで設定されたアイドルタイムアウト値以上であることを確認してください。アイドルタイムアウト値未満の場合は、タイムアウトしたユーザーセッションのモニタが続行され、最終的にハングする可能性があります。
Global Absolute Time	認証プロキシユーザセッションがアクティブなままでいることのできる時間の長さ（分単位）。このタイマーが期限切れになったあとは、新しいリクエストの場合と同様、ユーザセッションで接続確立のプロセス全体を実行する必要があります。有効な範囲は 0 ～ 35,791 です。デフォルトは 0 で、グローバルな絶対タイムアウトは設定されません。ユーザセッションはアクティブであるかぎり保持されます。
[Interface Timeout] テーブル	このテーブルには、グローバルタイムアウト値とは異なるタイムアウト値を設定するインターフェイスが含まれます。すべてのインターフェイスにグローバル値を使用する場合は、このテーブルに何も設定する必要はありません。 • カスタマイズされたタイムアウト値を持つインターフェイスを追加するには、[行の追加（Add Row）] ボタンをクリックし、 Firewall AAA IOS Timeout Value Setting （40 ページ）に入力します。 • 設定を編集するには、設定を選択して [行の編集（Edit Row）] ボタンをクリックします。 • 設定を削除するには、設定を選択して [行の削除（Delete Row）] ボタンをクリックします。

Firewall AAA IOS Timeout Value Setting

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

[Firewall AAA IOS Timeout Value Setting] ダイアログボックスを使用して、特定のインターフェイスのアイドル タイムアウト値と絶対タイムアウト値を設定します。これらの値は、[ファイアウォール（Firewall）] > [設定（Settings）] > [ScanSafe Webセキュリティ（ScanSafe Web

Security）] ポリシーの [サーバータイムアウト（Server Timeout）] タブで設定されたグローバルタイムアウト値を上書きします。

ナビゲーション パス

[AAA] ページ （37 ページ）の [詳細（Advanced）] タブで、インターフェイスのテーブルの下にある **[**行の追加（Add Row）] ボタンをクリックするか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 9 : [Firewall AAA IOS Timeout Value Setting] ダイアログボックス

要素	説明
インターフェイス	タイムアウト値を設定するインターフェイスまたはインターフェイスロール。インターフェイスまたはロールの名前を入力します。または、[選択（Select）] をクリックしてリストから名前を選択するか、新しいインターフェイスロールを作成します。複数のエントリを指定する場合は、カンマで区切ります。
[Auth Proxy] タブ	
Inactivity/Cache Time	インターフェイス上のセッションにユーザ アクティビティがない場合に、ユーザの認証プロキシが保持される時間の長さ（分単位）。このタイマーが期限切れになると、動的なユーザ アクセス コントロール リスト（ACL）に従ってユーザセッションがクリアされるので、ユーザは再度認証を受ける必要があります。有効な範囲は 1 ～ 2,147,483,647 です。デフォルトは、グローバル非アクティブタイムアウト値（デフォルトは 60 分）です。
Absolute Time	認証プロキシユーザセッションをインターフェイスでアクティブなまま維持できる時間の長さ（分単位）。このタイマーが期限切れになったあとは、新しいリクエストの場合と同様、ユーザセッションで接続確立のプロセス全体を実行する必要があります。有効な範囲は 1 ～ 35,791 です。デフォルトは 0 で、絶対タイムアウトは設定されません。ユーザセッションはアクティブであるかぎり保持されます。
Authentication Proxy Method（IOS）	これらのタイムアウト値を適用するプロトコル。HTTP、FTP、または Telnet を自由に組み合わせて選択できます。
[HTTP/NTLM] タブ	[HTTP] 領域と [NTLM] 領域には、次の同じフィールドと選択項目があります。 HTTP/NTLM の [非アクティブ/キャッシュ時間（Inactivity/Cache Time）] および [絶対時間（Absolute Time）] を設定し、必要な場合には [パッシブ認証の有効化（Enable Passive Authentication）] を選択します。最後に、適用する [IDポリシー（Identity Policy）] を選択します。

要素	説明
[Method Order] タブ	使用する各方式のチェックボックスを選択し、上向きおよび下向き矢印を使用して方式を目的の順序に配置します。
[AAA Settings] タブ	[AAA設定（AAA Settings）] タブを選択して、下の説明に従い、認証、許可、アカウントの設定を指定します。
Authenticate Using	[Authenticate Using] セクションでは、認証に使用するサーバ グループを選択できます。選択肢は次のとおりです。 • なし（None）：認証を行いません。 • [デフォルト（Default）]：デフォルトの認証サーバーグループを使用します。 • [カスタム（Custom）]：ユーザーが指定した認証サーバーグループの選択を有効にします。 次に、[選択（Select）] をクリックして、サーバーグループを指定または追加します。
Authorize Exec Operation Using	[次を使用して実行操作を許可する（Authorize Exec Operation Using）] セクションでは、実行操作の許可に使用するサーバーグループを選択できます。選択肢は次のとおりです。 • [なし（None）]：許可はしません。 • [デフォルト（Default）]：デフォルトの許可サーバーグループを使用します。 • [カスタム（Custom）]：ユーザーが指定した許可サーバーグループの選択を有効にします。 次に、[選択（Select）] をクリックして、サーバーグループを指定または追加します。
Perform Exec Operation Using	[Authorize Exec Operation Using] セクションでは、実行操作の実行に使用するサーバ グループを選択できます。選択肢は次のとおりです。 • [なし（None）]：許可はしません。 • [デフォルト（Default）]：デフォルトのサーバーグループを使用します。 • [カスタム（Custom）]：ユーザーが指定したサーバーグループの選択を有効にします。次に、[選択（Select）] をクリックして、サーバーグループを指定または追加します。

要素	説明
Accounting Notice	[Accounting Notice] を使用して、アカウンティング操作を指定します。 • [なし（None）]：アカウンティング通知は行いません。 • [開始-停止（Start-stop）]：操作の最初と最後にアカウンティング通知を行います。 • [停止のみ（Stop-only）]：操作の最後にのみアカウンティング通知を行います。
Accounting Server Groups	使用するアカウンティング サーバー グループを指定します。アカウンティング サーバー グループを入力または選択します。 （注） アカウンティング サーバ グループを選択する場合、アカウンティング サーバ グループを追加することもできます。
Use Broadcast for Accounting	アカウンティング通知をブロードキャストするには、このチェックボックスを選択します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。