



## AAA

---

AAA（認証、許可、アカウントティング）では、TACACS+ プロトコルと RADIUS プロトコルを使用して、セキュリティ機能がシームレスに統合されます。

CSPM は、AAA を実装して、パススルー トラフィックと管理トラフィックの認証、許可、アカウントティングを実行します。パススルー トラフィックは、発信元から管理対象デバイスを經由して宛先に到達します。管理トラフィックは、CSPM サーバから管理対象デバイスに到達します。



(注)

管理対象デバイスが AAA サーバを使用してセッションを認証する前に、トポロジで TACACS+ または RADIUS クライアント / サーバ製品のタイプを実行するホストを定義する必要があります。

管理対象デバイスに対して通過するセッションの認証を要求するには、AAA パネルを使用します。これらのセッションは、TACACS+ または RADIUS サーバを通して認証します。また、その管理対象デバイス用のすべての管理セッションを、TACACS+ サーバを通して認証するように要求することもできます。

## AAA について

ここでは、AAA（認証、許可、アカウントティング）の概要と、CSPM がどのように TACACS+ プロトコルと RADIUS プロトコルを使用して AAA を実装するかを説明します。AAA アーキテクチャの詳細については、RFC2904 と RFC2989 を参照してください。

AAA では次のサービスが実行されます。

- 認証は、ネットワークまたはネットワーク サービスへのアクセスを許可する前にユーザを識別します。認証は、ユーザ名とパスワード、身元証明要求と応答、メッセージングのサポート、および選択したセキュリティ プロトコルによっては暗号化など、ユーザを識別する方法を提供します。
- 許可は、識別されたユーザの特権が記述されたアトリビュートと値のペアのセットの集合です。これらのアトリビュートと値のペアは、TACACS+ または RADIUS サーバ データベースに保持されている情報と比較されます。



(注) RADIUS サーバは、PIX Firewall を併用した場合の許可をサポートしていません。

- アカウントティングは、ユーザによってアクセスされたサービスおよび消費されたネットワーク リソースを記録します。アカウントティングは、ユーザの ID、開始時刻と停止時刻、実行したコマンド、パケット数、バイト数などの情報を収集し、配布する方法を提供します。

AAA ベースのセキュリティ ソリューションの実装と管理は、ネットワーク要素の数と複雑なデバイス構成によってわかりにくくなっています。しかし、CSPM は、AAA を統合することで、これまで複雑だったデバイスレベルの設定を、簡単で、直感的で、高度な AAA セキュリティ ポリシーに置き換えました。AAA を許可するように CSPM を設定すると、デバイスごとに必要なすべての設定が自動的に生成されます。

AAA に CSPM を実装することで、パススルー トラフィックまたは管理トラフィック用の認証、アカウントティング、および許可を実行できるようになりました。パススルー トラフィックは、発信元から管理対象デバイスを経由して宛先に到達します。管理トラフィックは、CSPM サーバから管理対象デバイスに到達します。



(注) AAA を使用して IPsec ベースのトラフィック フローを認証するには、IPsec トンネル グループ用の IPsec トンネル テンプレートで xauth を有効にする必要があります。

パススルー トラフィックまたは管理トラフィックの認証の詳細については、次の項を参照してください。

- [パススルー トラフィック認証のチェックリスト \(P.24-8\)](#)。パススルー トラフィックを認証するように CSPM を設定する情報を提供します。
- [管理トラフィック認証のチェックリスト \(P.24-10\)](#)。管理トラフィックを認証するように、CSPM を設定する情報を提供します。

CSPM は、AAA サーバと認証プロキシ (いずれもネットワーク トポロジ内) とセキュリティ ポリシーを使用して、AAA をサポートします。AAA サーバは、トポロジ内のホストであり、TACACS+ または RADIUS サービスのいずれかを実行します。認証プロキシは、AAA サービスを要求するクライアントと AAA サーバとの間の通信を行うゲートウェイ デバイスです。最後に、CSPM は、セキュリティ ポリシーを使用して、認証する必要があるトラフィックを定義します。

認証が試行されたときに、次の 3 つのうちのいずれかの理由がある場合は拒否されます。これらは、AAA サーバ データベース内でユーザ名が見つからない場合、ユーザからの要求に不正なユーザ名とパスワードが使用されている場合、管理対象デバイスが AAA サーバに到達できない場合です。管理対象デバイスは、アクティブなサーバを検出するか、またはサーバのリストがすべて終了するまで、サーバを上から下へ順番に照会します。一致するものが見つからなければ、セッション要求は拒否されます。

