IOS 및 ASA/PIX/FWSM의 ACS 셸 명령 권한 부여 집합 구성 예

목차

소개

이 문서에서는 Cisco IOS® 라우터 또는 스위치와 같은 AAA 클라이언트 및 TACACS+를 권한 부여 프로토콜로 사용하는 Cisco Security Appliance(ASA/PIX/FWSM)에 대해 Cisco Secure ACS(Access Control Server)의 셸 권한 부여 집합을 구성하는 방법에 대해 설명합니다.

참고: ACS Express는 명령 권한 부여를 지원하지 않습니다.

사전 요구 사항

요구 사항

이 문서에서는 기본 컨피그레이션이 AAA 클라이언트와 ACS 둘 다에 설정되어 있다고 가정합니다.

ACS에서 **Interface Configuration(인터페이스 컨피그레이션) > Advanced Options(고급 옵션)**를 선택하고 **Per-user TACACS+/RADIUS Attributes(사용자별 TACACS+/RADIUS 특성) 확인란**이 선택

되었는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 3.3 이상을 실행하는 Cisco Secure Access Control Server(ACS)를 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 참조하십시오.

명령 권한 부여 집합

명령 권한 부여 세트는 지정된 네트워크 디바이스에서 실행되는 각 명령의 권한 부여를 제어하는 중앙 메커니즘을 제공합니다. 이 기능은 권한 부여 제한을 설정하는 데 필요한 확장성과 관리 편의성을 크게 향상시킵니다.

ACS에서 기본 명령 권한 부여 세트는 셸 명령 권한 부여 세트 및 PIX 명령 권한 부여 세트를 포함합니다. CiscoWorks Management Center for Firewalls와 같은 Cisco 디바이스 관리 애플리케이션은 ACS에 추가 명령 권한 부여 세트 유형을 지원하도록 지시할 수 있습니다.

참고: PIX 명령 권한 부여 세트에서는 TACACS+ 명령 권한 부여 요청이 서비스를 pixshell로 식별해야 *합니다*. 이 서비스가 방화벽에서 사용하는 PIX OS 버전에서 구현되었는지 확인합니다. 그렇지 않은 경우 Shell Command Authorization Sets를 사용하여 PIX 디바이스에 대한 명령 권한 부여를 수행합니다. 자세한 내용은 사용자 그룹에 대한 셸 명령 권한 부여 집합 구성을 참조하십시오.

참고: PIX OS 버전 6.3부터는 pixshell 서비스가 구현되지 않았습니다.

참고: Cisco Security Appliances(ASA/PIX)에서는 현재 로그인 중에 사용자를 활성화 모드로 직접 전환할 수 없습니다. 사용자가 수동으로 활성화 모드를 시작해야 합니다.

디바이스 호스팅 관리 텔넷 세션을 더 효과적으로 제어할 수 있도록 TACACS+를 사용하는 네트워크 디바이스는 실행하기 전에 각 명령행에 대한 권한 부여를 요청할 수 있습니다. 지정된 디바이스에서 특정 사용자가 실행하도록 허용하거나 거부하는 명령 집합을 정의할 수 있습니다. ACS는 다음과 같은 기능으로 이 기능을 더욱 향상시켰습니다.

- **재사용 가능한 명명된 명령 권한 부여 세트** - 사용자 또는 사용자 그룹을 직접 인용하지 않고 명명된 명령 권한 부여 세트를 생성할 수 있습니다. 서로 다른 액세스 프로필을 정의하는 여러 명령 권한 부여 집합을 정의할 수 있습니다. 예를 들면 다음과 같습니다.*Help desk* 명령 권한 부여 집합을 사용하면 show run과 같은 상위 레벨 찾아보기 명령에 대한 액세스를 허용하고 모든 **컨피그레이션 명령**을 거부할 수 있습니다.모든 *네트워크 엔지니어* 명령 권한 부여 집합에는 기업 내 모든 네트워크 엔지니어에 대해 허용되는 명령의 제한된 목록이 포함될 수 있습니다.로컬 *네트워크 엔지니어* 명령 권한 부여 집합은 모든 명령을 허용할 수 있으며 IP 주소 구성 명령을 포함할 수 있습니다.
- **Fine Configuration Granularity**(미세 컨피그레이션 세분화) - 명명된 명령 권한 부여 집합과 NDG(네트워크 디바이스 그룹) 간의 연결을 생성할 수 있습니다. 따라서 사용자가 액세스하는

네트워크 디바이스에 따라 사용자에 대해 서로 다른 액세스 프로필을 정의할 수 있습니다. 동일한 명명된 명령 권한 부여 집합을 둘 이상의 NDG와 연결하고 둘 이상의 사용자 그룹에 사용할 수 있습니다. ACS는 데이터 무결성을 적용합니다. 명명된 명령 권한 부여 세트는 ACS 내부 데이터베이스에 유지됩니다. ACS 백업 및 복원 기능을 사용하여 백업 및 복원할 수 있습니다. 명령 권한 부여 집합을 다른 컨피그레이션 데이터와 함께 보조 ACS에 복제할 수도 있습니다.

Cisco 디바이스 관리 애플리케이션을 지원하는 명령 권한 부여 세트 유형의 경우 명령 권한 부여 세트를 사용할 때와 유사한 이점을 제공합니다. 디바이스 관리 애플리케이션에서 다양한 권한에 대한 권한 부여를 적용하기 위해 디바이스 관리 애플리케이션의 사용자가 포함된 ACS 그룹에 명령 권한 부여 세트를 적용할 수 있습니다. ACS 그룹은 디바이스 관리 애플리케이션 내에서 서로 다른 역할에 해당할 수 있으며, 사용자는 각 그룹에 서로 다른 명령 권한 부여 집합을 적용할 수 있습니다.

ACS에는 명령 권한 부여 필터링의 세 가지 순차적 단계가 있습니다. 각 명령 권한 부여 요청은 나열된 순서대로 평가됩니다.

1. **Command Match**(명령 일치) - ACS는 처리되는 명령이 명령 권한 부여 집합에 나열된 명령과 일치하는지 여부를 확인합니다. 명령이 일치하지 않으면 명령 권한 부여는 Unmatched Commands 설정에 의해 결정됩니다. *허용 또는 거부*. 그렇지 않으면 명령이 일치하면 평가가 계속됩니다.
2. **Argument Match**(인수 일치) - ACS는 제공된 명령 인수가 명령 권한 부여 집합에 나열된 명령 인수와 일치하는지 여부를 확인합니다.인수가 일치하지 않으면 Permit Unmatched Args 옵션의 활성화 여부에 따라 명령 권한 부여가 결정됩니다. 일치하지 않는 인수가 허용되면 명령이 승인되고 평가가 종료됩니다. 그렇지 않으면 명령이 승인되지 않고 평가가 종료됩니다.모든 인수가 일치하면 평가가 계속됩니다.
3. **Argument Policy**(인수 정책) - ACS에서 명령의 인수가 명령 권한 부여 집합의 인수와 일치하는지 확인하면 ACS에서 각 명령 인수가 명시적으로 허용되는지 여부를 확인합니다. 모든 인수가 명시적으로 허용되는 경우 ACS는 명령 권한 부여를 수행합니다. 인수가 허용되지 않으면 ACS는 명령 권한 부여를 거부합니다.

셸 명령 권한 부여 집합 추가

이 섹션에서는 명령 권한 부여 집합을 추가하는 방법을 설명하는 다음 시나리오를 제공합니다.

- 시나리오 1: 읽기-쓰기 액세스 또는 전체 액세스 권한
- 시나리오 2: 읽기 전용 액세스 권한
- 시나리오 3: 제한된 액세스에 대한 권한

참고: 명령 권한 부여 세트를 만드는 방법에 대한 자세한 내용은 User Guide for Cisco Secure Access Control Server 4.1의 Adding a Command Authorization Set 섹션을 참조하십시오. 명령 권한 부여 세트를 편집하고 삭제하는 방법에 대한 자세한 내용은 명령 권한 부여 세트 편집 및 명령 권한 부여 세트 삭제를 참조하십시오.

