TACACS+ を使用したダイヤル認証のための Cisco ルータの設定

内容

概要

このドキュメントでは、UNIX上で稼働するTACACS+を使用したダイヤル認証用にCiscoルータを設定する方法について説明します。TACACS+は、市販されているCisco Secure ACS for WindowsやCisco Secure ACS for UNIXほど多くの機能を提供していません。

これまでシスコから提供されていた TACACS+ は提供が終了しており、シスコのサポートの対象外になっています。

現在は、任意のインターネット検索エンジンで「TACACS+ フリーウェア」を検索すると、フリーウェア バージョンの TACACS+ が多数見つかります。シスコでは、特定の TACACS+ フリーウェア の実装を推奨することは特にしていません。

Cisco Secure Access Control Server（ACS）は通常のシスコ営業担当者および世界各地の販売チャネルを通じて購入できます。Cisco Secure ACS for Windows には、Microsoft Windows ワークステーションへの単体インストールに必要なすべてのコンポーネントが付属しています。Cisco Secure ACS Solution Engine は Cisco Secure ACS のソフトウェア ライセンスがプリインストールされた状態で出荷されます。製品番号についてはCisco Secure ACS 4.0製品速報を参照してください。シスコ発注ホームページ（登録ユーザ専用）からご注文ください。

注：Cisco Secure ACS for Windows（登録ユーザ専用）の90日間の試用版を入手するには、関連するサービス契約を持つCCOアカウントが必要です。

このドキュメントのルータ設定は、Cisco IOS®ソフトウェアリリース11.3.3が稼働するルータで開発されました。Cisco IOSソフトウェアリリース12.0.5.T以降では、**tacacs+の代わりにgroup tacacs+を使用しています。aaa authentication login default tacacs+ enableなどの文は、aaa authentication login default group tacacs+ enableと表示されます。**

TACACS+フリーウェアおよびユーザガイドは、anonymous ftpで/pub/tacacsディレクトリのftp-eng.cisco.comにダウンロードできます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このドキュメントで使用されるコマンドに関する詳細な情報を見つけるには、コマンド検索ツール（登録ユーザ専用）を使用してください。

このドキュメントでは、次の構成を使用します。

- ルータの設定
- フリーウェアサーバのTACACS+設定ファイル

ルータの設定

```
!
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication ppp default if-needed tacacs+
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 1 default tacacs+ if-
authenticated
aaa authorization commands 15 default tacacs+ if-
authenticated
aaa authorization network default tacacs+
enable password ww
!
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
```

```
!
interface Ethernet0
 ip address 10.6.1.200 255.255.255.0
!
 !--- Challenge Handshake Authentication Protocol !---
(CHAP/PPP) authentication user. interface Async1 ip
unnumbered Ethernet0 encapsulation ppp async mode
dedicated peer default ip address pool async no cdp
enable ppp authentication chap ! !--- Password
Authentication Protocol (PAP/PPP) authentication user.
interface Async2 ip unnumbered Ethernet0 encapsulation
ppp async mode dedicated peer default ip address pool
async no cdp enable ppp authentication pap ! !---
Authentication user with autocommand PPP. interface
Async3 ip unnumbered Ethernet0 encapsulation ppp async
mode interactive peer default ip address pool async no
cdp enable ! ip local pool async 10.6.100.101
10.6.100.103 tacacs-server host 171.68.118.101 tacacs-
server timeout 10 tacacs-server key cisco ! line 1
session-timeout 20 exec-timeout 120 0 autoselect during-
login script startup default script reset default modem
Dialin transport input all stopbits 1 rxspeed 115200
txspeed 115200 flowcontrol hardware ! line 2 session-
timeout 20 exec-timeout 120 0 autoselect during-login
script startup default script reset default modem Dialin
transport input all stopbits 1 rxspeed 115200 txspeed
115200 flowcontrol hardware ! line 3 session-timeout 20
exec-timeout 120 0 autoselect during-login autoselect
ppp script startup default script reset default modem
Dialin autocommand ppp transport input all stopbits 1
rxspeed 115200 txspeed 115200 flowcontrol hardware ! end
```

フリーウェアサーバのTACACS+設定ファイル

```
!--- Handshake with router !--- AS needs 'tacacs-server
key cisco'. key = "cisco" !--- User who can Telnet in to
configure. user = admin { default service = permit login
= cleartext "admin" } !--- CHAP/PPP authentication line
1 - !--- password must be cleartext per CHAP
specifications. user = chapuser { chap = cleartext
"chapuser" service = ppp protocol = ip { default
attribute = permit } } !--- PPP/PAP authentication line
2. user = papuser { login = file /etc/passwd service =
ppp protocol = ip { default attribute = permit } } !---
Authentication user line 3. user = authauto { login =
file /etc/passwd service = ppp protocol = ip { default
attribute = permit } }
```

Microsoft Windowsセットアップ

ユーザ1 および2 向けのMicrosoft Windowsセットアップ

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

手順ごとの説明

次に示す手順を実行します。

注：PCの設定は、使用しているオペレーティングシステムのバージョンによって若干異なります。

1. [Start] > [Programs] > [Accessories] > [Dial-Up Networking] を選択して、[Dial-Up Networking]ウィンドウを開きます。
2. [接続]メニューから[新しい接続を作成]を選択し、接続の名前を入力します。
3. モデム固有の情報を入力し、[Configure]をクリックします。
4. [全般のプロパティ]ページで、モデムの最高速度を選択します。ただし、[この速度で接続するのみ]チェックボックスはオンにしないでください。
5. [Configure/Connection Properties]ページで、8データビット、パリティなし、1ストップビットを使用します。使用するコール設定は、[ダイヤルする前にダイヤルトーンを待つ]と[200秒後に接続しない場合はキャンセル]です。
6. [接続]ページで、[詳細設定]をクリックします。[Advanced Connection Settings]で、[Hardware Flow Control]と[Modulation Type Standard]のみを選択します。[Configure/Options properties]ページでは、[Status Control]の下のボックス以外は何もチェックしないでください。
7. [OK]をクリックし、[Next]をクリックします。
8. 通知先の電話番号を入力し、[次へ]をもう一度クリックし、[完了]をクリックします。
9. 新しい接続アイコンが表示されたら、それを右クリックし、[Properties] > [Server Type]を選択します。
10. PPP:WINDOWS 95、WINDOWS NT 3.5、Internetを選択し、Advancedオプションはチェックしません。
11. Allowed Network Protocolsの下のTCP/IPをチェックします。
12. [TCP/IP Settings...]で、[Server assigned IP address] 、[Server assigned name server addresses] 、[Use default gateway on remote network]の順に選択し、[OK]をクリックします。
13. ユーザがアイコンをダブルクリックして[接続先(Connect To)]ウィンドウを表示し、ダイヤルするには、[ユーザ名(User Name)]フィールドと[パスワード(Password)]フィールドに入力し、[接続(Connect)]をクリックします。

ユーザ3 向けのMicrosoft Windowsセットアップ

ユーザ3（autocommand PPPを使用する認証ユーザ）の設定は、次の例外を除き、ユーザ1と2の設定と同じです。

- [Configure/Options properties]ページ（ステップ6）で、[Bring up terminal window after dialing]をオンにします。
- ユーザがアイコンをダブルクリックして[接続先(Connect To)]ウィンドウを開き、ダイヤルすると（ステップ13）、[ユーザ名(User name)]フィールドと[パスワード(Password)]フィールドに入力しません。ユーザが[Connect]をクリックします。ルータへの接続が確立されると、ユーザは黒いウィンドウにユーザ名とパスワードを入力します。認証後、ユーザはContinue (F7)を押す。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ルータ

debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **terminal monitor**：現在のターミナルおよびセッションの**debug**コマンド出力とシステムエラーメッセージを表示します。
- **debug ppp negotiation**:PPPの開始時に送信されるPPPパケットを表示します。PPPの開始時にはPPPオプションがネゴシエートされます。
- **debug ppp packet**：送受信されたPPPパケットを表示します。（このコマンドは、下位レベルのパケット ダンプを表示します。）
- **debug ppp chap**：クライアントが認証（Cisco IOSソフトウェアリリース11.2より前）を通過しているかどうかに関する情報を表示します。
- **debug aaa authentication**：認証、許可、アカウンティング(AAA)/TACACS+認証に関する情報を表示します。
- **debug aaa authorization**：AAA/TACACS+ 許可に関する情報を表示します。

サーバ

注： これは、シスコのTACACS+ Freewareサーバコードを前提としています。

```
tac_plus_executable -C config.file -d 16
  tail -f /var/tmp/tac_plus.log
```

関連情報

- **TACACS+ に関するサポート ページ**
- **IOS での TACACS+ に関するドキュメント**
- Cisco Secure Access Control Server
- CiscoSecure 2.x TACACS+のセットアップおよびデバッグ
- テクニカル サポートとドキュメント – Cisco Systems