CiscoSecure 2.x TACACS+ 설정 및 디버깅

목차

소개

이 문서는 Cisco Secure TACACS+ 컨피그레이션의 설정 및 디버깅에 처음 Cisco Secure 2.x 사용자를 지원하기 위해 작성되었습니다.Cisco Secure 기능에 대한 완전한 설명은 아닙니다.

서버 소프트웨어 및 사용자 설정에 대한 자세한 내용은 Cisco Secure 설명서를 참조하십시오.라우터 명령에 대한 자세한 내용은 해당 릴리스에 대한 Cisco IOS Software 문서를 참조하십시오.

사전 요구 사항

요구 사항

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure ACS 2.x 이상
- Cisco IOS® 소프트웨어 릴리스 11.3.3 이상

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

Cisco Secure 설정

다음 단계를 완료하십시오.

1. UNIX 서버에 Cisco Secure 코드를 설치하려면 소프트웨어와 함께 제공된 지침을 사용해야 합니다.
2. 제품이 중지되고 시작되는지 확인하려면 /etc/rc0.d `cd` 입력하고 root로 실행합니다./K80Cisco Secure(데몬을 중지하려면).cd `/etc/rc2.d` 입력하고 루트로 ./S80Cisco Secure(데몬을 시작하려면) 실행합니다.시작 시 다음과 같은 메시지가 표시됩니다.
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   $BASE/utils/psg 실행하여 각 개별 프로세스(예: SQLAnywhere 또는 다른 데이터베이스 엔진, Cisco Secure 데이터베이스 서버 프로세스, Netscape Web Server, Netscape Web Admin, Acme Web Server, Cisco Secure AAA 프로세스 또는 Auto Restart 프로세스)를 하나 이상 실행해야 합니다.
3. 올바른 디렉토리에 있는지 확인하려면 셸 환경에서 환경 변수 및 경로를 설정합니다.c-shell은 여기에서 사용됩니다.**$BASE**는 Cisco Secure가 설치된 디렉토리이며 설치 중에 선택됩니다.여기에는 DOCS, DBServer, CSU 등의 디렉토리가 포함됩니다.이 예에서는 /opt/CSCOacs에 설치하는 것으로 가정하지만, 시스템에서 다를 수 있습니다.
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY는 기본 Cisco Secure 데이터베이스가 설치된 디렉터리이며 설치 중에 선택됩니다.제품과 함께 제공되는 기본 데이터베이스인 SQLAnywhere가 사용된 경우 데이터베이스, doc 등의 디렉토리가 포함됩니다.이 예에서는 /opt/CSCOacs/SYBSsa50에 설치하는 것으로 가정하지만 시스템에서 다를 수 있습니다.
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   셸 환경에서 경로를 추가할 대상:
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD - $BASE/config**CSU.cfg**는 Cisco Secure 서버 제어 파일입니다.이 파일의 백업 복사본을 만듭니다.이 파일에서 `LIST config_license_key` 소프트웨어를 구매한 경우 라이센스 프로세스를 통해 받은 라이센스 키를 표시합니다.4포트 평가판 라이센스인 경우 이 라인을 제외할 수 있습니다.NAS **config_nas_config** 섹션에는 기본 NAS(Network Access Server) 또는 라우터 또는 설치 중에 입력하는 NAS가 포함될 수 있습니다.이 예에서 디버깅을 위해 *모든* NAS가 키 *없이* Cisco Secure 서버와 통신하도록 허용할 수 있습니다.예를 들어 `/* NAS` 을 포함하는 행에서 NAS 이름과 키를 제거하면 `*/`" 및*/*NAS/Cisco 보안 비밀 키 */로 이동할 수 있습니다.*그 지역의 유일한 탄자는 다음과 같다.
   ```
   NAS config_nas_config = {
     {
       "",          /* NAS name can go here */
       "",              /* NAS/Cisco Secure secret key */
       "",                          /* message_catalogue_filename */
       1,                           /* username retries */
       2,                           /* password retries */
       1                            /* trusted NAS for SENDPASS */
     }
   };

   AUTHEN config_external_authen_symbols = {
   ```
   이렇게 하면 키를 교환하지 않고 모든 NAS와 통신할 수 있음을 Cisco Secure에 알립니다.