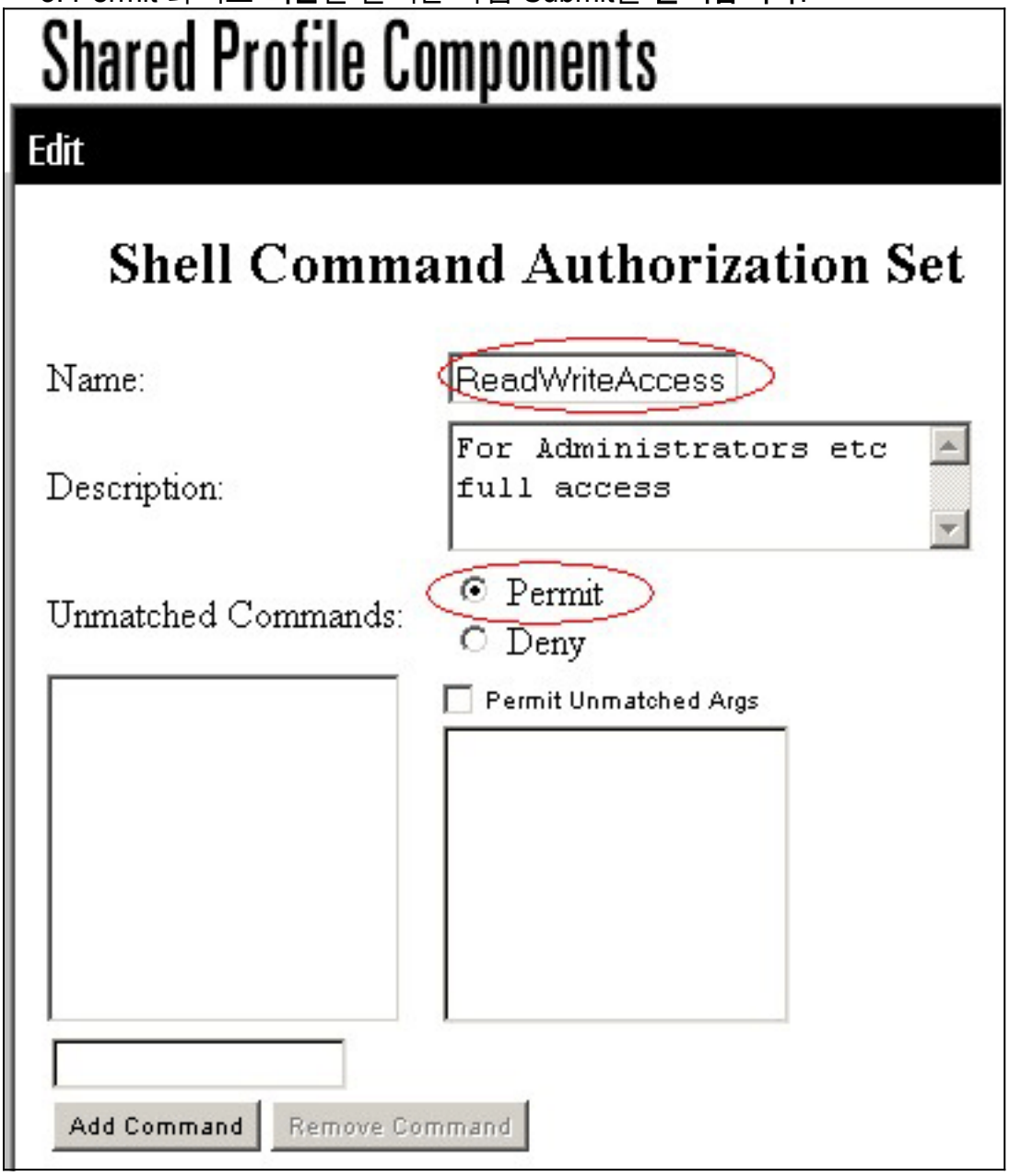
시나리오 1: 읽기-쓰기 액세스 또는 전체 액세스 권한

이 시나리오에서는 사용자에게 읽기/쓰기(또는 전체) 액세스 권한이 부여됩니다.

Shared Profile Components 창의 Shell Command Authorization Set 영역에서 다음 설정을 구성합니다.

1. Name 필드에 명령 권한 **부여** 집합 이름으로 ReadWriteAccess를 입력합니다.
2. Description 필드에 명령 권한 부여 세트에 대한 설명을 입력합니다.

3. Permit 라디오 **버튼**을 클릭한 다음 Submit을 **클릭합니다**.

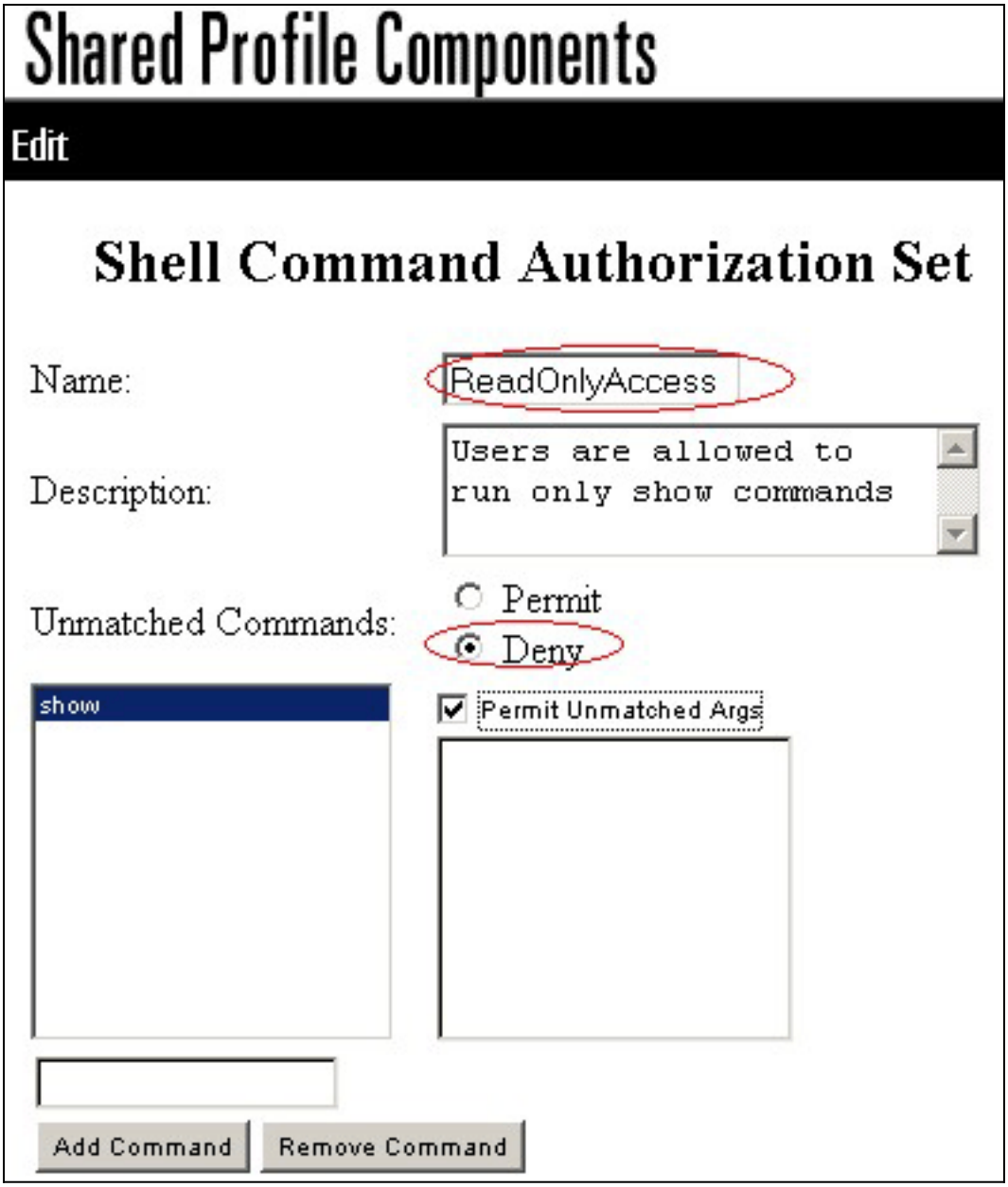


시나리오 2: 읽기 전용 액세스 권한

이 시나리오에서 사용자는 **show** 명령만 사용할 수 있습니다.

Shared Profile Components 창의 Shell Command Authorization Set 영역에서 다음 설정을 구성합니다.

1. Name 필드에 명령 권한 **부여** 집합의 이름으로 ReadOnlyAccess를 입력합니다.
2. Description 필드에 명령 권한 부여 세트에 대한 설명을 입력합니다.
3. Deny 라디오 **버튼**을 클릭합니다.
4. Add Command 버튼 **위**의 필드에 show 명령을 입력한 다음 Add **Command**를 클릭합니다.
5. Permit Unmatched **Args 확인란을** 선택하고 Submit을 클릭합니다.

