잠금 및 키: 동적 액세스 목록

목차

소개

Lock-and-key 액세스를 사용하면 사용자 인증 프로세스를 통해 특정 소스/대상 호스트에 사용자당 액세스를 허용하는 동적 액세스 목록을 설정할 수 있습니다. 사용자 액세스는 보안 제한에 영향을 미치지 않으면서 Cisco IOS® 방화벽을 통해 동적으로 허용됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 경우 랩 환경은 Cisco IOS® Software Release 12.3(1)을 실행하는 2620 라우터로 구성되었습니다. 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 규칙을 참조하십시오.

스푸핑 고려 사항

Lock-and-key 액세스는 외부 이벤트에서 Cisco IOS Firewall을 열 수 있도록 합니다. 이 오프닝이 발생하면 라우터는 소스 주소 스푸핑에 취약합니다. 이를 방지하려면 인증 또는 암호화와 함께 IP 암호화를 사용하여 암호화 지원을 제공합니다.

스푸핑은 모든 기존 액세스 목록에 문제가 있습니다. 잠금 및 키 액세스는 이 문제를 해결하지 않습니다.

잠금 및 키 액세스는 네트워크 방화벽을 통과하는 잠재적인 경로를 제공하므로 동적 액세스를 고려해야 합니다. 인증된 주소를 스푸핑하는 또 다른 호스트는 방화벽 뒤에 액세스할 수 있습니다. 동적 액세스를 사용하면 인증한 주소를 스푸핑하는 권한 없는 호스트가 방화벽 뒤에서 액세스할 수 있습니다. 잠금 및 키 액세스로 인해 주소 스푸핑 문제가 발생하지 않습니다. 이 문제는 사용자의 관심사로만 식별됩니다.

성능

이러한 두 상황에서는 성능이 저하됩니다.

- 각 동적 액세스 목록은 SSE(Silicon Switching Engine)에서 액세스 목록을 강제로 재구축합니다. 이로 인해 SSE 스위칭 경로가 일시적으로 느려집니다.
- 동적 액세스 목록에는 유휴 시간 제한 기능이 필요합니다(시간 제한이 기본값으로 남아 있더라도). 따라서 동적 액세스 목록은 SSE로 전환할 수 없습니다. 이러한 항목은 프로토콜 빠른 스위칭 경로에서 처리됩니다.

보더 라우터 컨피그레이션을 확인합니다. 원격 사용자는 보더 라우터에 액세스 목록 항목을 생성합니다. 액세스 목록이 동적으로 확장되고 축소됩니다. 유휴 시간 초과 또는 최대 시간 초과 기간이 만료되면 항목이 목록에서 동적으로 제거됩니다. 큰 액세스 목록은 패킷 스위칭 성능을 떨어뜨립니다.

잠금 및 키 액세스 사용 시기

잠금 및 키 액세스를 사용하는 경우의 두 가지 예는 다음과 같습니다.

- 원격 호스트가 인터넷을 통해 인터네트워크의 호스트에 액세스할 수 있도록 하려면 Lock-and-key 액세스는 개별 호스트 또는 네트워크 기반으로 방화벽 너머에 대한 액세스를 제한합니다.
- 네트워크의 호스트 하위 집합이 방화벽으로 보호되는 원격 네트워크의 호스트에 액세스하려는 경우 lock-and-key 액세스를 사용하면 TACACS+ 또는 RADIUS 서버를 통해 인증함으로써 원하는 호스트 집합만 액세스 권한을 얻을 수 있습니다.

잠금 및 키 액세스 작업

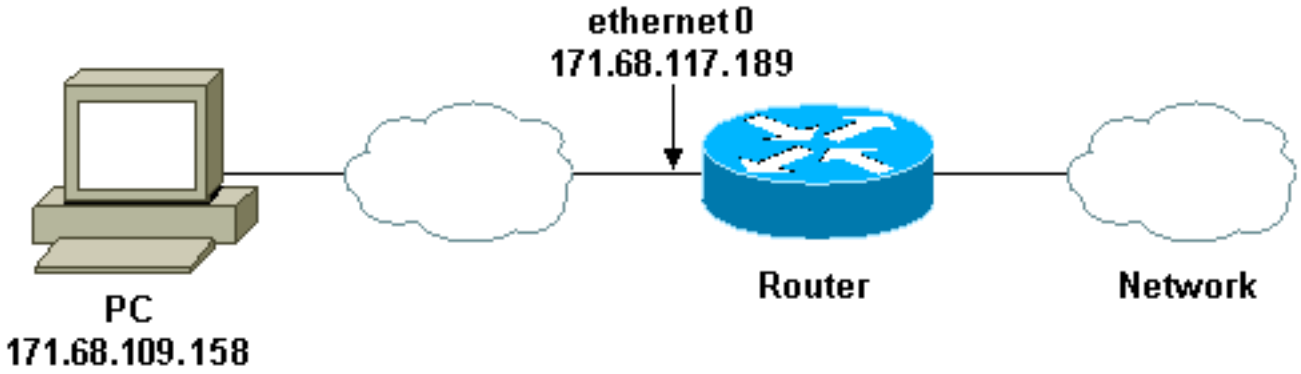
이 프로세스에서는 잠금 및 키 액세스 작업에 대해 설명합니다.

1. 사용자가 잠금 및 키 액세스를 위해 구성된 보더 라우터에 대한 텔넷 세션을 엽니다.
2. Cisco IOS 소프트웨어가 텔넷 패킷을 수신합니다. 사용자 인증 프로세스를 수행합니다. 사용

자가 액세스를 허용하기 전에 인증을 통과해야 합니다. 인증 프로세스는 라우터나 TACACS+ 또는 RADIUS 서버와 같은 중앙 액세스 서버에서 수행됩니다.

샘플 구성 및 문제 해결

네트워크 다이어그램



인증 쿼리 프로세스에 TACACS+ 서버를 사용하는 것이 좋습니다. TACACS+는 인증, 권한 부여 및 계정 관리 서비스를 제공합니다. 또한 프로토콜 지원, 프로토콜 사양 및 중앙 집중식 보안 데이터베이스를 제공합니다.

라우터 또는 TACACS+ 또는 RADIUS 서버에서 사용자를 인증할 수 있습니다.

참고: 이 명령은 달리 명시되지 않는 한 전역적입니다.

라우터에서 로컬 인증을 위해 사용자의 **사용자 이름**이 필요합니다.

```
username test password test
```

vty 라인에 **로그인 로컬**가 있으면 이 사용자 이름이 사용됩니다.

```
line vty 0 4
login local
```

사용자가 access-enable 명령을 실행할 **것을** 신뢰하지 않는 경우 다음 두 가지 중 하나를 수행할 수 있습니다.

- 사용자 단위로 시간 제한을 사용자와 연결합니다.

```
username test autocommand access-enable host
timeout 10
```

또는

- 텔넷에 있는 모든 사용자에게 동일한 시간 제한을 적용합니다.

```
line vty 0 4
login local
autocommand access-enable host timeout 10
```

참고: 구문의 **10**은 액세스 목록의 유휴 시간 제한입니다. 동적 액세스 목록에서 절대 시간 초과로 재정의됩니다.

사용자(모든 사용자)가 라우터에 로그인하고 **access-enable** 명령을 실행할 때 적용되는 확장 액세스 목록을 정의합니다. 필터에 있는 이 "구멍"의 최대 절대 시간은 15분으로 설정됩니다. 15분 후에, 그 구멍은 아무도 그것을 사용하든 말든 닫습니다. 이름 **testlist**가 있어야 하지만 중요하지 않습니다. 소스 또는 대상 주소를 구성하여 사용자가 액세스할 수 있는 네트워크를 제한합니다(여기서 사용자는 제한되지 않음).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

라우터에 텔넷하는 기능을 제외한 모든 것을 차단하는 데 필요한 액세스 목록을 정의합니다(구멍을 열기 위해 사용자가 라우터에 텔넷해야 함). 여기서 IP 주소는 라우터의 이더넷 IP 주소입니다.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

끝에 암시적 **거부**가 있습니다(여기에 입력하지 않음).

사용자가 들어오는 인터페이스에 이 액세스 목록을 적용합니다.

```
interface ethernet1
       ip access-group 120 in
```

넌 끝났어

현재 라우터에서 필터로 표시되는 내용은 다음과 같습니다.

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

내부 네트워크에 액세스하는 사용자는 라우터에 텔넷할 때까지 아무 것도 볼 수 없습니다.

참고: **10**은 액세스 목록의 유휴 시간 제한입니다. 동적 액세스 목록에서 절대 시간 초과로 재정의됩니다.