5. 디버깅 정보를 /var/log/csuslog로 이동하려면 CSU.cfg의 맨 위 섹션에 한 줄이 있어야 합니다. 이 섹션은 디버깅 작업을 서버에 알려 줍니다.0X7FFFFF는 가능한 모든 디버깅을 추가합니다 .이에 따라 이 행을 추가하거나 수정합니다.
   ```
   NUMBER config_logging_configuration = 0x7FFFFFFF;
   ```
   이 추가 행은 디버깅 정보를 local0으로 전송합니다.
   ```
   NUMBER config_system_logging_level = 0x80;
   ```
   또한 /etc/syslog.conf 파일을 수정하려면 다음 항목을 추가하십시오.
   ```
   local0.debug /var/log/csuslog
   ```
   그런 다음 syslogd를 재활용하여 다시 읽습니다.
   ```
   kill -HUP `cat /etc/syslog.pid`
   ```
   Cisco Secure Server 재활용:
   ```
   /etc/rc0.d/K80Cisco Secure
   /etc/rc2.d/S80Cisco Secure
   ```
   아직 시작해야해요
6. 브라우저를 사용하여 사용자, 그룹 등을 추가하거나 CSimport 유틸리티를 추가할 수 있습니다 .이 문서 끝에 있는 플랫 파일의 샘플 사용자는 CSimport를 사용하여 데이터베이스로 쉽게 이동할 수 있습니다.이러한 사용자는 테스트 목적으로 작업하며, 사용자가 자신의 사용자를 가져오면 삭제할 수 있습니다.가져온 사용자는 GUI를 통해 볼 수 있습니다.CSimport를 사용하려는 경우
   ```
   CD $BASE/utils
   ```
   이 문서의 끝에 사용자 및 그룹 프로필을 시스템의 아무 곳이나 있는 파일(예: $BASE/utils 디렉토리)에 넣고 데몬을 실행합니다(예: /etc/rc2.d/S80Cisco Secure 및 사용자 루트로). test(-t) 옵션을 사용하여 CSimport를 실행합니다.
   ```
   ./CSimport -t -p <path_to_file> -s <name_of_file>
   ```
   이 테스트에서는 사용자의 구문을 테스트합니다.다음과 같은 메시지를 수신해야 합니다.
   ```
   Secure config home directory is: /opt/CSCOacs/config/CSConfig.ini
   hostname = berry and port = 9900 and clientid = 100
   /home/ddunlap/csecure/upgrade.log exists, do you want to write over 'yes' or 'no' ?
   yes
   Sorting profiles...
   Done sorting 21 profiles!
   Running the database import test...
   ```
   다음 메시지를 수신해서는 안 됩니다.
   ```
   Error at line 2: password = "adminusr"
   Couldn't repair and continue parse
   ```
   오류가 있는지 여부를 확인하려면 upgrade.log를 검사하여 프로필을 체크 아웃했는지 확인합니다.오류가 수정되면 $BASE/utils 디렉토리에서 데몬이 실행(/etc/rc2.d/S80Cisco Secure)되고 사용자 루트로 CSimport를 commit(-c) 옵션과 함께 실행하여 사용자를 데이터베이스로 이동합니다.
   ```
   ./CSimport -c -p <path_to_file> -s <name_of_file>
   ```
   화면 또는 upgrade.log에 오류가 없어야 합니다.
7. 지원되는 브라우저는 Cisco Secure Compatibility 기술 팁에 나열되어 있습니다.PC 브라우저에서 Cisco Secure/Solaris 상자 http://#을 가리킵니다. **#.#.#.#/cs** 여기서 **#.#.#.#**은 Cisco Secure/Solaris 서버의 IP입니다.표시되는 화면에서 사용자가 **수퍼유저**를 입력하고 비밀번호에 **changeme**를 입력합니다.이 시점에서 비밀번호를 변경하지 마십시오.이전 단계에서 CSimport를 사용하는 경우 사용자/그룹이 추가된 것을 확인할 수 있습니다. 또는 찾아보기 블록을 클릭하고 GUI를 통해 사용자 및 그룹을 수동으로 추가할 수 있습니다.