## RADIUS 認証サーバについて

RADIUS とは、Remote Authentication Dial-In User Service (リモート認証ダイヤルイン ユーザ サービス) の略です。RADIUS は当初リモート ユーザの認証用に設計された、オープンでスケーラブルなクライアント / サーバ セキュリティ システムです。ユーザは共有秘密情報 (ユーザ名とパスワード) を送信することで RADIUS サーバに認証されます。ユーザ認証データおよびセキュリティ情報はすべて、RADIUS サーバの中央データベースに格納されます。

CSPM を使用すると、管理対象デバイスが CSPM を通過するトラフィックの認証に RADIUS サーバを使用することを指定できます。ただし、TACACS+ サーバとは異なり、CSPM サーバと管理対象デバイス間の管理通信の認証に、RADIUS サーバは使用できません。

RADIUS は、Livingston Enterprises によって開発された、オープンでスケーラブルなクライアント / サーバ モードの認証システムです。これは、モデムを使用してネットワーク サービスにアクセスするリモート ユーザを認証するために設計されました。

RADIUS ベースの認証は、秘密のユーザ名とパスワードを RADIUS サーバと呼ばれる中央位置に格納されたデータと比較することによって行われます。RADIUS サーバは認証要求を受信し、RADIUS サーバ データベースに格納された情報に基づいてその要求を許可または拒否します。正しいユーザ名とパスワードを送信すると、RADIUS サーバはサービスを要求しているクライアントに認証の確認応答を返します。

PIX Firewall などの一部の管理対象デバイスでは RADIUS を使用して、ユーザがダイヤルアップ接続を使用しているかどうかに関係なく、そのユーザを認証します。RADIUS ユーザ認証を必要とするネットワーク サービスの要求を受信すると、管理対象デバイスは、ファイアウォールが動作するように設定された RADIUS サーバにユーザ名とパスワードを送信します。RADIUS サーバからの応答に応じて、管理対象デバイスでは要求されたネットワーク サービスを許可するか、またはそのユーザの接続を拒否します。



(注) RADIUS サーバは、PIX Firewall と併用する場合の許可はサポートしていません。

アクティブな RADIUS サーバを使用する場合は、ネットワーク トポロジで RADIUS サーバの配置場所を指定し、管理対象デバイスが認証要求を RADIUS サーバにルーティングできるように設定します。この場合、RADIUS ベースのユーザ認証を必要とする各ネットワーク サービスそれぞれについて、管理対象デバイスでは実際の認証のために要求を RADIUS サーバに転送します。

## TACACS+ 認証サーバについて

TACACS とは、Terminal Access Control Access Control System (ターミナル アクセス コントロール アクセス コントロール システム) の略です。TACACS+ は、個別のサーバを使用して認証シーケンスを実行するユーザ認証のモードです。

CSPM を使用すると、管理対象デバイスが CSPM を通過するトラフィックの認証に TACACS+ サーバを使用することを指定できます。また、管理対象デバイスが TACACS+ サーバを使用して、CSPM サーバと管理対象デバイス間の管理通信を認証することも指定できます。

TACACS+ は、拡張型の許可およびアカウントिंग機能も備えた TCP ベースのユーザ認証モードです。TACACS+ はオープン プロトコルであるため、どのようなユーザ名またはパスワードのデータベースにもポートできます。

TACACS+ 認証は、MD5 暗号化秘密、共有情報 (ユーザ名とパスワードの組み合わせ) を TACACS+ サーバに転送することによって行われます。TACACS+ は ARA、SLIP、PAP、CHAP および標準 Telnet のパスワード タイプを転送できるため、さまざまなクライアントが異なるプロトコルに対して同じユーザ名およびパスワードを使用できます。TACACS+ 認証はさらに、TACACS+ サーバからの複数のチャレンジ応答デマンドもサポートします。

PIX Firewall などの一部の管理対象デバイスでは TACACS+ を使用して、ユーザがダイヤルアップ接続を使用しているかどうかに関係なく、そのユーザを認証できるようにします。管理対象デバイスでは TACACS+ ユーザ認証を必要とするネットワーク サービスのセッション要求を受信すると、管理対象デバイスが動作するように設定された TACACS+ サーバにユーザ名とパスワードを送信します。TACACS+ サーバからの応答に応じて、管理対象デバイスではネットワーク サービス セッションを許可するか、またはユーザに対してその接続を拒否します。

アクティブな TACACS+ サーバを使用する場合は、ネットワーク トポロジで TACACS+ サーバの配置場所を指定し、管理対象デバイスが認証要求を TACACS+ サーバにルーティングできるように設定します。この場合、TACACS+ ユーザ認証を必要とする各ネットワーク サービスそれぞれについて、管理対象デバイスでは実際の認証のために要求をサーバに転送します。

