TACACS+를 사용하여 다이얼 인증을 위해 Cisco 라우터 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[구성](#)
[Microsoft Windows 설치](#)
[사용자 1 및 2용 Microsoft Windows 설치](#)
[단계별 지침](#)
[사용자 3용 Microsoft Windows 설치](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[라우터](#)
[서버](#)
[관련 정보](#)

소개

이 문서에서는 UNIX에서 실행되는 TACACS+를 사용하여 다이얼 인증을 위해 Cisco 라우터를 구성하는 방법에 대해 설명합니다.TACACS+는 상업적으로 사용 가능한 Cisco Secure ACS for Windows 또는 UNIX용 Cisco Secure ACS만큼 많은 기능을 제공하지 않습니다.

이전에 Cisco Systems에서 제공한 TACACS+ 소프트웨어는 중단되었으며 Cisco Systems에서 더 이상 지원하지 않습니다.

오늘날 자주 사용하는 인터넷 검색 엔진에서 "TACACS+ 프리웨어"를 검색할 때 사용 가능한 TACACS+ 프리웨어 버전이 많이 있습니다.Cisco에서는 특정 TACACS+ 프리웨어 구현을 특별히 권장하지 않습니다.

Cisco ACS(Secure Access Control Server)는 전 세계의 일반 Cisco 영업 및 유통 채널을 통해 구매할 수 있습니다.Windows용 Cisco Secure ACS에는 Microsoft Windows 워크스테이션의 독립적인 설치에 필요한 모든 구성 요소가 포함되어 있습니다.Cisco Secure ACS Solution Engine은 사전 설치된 Cisco Secure ACS 소프트웨어 라이센스와 함께 제공됩니다.제품 번호는 Cisco Secure ACS 4.0 제품 게시판을 참조하십시오.Cisco Ordering Home Page(등록된 고객만 해당)를 방문하여 주문하십시오.

참고: Cisco Secure ACS for Windows의 90일 평가판 버전을 받으려면 연결된 서비스 계약이 있는 CCO 계정(등록된 고객만 해당)이 필요합니다.

이 문서의 라우터 컨피그레이션은 Cisco IOS® 소프트웨어 릴리스 11.3.3을 실행하는 라우터에서 개발되었습니다. Cisco IOS 소프트웨어 릴리스 12.0.5.T 이상에서는 **tacacs+** 대신 **그룹 tacacs+를** 사용합니다.aaa **authentication login default tacacs+ enable**과 같은 명령문은 **aaa authentication login default group tacacs+ enable**로 **표시됩니다**.

익명 ftp를 통해 /pub/tacacs 디렉토리의 ftp-eng.cisco.com에 TACACS+ 프리웨어 및 사용자 가이드를 다운로드할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 추가 정보를 찾습니다.

이 문서에서는 다음 구성을 사용합니다.

