PIX 6.2：認証および認可コマンドの設定例

内容

概要

PIXコマンドの許可とローカル認証の拡張は、バージョン6.2で導入されました。このドキュメントでは、PIXでこれを設定する方法の例を示します。以前から使用可能な認証機能も利用できますが、このドキュメントでは説明していません（Secure Shell（SSH）、PC からの IPSec クライアント接続など）。 実行するコマンドは、PIX でローカルに制御することも、TACACS+ を通じてリモートから制御することもできます。RADIUS によるコマンド許可はサポートされていません。これは、RADIUS プロトコルの制限です。

ローカルのコマンド許可を行うには、コマンドとユーザを特権レベルに割り当てます。

リモートのコマンド許可は、TACACS+ の Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サーバを通じて行います。AAA サーバに到達できない場合に備えて、複数の AAA サーバを定義できます。

認証は、以前に設定した IPSec や SSH 接続でも機能します。SSH 認証では、次のコマンドを発行する必要があります。

aaa authentication ssh console <*LOCAL* | *server_tag*>

注：認証にTACACS+またはRADIUSサーバグループを使用する場合、AAAサーバが使用できない場合は、ローカルデータベースをフォールバック方式として使用するようにPIXを設定できます。

次に例を示します。

```
pix(config)#aaa authentication ssh console TACACS+ LOCAL
```

LOCALだけを入力する場合は、ローカルデータベースをメインの認証方式（フォールバックなし）として使用することもできます。

たとえば、ローカル データベースにユーザ アカウントを定義し、SSH 接続にローカル認証を実行するには、次のコマンドを発行します。

```
pix(config)#aaa authentication ssh console LOCAL
```

PIXソフトウェアバージョン5.2から6.2を実行するPIXファイアウォールへのAAA認証アクセスの作成方法と、AAAサーバがダウンした場合の認証、syslog、アクセスの詳細については、『Cisco Secure PIX Firewall(5.2 ～ 6.2)での認証と有効化』を参照してください。

セキュリティ アプライアンスで適用されている変換を確認するには、『PIX/ASA：TACACS+およびRADIUSサーバを使用したネットワークアクセスのカットスループロキシの設定例』を参照してください。

設定が正しく行われていれば、PIX からロックアウトされることはありません。設定を保存しなければ、PIX をリブートしたときに前の設定状況に戻ります。設定ミスが原因で PIX にアクセスできない場合は、「PIX のパスワード復旧手順と AAA 設定の復旧手順」を参照してください。

はじめに

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

前提条件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- PIX ソフトウェア バージョン 6.2
- Cisco Secure ACS for Windows バージョン 3.0（ACS）
- Cisco Secure ACS for UNIX（CSUnix）バージョン 2.3.6

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動していま

す。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

認証/許可を追加する前のテスト

新しい 6.2 の認証/許可機能を実装する前に、次のコマンドを使用して、現在 PIX にアクセスできることを確認します。

```
!--- IP range allowed to Telnet to the PIX (values depend on network). telnet 172.18.124.0
255.255.255.0
!--- Telnet password. passwd <password>
!--- Enable password. enable password <password>
```

特権設定について

PIXのほとんどのコマンドはレベル15ですが、レベル0のコマンドもあります。すべてのコマンドの現在の設定を表示するには、次のコマンドを使用します。

```
show privilege all
```

ほとんどのコマンドは、次の例のように、デフォルトでレベル 15 です。

```
privilege configure level 15 command route
```

次の例のように、少数のコマンドがレベル 0 になっています。

```
privilege show level 0 command curpriv
```

PIX はイネーブル モードと設定モードで動作可能です。show logging など、一部のコマンドは両方のモードで使用できます。このようなコマンドに特権を設定するには、次の例のように、そのコマンドが分類されているモードを指定する必要があります。もう 1 つのモード オプションは enable です。logging is a command available in multiple modes エラー メッセージが表示されます。モードを設定しない場合は、**mode [enable|configure]コマンドを使用**します。

```
privilege show level 5 mode configure command logging
```

次の例では clock コマンドを取り上げています。clock コマンドの現在の設定を確認するには、次のコマンドを発行します。

```
show privilege command clock
```

show privilege command clock の出力から、clock コマンドには次の 3 つの形式が存在することがわかります。

```
!--- Users at level 15 can use the show clock command.

privilege show level 15 command clock
!--- Users at level 15 can use the clear clock command.

Privilege clear level 15 command clock
!--- Users at level 15 can configure the clock !--- (for example, clock set 12:00:00 Jan 01
2001).

privilege configure level 15 command clock
```