## 仮想アドレスと PIX Firewall

PIX Firewall は、パススルー トラフィックを認証する間、仮想アドレスを使用します。PIX Firewall を認証プロキシとして使用する場合、クライアントが AAA サービスの起動に使用する必要があるプロトコルとして HTTP、FTP、または Telnet を選択できます。HTTP または Telnet を選択すると、PIX Firewall は、仮想 HTTP または Telnet サーバを使用して、クライアントと AAA サーバにおける事前認証通信の間、HTTP または Telnet 要求を代行受信します。

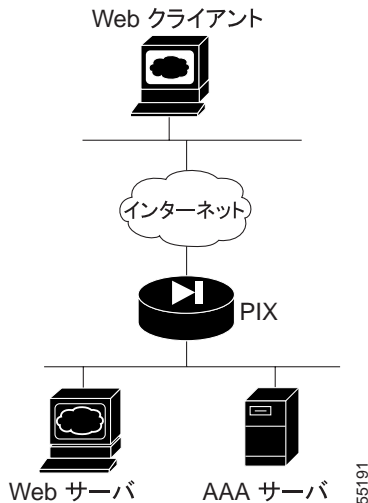
CSPM は、クライアントと認証プロキシとの間の認証トラフィックを許可するコマンドを生成します。ただし、PIX Firewall 上の仮想サーバに対して仮想アドレスを指定する必要があります。

仮想アドレスは、PIX Firewall 上の仮想 HTTP または Telnet サーバの IP アドレスを識別します。仮想アドレスは、要求元のクライアントに最も近い PIX Firewall のインターフェイスにルーティング可能な有効で未使用の IP アドレスです。仮想 HTTP サーバは、HTTP サービスを要求しているユーザを事前認証します。仮想 Telnet サーバは、Telnet サービスを要求しているユーザを事前認証します。

事前認証は、要求に対する早期の拒否を防ぎます。たとえば、Web サーバの場合は、内容を表示する前にログインすることが要求されます。ユーザが Web サーバの内容をブラウズしようとする、HTTP 要求がユーザのコンピュータから Web サーバに送信されます。PIX Firewall はこのトラフィックを代行受信して、AAA ユーザ名とパスワードを要求します。ユーザは、認証用に AAA サーバに送信するユーザ名とパスワードを提供します。しかし、ユーザ名とパスワードは、HTTP トラフィックの一部として送信されるため、Web サーバにも送信されます。AAA ユーザ名とパスワードが Web サーバへのログインに必要なユーザ名とパスワードに一致しない場合、要求は失敗します。仮想 HTTP サーバは、要求が拒否される前に事前認証用の HTTP トラフィックを代行受信することでこの問題を解決します。

**図 24-1** とそれに続くシナリオでは、PIX Firewall が、仮想 HTTP または Telnet サーバを使用してユーザを事前に認証する方法を説明しています。

図 24-1 仮想 HTTP サーバを使用したパススルー トラフィックの認証



PIX Firewall のフレームワークには、基本的な HTTP サーバが組み込まれています。この仮想サーバは、HTTP をサービスとし、Use Authentication を非ターミナルアクションとするポリシー規則で発信元として指定された任意のクライアントからの HTTP 要求を代行受信します。次の一連のイベントでは、上記のトポロジに対するシナリオを説明します。

1. ユーザ (Web クライアント) は、Web サーバ (仮想 IP アドレス) をブラウズします。HTTP 要求を送信することで、Web クライアントはパススルー トラフィック用の認証を開始します。
2. PIX Firewall 上の仮想 HTTP サーバは、接続を代行受信し、要求を AAA 要求と (ユーザ名とパスワード) HTTP 要求 (Web サーバ用のアドレス) の 2 つに分割します。
3. 仮想 HTTP サーバは、AAA 要求を AAA サーバに転送します。
4. 仮想 HTTP サーバは、HTTP 要求を Web サーバに送信します。
5. Web サーバがページに対する要求を受信すると、この要求には認証が必要であることを認識しているため、クライアントに認証要求を送信します。
6. ユーザは、ユーザ名とパスワードを提供します。

- ユーザ名とパスワードが AAA データベース内のユーザ名とパスワードのペアと完全に一致していると、AAA サーバは、PIX Firewall に対してパススルー トラフィックを許可するよう指示し、ユーザは Web サーバのブラウザを許可されます。



(注) 仮想 Telnet サーバの場合も、同じ概念が適用されます。

仮想 HTTP または仮想 Telnet サーバ用の仮想アドレスを選択する場合は、注意する必要があります。ポリシー規則が仮想アドレスと同じアドレスを使用しており、そのアドレスが宛先よりも安全性の低い側にある場合、PIX Firewall へのトラフィックを許可するには NAT 規則を作成する必要があります。