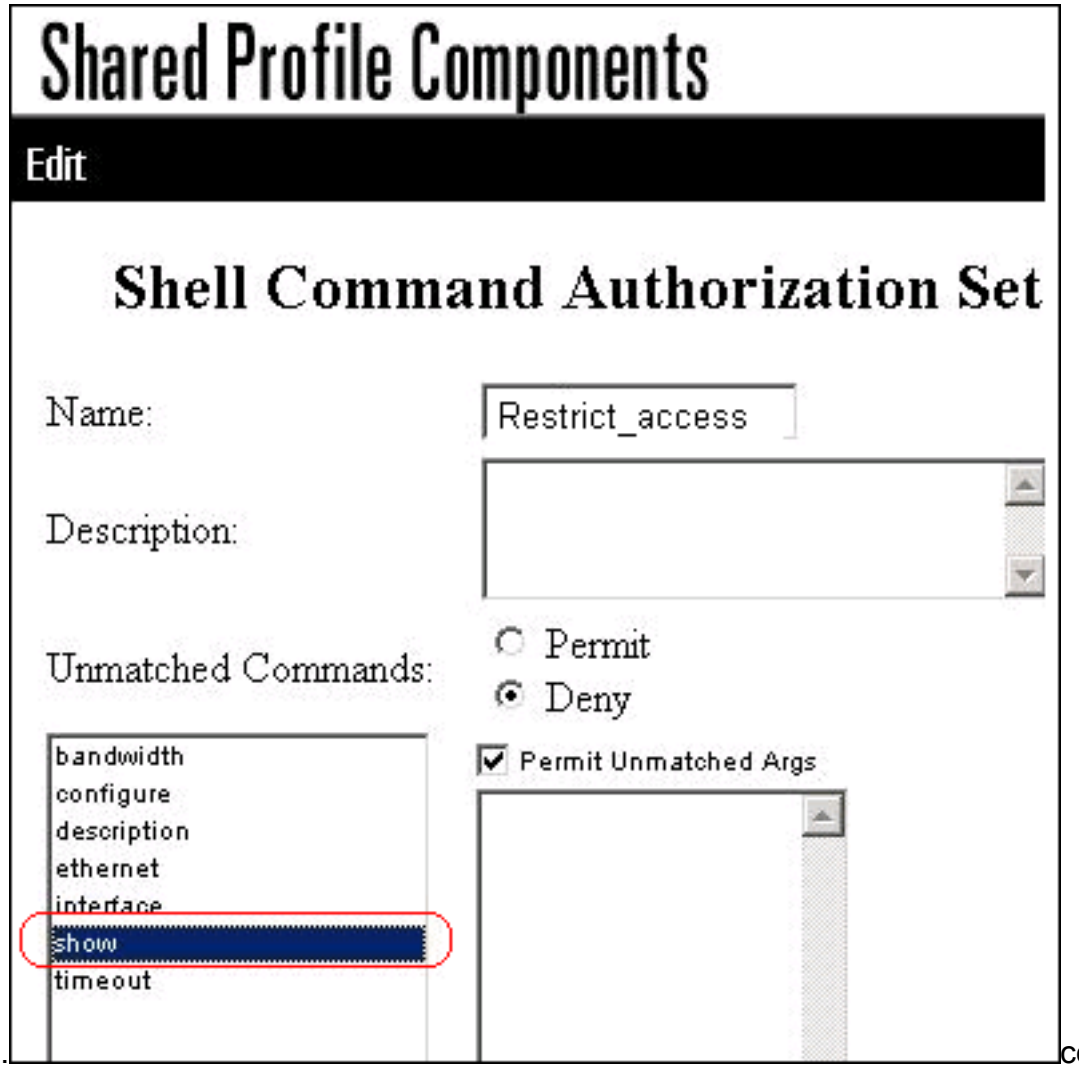


시나리오 3: 제한된 액세스에 대한 권한

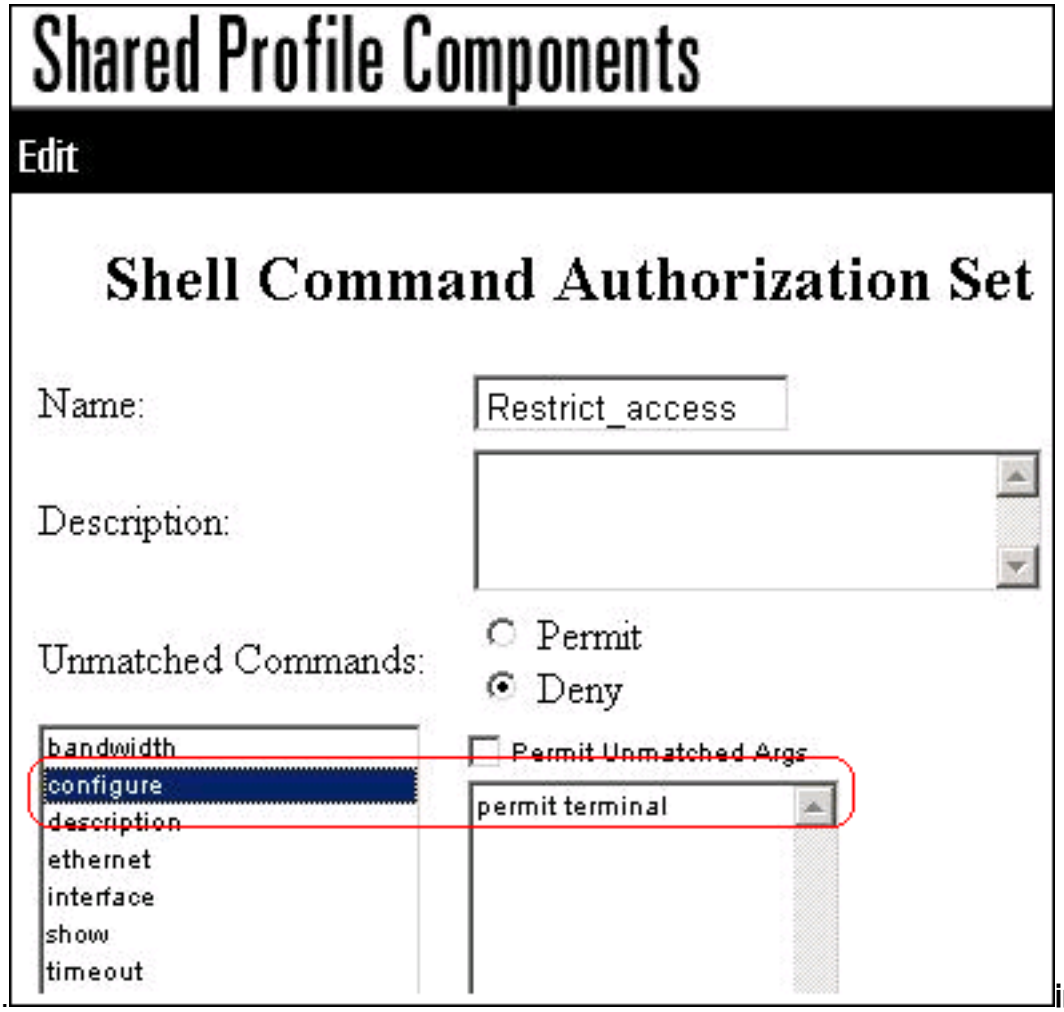
이 시나리오에서 사용자는 선택적 명령을 사용할 수 있습니다.

Shared Profile Components 창의 Shell Command Authorization Set 영역에서 다음 설정을 구성합니다.

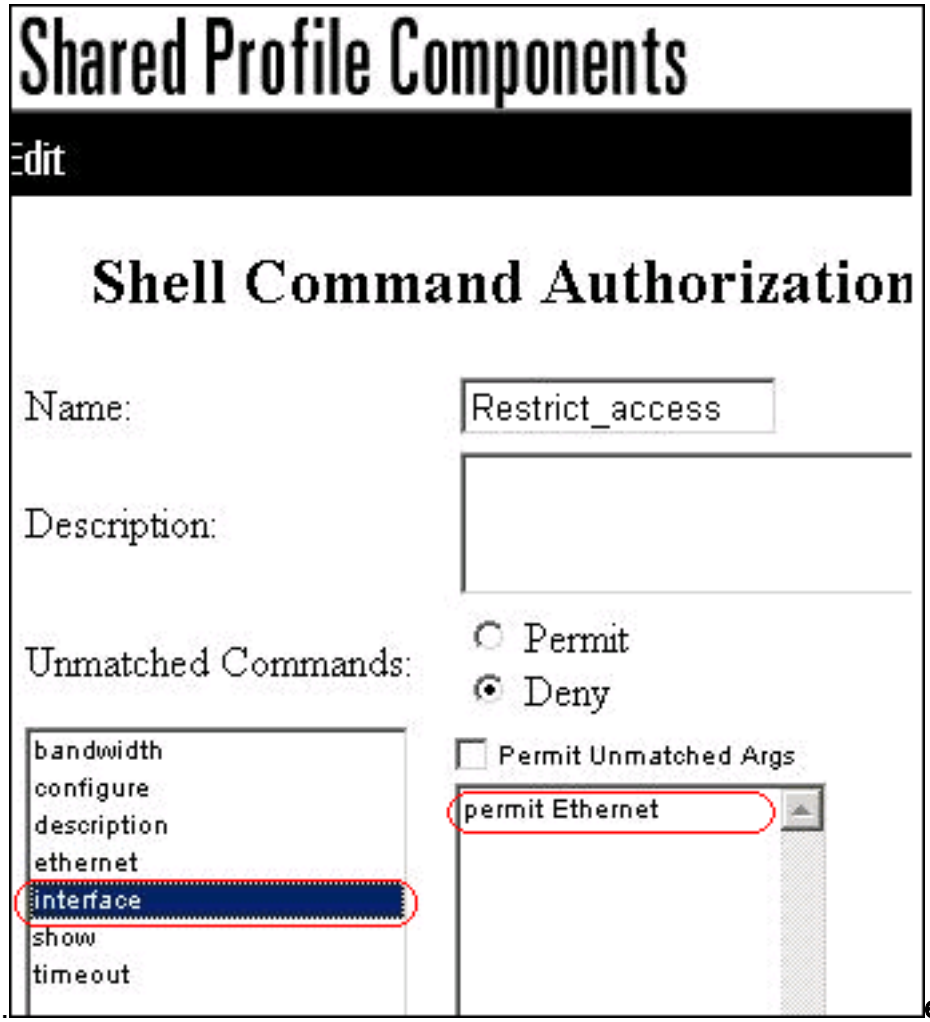
1. name 필드에 명령 권한 부여 **집합**의 이름으로 Restrict_access를 입력합니다.
2. Deny 라디오 **버튼**을 클릭합니다.
3. AAA 클라이언트에서 허용할 명령을 입력합니다.Add Command(명령 추가) 버튼 위에 있는 필드에 **show** 명령을 입력하고 Add Command(**명령 추가)를 클릭합니다**



