TACACS+ 인증을 사용하여 Cisco 라우터 구성

목차

소개

이 문서에서는 UNIX에서 실행되는 TACACS+를 사용하여 인증을 위해 Cisco 라우터를 구성하는 방법에 대해 설명합니다.TACACS+는 Windows용 Cisco Secure ACS 또는 Cisco Secure ACS UNIX를 상용으로 제공하는 기능과 같은 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.Cisco Ordering Home Page(등록된 고객만 해당)를 방문하여 주문하십시오.

참고: Windows용 Cisco Secure ACS의 90일 평가판을 받으려면 연결된 서비스 계약이 있는 CCO 계정이 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 사용하므로 **aaa 인증 로그인 기본 tacacs+ enable**과 같은 명령문은 **aaa 인증 로그인 기본 그룹 tacacs+ enable**로 **나타납니다**.

라우터 명령에 대한 자세한 내용은 Cisco IOS Software 문서를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS Software 릴리스 11.3.3 및 Cisco IOS Software 릴리스 12.0.5.T 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

인증

다음 단계를 완료하십시오.

1. UNIX 서버에서 TACACS+(TAC+) 코드를 컴파일했는지 확인합니다.여기서 서버 컨피그레이션에서는 Cisco TAC+ 서버 코드를 사용한다고 가정합니다.라우터 컨피그레이션은 서버 코드가 Cisco 서버 코드인지 여부를 확인해야 합니다.TAC+는 루트로 실행해야 합니다.필요한 경우 루트로 이동합니다.
2. 이 문서 끝에 test_file을 복사하여 TAC+ 서버에 배치하고 이름을 **test_file로 지정합니다** .tac_**plus_executable** 데몬이 **test_file**로 시작하는지 **확인합니다**.이 명령에서 **-P** 옵션은 컴파일 오류를 확인하지만 데몬은 시작하지 않습니다.
   ```
   tac_plus_executable -P -C test_file
   ```
   test_file의 내용이 창 아래로 스크롤될 수 있지만 을 없거나 가 또는 와 같은 메시지는 볼 수 없습니다.오류가 있는 경우 test_file 경로를 확인하고 입력 내용을 다시 확인한 다음 계속하기 전에 다시 테스트하십시오.
3. 라우터에서 TAC+를 구성하기 시작합니다.enable 모드를 시작하고 **configure terminal**을 명령 집합 앞에 입력합니다.이 명령 구문은 **tac_plus_executable**이 실행되고 있지 않을 경우 라우터에서 처음**으로** 잠기지 않도록 합니다.

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
names of lists, and the methods !--- listed on the same lines are the methods !--- in the
order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !--- it
is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP address. !
tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being
locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8
login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400
```