- 라우터 컨피그레이션
- Freeware 서버의 TACACS+ 구성 파일

라우터 컨피그레이션

```
!
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
```

Freeware 서버의 TACACS+ 구성 파일

```
!--- 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 설치

사용자 1 및 2용 Microsoft Windows 설치

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

단계별 지침

다음 단계를 완료합니다.

참고: PC 구성은 사용하는 운영 체제 버전에 따라 약간 다를 수 있습니다.

1. **시작 > 프로그램 > 보조프로그램 > 전화 접속 네트워킹**을 선택하여 전화 접속 네트워킹 창을 엽니다.
2. Connections 메뉴**에서 Make New Connection**(새 연결 만들기)을 선택하고 연결 이름을 입력합니다.
3. 모뎀별 정보를 입력하고 구성을 **클릭합니다**.
4. 일반 속성 페이지에서 모뎀의 최고 속도를 선택하되 **이 속도로만 연결**.. 확인란을 선택하지 마십시오.
5. Configure/Connection Properties(구성/연결 속성) 페이지에서 8개의 데이터 비트, 패리티 없음 및 1개의 정지 비트를 사용합니다.사용할 통화 기본 설정은 **전화 걸기 전 신호음 대기**와 **200초 후 연결되지 않은 경우 통화 취소 입니다**.
6. 연결 페이지에서 **고급**을 클릭합니다.Advanced Connection Settings(고급 연결 설정)에서 Hardware **Flow Control(하드웨어 흐름 제어**)과 Modulation Type Standard(**변조 유형 표준)만** 선택합니다.Configure/Options 속성 페이지에서 Status Control 아래의 상자를 제외하고 아무것도 선택하지 않아야 합니다.
7. OK(**확인)**를 클릭한 다음 **Next(다음)**를 클릭합니다.
8. 대상의 전화 번호를 입력하고 **Next(다음)**를 다시 클릭한 다음 **Finish(마침)**를 클릭합니다.
9. 새 연결 아이콘이 나타나면 마우스 오른쪽 단추를 클릭하고 Properties(속성) **> Server Type(서버 유형)을** 선택합니다.
10. PPP**:WINDOWS 95, WINDOWS NT 3.5, Internet을 선택하고** 고급 옵션을 선택하지 않습니다.
11. Allowed **Network** Protocols 아래에서 **TCP/IP**를 선택합니다.
12. TCP/IP Settings..(TCP/IP 설정...)에서 **Server assigned IP address(서버 할당 IP 주소)**, Server assigned name server addresses(**서버 할당 이름 서버 주소)**, **Use default gateway on remote network(원격 네트워크에서 기본 게이트웨이 사용)를** 선택한 다음 **OK(확인)를 클릭합니다**.
13. 전화를 걸려면 연결 대상 창을 표시하기 위해 아이콘을 두 번 클릭하면 사용자 이름 및 암호 필드를 입력한 다음 **연결**을 클릭해야 합니다.

사용자 3용 Microsoft Windows 설치

사용자 3에 대한 컨피그레이션(자동 명령 PPP가 있는 인증 사용자)은 다음 예외를 제외하고 사용자 1과 2에 대해 동일합니다.

- 구성/옵션 속성 페이지(6단계)에서 전화 **걸기 후 터미널 창**을 **표시합니다**.
- 사용자가 아이콘을 두 번 클릭하여 Connect To(연결 대상) 창을 열어 전화를 걸면(13단계) User name(사용자 이름) 및 Password(비밀번호) 필드가 채워지지 않습니다.사용자가 **연결**을 클릭합니다.라우터에 연결되면 사용자는 검정색 창에 사용자 이름과 비밀번호를 입력합니다 .인증 후 사용자는 Continue(**F7)를 누릅니다**.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

라우터

debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **terminal monitor**—현재 터미널 및 세션에 대한 **debug** 명령 출력 및 시스템 오류 메시지를 표시합니다.
- **debug ppp negotiation** - PPP 시작 중에 전송된 PPP 패킷을 표시합니다. 여기서 PPP 옵션은 협상됩니다.
- **debug ppp packet** - 보내고 받은 PPP 패킷을 표시합니다.(이 명령은 낮은 수준의 패킷 덤프를 표시합니다.)
- **debug ppp chap** - 클라이언트가 인증을 통과하는지 여부에 대한 정보를 표시합니다(Cisco IOS Software Release 11.2 이전).
- **debug aaa authentication** - AAA(authentication, authorization, and accounting)/TACACS+ 인증에 대한 정보를 표시합니다.
- **debug aaa authorization** - AAA/TACACS+ 권한 부여에 대한 정보를 표시합니다.

서버

참고: 여기서는 Cisco의 TACACS+ Freeware 서버 코드를 가정합니다.

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

관련 정보

- TACACS+ 지원 페이지
- IOS 설명서의 TACACS+
- Cisco Secure Access Control Server
- CiscoSecure 2.x TACACS+ 설정 및 디버깅
- 기술 지원 및 문서 – Cisco Systems