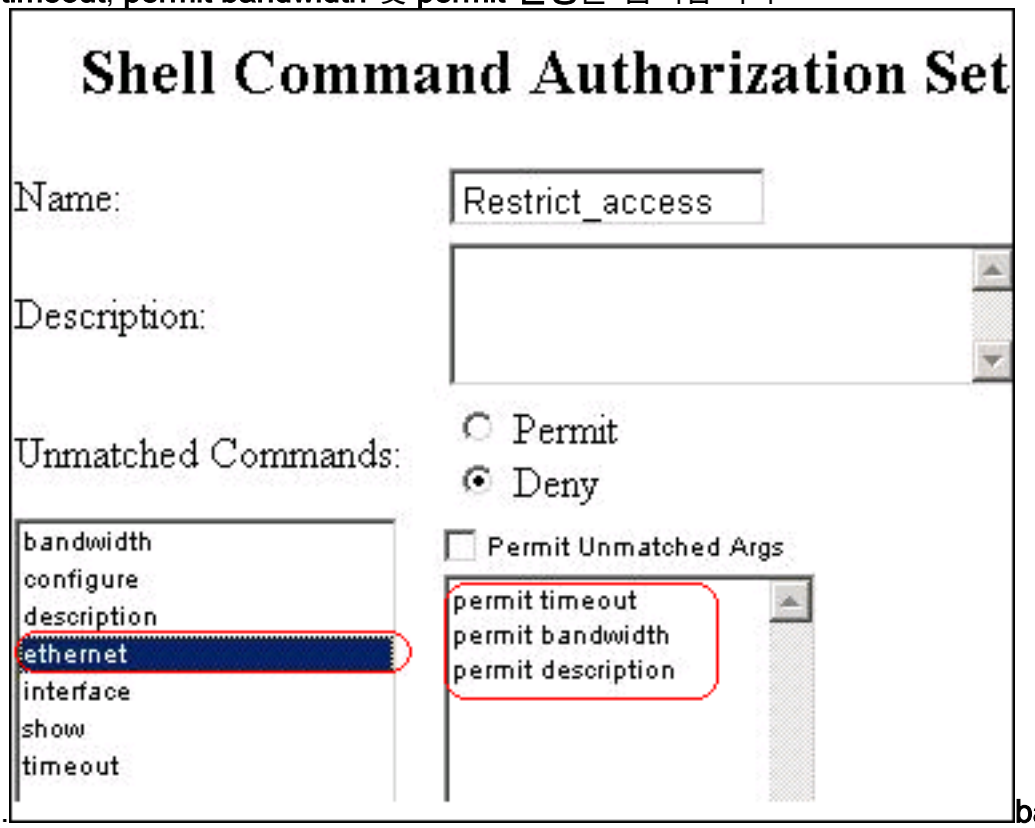
configure 명령을 **입력하고** Add Command를 **클릭합니다**.configure **명령**을 선택하고 오른쪽 **필드**에 permit terminal을 입력합니다



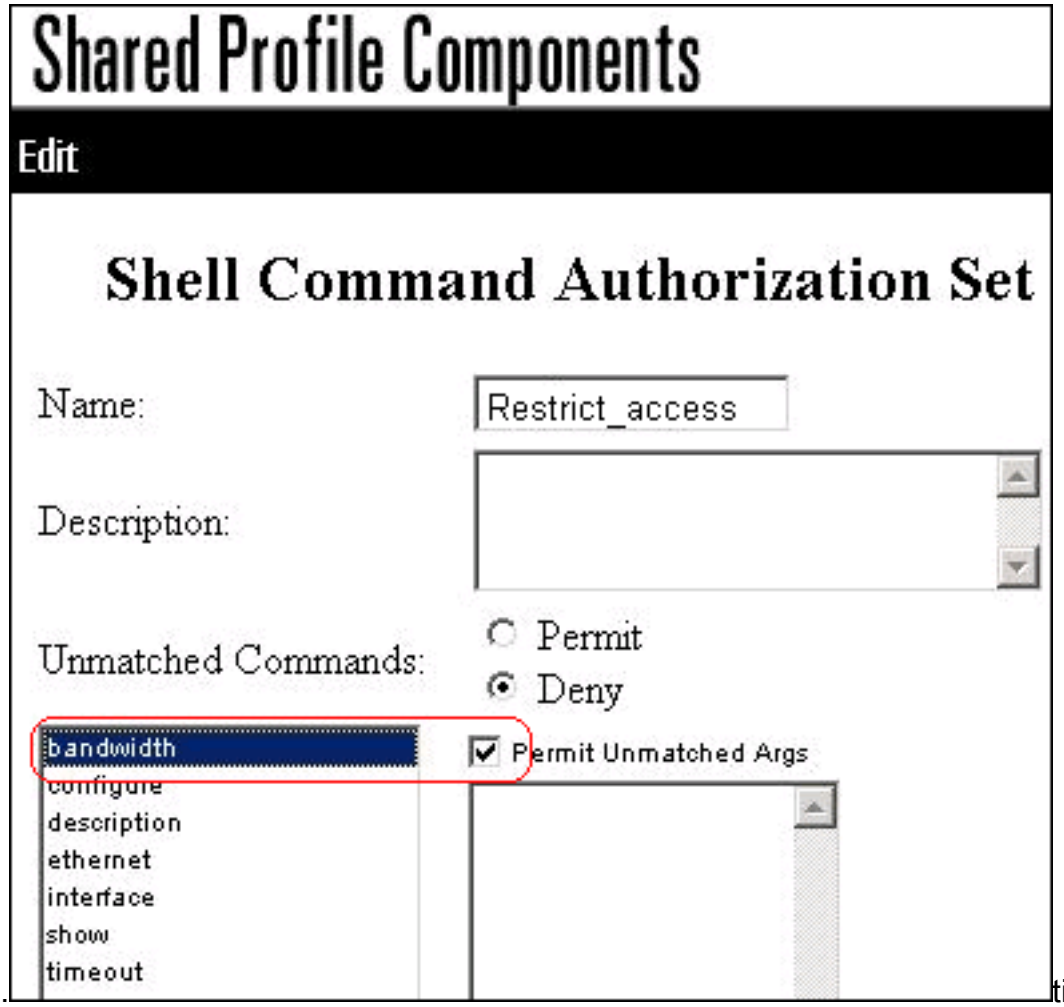
interface 명령을 **입력하고** Add Command를 **클릭합니다**.**interface** 명령을 선택하고 오른쪽 **필드**에 permit Ethernet을 입력합니다



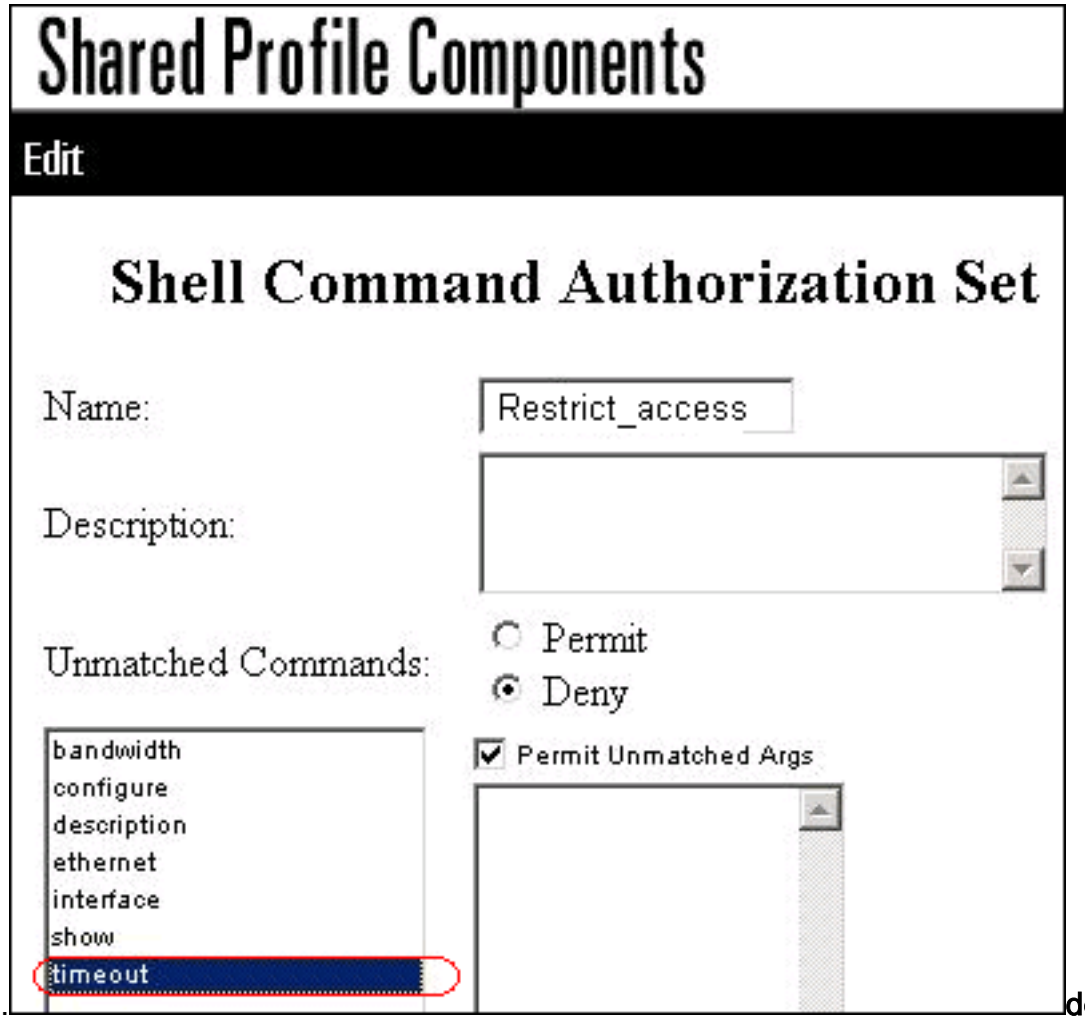
ethernet 명령을 입력하고 Add Command(명령 추가)를 클릭합니다.interface 명령을 선택하고 오른쪽의 필드에 permit timeout, permit bandwidth 및 permit 설명을 입력합니다