인증 설정

참고: 이 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 표시합

니다.

이때 라우터를 구성합니다.

1. 라우터를 구성하는 동안 Cisco Secure를 종료하십시오.
   ```
   /etc/rc0.d/K80Cisco Secure to stop the daemons.
   ```
2. 라우터에서 TACACS+ 구성을 시작합니다.enable 모드를 입력하고 명령 집합 앞에 conf t를 입력합니다.이 구문은 *처음에* Cisco Secure가 실행되지 않는 경우 라우터에서 잠기지 않도록 합니다.ps `-ef | grep Secure`를 실행하여 Cisco Secure가 실행되고 있지 않은지 확인한 다음, 다음과 같은 경우 -9를 실행합니다.

   ```
   !--- Turn on TACACS+ aaa new-model enable password whatever !--- These are lists of
   authentication methods, !--- that is, vtymethod and conmethod 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 Cisco Secure not being started, !--- the
   enable password is accepted !--- because it is in each list. aaa authentication login
   vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable !--- Point the
   router to the server, that is, !--- #.#.#.# 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 vty 0 4 password
   whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0
   0 login authentication vtymethod
   ```
3. 계속하기 전에 텔넷과 콘솔 포트를 통해 라우터에 계속 액세스할 수 있는지 테스트합니다.Cisco Secure가 실행되고 있지 않으므로 enable 비밀번호를 허용해야 합니다.**주의:** 콘솔 포트 세션을 활성 상태로 유지하고 활성화 모드로 유지합니다.이 세션은 시간 초과해서는 안 됩니다.이 시점부터 라우터에 대한 액세스를 제한하기 시작하며, 자신을 잠그지 않고도 구성을 변경할 수 있어야 합니다.라우터에서 서버-라우터 상호 작용을 보려면 다음 명령을 실행합니다.
   ```
   terminal monitor
   debug aaa authentication
   ```
4. 루트로 서버에서 Cisco Secure를 시작합니다.
   ```
   /etc/rc2.d/S80Cisco Secure
   ```
   이렇게 하면 프로세스가 시작되지만 S80Cisco Secure에서 구성한 것보다 더 많은 디버깅을 활성화하려는 경우 다음과 같습니다.
   ```
   ps -ef | grep Cisco Secure
   kill -9 <pid_of CS_process>

   CD $BASE/CSU
   ./Cisco Secure -cx -f $BASE/config/CSU.cfg to start the Cisco Secure process with debugging
   ```
   `-x` 옵션을 사용하면 Cisco Secure는 전경 모드로 실행되므로 라우터 간 서버 상호 작용을 관찰할 수 있습니다.오류 메시지가 표시되지 않아야 합니다.-x 옵션으로 인해 Cisco Secure 프로세스가 시작되고 정지해야 합니다.
5. 다른 창에서 Cisco Secure가 시작되었는지 확인합니다.ps `-ef` 입력하고 Cisco Secure 프로세스를 찾습니다.
6. 텔넷(vty) 사용자는 이제 Cisco Secure를 통해 인증해야 합니다.라우터에서 디버그를 사용하여 네트워크의 다른 부분에서 라우터에 텔넷합니다.라우터가 사용자 이름 및 비밀번호 프롬프트를 생성해야 합니다.다음 사용자 ID/비밀번호 조합을 사용하여 라우터에 액세스할 수 있어야 합니다.
   ```
   adminusr/adminusr
   operator/oper
   desusr/encrypt
   ```
   상호 작용, 즉 어디서 전송되는지, 응답하고 요청하는 등 상호 작용을 볼 수 있는 서버와 라우터를 확인합니다.계속하기 전에 모든 문제를 수정하십시오.
7. 사용자가 Cisco Secure를 통해 인증하여 활성화 모드로 전환하려면 콘솔 포트 세션이 계속 활

성 상태인지 확인하고 다음 명령을 라우터에 추가합니다.

```
!--- For enable mode, list 'default' looks to Cisco Secure !--- then enable password if Cisco Secure is not running. aaa authentication enable default tacacs+ enable
```