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test

Connection closed by foreign host.
```

필터는 다음과 같습니다.

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

소스 IP 주소를 기반으로 한 이 사용자의 필터에 구멍이 있습니다. 다른 사람이 이렇게 하면 *두 개의 구멍이* 보입니다.

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

이러한 사용자는 소스 IP 주소에서 모든 대상 IP 주소에 대한 완전한 IP 액세스를 가질 수 있습니다.

TACACS+ 사용

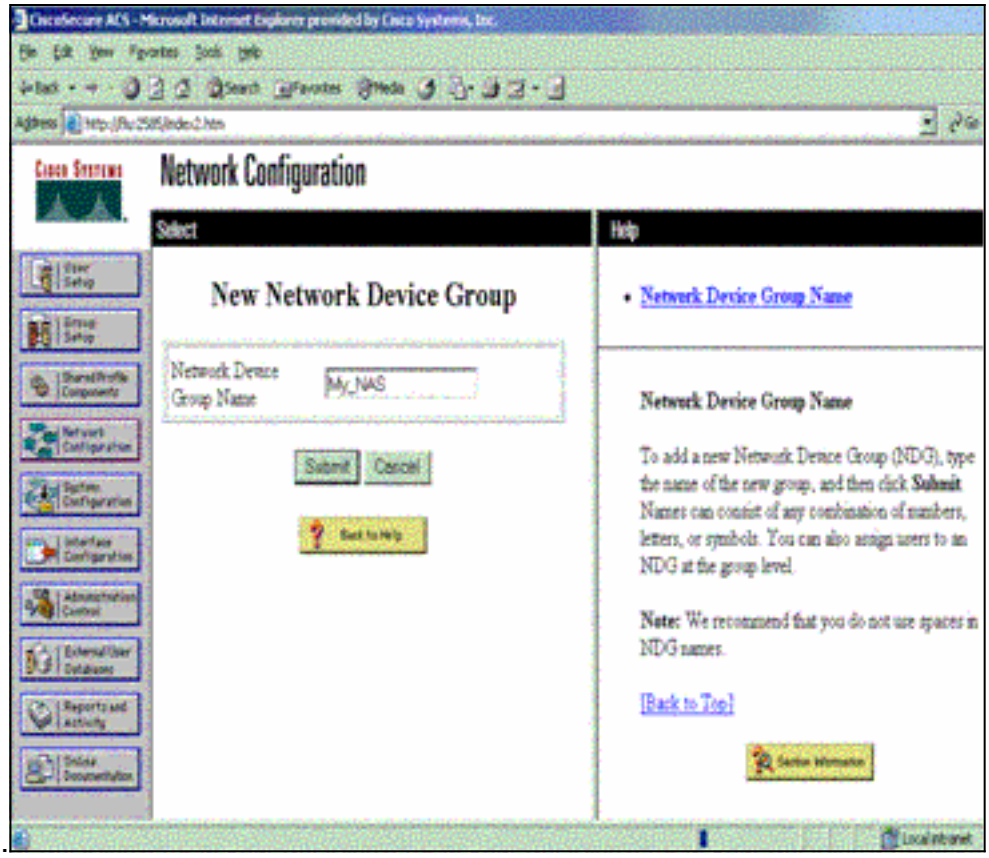
TACACS+ 구성

TACACS+를 사용하기 위해 TACACS+ 서버에서 인증 및 권한 부여를 강제로 수행하도록 TACACS+ 서버를 구성합니다(다음 출력에 표시됨).