たとえば、P.24-7 の [図 24-1](#) で、Web サーバ (10.10.10.30) を、外部に対しては 30.30.30.30 として知らせる必要があると仮定します。CSPM は、仮想 http 30.30.30.30 コマンドを作成しますが、Web サーバを仮想 IP アドレスにマップするスタティック マッピング規則は作成しません。スタティック マッピング規則がない場合は、Web サーバから PIX Firewall へのトラフィックは正しくルーティングされません。次のスタティック マッピング規則を作成して、Web サーバのアドレスを仮想 HTTP アドレスにマップする必要があります。

図 24-2 仮想アドレス用のスタティック マッピング規則

Rule	Translate object	via interface(s)	using address	through	with	mask
S0	Web Server	outside	30 .30 .30 .30	30 .30 .30 .30	32	

## パススルー トラフィック認証のチェックリスト

管理対象デバイスを通るトラフィックを認証する AAA サーバを指定できません。この AAA の実装では、クライアントは認証プロキシを通してサービスを要求しているポリシー規則の発信元です。認証プロキシは、クライアントと AAA サーバとの間の通信を行うゲートウェイ デバイスです。AAA サーバは、

TACACS+ または RADIUS サービス（認証、認可、アカウントリング）を提供するホストです。AAA サーバは、非ターミナルアクションの Use Authentication を含むポリシー規則で指定されたこれらのサービスを提供します。

次のチェックリストは、パススルー トラフィックを認証するために必要なステップの概要を示しています。ステップ カラムに記載されている各ステップには、いくつかのサブステップが含まれている可能性があり、記載されている順序で実行する必要があります。各ステップの実行時に使用する特定のタスクの参照先は、リファレンス カラムに示されています。

パススルー トラフィックを認証するには、次の手順を実行します。

---

### ステップ 1 AAA サーバのセットアップ

パススルー トラフィックを認証するには、まず適切なサービスを持つネットワーク トポロジ内に AAA サーバを作成する必要があります。次に、認証された管理 トラフィックを受信するように管理対象デバイスを設定します。これには、次のタスクを実行します。

1. AAA サーバ ホストをトポロジに追加します。
2. TACACS+ または RADIUS サービスを AAA サーバ ホストに追加します。

詳細については、次の各項を参照してください。

- [ホストをトポロジに追加する \(P.9-98\)](#)
- [Authentication Server パネル \(P.9-103\)](#)

### ステップ 2 管理対象デバイスの設定

認証プロキシとして動作する各管理対象デバイス用のパススルー トラフィックを認証するための AAA サーバを指定する必要があります。次に、手動で AAA ブートストラップ コマンドを入力します。

詳細については、次の各項を参照してください。

- [AAA サーバを使用したパススルー トラフィックの認証 \(P.24-13\)](#)
- [管理対象デバイスの AAA 用のブートストラップ \(P.24-16\)](#)

### ステップ 3 ポリシーの作成

各管理対象デバイス用に AAA サーバと AAA パラメータを定義しましたが、認証を必要とするサービスは定義していません。このプロセスの最終ステップは、選択したサービスに認証を要求するポリシーを作成し、これらのポリシー規則用にデバイス固有のコマンドセットを生成して、管理対象デバイスにコマンドセットを発行することです。

詳細については、次の各項を参照してください。

- [Policy Wizard \(P.16-2\)](#)
- [アクション \(P.15-13\)](#)

## 管理トラフィック認証のチェックリスト

CSPM サーバとそれが制御する管理対象デバイスとの間の管理トラフィックを AAA サーバが認証するように指定できます。CSPM サーバが提供する認証情報を使用して、管理対象デバイスは TACACS+ サーバを照会します。管理対象デバイスは、アクティブなサーバが見つかるまで、指定された順序で TACACS+ サーバを照会します。アクティブなサーバや一致するユーザ名が見つからない場合、セッション要求は拒否されます。



(注) 管理対象デバイス用の管理トラフィックを認証できるのは、TACACS+ サーバだけです。

次のチェックリストは、管理トラフィックの認証に必要なステップの概要を示しています。ステップ カラムに記載されている各ステップには、いくつかのサブステップが含まれている可能性があり、記載されている順序で実行する必要があります。各ステップの実行時に使用する特定のタスクの参照先は、リファレンス カラムに示されています。

## ステップ 1 AAA サーバのセットアップ

管理トラフィックを認証するには、適切なサービスを持つネットワーク トポロジ内に AAA サーバを作成する必要があります。次に、認証された管理トラフィックを受信するように管理対象デバイスを設定します。これには、次のタスクを実行します。