認証/許可 - ローカル ユーザ名

clock コマンドの特権レベルを変更する前に、次の例のように、コンソール ポートから管理ユーザを設定して、LOCAL ログイン認証をオンにする必要があります。

```
GOSS(config)# username poweruser password poweruser privilege 15
GOSS(config)# aaa-server LOCAL protocol local
GOSS(config)# aaa authentication telnet console LOCAL
```

次の例のように、ユーザの追加を確認するメッセージが表示されます。

```
GOSS(config)# 502101: New user added to local dbase:
      Uname: poweruser Priv: 15 Encpass: Nimjl8wRa7VAmpm5
```

ユーザ「poweruser」は、PIXにTelnetで接続し、既存のローカルPIXイネーブルパスワード (enable password <*password*>*コマンドのパスワード)を使用してイネーブルモードに入れる必要があります*。

次の例のように、イネーブル モードに入るための認証を追加することで、セキュリティをさらに強化できます。

```
GOSS(config)# aaa authentication enable console LOCAL
```

これによってユーザは、ログインとイネーブルの両方のパスワードの入力が必要になります。この例では、パスワード「poweruser」がログインとイネーブルの両方に使用されています。ユーザ「poweruser」は、PIX に Telnet で接続し、ローカルの PIX パスワードでイネーブル モードに入ることができます。

一部のユーザに対して特定のコマンドの使用のみを許可する場合は、次の例のように、権限の低いユーザを設定します。

```
GOSS(config)# username ordinary password ordinary privilege 9
```

実際にはすべてのコマンドがレベル 15 であるため、「ordinary」ユーザが使用できるように一部のコマンドをレベル 9 に下げる必要があります。ここでは次の例のように、レベル 9 のユーザに対して show clock コマンドの使用は許可し、クロックの再設定は許可しないようにします。

```
GOSS(config)# privilege show level 9 command clock
```

また、次の例のように、ユーザが PIX からログアウトできるようにする必要があります（この操作を行うときのユーザのレベルは 1 または 9 です）。

```
GOSS(config)# privilege configure level 1 command logout
```

次の例のように、ユーザが enable コマンドを使用できるようにする必要があります（この操作を行う際のユーザのレベルは 1 です）。

```
GOSS(config)# privilege configure level 1 mode enable command enable
```

次の例のように、disable コマンドをレベル 1 に移すと、レベル 2 ～ 15 の全ユーザがイネーブル モードから出ることができます。

```
GOSS(config)# privilege configure level 1 command disable
```

ユーザ「ordinary」として Telnet で接続し、同じユーザでイネーブル ユーザとなる場合（パスワードも「ordinary」）、次の例のように privilege configure level 1 command disable を使用する必要があります。

```
GOSS# show curpriv
Username : ordinary
Current privilege level : 9
Current Mode/s : P_PRIV
```

まだ元のセッション（認証を追加する前のセッション）が開いたままの場合、最初にユーザ名を使用してログインしていないため、PIX はこのセッションのユーザを認識できません。このケースで debug コマンドを発行すると、ユーザ「enable_15」または「enable_1」（対応するユーザ名がないユーザ）についてのメッセージが表示されます。そのため、コマンド許可を設定する前にユーザ「poweruser」（「レベル 15」のユーザ）として PIX に Telnet 接続してください。これによって PIX が、実行されるコマンドにユーザ名を対応付けられるようになります。次のコマンドを使用すると、コマンド許可をテストする準備は完了です。

```
GOSS(config)# aaa authorization command LOCAL
```

ユーザ「poweruser」は Telent で接続してイネーブル モードに入り、すべてのコマンドを実行できます。次の例のように、ユーザ「ordinary」は、show clock、enable、disable、および logout コマンドは使用できますが、それ以外のコマンドは使用できません。

```
GOSS# show xlate
Command authorization failed
```

AAA サーバによる認証/許可

AAA サーバを使用してユーザの認証と許可を行うこともできます。コマンド許可が可能なため、TACACS+ が最適ですが、RADIUS も使用できます。次の例のように、PIX に以前の AAA Telnet/console コマンドが残っているかどうかを確認します（これまで LOCAL AAA コマンドを使用していた場合）。

```
GOSS(config)# show aaa
AAA authentication telnet console LOCAL
AAA authentication enable console LOCAL
AAA authorization command LOCAL
```