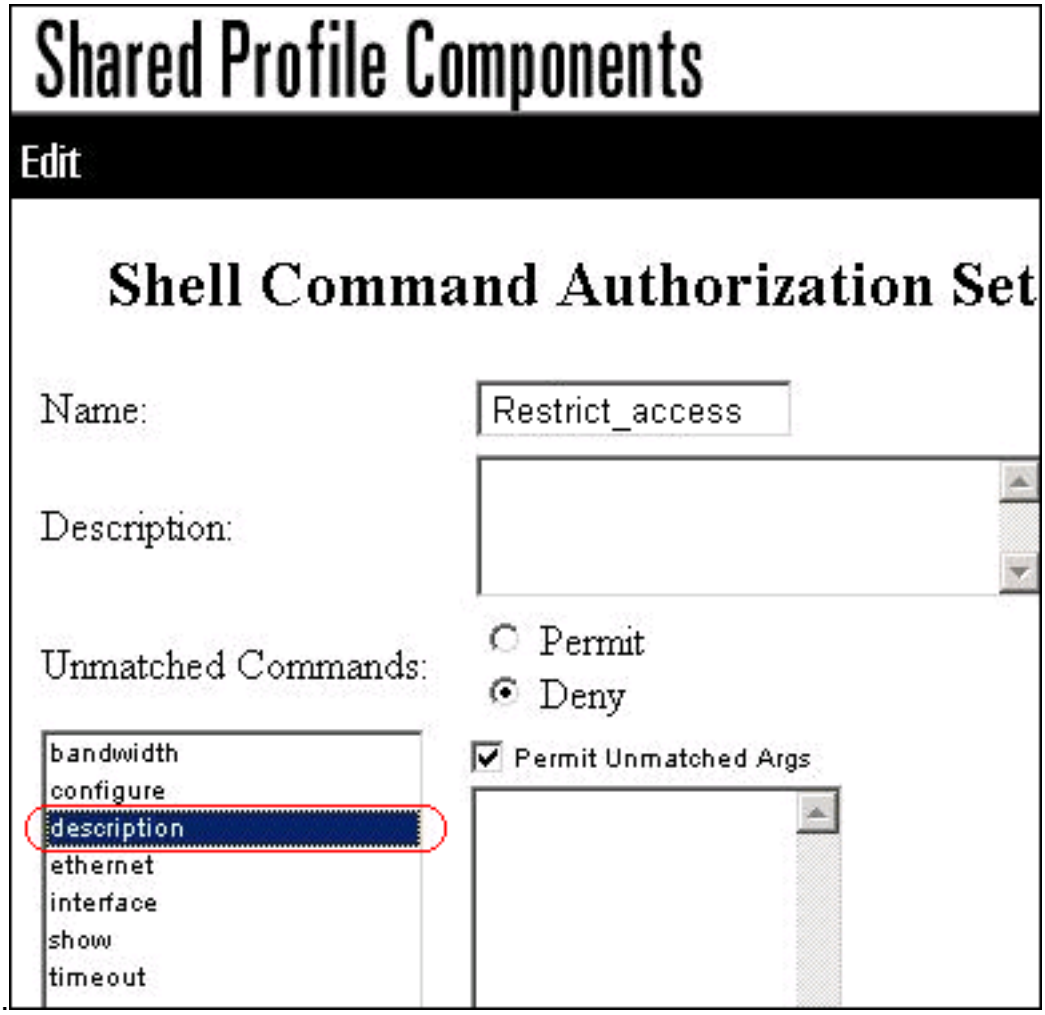
bandwidth 명령을 입력하고 Add Command를 클릭합니다



timeout 명령을 **입력하고** Add **Command(명령 추가)**를 클릭합니다



description 명령을 **입력하고** Add **Command(명령 추가)**를 클릭합니다



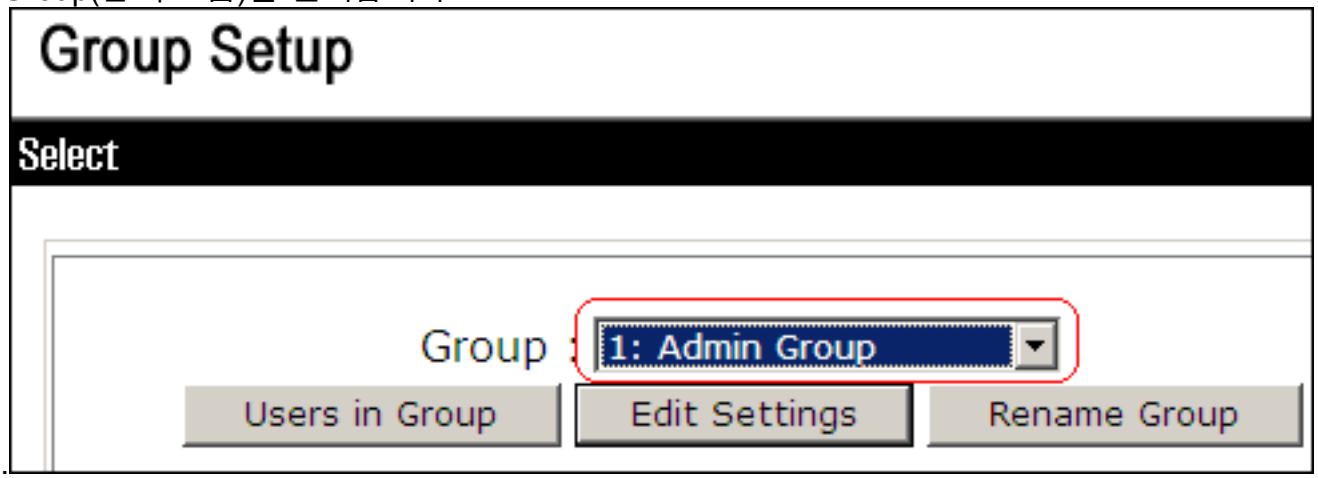
4. Submit(제출)**을 클릭합니다**.

셸 명령 권한 부여 집합을 사용자 그룹에 연결

사용자 그룹에 대한 셸 명령 권한 부여 집합 컨피그레이션을 구성하는 방법에 대한 자세한 내용은 Cisco Secure Access Control Server 4.1용 사용자 가이드의 사용자 그룹에 대한 셸 명령 권한 부여 집합 구성 섹션을 참조하십시오.

셸 명령 권한 부여 집합(읽기/쓰기 액세스)을 사용자 그룹(관리 그룹)에 연결

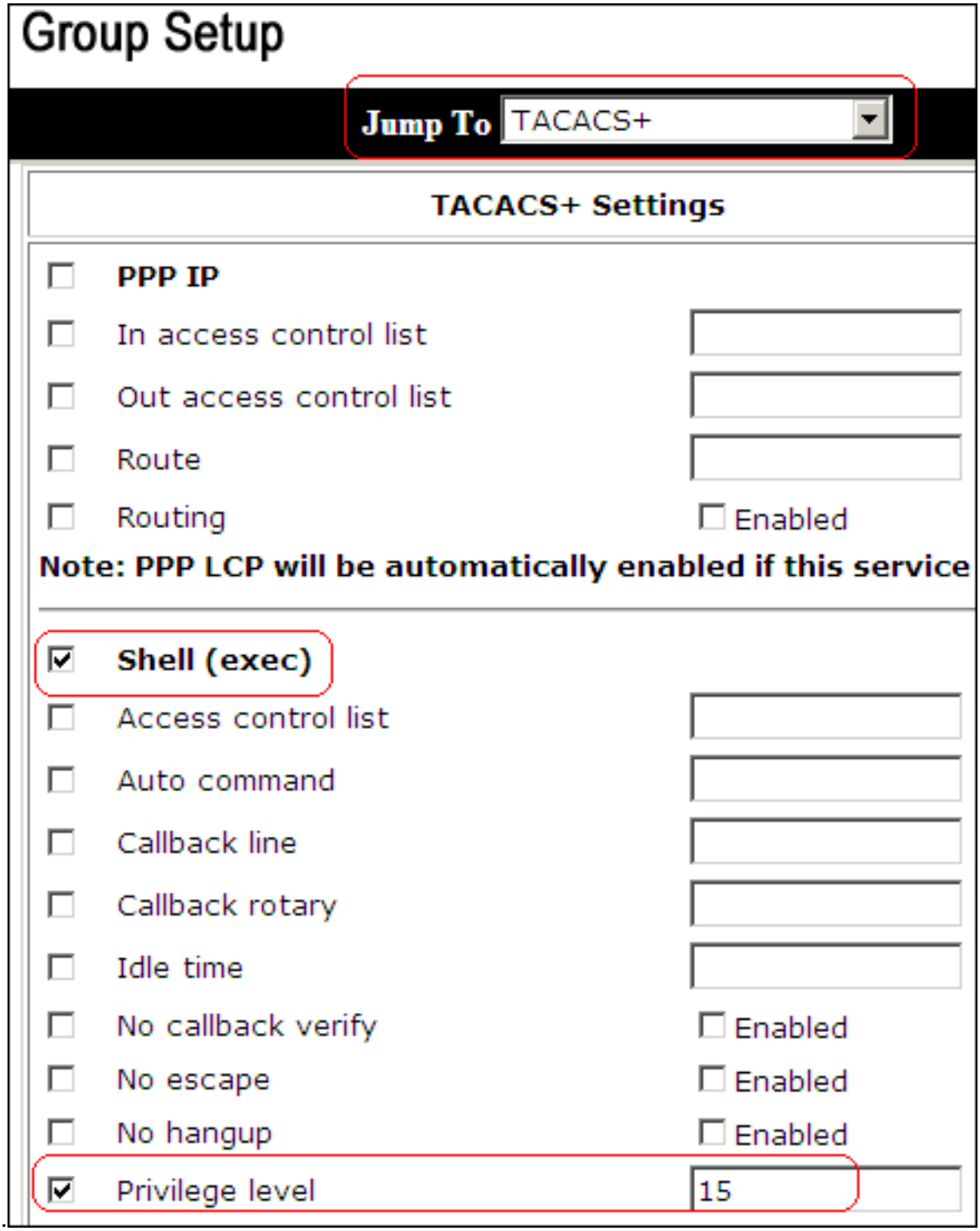
1. ACS 창에서 **Group Setup(그룹 설정)**을 클릭하고 Group(그룹) 드롭다운 **목록**에서 Admin Group(관리 그룹)을 선택합니다