```
flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being
locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
```

4. 계속하기 전에 텔넷과 콘솔 포트를 통해 라우터에 계속 액세스할 수 있는지 테스트합니다 .tac_plus_executable이 실행되고 있지 않으므로 enable 비밀번호를 수락해야 합니다.**참고:** 콘솔 포트 세션을 활성 상태로 유지하고 활성화 모드로 유지합니다.이 세션은 시간 초과해서는 안 됩니다.이 시점에서는 라우터에 대한 액세스가 제한되므로, 자신을 잠그지 않고도 구성을 변경할 수 있어야 합니다.다음 명령을 실행하여 라우터에서 서버-라우터 상호 작용을 확인합니다.
```
terminal monitor
  debug aaa authentication
```
5. 루트로 서버에서 TAC+를 시작합니다.
```
tac_plus_executable -C test_file -d 16
```
6. TAC+가 시작되었는지 확인합니다.
```
ps -aux | grep tac_plus_executable
```
또는
```
ps -ef | grep tac_plus_executable
```
TAC+가 시작되지 않으면 일반적으로 test_file의 구문에 문제가 있습니다.이를 수정하려면 1단계로 돌아갑니다.
7. **tail -f /var/tmp/tac_plus.log을 입력하여** 서버에서 라우터 간 상호 작용을 확인합니다.**참고:** 5단계의 `-d 16` 옵션은 모든 트랜잭션의 출력을 /var/tmp/tac_plus.log폴더로 전송합니다.
8. 텔넷(VTY) 사용자는 이제 TAC+를 통해 인증해야 합니다.라우터와 서버에서 디버깅을 진행하는 경우(4단계와 7단계) 네트워크의 다른 부분에서 라우터로 텔넷합니다.라우터가 사용자 이름 및 비밀번호 프롬프트를 생성하며, 이에 응답합니다.
```
'authenuser'    (username from test_file)
'admin'    (password from test_file)
```
사용자 `authenuser`는 `admin` 그룹에 있으며 비밀번호 `admin`이 있습니다.TAC+ 상호 작용을 볼 수 있는 서버 및 라우터를 확인합니다. 보낸 위치, 응답, 요청 등이 표시됩니다.계속하기 전에 모든 문제를 수정하십시오.
9. 사용자가 활성화 모드로 전환하기 위해 TAC+를 통해 인증하도록 하려면 콘솔 포트 세션이 활성 상태인지 확인하고 다음 명령을 라우터에 추가합니다.
```
!--- For enable mode, list 'default' looks to TAC+ !--- then enable password if TAC+ does
not run. aaa authentication enable default tacacs+ enable
```
이제 사용자는 TAC+를 통해 활성화해야 합니다.
10. 라우터와 서버에서 디버깅을 진행하는 경우(4단계와 7단계) 네트워크의 다른 부분에서 라우터로 텔넷합니다.라우터가 사용자 이름 및 비밀번호 프롬프트를 생성하며, 이에 응답합니다.
```
'authenuser'    (username from test_file)
'admin'    (password from test_file)
```
enable 모드를 시작하면 라우터가 비밀번호를 요청하며, 이 비밀번호를 회신합니다.
```
'cisco'  ($enable$ password from test_file)
```
TAC+ 상호 작용을 볼 수 있는 서버 및 라우터를 확인합니다. TAC+ 상호 작용은 어디서 전송되는지, 응답, 요청 등을 확인합니다.계속하기 전에 모든 문제를 수정하십시오.
11. TAC+가 다운된 경우에도 사용자가 라우터에 계속 액세스할 수 있도록 콘솔 포트에 연결되어 있는 동안 서버에서 TAC+ 프로세스를 종료합니다.
```
ps -aux | grep tac_plus_executable
```
또는
```
ps -ef | grep tac_plus_executable)
  kill -9 pid_of_tac_plus_executable
```
텔넷을 반복하고 이전 단계를 활성화합니다.그런 다음 라우터는 TAC+ 프로세스가 응답하지 않음을 인식하고 사용자가 기본 비밀번호로 로그인하고 활성화할 수 있도록 합니다.
12. TAC+를 통해 콘솔 포트 사용자의 인증을 확인합니다.이를 위해 TAC+ 서버를 다시 시작(5단계 및 6단계)하고 라우터에 대한 텔넷 세션을 설정합니다(TAC+를 통해 인증해야 함).콘솔 포

트를 통해 라우터에 로그인할 수 있을 때까지 텔넷을 통해 라우터에 라우터로 연결된 상태로 유지됩니다.콘솔 포트를 통해 라우터에 대한 원래 연결에서 로그아웃한 다음 콘솔 포트에 다시 연결합니다.사용자 ID와 비밀번호(10단계 참조)를 사용하여 로그인하고 활성화하는 콘솔 포트 인증은 이제 TAC+를 통해야 합니다.

13. 텔넷 세션 또는 콘솔 포트를 통해 계속 연결되어 있고 라우터와 서버에서 디버깅을 진행하는 동안(4단계 및 7단계) 1행에 모뎀 연결을 설정합니다.이제 회선 사용자는 TAC+를 통해 로그인하여 활성화해야 합니다.라우터가 사용자 이름 및 비밀번호 프롬프트를 생성하며, 이에 응답합니다.

    ```
    'authenuser'    (username from test_file)
    'admin'    (password from test_file)
    ```

    enable 모드를 시작하면 라우터가 비밀번호를 요청합니다.회신:

    ```
    'cisco'    ($enable$ password from test_file)
    ```

    TAC+ 상호 작용이 표시되는 서버 및 라우터를 확인합니다. TAC+ 상호 작용은 어디서 전송되는지, 응답, 요청 등을 확인합니다.계속하기 전에 모든 문제를 수정하십시오.이제 사용자는 TAC+를 통해 활성화해야 합니다.

권한 부여 추가

권한 부여를 추가하는 것은 선택 사항입니다.

기본적으로 라우터에는 3가지 명령 레벨이 있습니다.

- 사용 안 함, 사용, 종료, 도움말 및 로그아웃을 포함하는 권한 수준 0
- 권한 수준 1 - 텔넷의 일반 레벨 - 프롬프트에 가 표시됨`>`
- privilege level 15 - enable level - prompt에 `router#`

사용 가능한 명령은 IOS 기능 집합, Cisco IOS 버전, 라우터 모델 등에 따라 다르기 때문에 레벨 1 및 15의 모든 명령에 대한 포괄적인 목록이 없습니다. 예를 들어, **show ipx route**는 IP 전용 기능 집합에 없고, **show ip nat trans는** Cisco IOS Software Release 10.2.x에 없습니다. NAT는 당시 도입되지 않았고 전원 모델이 없는 **show environment는**라우터가 없기 때문입니다 공급 및 온도 모니터링.특정 레벨의 특정 라우터에서 사용 가능한 명령은 를 입력할 때 찾을 수 있습니다.해당 권한 레벨에서 라우터의 프롬프트에 표시됩니다.

Cisco 버그 ID CSCdi82030(등록된 고객만 해당)이 구현될 때까지 콘솔 포트 권한이 기능으로 추가되지 않았습니다.콘솔 포트 권한 부여는 기본적으로 해제되어 라우터에서 실수로 잠길 가능성을 줄입니다.사용자가 콘솔을 통해 라우터에 물리적으로 액세스할 수 있는 경우 콘솔 포트 권한 부여는 매우 효과적이지 않습니다.그러나 Cisco 버그 ID CSCdi82030(등록된 고객만)이 명령에서 구현된 이미지에서 `con 0`에서 콘솔 포트 권한을 설정할 수 있습니다.