8. 이제 Cisco Secure를 통해 **활성화해야** 합니다.라우터에서 디버그를 사용하여 네트워크의 다른 부분에서 라우터에 텔넷합니다.라우터가 사용자 이름/비밀번호를 요청하면 `operator/oper`로 응답합니다.사용자 운영자가 enable 모드(권한 레벨 15)를 시작하려고 하면 비밀번호 "cisco"가 필요합니다.다른 사용자는 권한 수준 문(또는 Cisco Secure daemon down)이 없으면 enable 모드를 시작할 수 없습니다.Cisco Secure Interaction(예: 전송 대상, 응답, 요청 등)이 표시되는 서버 및 라우터를 확인합니다.계속하기 전에 문제를 수정하십시오.
9. Cisco Secure가 다운된 경우에도 사용자가 라우터에 계속 액세스할 수 있도록 콘솔 포트에 연결되어 있는 동안 서버에서 Cisco Secure 프로세스를 중단합니다.
   ```
   'ps -ef' and look for Cisco Secure process
   kill -9 pid_of_Cisco Secure
   ```
   텔넷을 반복하고 이전 단계를 활성화합니다.라우터는 Cisco Secure 프로세스가 응답하지 않으며 사용자가 기본 enable 비밀번호로 로그인 및 활성화할 수 있음을 인식해야 합니다.
10. Cisco Secure 서버를 다시 시작하고 라우터에 텔넷 세션을 설정합니다. 이 세션은 Cisco Secure를 통해 사용자 ID/비밀번호 **운영자/작업**을 통해 인증해야 Cisco Secure를 통해 콘솔 포트 사용자의 인증을 확인할 수 있습니다.콘솔 포트를 통해 라우터에 로그인할 수 있을 때까지 텔넷(telnet)을 라우터에 유지하고 활성화(enable) 모드로 유지합니다. 예를 들어 콘솔 포트를 통해 라우터에 대한 원래 연결에서 로그아웃한 다음 콘솔 포트에 다시 연결합니다.이전 사용자 ID/비밀번호 조합을 사용하여 로그인하기 위한 콘솔 포트 인증은 이제 Cisco Secure를 통해야 합니다.예를 들어 사용자 ID/비밀번호 **운영자/oper**를 활성화하려면 **cisco**를 사용해야 **합니다**.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

권한 부여 추가

권한 부여를 추가하는 것은 선택 사항입니다.

기본적으로 라우터에는 3가지 명령 레벨이 있습니다.

- 권한 레벨 0 - 비활성화, 활성화 종료, 도움말 및 로그아웃 포함
- 권한 수준 1—텔넷 및 프롬프트의 일반 레벨 에 표시>
- 권한 수준 15 - 레벨 및 프롬프트가 `router#`로 표시됩니다.

사용 가능한 명령은 Cisco IOS 기능 집합, Cisco IOS 소프트웨어 릴리스, 라우터 모델 등에 따라 다르므로 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.X 코드에 없습니다. NAT는 현재에 NAT가 포함되어 있지 않으므로 현재 환경은표시되지 않습니다. 전원 공급 장치 및 온도 모니터링이 없는 라우터 모델

특정 레벨의 특정 라우터에서 사용 가능한 명령은 를 입력하는 것을 찾을 수 있습니다.해당 권한 레벨에서 라우터의 프롬프트에 표시됩니다.

CSCdi82030이 구현될 때까지 콘솔 포트 권한 부여가 기능으로 추가되지 않았습니다.콘솔 포트 권한 부여는 기본적으로 해제되어 실수로 라우터에서 잠길 가능성을 줄입니다.사용자가 콘솔을 통해 라우터에 물리적으로 액세스할 수 있는 경우 콘솔 포트 권한 부여는 매우 효과적이지 않습니다.그러나 CSCdi82030이 **authorization exec default|WORD** 명령과 함께 구현된 Cisco IOS 이미지에서 **line con 0** 명령**에서** 콘솔 포트 권한 부여를 설정할 수 있습니다.

다음 단계를 완료하십시오.