1. AAA サーバ ホストをトポロジに追加します。
2. TACACS+ サービスをトポロジの AAA サーバ ホストに追加します。

詳細については、次の各項を参照してください。

- [ホストをトポロジに追加する \(P.9-98\)](#)
- [Authentication Server パネル \(P.9-103\)](#)

## ステップ 2 管理対象デバイスの設定

認証済みの管理トラフィックを受信する各管理対象デバイスに対して、管理トラフィックを認証する AAA サーバを指定します。

詳細については、[P.24-14 の「AAA サーバを使用した管理トラフィックの認証」](#)を参照してください。

## ステップ 3 コマンドセットの生成

コマンド セットは、CSPM 設定を保存およびアップデートしたときに自動的に生成されます。

File メニューで Save and Update をクリックしたときに、管理対象デバイスに対してコマンド セットを自動的に発行するよう CSPM を設定した場合は、コマンド セットを生成する前にこの機能をディセーブルにする必要があります。

詳細については、[P.17-8 の「コマンドの生成」](#)を参照してください。

## ステップ 4 管理対象デバイスへのコマンドの発行

コマンド セットを管理対象デバイスに発行するには、次の 2 つのステップを実行します。

まず、各管理対象デバイスを手動でブートストラップします。認証済みのトラフィックを通して管理対象デバイスと通信するように CSPM を設定しているため、CSPM はただちにこれを試行します。しかし、管理対象デバイスは、認証されたトラフィックを受信するように設定されていません。最初のステップで、認証された管理トラフィックを管理対象デバイスが受信できるようにします。

次に、コマンドを管理対象デバイスに発行する必要があります。

各管理対象デバイスに対して次の 2 つのステップを実行することを推奨します。一番遠方にある管理対象デバイスから開始して、一番近い管理対象デバイスで終了するように設定を行います。この場合の遠方とは、CSPM サーバの視点から見て、他の管理対象デバイスの後ろにある管理対象デバイスを示します。

1. 管理対象デバイスをブートストラップします。
2. コマンドセットを管理対象デバイスに発行します。

CSPM から認証された管理トラフィックを受信する各管理対象デバイスに対して、ステップ 1 とステップ 2 を繰り返します。

詳細については、次の各項を参照してください。

- [管理対象デバイスの AAA 用のブートストラップ \(P.24-16\)](#)
  - [コマンドの発行 \(P.17-21\)](#)
-

## AAA のタスク リスト

CSPM 内の AAA に関連する次のタスクを実行できます。タスクを実行するための具体的な手順については、対応するセクションを参照してください。

- [AAA サーバを使用したパススルー トラフィックの認証 \(P.24-13\)](#)
- [AAA サーバを使用した管理トラフィックの認証 \(P.24-14\)](#)
- [管理対象デバイスの AAA 用のブートストラップ \(P.24-16\)](#)
- [管理対象デバイス用の AAA のディセーブル化 \(P.24-20\)](#)



### AAA サーバを使用したパススルー トラフィックの認証

トポロジで定義された 1 台以上の AAA サーバを、選択した管理対象デバイスが自身を通過するトラフィックの認証に使用する AAA サーバとして指定できます。管理対象デバイスは、要求元のユーザが提供した認証情報を使用して、各 AAA サーバを照会します。これらの AAA サーバは、アクティブなサーバが検出されるか、またはサーバのリストが終了するまで順番に照会されます。一致するものが見つからなければ、セッション要求は拒否されます。

管理対象デバイスを通過する認証トラフィックに使用する AAA サーバを指定するには、次の手順を実行します。

---

**ステップ 1** CSPM タスクバーの **Topology** をクリックして、トポロジを表示します。

**ステップ 2** パススルー トラフィックの認証用 AAA サーバを指定する **PIX Firewall** () または **IOS Router** () のアイコンを右クリックし、ショートカットメニューの **Properties** をクリックします。

**ステップ 3** AAA パネルを表示するには、AAA タブをクリックします。

結果：View ペインに AAA パネルが表示されます。

**ステップ 4** パススルー トラフィックの認証に使用するサーバを指定するには、Available AAA servers ボックスのサーバを選択し、AAA servers for pass-through traffic ボックスに対応する **Add** ボタンをクリックします。