```
authorization exec default|WORD
```

1. TAC+를 통해 모든 또는 일부 레벨에서 명령을 인증하도록 라우터를 구성할 수 있습니다.이 라우터 컨피그레이션을 사용하면 모든 사용자가 명령별 권한 부여를 서버에 설정할 수 있습니다.여기서는 TAC+를 통해 모든 명령에 권한을 부여하지만, 서버가 다운되면 권한 부여가 필요하지 않습니다.

    ```
    aaa authorization commands 1 default tacacs+ none
      aaa authorization commands 15 default tacacs+ none
    ```

2. TAC+ 서버가 실행되는 동안 사용자 ID authenuser를 사용하여 라우터에 **텔넷**.authenuser는 test_file에 기본 서비스 = permit을 가지므로 이 사용자는 모든 기능을 수행할 수 있어야 합니다.라우터에서 enable 모드**를** 입력하고 권한 부여 디버깅을 설정합니다.

    ```
    terminal monitor
      debug aaa authorization
    ```

3. 사용자 ID **권한** 부여 및 비밀번호 **운영자**를 사용하여 라우터에 **텔넷합니다**.이 사용자는 traceroute 및 **logout** 두 개의 show 명령**을** 수행할 수 없습니다(test_file 참조).TAC+ 상호 작용(보낸 위치, 응답, 요청 등)이 표시되는 서버와 라우터를 확인합니다. 계속하기 전에 모든 문제를 수정하십시오.
4. autocommand에 대해 사용자를 구성하려면 test_file에서 임시 주석 처리된 사용자를 제거하고 유효한 IP 주소 대상을 #.#.#.# 대신 배치합니다.TAC+ 서버를 중지하고 시작합니다.라우터에서:
   ```
   aaa authorization exec default tacacs+
   ```
   사용자 ID **임시** 및 비밀번호가 **일시적인** 라우터에 **텔넷합니다**.**telnet #.#.#**이 실행되며 사용자 임시 항목이 다른 위치로 전송됩니다.

계정 추가

어카운팅 추가는 선택 사항입니다.

계정 파일에 대한 참조는 test_file - accounting 파일 = /var/log/tac.log에 있습니다.그러나 라우터에 구성되지 않은 경우(라우터가 11.0 이후 버전의 Cisco IOS 소프트웨어를 실행하는 경우) 어카운팅은 수행되지 않습니다.

1. 라우터에서 어카운팅을 활성화합니다.
   ```
   aaa accounting exec default start-stop tacacs+
     aaa accounting connection default start-stop tacacs+
     aaa accounting network default start-stop tacacs+
     aaa accounting system default start-stop tacacs+
   ```
   참고: 일부 버전에서는 AAA 어카운팅이 명령별 어카운팅을 수행하지 않습니다.해결 방법은 명령별 권한 부여를 사용하고 어카운팅 파일에 어커런스를 기록하는 것입니다.(Cisco 버그 ID CSCdi44140을 참조하십시오.) 이 고정 이미지를 사용하는 경우 [Cisco IOS Software Release 11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA as a01, 11.1(6.3)CA as a as a 1999-accounting도 활성화할 수 있습니다.
2. 서버에서 TAC+가 실행되는 동안 서버에 이 명령을 입력하여 어카운팅 파일에 들어가는 항목을 확인합니다.
   ```
   tail -f /var/log/tac.log
   ```
   그런 다음 라우터에 로그인하거나 로그아웃하고, 라우터에서 텔넷 나가는 등필요한 경우 라우터에 다음을 입력합니다.
   ```
   terminal monitor
     debug aaa accounting
   ```

테스트 파일