```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
```

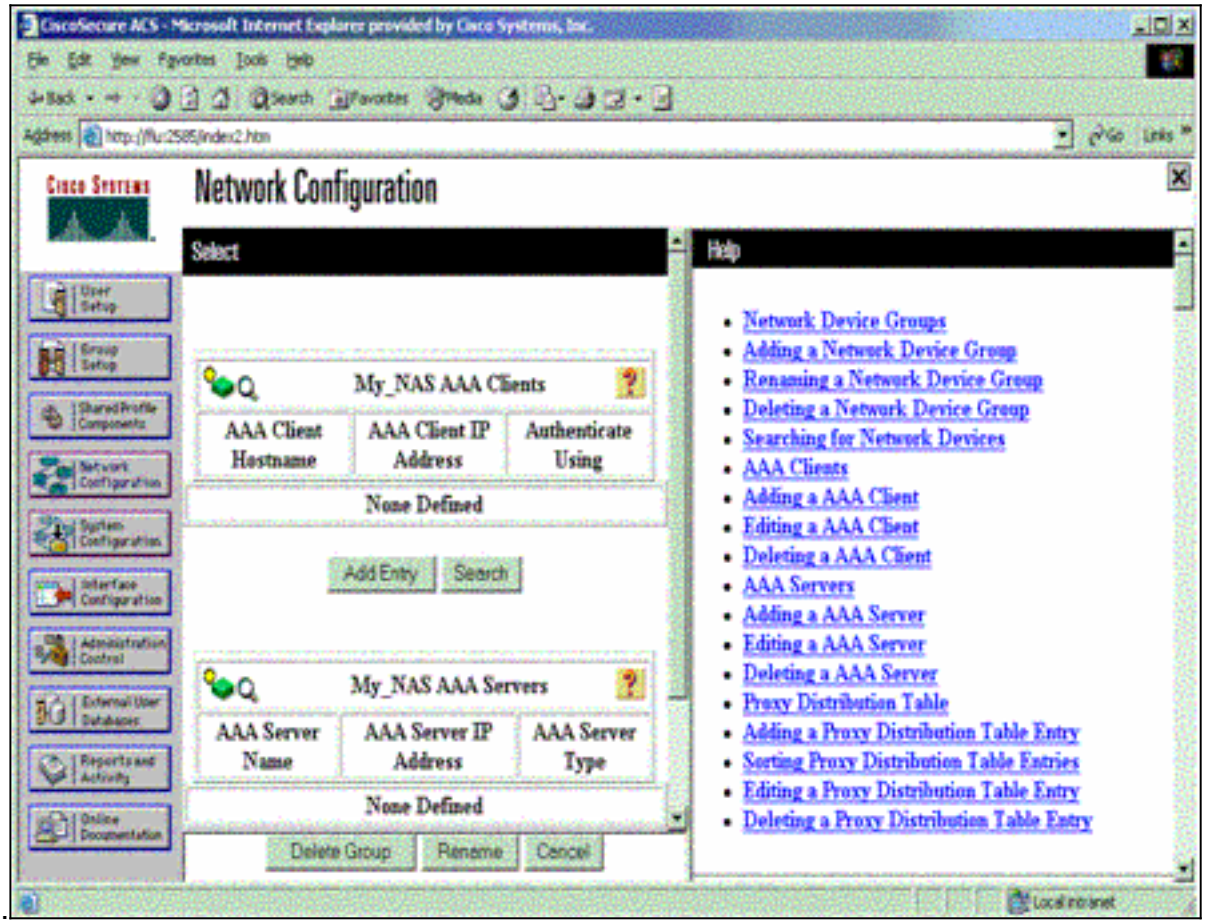
Windows용 Cisco Secure ACS에서 TACACS+를 구성하려면 다음 단계를 완료합니다.

1. 웹 브라우저를 엽니다. http://***<IP_address 또는 DNS_name>:2002*** 형식의 ACS 서버 주소를 입력합니다. 이 예에서는 기본 포트 2002를 사용합니다. 관리자로 로그인합니다.
2. Network **Configuration을 클릭합니다**. Add **Entry(항목 추가)**를 클릭하여 네트워크 액세스 서버(NAS)가 포함된 네트워크 장치 그룹을 생성합니다. 그룹의 이름을 입력하고 Submit(제출)을



클릭합니다.

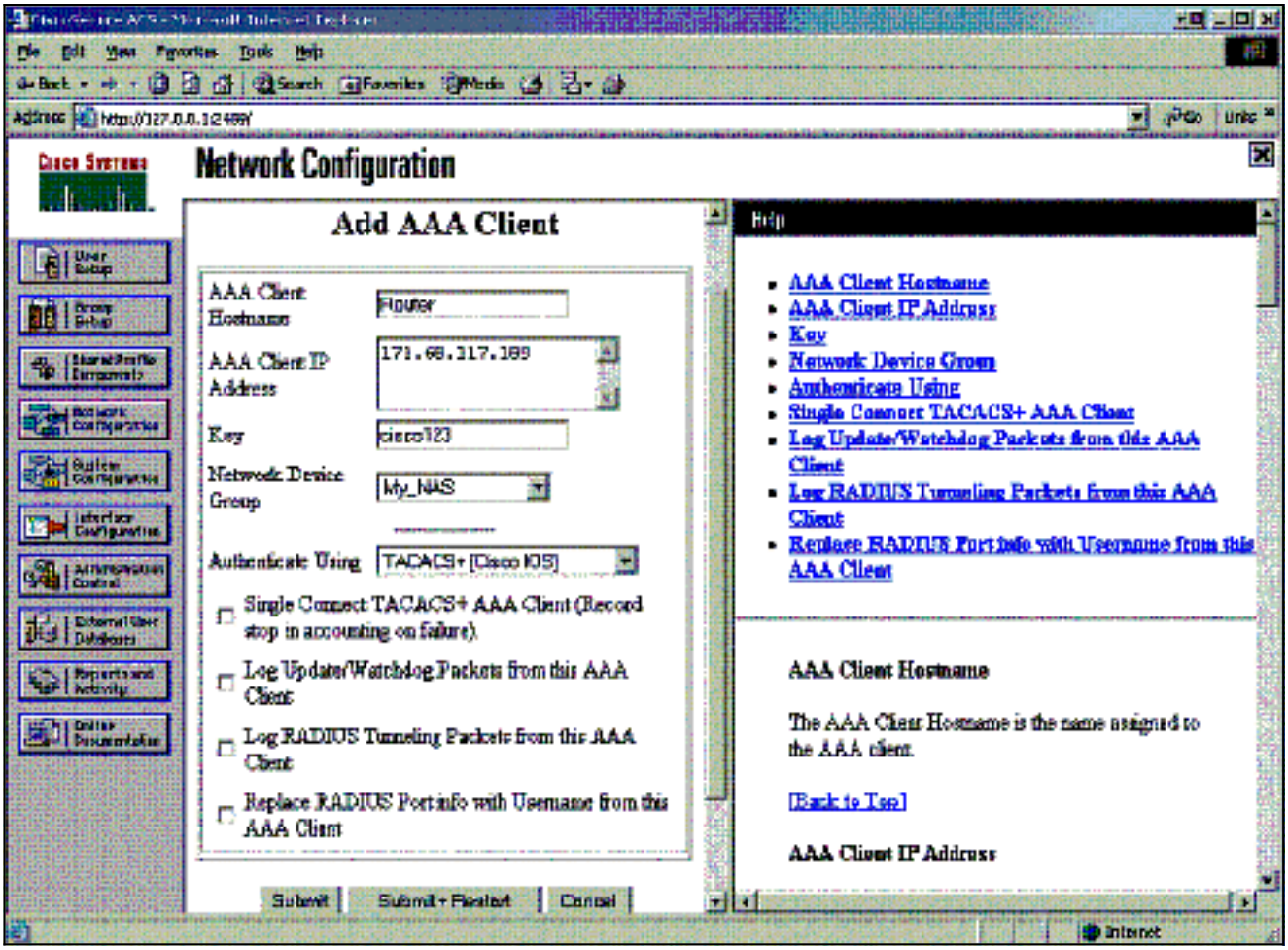
3. Add **Entry(항목 추가)**를 클릭하여 AAA(인증, 권한 부여 및 계정 관리) 클라이언트(NAS)를 추가합니다



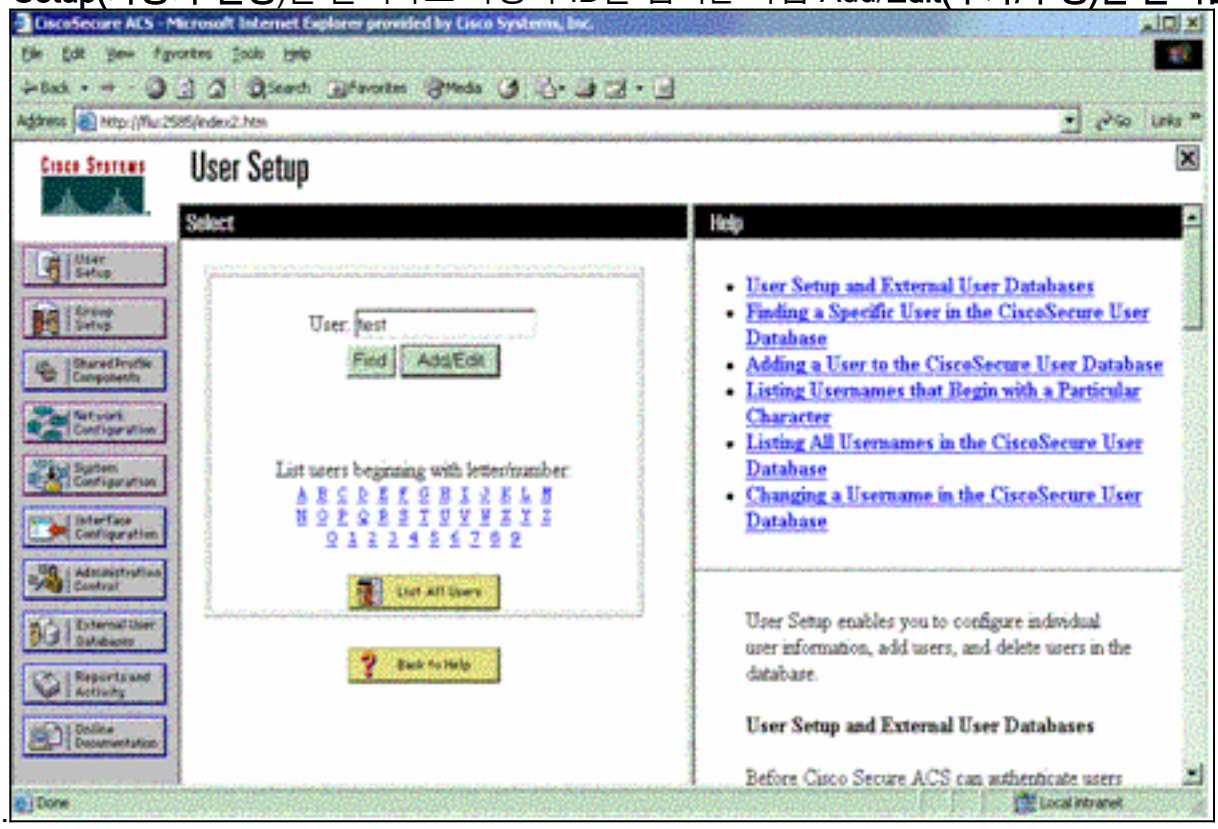
.

4. AAA 서버와 NAS 간의 통신을 암호화하는 데 사용되는 호스트 이름, IP 주소 및 키를 입력합니다. 인증 방법**으로 TACACS+(Cisco IOS)**를 선택합니다. 완료되면 Submit **+Restart**를 클릭하여 변경 사항을 적용합니다

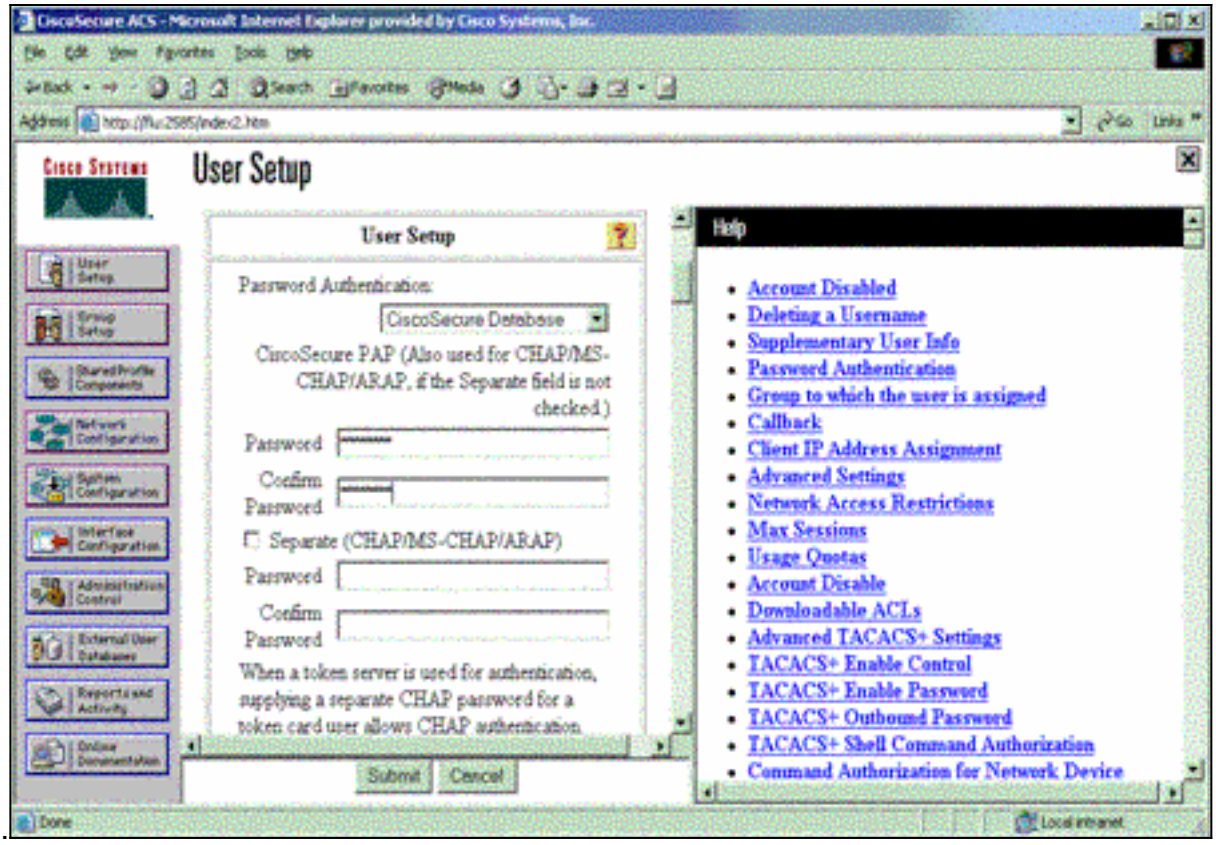
.



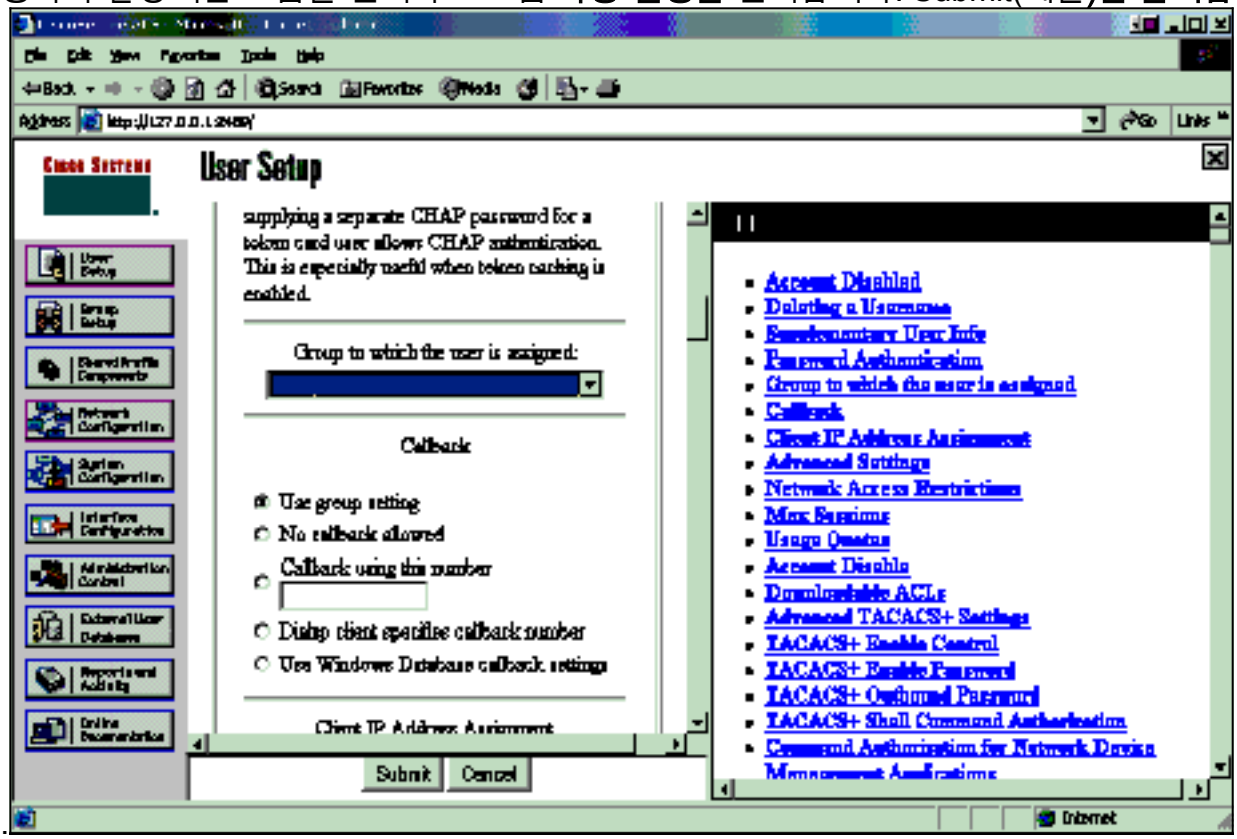
5. User **Setup(사용자 설정)**을 클릭하고 사용자 ID를 입력한 다음 Add/**Edit(추가/수정)를 클릭합니다**.



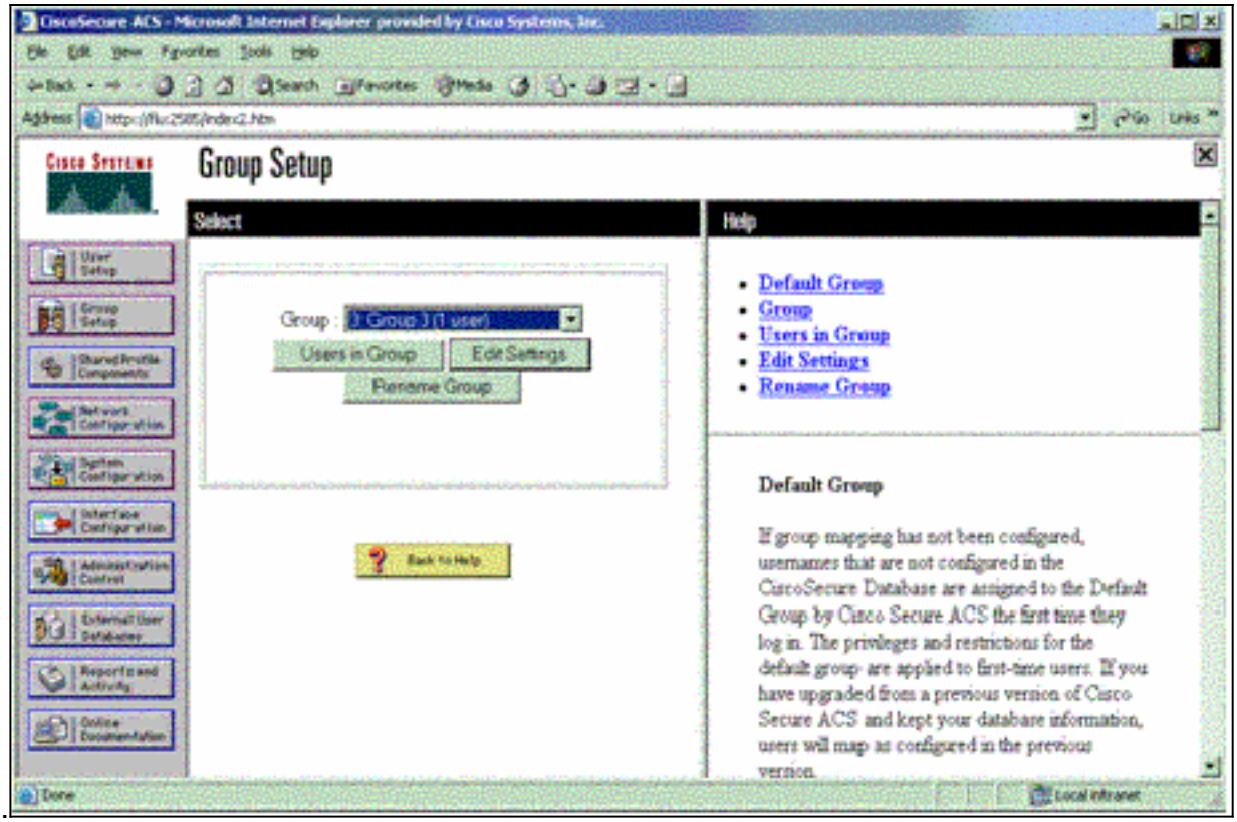
6. 사용자를 인증할 데이터베이스를 선택합니다. (이 예에서는 사용자가 "test"이고 ACS의 내부 데이터베이스가 인증에 사용됩니다.) 사용자의 비밀번호를 입력하고 비밀번호를 확인합니다



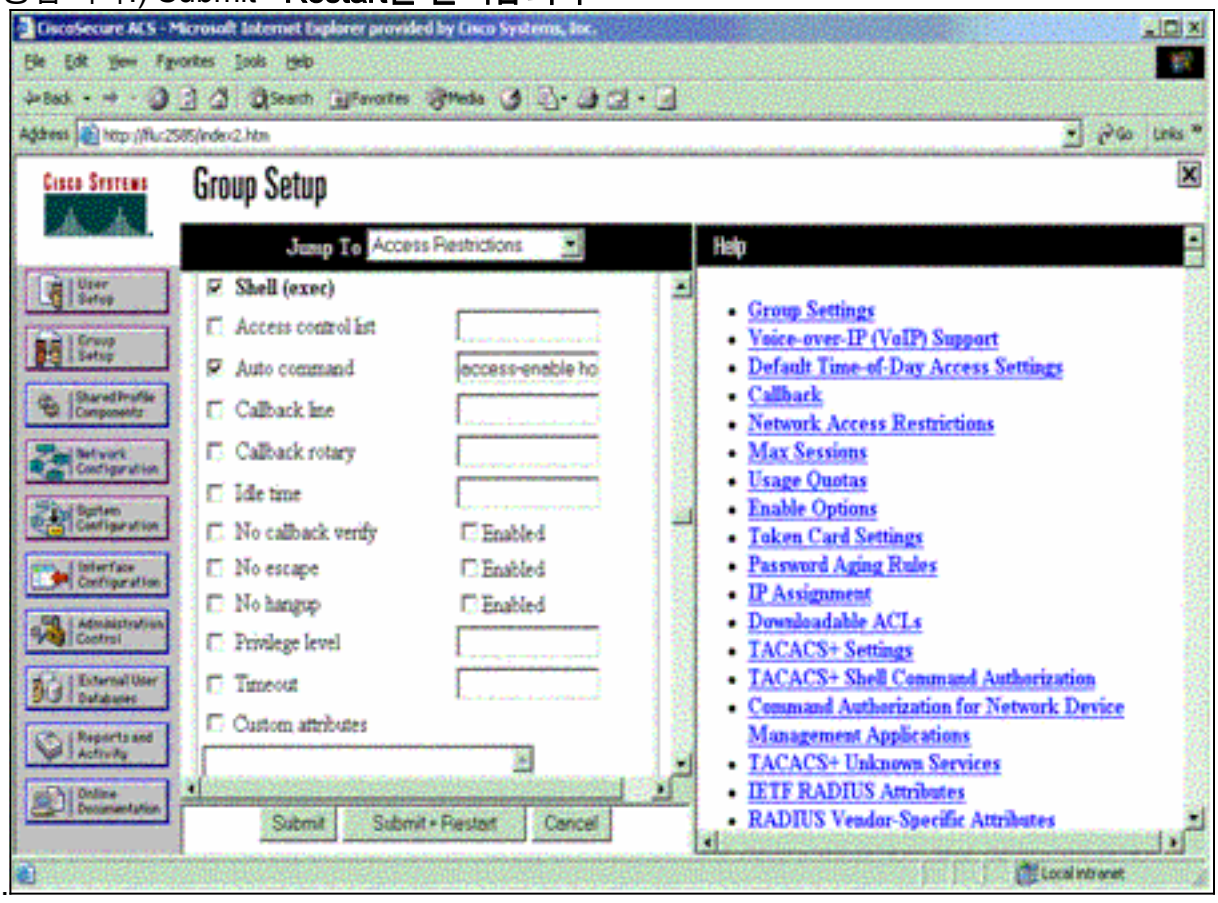