1. Cisco Secure를 통해 모든 레벨 또는 일부 레벨에서 명령을 인증하도록 라우터를 구성할 수 있습니다.이 라우터 컨피그레이션을 사용하면 모든 사용자가 명령별 권한 부여를 서버에 설정할 수 있습니다.Cisco Secure를 통해 모든 명령에 권한을 부여할 수 있지만 서버가 다운된 경우 권한 부여가 필요하지 않으므로 이 됩니다.Cisco Secure server down을 사용하여 다음 명령을 입력합니다.Cisco Secure를 통해 인증을 활성화하는 요구 사항을 제거하려면 이 명령을 입력합니다.
   ```
   no aaa authentication enable default tacacs+ none
   ```
   Cisco Secure를 통해 명령 권한 부여를 수행하도록 하려면 다음 명령을 입력합니다.
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. Cisco Secure Server가 실행되는 동안 텔넷은 사용자 ID/비밀번호 **loneusr/lonepwd를** 사용하여 라우터에 **연결됩니다**.이 사용자는 다음 이외의 명령을 수행할 수 없습니다.
   ```
   show version
   ping <anything>
   logout
   ```
   이전 사용자 **adminusr/adminusr**, **operator/oper**, **desusr/encrypt**는 `= permit`를 통해 모든 명령을 수행할 수 있어야 합니다.프로세스에 문제가 있는 경우 라우터에서 enable 모드를 시작하고 다음 명령을 사용하여 권한 부여 디버깅을 설정합니다.
   ```
   terminal monitor
   debug aaa authorization
   ```
   Cisco Secure Interaction(예: 전송 위치, 응답, 요청 등)이 표시되는 서버와 라우터를 확인합니다.계속하기 전에 모든 문제를 수정하십시오.
3. Cisco Secure를 통해 EXEC 세션을 인증하도록 라우터를 구성할 수 있습니다.aaa **authorization exec default tacacs+ none** 명령은 EXEC 세션에 대한 TACACS+ 권한 부여를 실행합니다.이를 적용하면 **시간/시간**, **텔넷/텔넷**, **토담/토담**, dpm/todpm, **공중제비/공중제비**에 영향을 **미칩니다.**이 명령을 라우터에 추가하고 사용자 **시간/시간**으로 라우터에 텔넷을 추가하면 exec 세션은 1분 동안 열려 있습니다(set timeout = 1). 사용자 **텔넷/텔넷**이 라우터로 들어가지만 다른 주소로 즉시 전송됩니다(set autocmd = "telnet 171.68.118.102"). **todam/todam** 및 todpm**/todpm** 사용자가 라우터에 액세스하거나 액세스할 수 없을 수 있습니다. 이 라우터는 테스트 중에 있는 시간에 따라 다릅니다.사용자 **공중제비**는 네트워크 10.31.1.x에서 라우터 coala.rtp.cisco.com에 텔넷만 연결할 수 있습니다.Cisco Secure는 라우터 이름을 확인하려고 시도합니다.IP 주소 10.31.1.5을 사용하는 경우 확인이 수행되지 않는 경우 유효하며, 이름 코알라를 사용하는 경우 확인이 완료된 경우 유효합니다.

계정 추가

어카운팅 추가는 선택 사항입니다.

1. 라우터가 Cisco IOS Software Release 11.0보다 나중에 Cisco IOS 소프트웨어 릴리스를 실행하는 경우 라우터에 구성되지 않은 경우 어카운팅이 수행되지 않습니다. 라우터에서 어카운팅을 활성화할 수 있습니다.
   ```
   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: Cisco 버그 ID CSCdi44140에서 명령 어카운팅이 손상되었지만 이 이미지가 고정된 이미지를 사용하는 경우 명령 어카운팅도 활성화할 수 있습니다.

2. 라우터에 계정 레코드 디버깅을 추가합니다.
```
terminal monitor
debug aaa accounting
```
3. 콘솔의 디버그는 사용자가 로그인할 때 서버에 들어가는 계정 레코드를 표시해야 합니다.
4. 회계 레코드를 root로 검색하려면
```
CD $BASE/utils/bin
./AcctExport <filename> no_truncate
```
`no_truncate`는 데이터가 데이터베이스에 보존됨을 의미합니다.

전화 접속 사용자 추가

다음 단계를 완료하십시오.

1. 전화 접속 사용자를 추가하기 전에 Cisco Secure의 다른 기능이 작동하는지 확인하십시오 .Cisco Secure 서버와 모뎀이 이 시점 이전에 작동하지 않으면 이 시점 이후에는 작동하지 않습니다.
2. 라우터 컨피그레이션에 이 명령을 추가합니다.
```
aaa authentication ppp default if-needed tacacs+
aaa authentication login default tacacs+ enable
aaa authorization network default tacacs+
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
```
인터페이스 컨피그레이션은 인증 방법에 따라 다르지만 이 예에서는 다음 컨피그레이션과 함께 다이얼인 회선이 사용됩니다.
```
interface Ethernet 0
ip address 10.6.1.200 255.255.255.0
! !--- 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 ! !--- 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 ! !--- login 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
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 ! access-list 101 deny icmp any any
```
3. Cisco Secure의 사용자 파일에서:chapuser - CHAP/PPP - 사용자가 1번 줄에서 다이얼합니다 .주소는 라우터에서 **피어 기본 ip 주소 풀 비동기 및 ip 로컬 풀 async 10.6.100.101 10.6.100.103**에 의해 할당됩니다.chapaddr - CHAP/PPP - 사용자가 1번 줄에서 다이얼합니다 .10.29.1.99 주소가 서버에 의해 할당됨chapacl - CHAP/PPP - 사용자가 1번 줄에서 다이얼합니다.주소 10.29.1.100이 서버에 할당되고 인바운드 액세스 목록 101이 적용됨(라우터에 정의되어야 함)papuser—PAP/PPP— 회선 2에서 사용자 다이얼합니다.주소는 라우터에서 **피어 기본 ip 주소 풀 비동기 및 ip 로컬 풀 async 10.6.100.101 10.6.100.103**에 의해 할당됩니다 .papaddr - PAP/PPP - 사용자가 행 2에서 전화를 겁니다.10.29.1.98 주소가 서버에 의해 할당됨papacl - PAP/PPP - 라인 2에서 사용자 다이얼합니다.주소 10.29.1.100이 서버에 할당되고 인바운드 액세스 목록 101이 적용되며, 라우터에 정의되어 있어야 합니다.loginauto - 회선 3에

서 사용자 다이얼자동 명령어를 통한 로그인 인증은 사용자가 PPP 연결을 사용하도록 하고 풀에서 주소를 할당합니다.

4. 사용자 로그인을 제외한 모든 사용자를 위한 Microsoft Windows 설치시작 **> 프로그램 > 보조 프로그램 > 전화 접속 네트워킹을 선택합니다**.Connections **> Make New Connection을 선택합니다**.연결 이름을 입력합니다.모뎀별 정보를 입력합니다.Configure(**구성) > General(일반**)에서 모뎀의 최고 속도를 선택하지만 아래 확인란을 선택하지 마십시오.Configure **> Connection**에서 8개의 데이터 비트, 패리티 없음 및 1개의 정지 비트를 사용합니다.통화 기본 설정**은 전화 걸기 전 신호음 대기**와 **200초 후 연결되지 않은 경우 통화 취소 입니다**.Advanced(고급)에서 Hardware **Flow Control(하드웨어 흐름 제어)** 및 Modulation Type Standard(**변조 유형 표준)만** 선택합니다.Configure **> Options**에서 상태 제어 아래 외에는 아무것도 확인하지 않습니다.**확인**을 **클릭합니다**.다음 창에서 대상의 전화 번호를 입력한 다음 **다음**을 클릭하고 **마침**을 클릭합니다.새 연결 아이콘이 나타나면 마우스 오른쪽 단추를 클릭하고 **속성**을 선택한 다음 **서버 유형**을 클릭합니다.PPP**:WINDOWS 95, WINDOWS NT 3.5, Internet을 선택하고** 고급 옵션을 선택하지 않습니다.Allowed network protocols(허용된 네트워크 프로토콜)에서 **TCP/IP** 이상을 **선택합니다**.TCP/IP 설정에서 **Server assigned IP address**, **Server assigned name server address** 및 **Use default gateway on remote network**를 선택합니다.**확인**을 **클릭합니다**.전화를 걸려면 연결 대상 창을 표시하려면 아이콘을 두 번 클릭하면 사용자 이름과 암호 필드를 입력한 다음 **연결**을 클릭해야 합니다.
5. Microsoft Windows 95 사용자 로그인자동 설치사용자 로그인 자동, 자동 명령 PPP가 있는 인증 사용자에 대한 컨피그레이션은 Configure(구성) **> Options(옵션)** 창을 제외한 다른 사용자에 대한 컨피그레이션**과** 동일합니다.전화를 **건 후 터미널 창 표시를 선택합니다**.아이콘을 두 번 클릭하여 연결할 연결 대상 창을 표시하면 사용자 이름 및 암호 필드를 입력하지 않습니다.Connect(**연결**)를 클릭하고 라우터에 연결한 후 표시되는 검은색 창에 사용자 이름과 비밀번호를 입력합니다.인증 후 **계속(F7)을** 클릭합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

서버

```
./Cisco Secure -cx -f $BASE/CSU $BASE/config/CSU.cfg
```

라우터

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.특정 명령에 대한 자세한 내용은 Cisco IOS Debug 명령 참조를 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** - 전송 및 수신된 PPP 패킷을 표시합니다.이 명령은 낮은 수준의 패킷 덤프를 표시합니다.
- **debug ppp chap** — CHAP(Challenge Authentication Protocol)를 구현하는 인터네트워크에서 트래픽 및 교환에 대한 정보를 표시합니다.
- **debug aaa authentication** - 사용 중인 인증 방법과 이러한 방법의 결과를 확인합니다.
- **debug aaa authorization** - 사용 중인 권한 부여 방법과 이러한 방법의 결과를 확인합니다.

Cisco Secure Users 파일

```
group = admin {
        password = clear "adminpwd"
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

group = oper {
        password = clear "oper"
        privilege = clear "cisco" 15
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

user = adminusr {
        password = clear "adminusr"
        default service = permit
        }

user = desusr {
        password = des "QjnXYd1kd7ePk"
        default service = permit
        }

user = operator {
        member = oper
        default service = permit
        }

user = time {
        default service = permit
        password = clear "time"
        service = shell  {
                set timeout = 1
                default cmd = permit
                default attribute = permit
        }
}

user = todam {
        password = clear "todam"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 0600 - 1200
```

```
        }
        }

user = todpm {
        password = clear "todpm"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 1200 - 2359
        }
        }

user = telnet {
        password = clear "telnet"
        service = shell  {
                set autocmd = "telnet 171.68.118.102"
                        }
        }

user = limit_lifetime {
        password = clear "cisco" from
        "2 may 2001" until
        "4 may 2001"
        }

user = loneusr {
        password = clear "lonepwd"
        service = shell  {
                cmd = show {
                permit "ver"
                }
                cmd = ping {
                permit "."
                }
                cmd = logout {
                permit "."
                }
        }
}

user = chapuser {
        default service = permit
        password = chap "chapuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = chapaddr {
        password = chap "chapaddr"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.99
                }
        }
}

user = chapacl {
        default service = permit
```

```
        password = chap "chapacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = papuser {
        default service = permit
        password = pap "papuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = papaddr {
        default service = permit
        password = pap "papaddr"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.98
                }
        }
}

user = papacl {
        default service = permit
        password = chap "papacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = loginauto {
        default service = permit
        password = clear "loginauto"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        }
        }
 }

user = somerouters {
   password = clear "somerouters"
   allow koala ".*" "10\.31\.1\.*"
   allow koala.rtp.cisco.com ".*" "10\.31\.1\.*"
   allow 10.31.1.5 ".*" "10\.31\.1\.*"
   refuse ".*" ".*" ".*"
```

```
service=shell {
default cmd=permit
default attribute=permit
}
}
```

관련 정보

- UNIX용 Cisco Secure ACS 제품 지원
- 보안 제품 필드 알림(Cisco Secure UNIX 포함)