結果: AAA サーバが、AAA servers for pass-through traffic ボックスに表示されます。

**ステップ 5** 「*hostname*」ボックス用の AAA Key をアクティブにするには、AAA servers for pass-through traffic ボックスに追加したサーバを選択します。

**ステップ 6** 選択した管理対象デバイスと選択した AAA サーバの間で使用される共有秘密を指定するには、「*hostname*」ボックスの AAA Key に該当するキーを入力します。

この値には、少なくとも 8 文字の英数字を使用する必要がありますが、?、"、タブ文字、および改行文字 (Enter キー) を含むことはできません。

**ステップ 7** AAA servers for pass-through traffic ボックスに追加する各 AAA サーバに対して、ステップ 4 からステップ 6 を繰り返します。

**Move Up** と **Move Down** をクリックして、リスト内のサーバの順序を決定します。照会の順序はトップダウン順で決まります。

**ステップ 8** 変更を適用して AAA パネルを閉じるために、**OK** をクリックします。

**ステップ 9** 変更内容をすべて保存するために、**File> Save** を選択します。

---

## AAA サーバを使用した管理トラフィックの認証



CSPM サーバとそれを制御する管理対象デバイス間の任意の管理トラフィックを認証する AAA サーバを指定できます。CSPM サーバが提供する認証情報を使用して、管理対象デバイスは各 TACACS+ サーバを照会します。TACACS+ サーバは、一致するユーザ名が見つかるか、またはサーバのリストが終了するまで、上から下に照会されます。一致するものが見つからなければ、セッション要求は拒否されます。



(注) 管理対象デバイス用の管理トラフィックを認証できるのは、TACACS+ サーバだけです。

---

管理対象デバイスを制御する管理トラフィックの認証に使用する AAA サーバを指定するには、次の手順を実行します。

- 
- ステップ 1 CSPM タスクバーの **Topology** をクリックして、トポロジを表示します。
- ステップ 2 管理トラフィック認証用の TACACS+ サーバを指定する **PIX Firewall** (  ) のアイコンまたは **IOS Router** (  ) のアイコンを右クリックし、ショートカットメニューの **Properties** をクリックします。
- ステップ 3 AAA パネルを表示するには、**AAA** タブをクリックします。

結果：View ペインに AAA パネルが表示されます。

- ステップ 4 管理トラフィックの認証用 TACACS+ サーバを指定するには、Available AAA servers ボックスでそのサーバを選択して、AAA servers for device administration ボックスに対応する **Add** ボタンをクリックします。



---

(注) 選択した管理対象デバイスのコントロール パネルで AAA ユーザ名とパスワードを指定する必要があります。この情報は、CSPM サーバを TACACS+ サーバに対して認証するときに使用されます。

---

結果：TACACS+ サーバが、AAA servers for device administration ボックスに表示されます。

- ステップ 5 「*hostname*」ボックス用の AAA Key をアクティブにするには、AAA servers for device administration ボックスに追加したサーバを選択します。
- ステップ 6 選択した管理対象デバイスと選択した AAA サーバの間で使用される共有秘密を指定するには、「*hostname*」ボックスの AAA Key に該当するキーを入力します。

この値には、少なくとも 8 文字の英数字を使用する必要がありますが、?、"、タブ文字、および改行文字 (Enter キー) を含むことはできません。

**ステップ 7** AAA servers for device administration ボックスに追加する各 TACACS+ サーバに対して、ステップ 4 からステップ 6 を繰り返します。

**Move Up** と **Move Down** をクリックして、リスト内のサーバの順序を決定します。照会の順序は、上から順に決定されます。

**ステップ 8** 変更を適用して AAA パネルを閉じるために、**OK** をクリックします。

**ステップ 9** 変更内容をすべて保存するために、**File> Save** を選択します。



---

## 管理対象デバイスの AAA 用のブートストラップ

CSPM に AAA を実装したことにより、AAA サービスを要求しているクライアントと AAA サーバ間で通信する認証プロキシとして管理対象デバイスを使用できます。管理対象デバイスは、CSPM サーバからの認証済み管理トラフィックも受信できます。ただし、認証済みのトラフィックを許可できるようにするには、管理対象デバイスがブートストラップされる必要があります。管理対象デバイスをブートストラップするには、AAA パネルを使用して、認証済みの管理トラフィックまたはパススルー トラフィック受信するように管理対象デバイスを設定する必要があります。パススルー トラフィックの場合、非ターミナル アクションが Use Authentication であるポリシー規則を作成して、認証をトリガーするトラフィックを指定する必要があります。次に、ブートストラップ コマンドを管理対象デバイスに手動で入力してから、その管理対象デバイスにコマンド セットを発行する必要があります。CSPM は、管理対象デバイスに必要なコマンドを生成しますが、共有秘密情報が平文で送信されることになるため、コマンドを管理対象デバイスに自動的に配布しません。ブートストラップ コマンドは、管理対象デバイスに関連する Command パネルの Commands/Messages ボックスから使用できます。

認証済みトラフィックを受信するように管理対象デバイスをブートストラップするには、次の手順を実行します。

ステップ 1 CSPM タスクバーの **Topology** をクリックして、トポロジを表示します。

ステップ 2 認証済みトラフィックを受信する **PIX Firewall** () または **IOS Router** () のアイコンを右クリックして、ショートカットメニューの **Properties** をクリックします。