2. Edit Settings(**설정 편집)를 클릭합니다**.

3. Jump To 드롭다운 목록에서 Enable Options를 **선택합니다**.
4. Enable Options 영역에서 **Max Privilege for any AAA client** 라디오 버튼을 클릭하고 드롭다운 목록에서 **Level 15**를 선택합니다

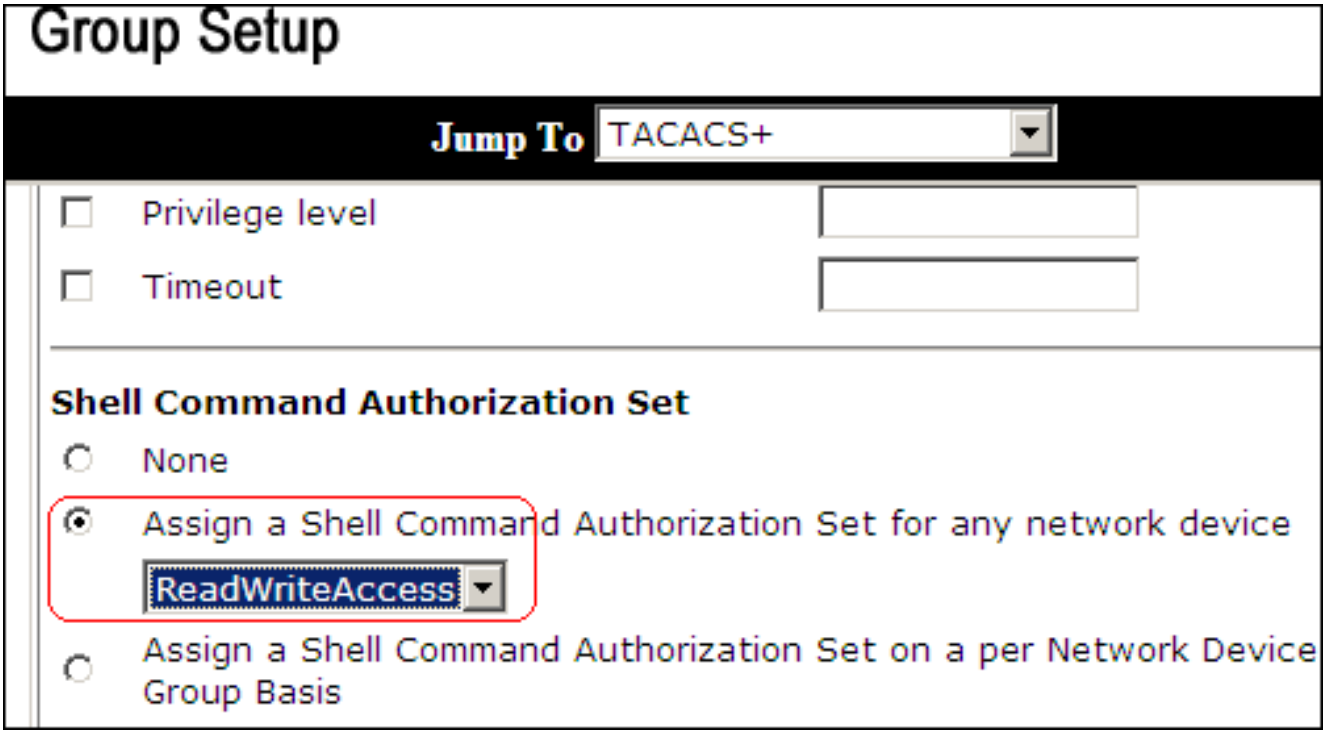
5. Jump To 드롭다운 목록에서 TACACS+를 선택합니다.
6. TACACS+ Settings(TACACS+ 설정) 영역에서 **Shell (exec)**(**셸(exec)**) 확인란을 선택하고, Privilege level(**권한 레벨)** 확인란을 선택한 다음, Privilege level(권한 레벨) 필드에 **15**를 입력



합니다.

7. Shell Command Authorization Set 영역에서 **Assign a Shell Command Authorization Set for any network device** 라디오 버튼을 클릭하고 드롭다운 목록에서 **ReadWriteAccess**를 선택합니다

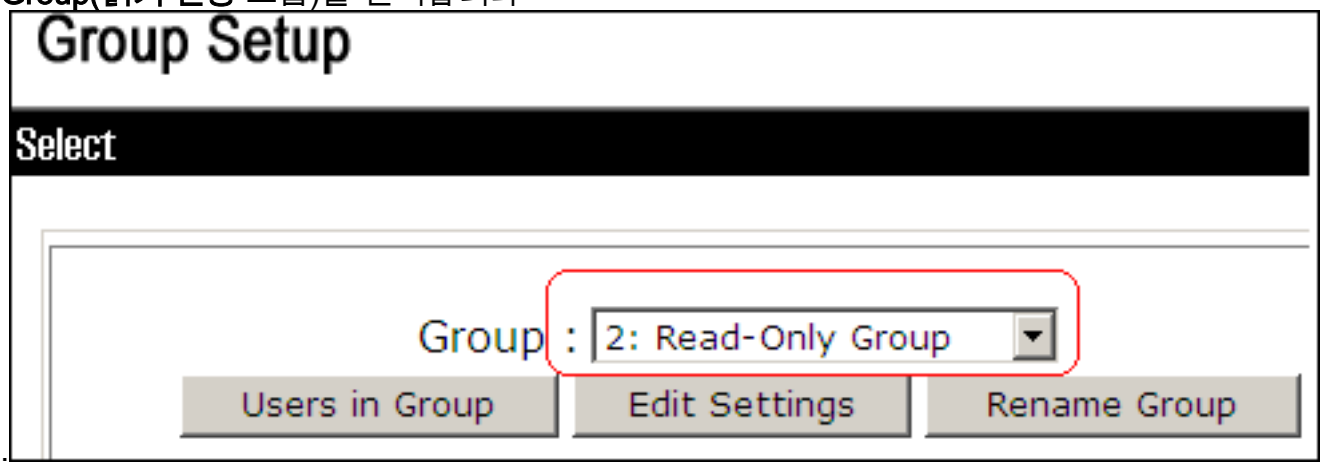
.



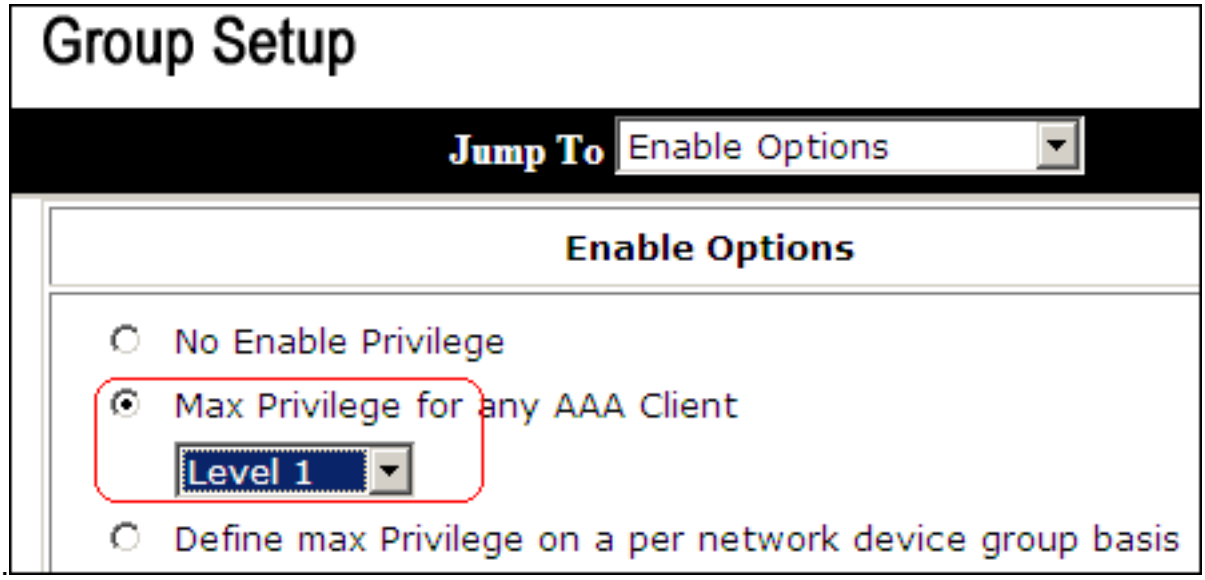
8. **Submit(제출)을 클릭합니다.**

셸 명령 권한 부여 집합(읽기 전용 액세스)을 사용자 그룹(읽기 전용 그룹)에 연결

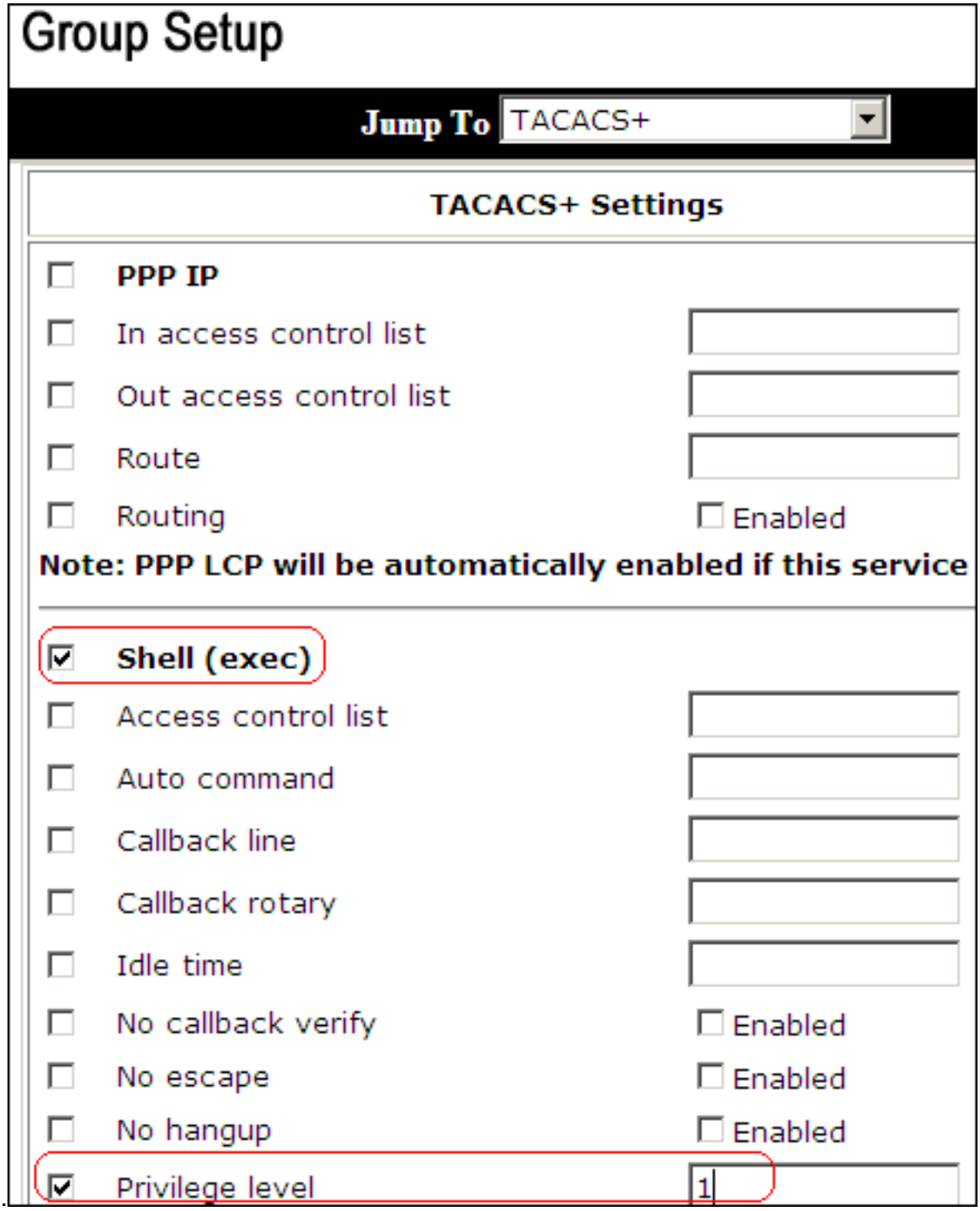
1. ACS 창에서 **Group Setup(그룹 설정)**을 클릭하고 Group(그룹) 드롭다운 목록에서 **Read-Only Group(읽기 전용** 그룹)을 선택합니다



2. Edit Settings(**설정 편집)를 클릭합니다**.
3. Jump To 드롭다운 목록에서 Enable Options를 **선택합니다**.
4. Enable Options 영역에서 **Max Privilege for any AAA client** 라디오 버튼을 클릭하고 드롭다운 목록에서 **Level 1**을 선택합니다



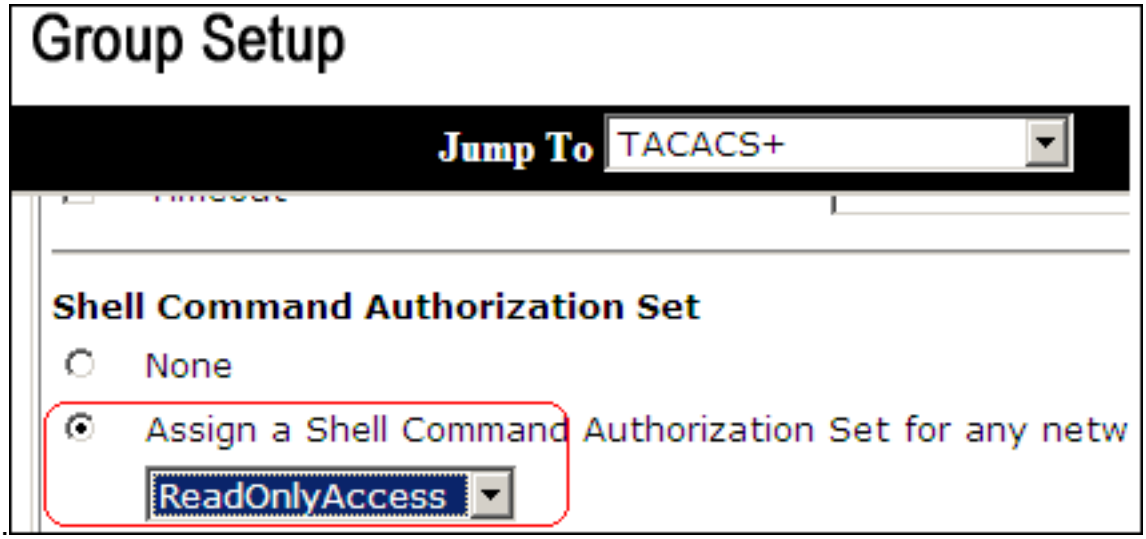
5. TACACS+ Settings(TACACS+ 설정) 영역에서 **Shell (exec)(셸(exec))** 확인란을 선택하고, Privilege level(**권한 레벨)** 확인란을 선택한 다음, Privilege level(권한 레벨) 필드에 **1**을 입력합



니다.

6. Shell Command Authorization Set 영역에서 **Assign a Shell Command Authorization Set for any network device** 라디오 버튼을 클릭하고 드롭다운 목록에서 **ReadOnlyAccess**를 선택합니

다.