7. 사용자가 할당되는 그룹을 선택하고 그룹 **사용 설정을** 선택합니다. Submit(제출)**을 클릭합니다**.



8. Group **Setup을 클릭합니다**. 7단계에서 사용자에게 할당된 그룹을 선택합니다. **설정 편집을 누릅니다**



9. 아래로 스크롤하여 TACACS+ Settings(TACACS+ 설정) 섹션으로 이동합니다. **Shell exec**에 대한 상자를 **선택합니다**. Auto **명령**의 확인란을 **선택합니다**. 사용자의 성공적인 권한 부여 시 수행할 auto-command를 입력합니다. (이 예에서는 **access-enable host timeout 10** 명령**을** 사용합니다.) Submit **+Restart를 클릭합니다**



TACACS+ 문제 해결

TACACS+ 문제를 해결하려면 NAS에서 이러한 **debug** 명령을 사용합니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug tacacs authentication**—TACACS+ 인증 프로세스에 대한 정보를 표시합니다. 일부 버전의 소프트웨어에서만 사용할 수 있습니다. 사용할 수 없는 경우 디버그 **tacacs**만 사용합니다.
- **debug tacacs authorization**—TACACS+ 권한 부여 프로세스에 대한 정보를 표시합니다. 일부 버전의 소프트웨어에서만 사용할 수 있습니다. 사용할 수 없는 경우 디버그 **tacacs**만 사용합니다.
- **debug tacacs events** - TACACS+ 헬퍼 프로세스의 정보를 표시합니다. 일부 버전의 소프트웨어에서만 사용할 수 있습니다. 사용할 수 없는 경우 디버그 **tacacs**만 사용합니다.

AAA 문제를 해결하려면 다음 명령을 사용합니다.

- **debug aaa authentication**—AAA/TACACS+ 인증에 대한 정보를 표시합니다.
- **debug aaa authorization** - AAA/TACACS+ 권한 부여에 대한 정보를 표시합니다.

샘플 **디버그** 출력은 ACS TACACS+ 서버에서 성공적인 인증 및 권한 부여 프로세스를 보여줍니다.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
 TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/82A2E088: Processing the reply packet
 TPLUS: Received authen response status GET_USER (7)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/8347F3FC: Processing the reply packet
 TPLUS: Received authen response status GET_PASSWORD (8)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
```

```
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

RADIUS 사용

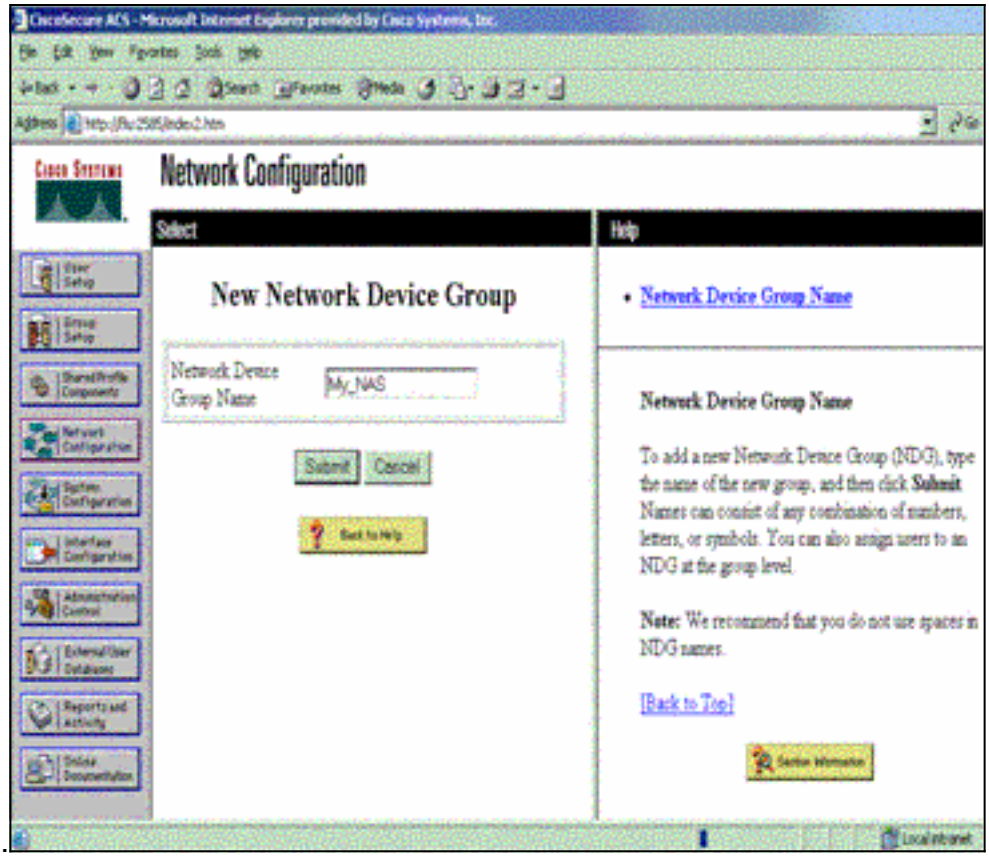
RADIUS 구성

RADIUS를 사용하려면 RADIUS 서버를 구성하여 권한 부여 매개 변수(autocommand)를 사용하여 RADIUS 서버에서 인증을 강제로 수행하도록 하고 다음 그림과 같이 공급업체별 특성 26에서 다운되도록 합니다.

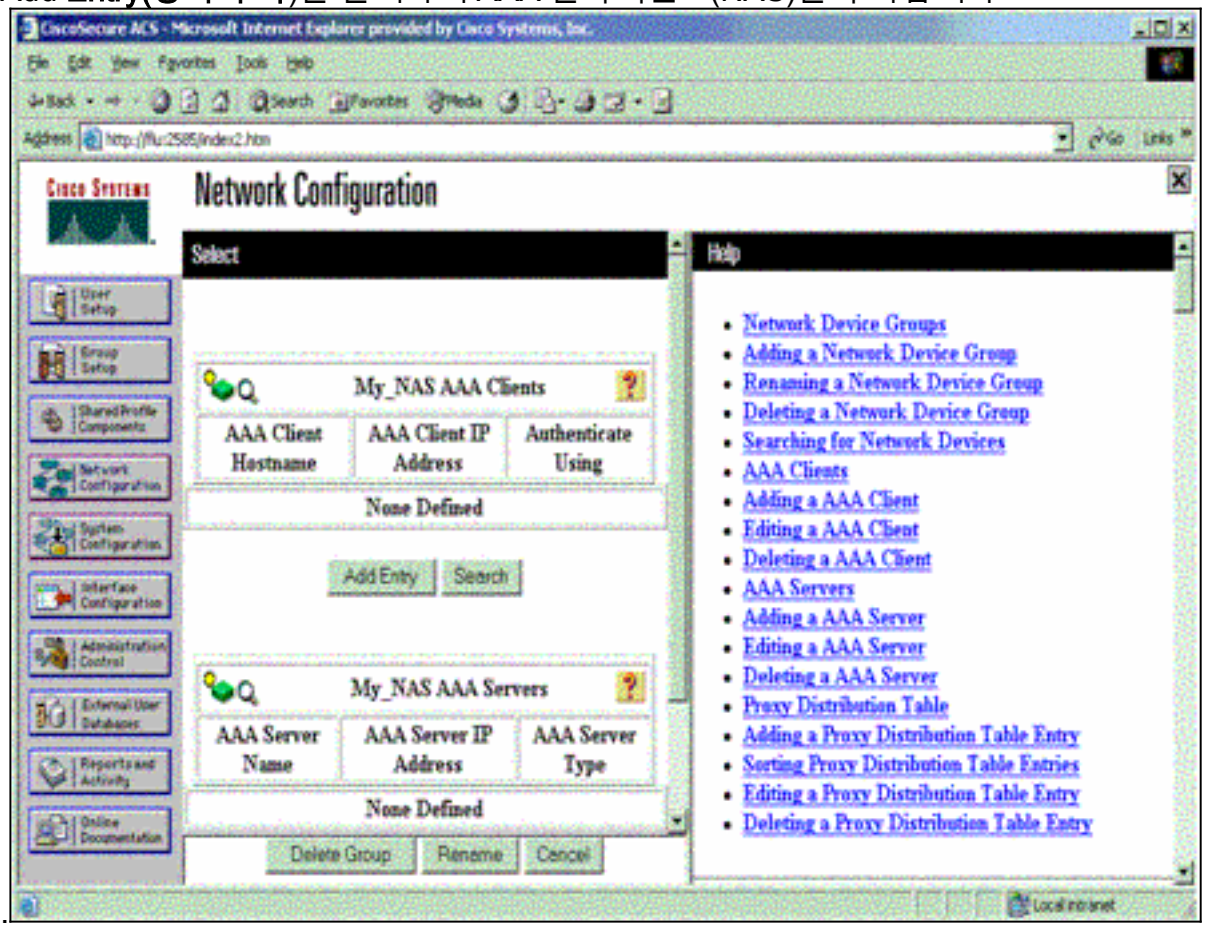
```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
   acct-port 1646 key cisco123
```

Windows용 Cisco Secure ACS에서 RADIUS를 구성하려면 다음 단계를 완료합니다.

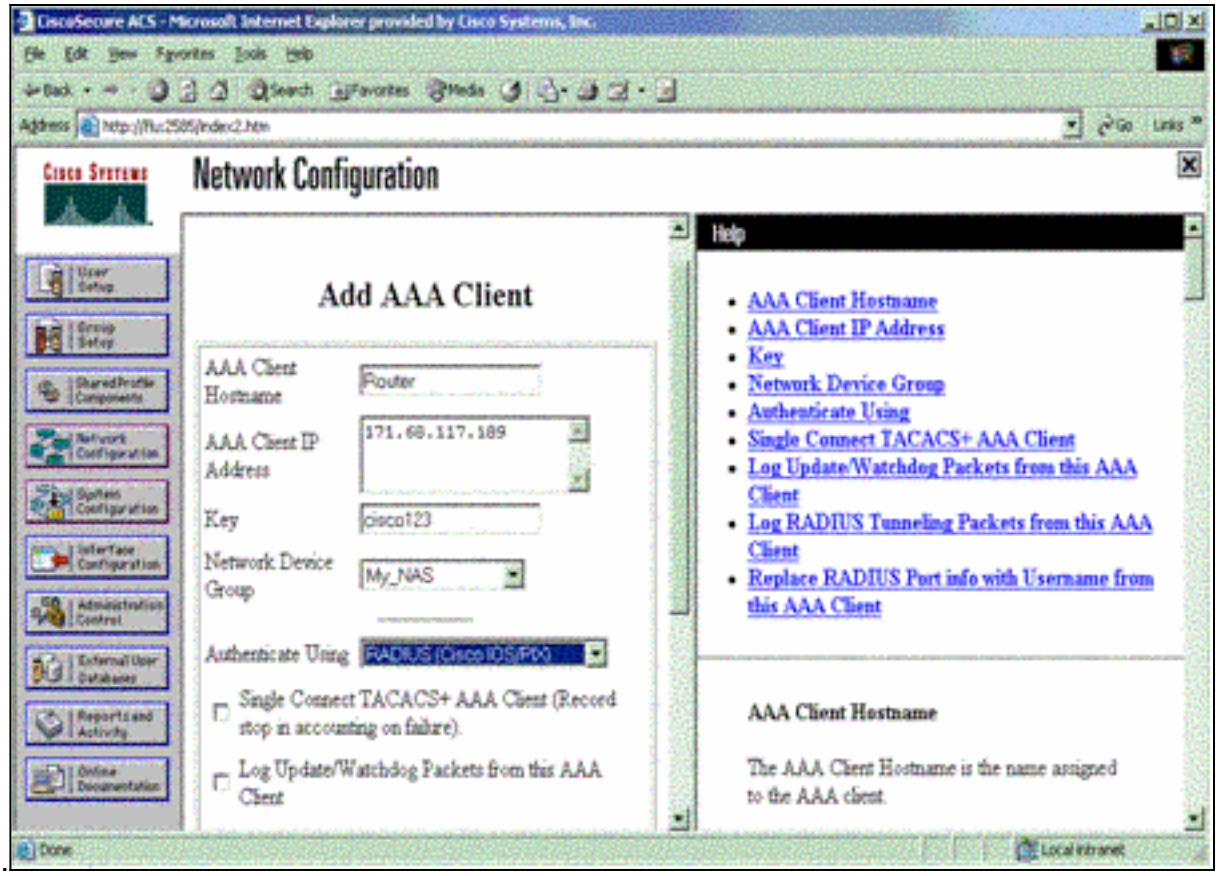
1. 웹 브라우저를 열고 ACS 서버의 주소를 입력합니다. 이 주소는 http://*<IP_address 또는 DNS_name>:2002 형식입니다*. 이 예에서는 기본 포트 2002를 사용합니다. 관리자로 로그인합니다.
2. Network **Configuration을 클릭합니다**. Add **Entry(항목 추가)**를 클릭하여 NAS를 포함하는 네트워크 디바이스 그룹을 생성합니다. 그룹의 이름을 입력하고 Submit(제출)을 **클릭합니다**