ステップ 3 Command パネルを表示するには、**Command** タブをクリックします。

結果：View ペインに Command パネルが表示されます。

ステップ 4 生成されたコマンドを確認するには、Command Review/Edit ボックスで **Generated Commands** をクリックします。

結果：選択した管理対象デバイスに対して未発行の生成済みコマンドのリストが、Commands/Messages ボックスに表示されます。

ステップ 5 AAA ブートストラップ コマンドを見つけるには、`Device bootstrap configuration` ヘッダーが見えるまで、Commands/Messages ボックスをスクロールダウンします。

ステップ 6 `Device bootstrap configuration` というヘッダーの後に表示されているコマンドのリストをコピーして、.txt ファイルに貼り付けます。



(注) `Device bootstrap configuration` というヘッダーの後にコマンドが表示されない場合は、File メニューの **Save and Update** をクリックして、ポリシー生成処理がエラーを起こさずに完了したかどうか確認してください。ポリシー生成を検証するには、CSPM タスクバーの **Status** をクリックします。それでもコマンドが表示されない場合は、[P.24-8 の「パスルー トラフィック認証のチェックリスト」](#) または [P.24-10 の「管理トラフィック認証のチェックリスト」](#) で示された概略ステップに従っているかどうかを確認します。

ステップ 7 シャープ記号 (#) を各行の先頭から削除します。



## ヒント

---

使用しているテキスト エディタに検索と置換の機能があれば、それを使用すると簡単にすべてのシャープ記号を削除できます。

---

結果：コマンド セットを管理対象デバイスに入力できる状態になります。CSPM がインストールされていないワークステーションから管理対象デバイスにアクセスする場合は、現在のアクセス ポイントから管理対象デバイスにアクセスできる場所、たとえば、フロッピー ディスクや FTP サーバにコマンド セットを保存する必要があります。

- ステップ 8 端末コンソールまたは Telnet セッションを使用して管理対象デバイスにアクセスします。管理対象デバイスにアクセスするとき、パスワード入力求められる場合があります。



---

(注) Telnet はクリア テキストで情報を送信するため、ブートストラップ設定情報は、コンソール端末から入力することを推奨します。

---

- ステップ 9 管理対象デバイスの設定モードに入ります。

PIX Firewall または Cisco IOS ルータで設定モードに入るには、次の手順を実行します。

- a. EXEC モード プロンプトで、**enable** と入力して **Enter** キーを押します。

結果：管理対象デバイスが特権 EXEC モードになります。管理対象デバイスの設定によっては、特権 EXEC モードに入る前に、パスワードの入力を求められる場合があります。



(注) 認証済み管理トラフィック用に Cisco IOS ルータをブートストラップする場合は、ルータのローカル データベースにユーザ名とパスワードが保存されていることを確認する必要があります。CSPM は、予防策として local メソッド タイプで aaa 認証コマンドを追加します。Local は、username コマンドと password コマンドでの定義に従って Cisco IOS ルータがそのローカル データベースを調査する許可を与え、デバイスへのユーザ アクセスを認証できるようにします。ローカル データベースにユーザ名とパスワードを保管することで、すべての AAA サーバがアクセス不能で認証を実行できない場合でも、ユーザは (ローカルに) 認証され、管理対象デバイスにアクセスできます。

- b. グローバル設定モードに入るには、`config t` と入力して Enter キーを押します。

結果：管理対象デバイスがグローバル設定モードになります。

ステップ 10 設定コマンドを入力するには、.txt ファイルからコマンドをコピーして、ターミナル セッションまたは Telnet セッションに貼り付けます。Device bootstrap configuration ヘッダーやヘッダーの上下に表示されている破線は貼り付けないでください。

結果：コマンドが 1 行ずつ管理対象デバイスに入力されます。コマンド セットのコマンドが 1 つずつ入力されるのに従って、管理対象デバイスは、自動的に適切な設定モードになります。

ステップ 11 設定ファイルにラベルを付けて保存します。



(注) AAA 機能をディセーブルにする必要がある場合は、`no aaa new-model` コマンドを手動で発行して、AAA 設定を管理対象デバイスから削除してから、CSPM で AAA 設定を変更し、AAA サーバ グループを削除しなければならないことがあります。AAA 機能をディセーブルにする場合の詳細については、P.24-20 の「管理対象デバイス用の AAA のディセーブル化」を参照してください。

## 管理対象デバイス用の AAA のディセーブル化

パススルー トラフィック用の認証プロキシまたは CSPM からの認証された管理トラフィックの受信者として機能する Cisco IOS ルータまたは PIX Firewall 用の AAA 機能をディセーブルにできます。



(注) Cisco IOS ルータ上に AAA コマンドが存在する場合は、**no aaa new-model** コマンドを発行して、AAA を手動でディセーブルにしないでください。このコマンドは、AAA アクセス制御モデルをディセーブルにして、既存のすべての AAA コマンドを事実上 CSPM から「隠蔽」します。Cisco IOS ルータ用の AAA コマンドを手動でディセーブルにする場合は、**no aaa new-model** コマンドを発行する前にデバイス コンソールを使用して既存の AAA コマンドをすべて削除します。

管理対象デバイスの AAA 機能をディセーブルにするには、次の手順を実行します。



**ステップ 1** AAA 機能が管理トラフィックに対してだけイネーブルである場合は、ステップ 4 に進みます。

**ステップ 2** Use Authentication アクションを削除するポリシー規則のそれぞれに対して、次のステップを実行します。



- a. CSPM タスクバーの Policy をクリックして、Policy Rule テーブルを表示します。
- b. 非ターミナル アクションの Use Authentication が含まれたポリシー規則を見つけるまで、Policy Rule テーブルをスクロールします。
- c. Use Authentication アクションが含まれたポリシー規則の Action カラムをダブルクリックします。  
結果：Action パネルが選択された状態で Policy Wizard が開きます。
- d. Use Authentication アクションを削除するには、AAA チェックボックスをオフにします。

結果：Use Authentication アクションが非表示になります。このポリシー規則によって指定されたトラフィックは、今後認証サービスを必要としません。

**ステップ 3** この管理対象デバイス上のパススルー トラフィックで使用する AAA サービスを削除するには、次の手順を実行します。

- a. CSPM タスクバーの **Topology** をクリックして、トポロジを表示します。
- b. AAA パススルー トラフィック設定をディセーブルにする **PIX Firewall** (  ) または **IOS Router** (  ) のアイコンを右クリックし、ショートカットメニューの **Properties** をクリックします。
- c. AAA パネルを表示するには、**AAA** タブをクリックします。  
結果：View ペインに AAA パネルが表示されます。
- d. AAA servers for pass-through traffic ボックスから AAA サーバをクリックして選択します。  
結果：1 度に選択できるサーバは 1 つだけです。選択したサーバが強調表示され、**Remove** がアクティブになります。
- e. 選択した AAA サーバを削除するには、**Remove** をクリックします。  
結果：選択した AAA サーバが、AAA servers for pass-through traffic ボックスから削除されます。
- f. パススルー トラフィック用に指定された AAA サーバがなくなるまで、ステップ d とステップ e を繰り返します。
- g. 変更内容を適用して選択したパネルを閉じるために、**OK** をクリックします。
- h. 加えた変更に基づいてコマンドを生成するには、**File > Save and Update** を選択します。  
結果：CSPM は、パススルー トラフィック用の AAA 機能の削除に必要なコマンドを生成します。
- i. 管理対象デバイスにコマンドを発行するには、**P.17-21 の「コマンドの発行」** の手順を実行します。  
結果：パススルー トラフィック用の AAA 機能がディセーブルになります。

**ステップ 4** この管理対象デバイス上の管理トラフィックで使用する AAA サービスを削除するには、次の手順を実行します。

- a. CSPM タスクバーの **Topology** をクリックして、トポロジを表示します。
- b. AAA 管理トラフィック設定をディセーブルにする **PIX Firewall** (  ) または **IOS Router** (  ) のアイコンを右クリックし、ショートカットメニューの **Properties** をクリックします。
- c. AAA パネルを表示するには、**AAA** タブをクリックします。  
結果：View ペインに AAA パネルが表示されます。

- d. AAA servers for device administration ボックスから AAA サーバをクリックして選択します。  
結果：1 度に選択できるサーバは 1 つだけです。選択したサーバが強調表示され、Remove がアクティブになります。
  - e. 選択した AAA サーバを削除するには、**Remove** をクリックします。  
結果：選択した AAA サーバが、AAA servers for device administration ボックスから削除されます。
  - f. デバイス管理用に指定された AAA サーバすべてについて、ステップ d とステップ e を繰り返します。
  - g. 変更内容を適用して選択したパネルを閉じるために、**OK** をクリックします。
  - h. 加えた変更に基づいてコマンドを生成するには、**File > Save and Update** を選択します。  
結果：CSPM は、デバイス管理用の AAA 機能の削除に必要なコマンドを生成します。
  - i. AAA 機能をディセーブルにするには、新しく生成されたコマンドを使用して管理対象デバイスをブートストラップします。P.24-16 の「[管理対象デバイスの AAA 用のブートストラップ](#)」の手順を実行します。  
結果：デバイス管理用の AAA 機能がディセーブルになります。
-