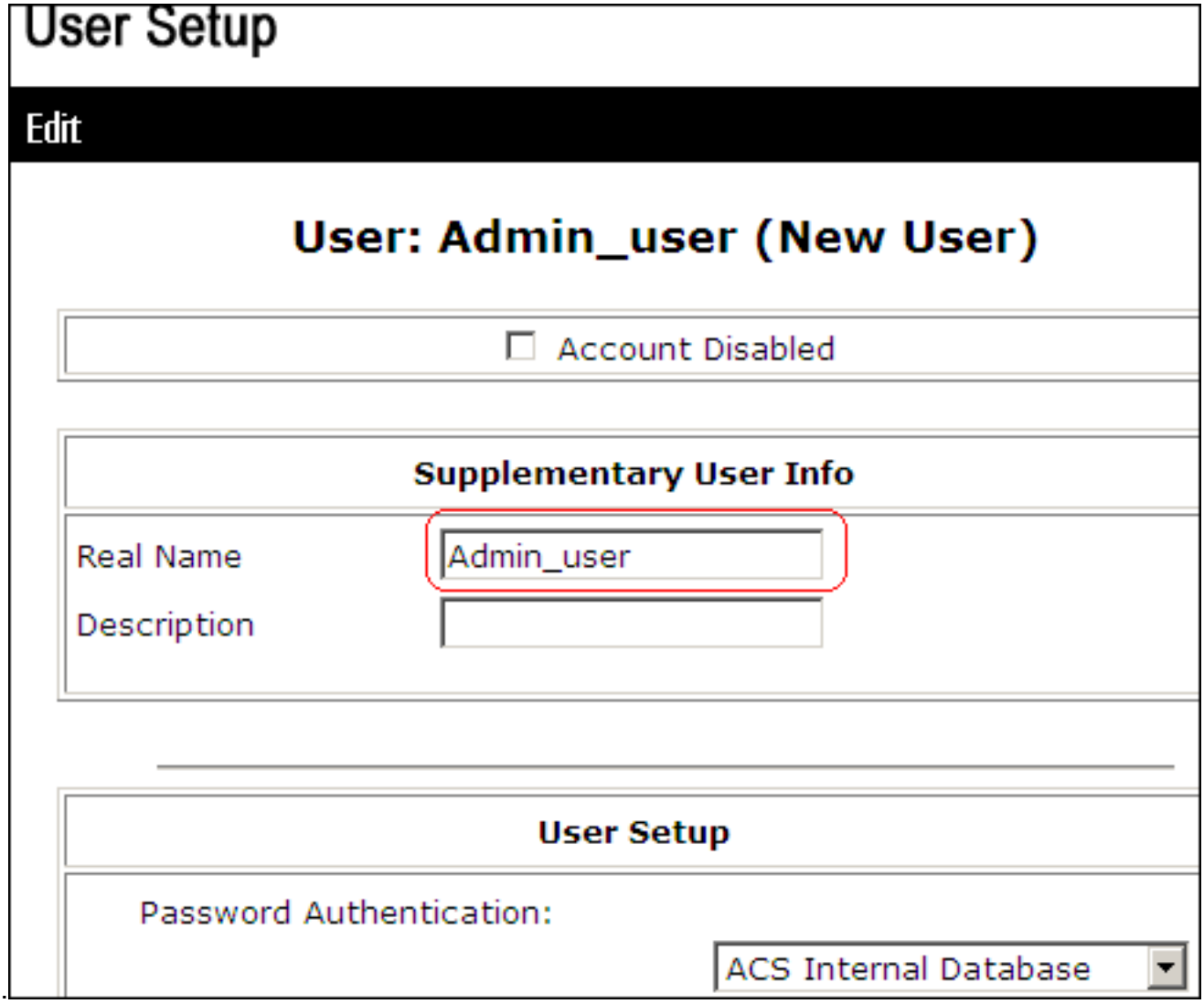
7. **Submit(제출)을 클릭합니다.**

셸 명령 권한 부여 집합(Restrict_access)을 사용자에게 연결

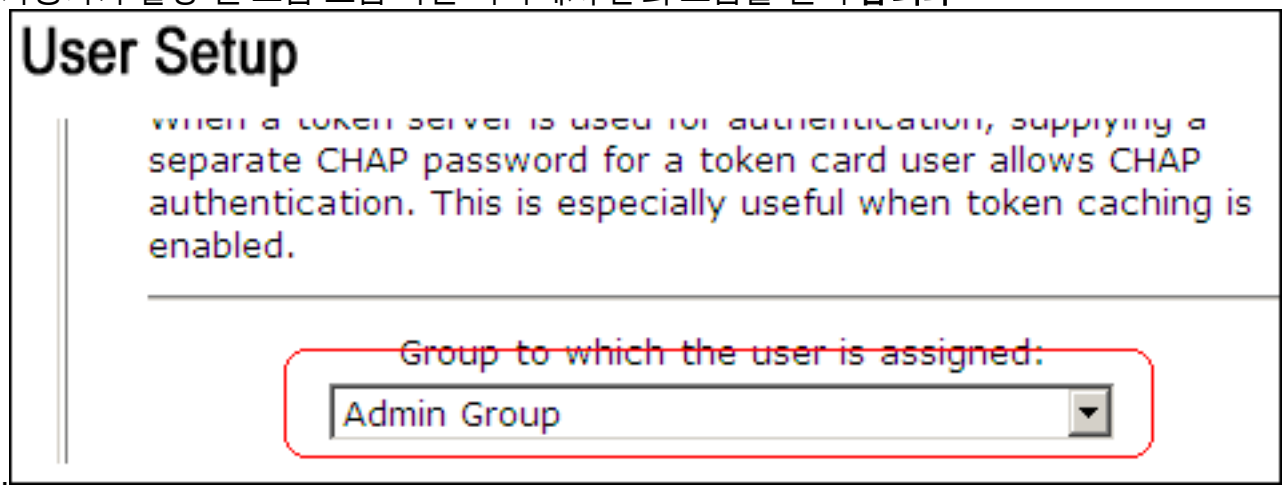
사용자에 대한 셸 명령 권한 부여 집합 컨피그레이션을 구성하는 방법에 대한 자세한 내용은 Cisco Secure Access Control Server 4.1용 사용자 가이드의 사용자에 대한 셸 명령 권한 부여 집합 구성 섹션을 참조하십시오.

참고: 사용자 수준 설정은 ACS의 그룹 수준 설정을 재정의합니다. 즉, 사용자에게 사용자 수준 설정에 셸 명령 권한 부여가 설정되어 있으면 그룹 수준 설정을 재정의합니다.

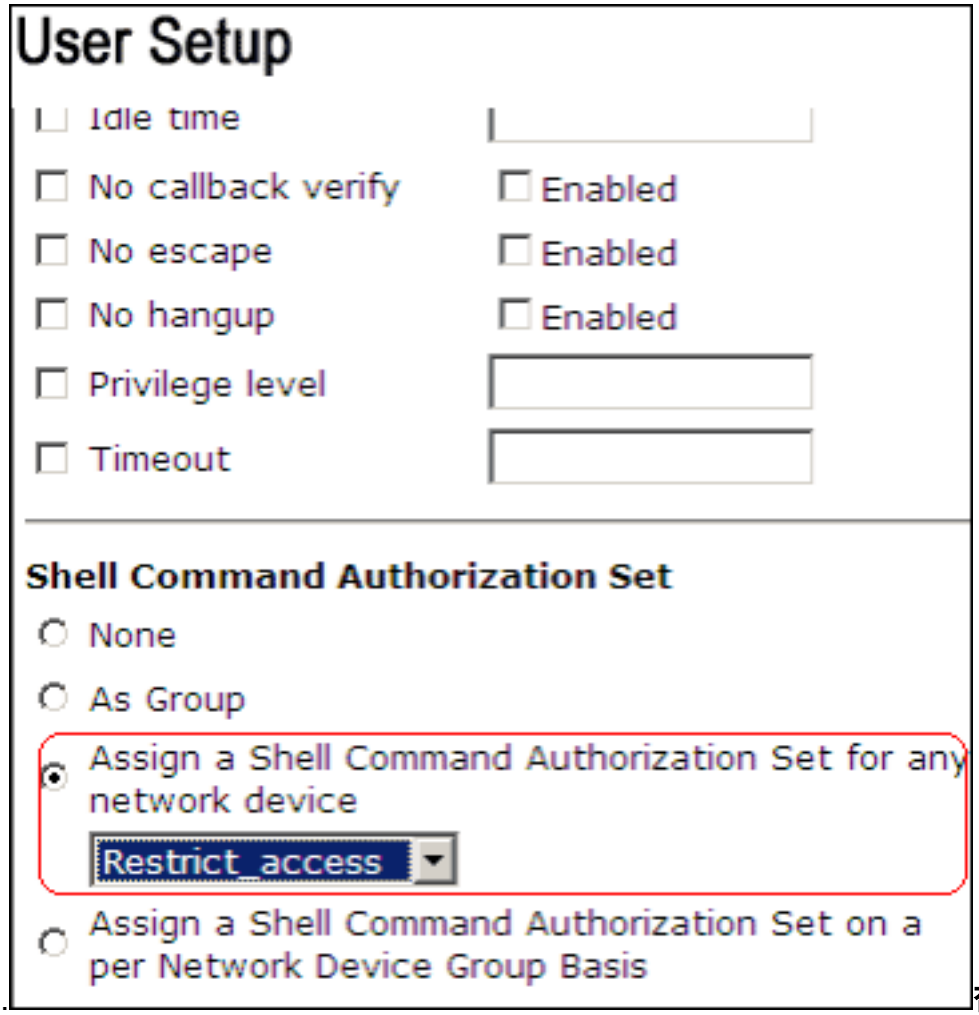
1. User **Setup(사용자 설정) > Add/Edit(추가/수정)**를 클릭하여 Admin_*user라는* 새 *사용자*를 Admin 그룹에 추가합니다



2. 사용자가 할당 된 그룹 드롭 다운 목록에서 관리 그룹을 선택 **합니다**



3. Shell Command Authorization Set 영역에서 **Assign a Shell Command Authorization Set for any network device** 라디오 버튼**을** 클릭하고 드롭다운 목록에서 **Restrict_access**를 선택합니다.**참고:** 이 시나리오에서 이 사용자는 관리 그룹의 일부입니다. Restrict_*access* 셸 권한 부여 집합이 적용됩니다. 읽기 *쓰기 액세스* 셸 권한 부여 집합을 적용할 수 없습니다



참고: Interface Configuration(인터페이스 컨피그레이션) 영역의 TACACS+(Cisco) 섹션에서 User(사용자) 열에서 **Shell(exec)** 옵션이 선택되어 있는지 확인합니다.

IOS 라우터 컨피그레이션

사전 설정 컨피그레이션 외에도 ACS 서버를 통해 명령 권한 부여를 구현하려면 IOS 라우터 또는 스위치에서 다음 명령이 필요합니다.

```
aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default  group tacacs+ local
aaa authorization commands 1 default  group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123
```

ASA/PIX/FWSM 컨피그레이션

사전 설정 컨피그레이션 외에도 ACS 서버를 통해 명령 권한 부여를 구현하려면 ASA/PIX/FWSM에서 다음 명령이 필요합니다.

```
aaa-server authserver protocol tacacs+
aaa-server authserver host 10.1.1.1
aaa authorization command authserver
```

참고: 읽기 전용 목적으로 ASDM에 대한 사용자 액세스를 제한하기 위해 RADIUS 프로토콜을 사용

할 수는 없습니다. RADIUS 패킷에는 인증과 권한 부여가 동시에 포함되므로 RADIUS 서버에서 인증된 모든 사용자의 권한 레벨은 15입니다. 명령 권한 부여 집합을 구현하여 TACACS를 통해 이를 달성할 수 있습니다.

참고: ACS에서 명령 권한 부여를 수행할 수 없는 경우에도 ASA/PIX/FWSM에서 입력된 각 명령을 실행하는 데 시간이 오래 걸립니다. ACS를 사용할 수 없고 ASA에 명령 권한 부여가 구성된 경우 ASA는 각 명령에 대해 명령 권한 부여를 계속 요청합니다.

문제 해결

오류: 명령 권한 부여 실패

문제

TACACS 로깅을 통해 방화벽에 로그인하면 명령이 작동하지 않습니다. 명령을 입력하면 다음 오류가 표시됩니다. .

솔루션

이 문제를 해결하려면 다음 단계를 완료하십시오.

1. 올바른 사용자 이름이 사용되고 모든 필수 권한이 사용자에게 할당되었는지 확인합니다.
2. 사용자 이름 및 권한이 올바른 경우 ASA가 ACS와 연결되어 있고 ACS가 활성 상태인지 확인합니다.

참고: 이 오류는 관리자가 로컬 및 TACACS 사용자에 대해 명령 권한 부여를 잘못 구성한 경우에도 발생할 수 있습니다. 이 경우 문제를 해결하려면 비밀번호 복구를 수행합니다.

관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(설명 요청)
- Cisco Secure Control Access Control Server 지원 페이지
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.