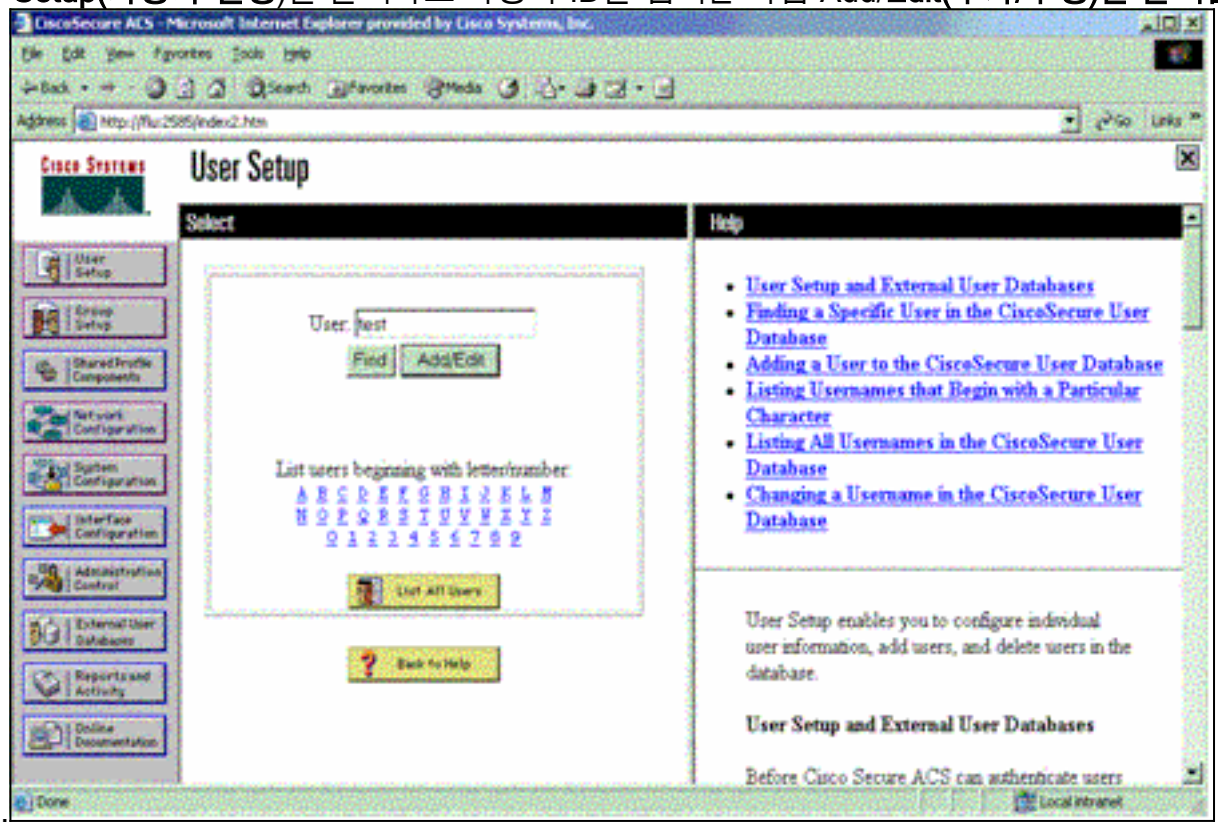
3. Add **Entry(항목 추가)**를 클릭하여 AAA 클라이언트(NAS)를 추가합니다



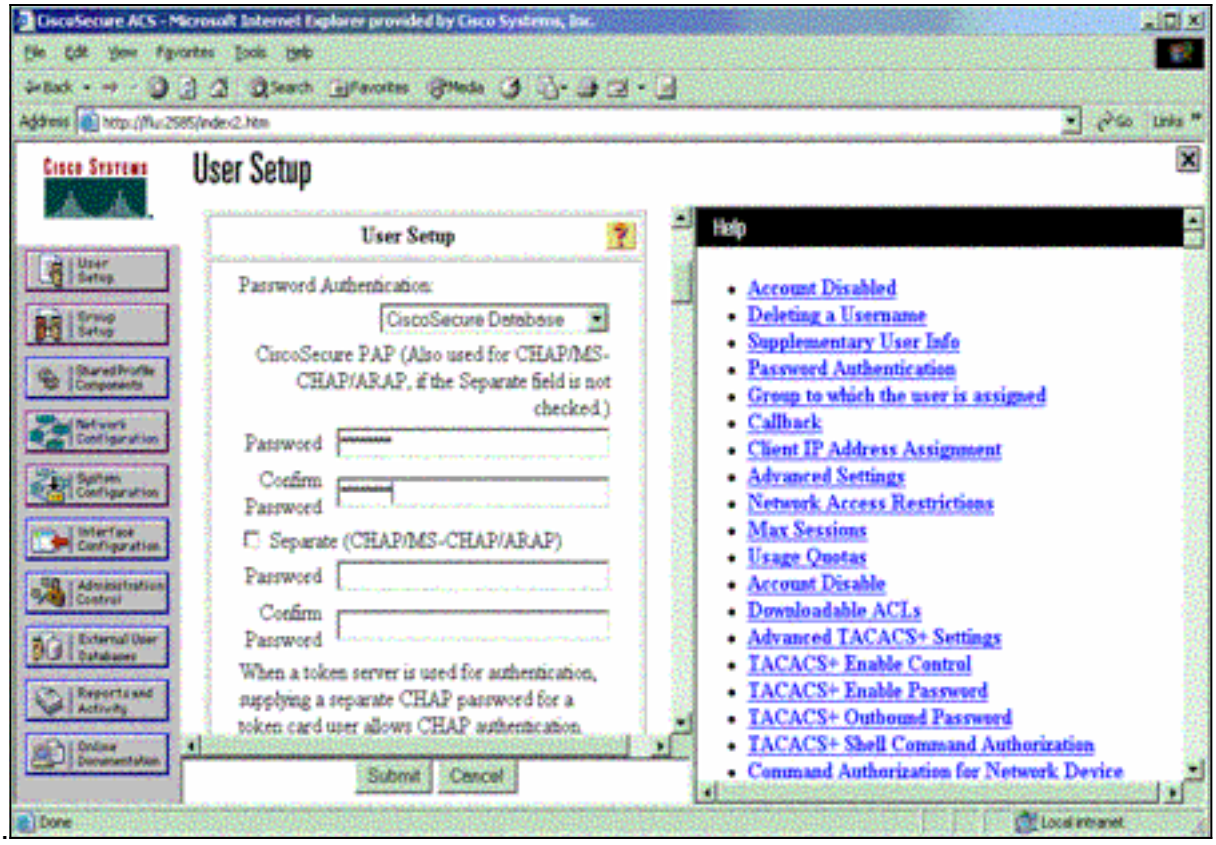
4. AAA 서버와 NAS 간의 통신을 암호화하는 데 사용되는 호스트 이름, IP 주소 및 키를 입력합니다. 인증 방법**으로 RADIUS(Cisco IOS/PIX)**를 선택합니다. 완료되면 Submit **+Restart를** 클릭하여 변경 사항을 적용합니다



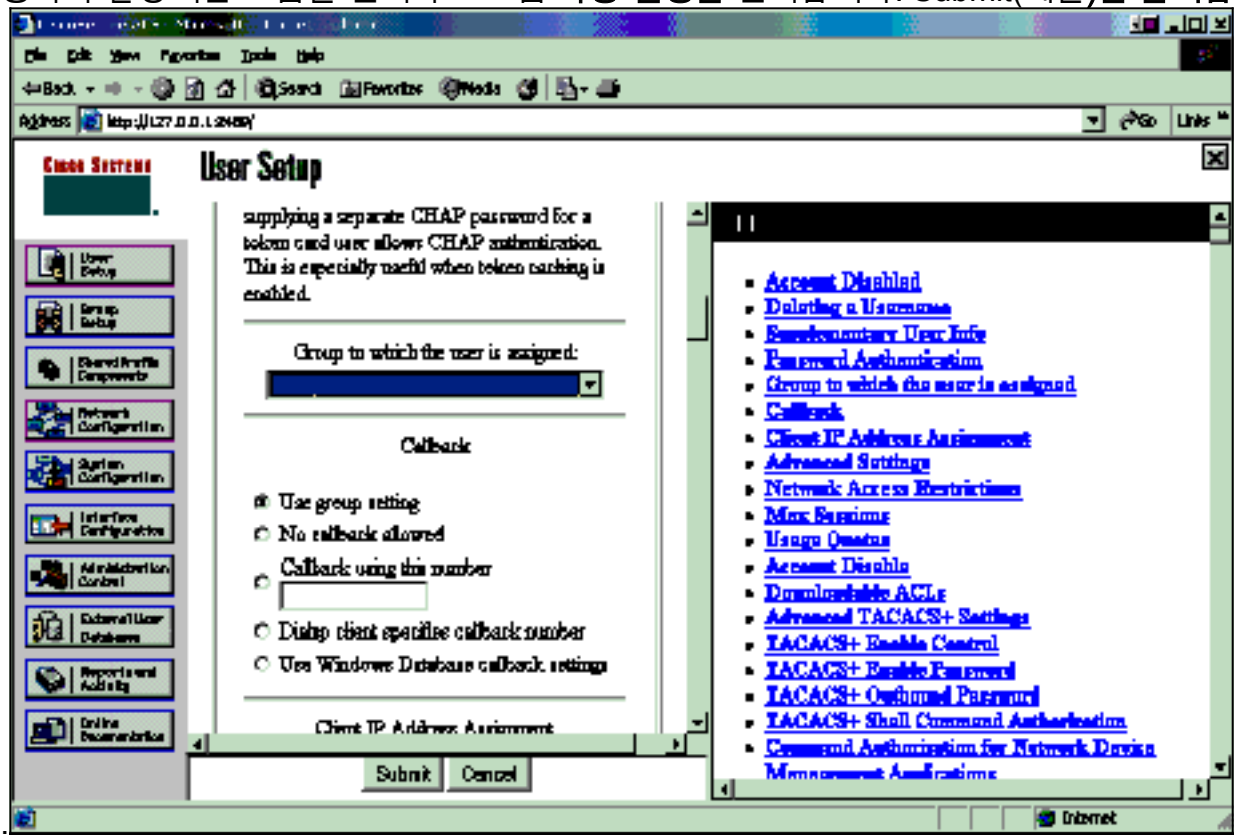
5. User **Setup(사용자 설정)**을 클릭하고 사용자 ID를 입력한 다음 Add/**Edit(추가/수정)를 클릭합니다**.



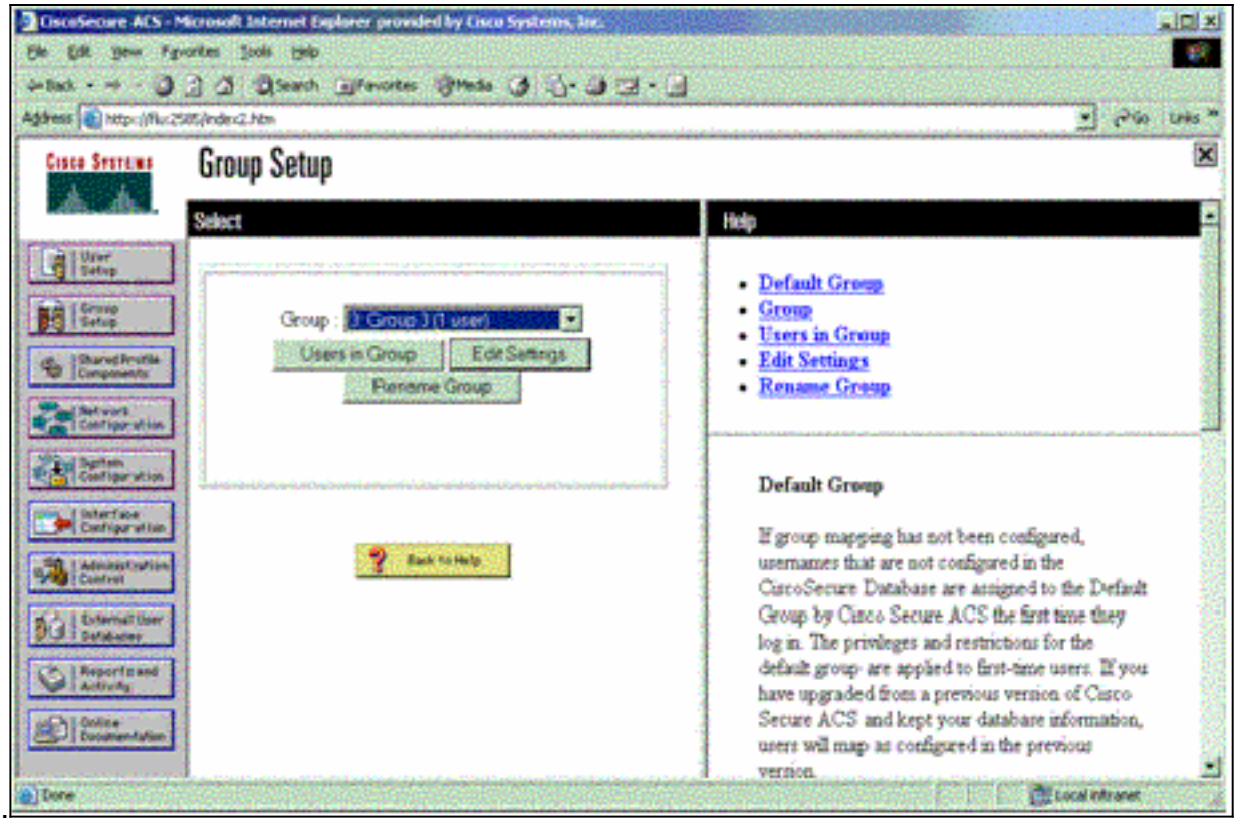
6. 사용자를 인증할 데이터베이스를 선택합니다. (이 예에서는 사용자가 "test"이고 ACS의 내부 데이터베이스가 인증에 사용됩니다.) 사용자의 비밀번호를 입력하고 비밀번호를 확인합니다



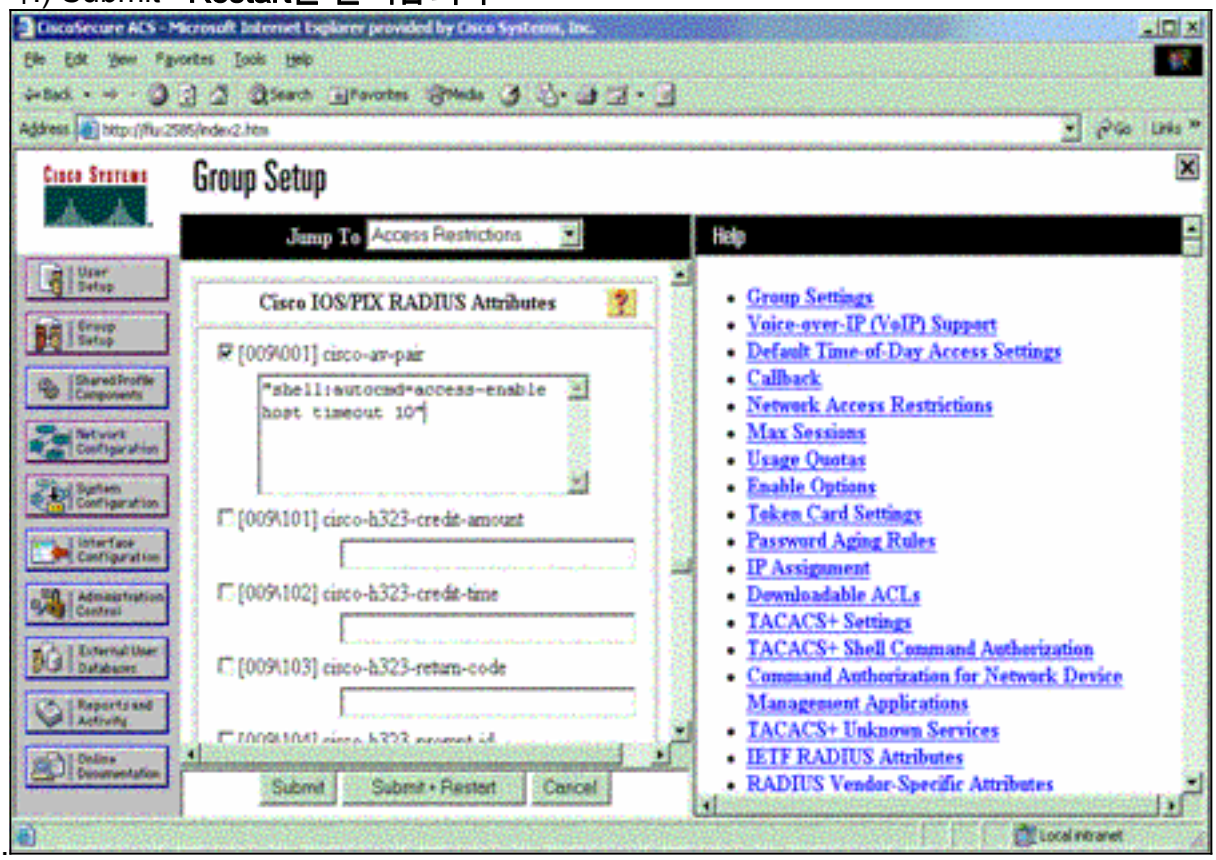
7. 사용자가 할당되는 그룹을 선택하고 그룹 **사용 설정을** 선택합니다. Submit(제출)**을 클릭합니다**.



8. **그룹 설정**을 클릭하고 이전 단계에서 사용자가 할당된 그룹을 선택합니다. Edit **Settings를 클릭합니다**



9. 아래로 스크롤하여 Cisco IOS/PIX RADIUS Attributes(Cisco IOS/PIX RADIUS 특성) 섹션으로 이동합니다. **cisco-av-pair**의 상자를 **선택합니다**. 사용자의 성공적인 권한 부여 시 수행할 shell 명령을 입력합니다. (이 예에서는 **shell:autocmd=access-enable host timeout 10을** 사용합니다.) Submit **+Restart를 클릭합니다**



RADIUS 문제 해결

RADIUS 문제를 해결하려면 NAS에서 이러한 debug 명령을 사용합니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug radius** - RADIUS와 관련된 정보를 표시합니다.