以前の AAA Telnet/console コマンドが残っている場合は、次のコマンドを使用して、それらのコマンドを削除します。

```
GOSS(config)# no aaa authorization command LOCAL
GOSS(config)# no aaa authentication telnet console LOCAL
GOSS(config)# no aaa authentication enable console LOCAL
```

ローカル認証の設定と同様に、次のコマンドを使用して、ユーザが PIX に Telnet 接続できることを確認します。

```
telnet 172.18.124.0 255.255.255.0
!--- IP range allowed to telnet to the PIX (values would depend on network). passwd <password>
!--- Telnet password. Enable password <password>
!--- Enable password.
```

使用しているサーバに応じて、PIX に AAA サーバを使用した認証と許可を設定します。

ACS - TACACS+

「Authenticate Using」TACACS+(Cisco IOS®ソフトウェア用)を使用して、ネットワーク設定でPIXを定義して、PIXと通信するようにACSを設定します。 ACS ユーザの設定は、PIX の設定によって異なります。ACS ユーザには、少なくともユーザ名とパスワードを設定する必要があります。

PIX では、次のコマンドを使用します。

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host   timeout 10
GOSS(config)# aaa authentication telnet console TACSERVER
```

この時点で、ACS ユーザは PIX に Telnet で接続し、既存のイネーブル パスワードを使用して PIX のイネーブル モードに入り、すべてのコマンドを実行できます。次のステップを実行します。

1. ACSでPIXのイネーブル認証を行う必要がある場合は、Interface Configuration > Advanced

TACACS+ Settingsの順に選択します。
2. Advanced TACACS+ Features in Advanced Configuration Options ボックスにチェックマークを付けます。
3. [Submit] をクリックします。これで、ユーザ設定の下に Advanced TACACS+ Settings が表示されるようになります。
4. AAA クライアントの最大特権をレベル 15 に設定します。
5. ユーザのイネーブル パスワード方式を選択します（別のイネーブル パスワードを設定することもできます）。
6. [Submit] をクリックします。

PIX で TACACS+ を介したイネーブル認証をオンにするには、次のコマンドを使用します。

```
GOSS(config)# aaa authentication enable console TACSERVER
```

この時点で、ACS ユーザは PIX に Telnet で接続し、ACS で設定したパスワードを使用してイネーブル モードに入ることができます。

PIX コマンド許可を追加する前に、ACS 3.0 にパッチを当てる必要があります。パッチは Software Center からダウンロードできます（登録ユーザ専用）。 また、Cisco Bug ID CSCdw78255（登録ユーザ専用）で、このパッチの詳細情報を参照できます。

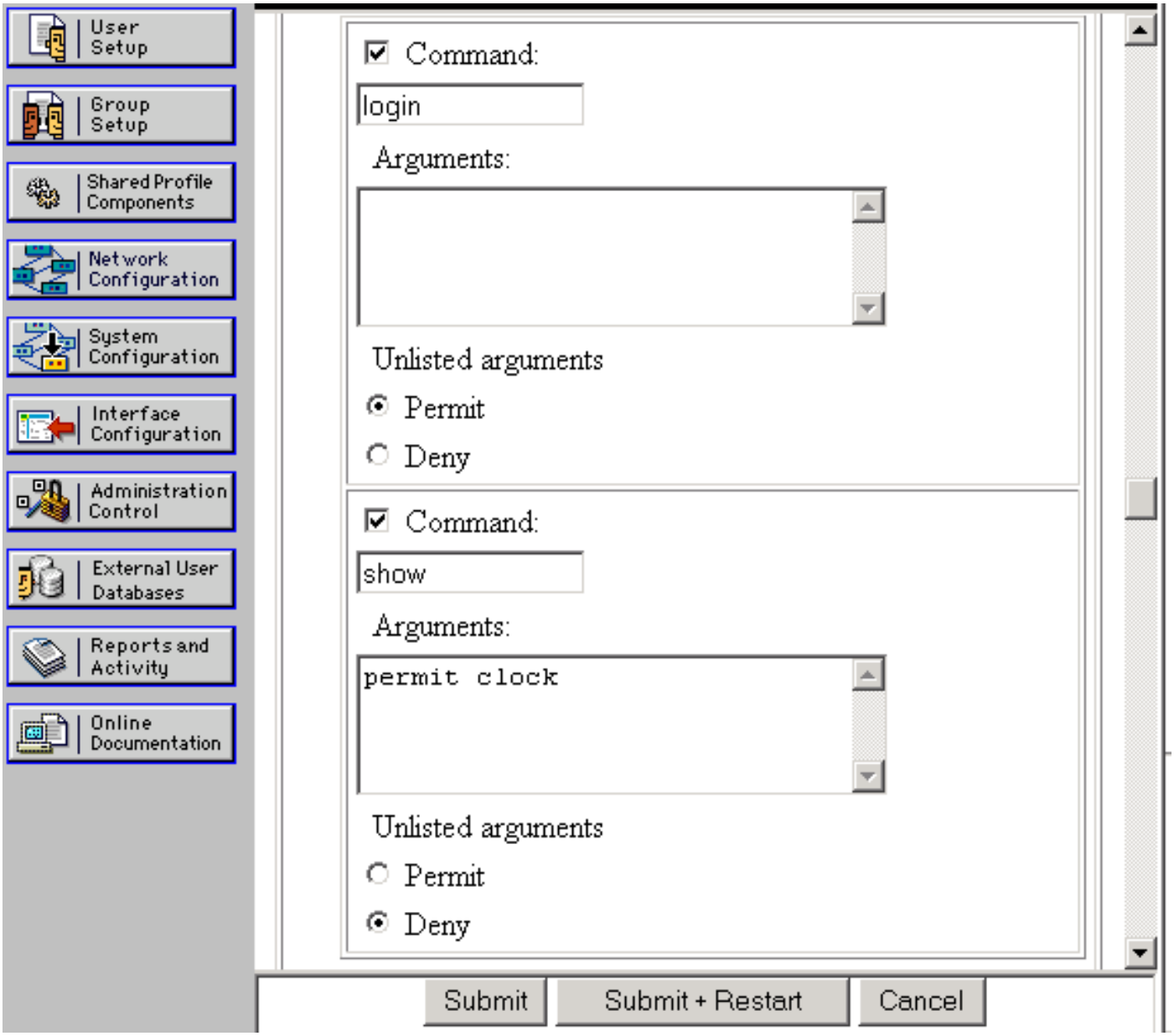
認証は、コマンド許可を行う前に有効になっている必要があります。ACSでコマンド許可を実行する必要がある場合は、ユーザまたはグループに対して**Interface Configuration > TACACS+ (Cisco) > Shell (exec)の順に選択し、Submit**をクリックします。これで、ユーザ（またはグループ）設定の下にシェル コマンド許可設定が表示されるようになります。

コマンド許可用に権限の高い ACS ユーザを少なくとも 1 つ設定し、一般の ACS ユーザよりも格段に豊富な Cisco IOS コマンドを許可することをお勧めします。

他の ACS ユーザには一部のコマンドだけを許可するようにコマンド許可を設定できます。ここでは次の手順を使用しています。

1. Group Settings を選択してドロップダウン ボックスから目的のグループを探します。
2. [Edit Settings] をクリックします。
3. Shell Command Authorization Set を選択します。
4. Command ボタンをクリックします。
5. login と入力します。
6. Unlisted Arguments の下の Permit を選択します。
7. logout、enable、および disable コマンドについて同じ操作を繰り返します。
8. Shell Command Authorization Set を選択します。
9. Command ボタンをクリックします。
10. show と入力します。
11. Arguments の下に permit clock と入力します。
12. Unlisted Arguments の下の deny を選択します。
13. [Submit] をクリックします。

上記の手順の例を次に示します。



まだ元のセッション（認証を追加する前のセッション）が開いたままの場合、最初に ACS ユーザ名を使用してログインしていないため、PIX はこのセッションのユーザを認識できません。このケースで debug コマンドを使用すると、ユーザ「enable_15」または「enable_1」（対応するユーザ名がない場合）についてのメッセージが表示されます。実行するコマンドとユーザ名を PIX が対応付けられるようにする必要があります。コマンド許可を設定する前にレベル 15 の ACS ユーザとして PIX に Telnet 接続すると、この対応付けを行うことができます。次のコマンドを使用すると、コマンド許可をテストする準備は完了です。

```
aaa authorization command TACSERVER
```

この時点で、Telnet 接続および全コマンドを使用できるイネーブル ユーザが 1 人と、5 つのコマンドのみ実行できる 2 番目のユーザが存在します。

CSUnix - TACACS+

他のネットワーク デバイスの場合と同様に、まず CSUnix が PIX と通信できるように設定します。CSUnix ユーザの設定は、PIX の設定によって異なります。CSUnix ユーザには、少なくともユーザ名とパスワードを設定する必要があります。この例では、3 つのユーザがすでに設定されて

います。

```
!--- This is our "poweruser" who can enable, use all commands, and log in. !--- The login
password is in the 'clear "********"' statement. !--- The enable password is in the 'clear
"********" 15' statement. user = pixtest{ password = clear "********" privilege = clear
"********" 15 service=shell { default cmd=permit default attribute=permit } } !--- This user can
Telnet in, enable, and use four commands !--- (such as show clock, logout, exit, and enable). !-
-- The login password is in the 'clear "********"' statement. !--- The enable password is in the
'clear "********" 15' statement.

user = limitpix{
password = clear "********"
privilege = clear "********" 15
service=shell {
cmd=show {
permit "clock"
}
cmd=logout {
permit ".*"
}
cmd=enable {
permit ".*"
}
cmd=exit {
permit ".*"
}
}
}

 !--- This user can Telnet in, but not enable. This user can use any !--- show commands in non-
enable mode as well as logout, exit, and ?.

user = oneuser{
password = clear "********"
service=shell {
cmd=show {
permit ".*"
}
cmd=logout {
permit ".*"
}
cmd="?" {
permit ".*"
}
cmd=exit {
permit ".*"
}
}
}
```

PIX では、次のコマンドを使用します。

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host
```

```
GOSS(config)# aaa authentication telnet console TACSERVER
```

この時点で、いずれかの CSUnix ユーザが PIX に Telnet で接続し、既存のイネーブル パスワードを使用して PIX のイネーブル モードに入り、すべてのコマンドを使用できます。

PIX で TACACS+ を介した認証を有効にします。

```
GOSS(config)# aaa authentication enable console TACSERVER
```

この時点で、「privilege 15」パスワードを持つ CSUnix ユーザが PIX に Telnet で接続し、それぞれの「enable」パスワードでイネーブル モードに入ることができます。

が開いたままの場合このケースで debug コマンドを発行すると、ユーザ「enable_15」または「enable_1」（対応するユーザ名がないユーザ）についてのメッセージが表示される場合があります。コマンド許可を設定する前に、ユーザ「pixtest」（「レベル 15」のユーザ）として PIX に Telnet 接続してください。これによって PIX が、実行されるコマンドにユーザ名を対応付けられるようになります。イネーブル認証は、コマンド許可を行う前に有効になっている必要があります。CSUnix でコマンド許可を実行する必要がある場合は、次のコマンドを追加します。

```
GOSS(config)# aaa authorization command TACSERVER
```

この 3 人のユーザのうち、「pixtest」はすべてのコマンドを実行可能で、他の 2 人のユーザは一部のコマンドのみ実行できます。

ACS - RADIUS

RADIUS によるコマンド許可はサポートされていません。ACS を使用した Telnet とイネーブル認証は可能です。ACS が PIX と通信できるように設定するには、Network Configuration で「Authenticate Using」に RADIUS（どのタイプでも可）を指定して PIX を定義します。 ACS ユーザの設定は、PIX の設定によって異なります。ACS ユーザには、少なくともユーザ名とパスワードを設定する必要があります。

PIX では、次のコマンドを使用します。

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius GOSS(config)
            # aaa-server RADSERVER (inside)
              host
```

```
GOSS(config)# aaa authentication telnet console RADSERVER
```

この時点で、ACSユーザはPIXにTelnetで接続し、PIX上の既存のイネーブルパスワードを使用してイネーブルモードに入り、すべてのコマンドを使用できます(PIXはRADIUSサーバにコマンドを送信しません。RADIUSコマンド許可はサポートされていません)。

PIX で ACS と RADIUS についてイネーブルにするには、次のコマンドを追加します。

```
aaa authentication enable console RADSERVER
```

TACACS+ とは異なり、RADIUS のログインと同じパスワードが RADIUS のイネーブルにも使用されます。

CSUnix - RADIUS

他のネットワーク デバイスの場合と同様に、CSUnix が PIX と通信できるように設定します。CSUnix ユーザの設定は、PIX の設定によって異なります。次のプロファイルは、認証とイネーブル モードへの切り替えに使用できます。

```
user = pixradius{
profile_id = 26
profile_cycle = 1
!--- The login password is in the 'clear "********"' statement; !--- this is used for the login,
enable, and non-enable commands.

password = clear "********" < pixradius
}
```

PIX では、次のコマンドを使用します。

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host
```

PIX で ACS と RADIUS についてイネーブルにするには、次のコマンドを使用します。

```
GOSS(config)# aaa authentication enable console RADSERVER
```

TACACS+ とは異なり、RADIUS のログインと同じパスワードが RADIUS のイネーブルにも使用されます。

ネットワーク アクセス制限

ネットワーク アクセス制限は ACS と CSUnix の両方で使用でき、管理目的で PIX に接続できるユーザを制限します。

- **ACS**:PIXは、Group SettingsのNetwork Access Restrictions領域で設定します。PIX の設定は、「Denied Calling/Point of Access Locations」または「Permitted Calling/Point of Access Locations」のどちらかになります（セキュリティ計画によって異なります）。
- **CSUnix**：これは、PIXへのアクセスは許可されているが、他のデバイスへのアクセスは許可

されていないユーザの例です。

```
user = naruser{
profile_id = 119
profile_cycle = 1
password = clear "********"
privilege = clear "********" 15
service=shell {
allow "10.98.21.50" ".*" ".*"
refuse ".*" ".*" ".*"
default cmd=permit
default attribute=permit
}
}
```

デバッグ

デバッグを有効にするには、次のコマンドを使用します。

```
logging on
logging
```

次に正常な状態と問題発生時のデバッグ例を示します。

- **適切なデバッグ**：ユーザはログインを使用し、イネーブ、およびコマンドを実行できます。
  ```
  307002: Permitted Telnet login session from 172.18.124.111
  111006: Console Login from pixpartial at console
  502103: User priv level changed: Uname: pixpartial From: 1 To: 15
  111009: User 'pixpartial' executed cmd: show clock
  ```
- **Bad debug**：次の例に示すように、ユーザの認可が失敗します。
  ```
  610101: Authorization failed: Cmd: uauth Cmdtype: show
  ```
- **リモートの AAA サーバが到達不能**
  ```
  AAA server host machine not responding
  ```

アカウンティング

現時点で実際にアカウンティングを可能にするコマンドはありませんが、PIX で syslog を有効にすれば、次の例のように、実行された操作を表示できます。

```
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
611103: User logged out: Uname: pixtest
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
502103: User priv level changed: Uname: pixtest From: 1 To: 15
111008: User 'pixtest' executed the 'enable' command.
111007: Begin configuration: 172.18.124.111 reading from terminal
111008: User 'pixtest' executed the 'configure t' command.
```

```
111008: User 'pixtest' executed the 'write t' command.
```

TAC サービス リクエストをオープンする場合に収集する情報

上記のトラブルシューティング手順を実行した後も、依然としてサポートが必要で、Cisco TAC でサービスリクエストをオープンする必要がある場合は、PIX ファイアウォールのトラブルシューティングに必要な次の情報を必ず収集してください。
• 問題の説明と関連するトポロジの詳細 • サービス リクエストをオープンする前に実行したトラブルシューティング • show tech-support コマンドの出力 • **logging buffered debugging コマンド実行後の show log コマンドの出力、あるいは、問題を示すコンソール キャプチャ（採取されている場合）** 収集したデータは、圧縮しないプレーンなテキスト形式（.txt）でサービス リクエストに添付してください。 情報をサービス リクエストに添付するには、TAC Service Request Tool（登録ユーザ専用）を使用してアップロードします。 Service Request Tool にアクセスできない場合は、電子メールへの添付で、attach@cisco.com に情報を送信できます。この場合は、メッセージの件名（Subject）行にサービス リクエスト番号を記入してください。

関連情報

- PIX コマンド リファレンス
- Cisco PIX Firewallソフトウェア：テクニカルサポートとドキュメント
- Cisco Secure Access Control Server for Windows – テクニカルサポートとドキュメント
- Cisco Secure Access Control Server for Unix：テクニカルサポートとドキュメント