```
- - - - - - - (cut here) - - - - - - -

# Set up accounting file if enabling accounting on NAS
accounting file = /var/log/tac.log

# Enable password setup for everyone:
user = $enable$ {
        login = cleartext "cisco"
        }

# Group listings must be first:
group = admin {
# Users in group 'admin' have cleartext password
```

```
        login = cleartext "admin"
        expires = "Dec 31 1999"
}

group = operators {
# Users in group 'operators' have cleartext password
        login = cleartext "operator"
        expires = "Dec 31 1999"
}

group = transients {
# Users in group 'transient' have cleartext password
        login = cleartext "transient"
        expires = "Dec 31 1999"
}

# This user is a member of group 'admin' & uses that group's password to log in.
#  The $enable$ password is used to enter enable mode.  The user can perform all commands.
 user = authenuser {
        default service = permit
        member = admin
        }

# This user is limitted in allowed commands when aaa authorization is enabled:
 user = telnet {
        login = cleartext "telnet"
        cmd = telnet {
        permit .*
        }
        cmd = logout {
        permit .*
        }
        }

# user = transient {
#       member = transients
#       service = exec {
        # When transient logs on to the NAS, he's immediately
        # zipped to another site
#       autocmd = "telnet #.#.#.#"
#       }
#       }

# This user is a member of group 'operators'
# & uses that group's password to log in
 user = authenuser {
        member = operators
# Since this user does not have 'default service = permit' when command
# authorization through TACACS+ is on at the router, this user's commands
# are limited to:
        cmd = show {
        permit ver
        permit ip
        }
        cmd = traceroute {
        permit .*
        }
        cmd = logout {
        permit .*
        }
}
- - - - (end cut here) - - - -
```

참고: 이 오류 메시지는 TACACS 서버에 연결할 수 없는 경우 생성됩니다.`%AAAA-3-DROPACTSNDFAIL:`

, : .TACACS+ 서버가 작동 중인지 확인합니다.

관련 정보

- 단일 사용자 네트워크 액세스 보안 TACACS+
- TACACS+(Terminal Access Controller Access Control System)
- Windows용 Cisco Secure Access Control Server
- 기술 지원 및 문서 – Cisco Systems