AAA 문제를 해결하려면 다음 명령을 사용합니다.

- **debug aaa authentication**—AAA/TACACS+ 인증에 대한 정보를 표시합니다.
- **debug aaa authorization** - AAA/TACACS+ 권한 부여에 대한 정보를 표시합니다.

샘플 **디버그** 출력은 RADIUS에 대해 구성된 ACS에서 성공적인 인증 및 권한 부여 프로세스를 보여 줍니다.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=====================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
 RADIUS/ENCODE(00000003): send packet; GET_USER
 RADIUS/ENCODE(00000003): ask "Password: "
 RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
 RADIUS:  AAA Unsupported     [152] 5
 RADIUS:   74 74 79                        [tty]
 RADIUS(00000003): Storing nasport 66 in rad_db
 RADIUS/ENCODE(00000003): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off
 RADIUS(00000003): Config NAS IP: 0.0.0.0
 RADIUS/ENCODE(00000003): acct_session_id: 1
 RADIUS(00000003): sending
 RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
   for Radius-Server 10.48.66.53
 RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
   id 21645/1, len 77
 RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
   BE B5 07 BD E9 05 5B 5D
 RADIUS:  User-Name           [1]   7   "test"
 RADIUS:  User-Password       [2]   18  *
 RADIUS:  NAS-Port            [5]   6   66
 RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
 RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
 RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
 RADIUS: Received from id 21645/1 10.48.66.53:1645,
   Access-Accept, len 93
 RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
   68 4B C3 FC 25 21 47 CD
 RADIUS:  Vendor, Cisco       [26]  51
 RADIUS:   Cisco AVpair       [1]   45
   "shell:autocmd=access-enable host timeout 10"
 RADIUS:  Class               [25]  22
 RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
   [CISCOACS:ac127c0]
 RADIUS:   31 2F 36 36                  [1/66]
 RADIUS(00000003): Received from id 21645/1
 AAA/AUTHOR/EXEC(00000003): processing AV
   autocmd=access-enable host timeout 10
 AAA/AUTHOR/EXEC(00000003): Authorization successful
```

관련 정보

- Cisco IOS Lock-and-Key 보안
- TACACS/TACACS+ 지원 페이지
- IOS 설명서의 TACACS+
- RADIUS 지원 페이지
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems