ASA 8.3 이상:CLI 및 ASDM 컨피그레이션과 함께 다운로드 가능한 ACL을 사용하여 VPN 액세스를 위한 RADIUS 권한 부여(ACS 5.x) 예

목차

소개

이 문서에서는 네트워크 액세스를 위해 사용자를 인증하도록 보안 어플라이언스를 구성하는 방법에 대해 설명합니다.RADIUS 권한 부여를 암시적으로 활성화할 수 있으므로 이 문서에는 보안 어플라이언스에서 RADIUS 권한 부여의 컨피그레이션에 대한 정보가 포함되어 있지 않습니다.보안 어플라이언스가 RADIUS 서버에서 받은 액세스 목록 정보를 처리하는 방법에 대한 정보를 제공합니다.

인증 시 보안 어플라이언스에 액세스 목록을 다운로드하거나 액세스 목록 이름을 다운로드하도록 RADIUS 서버를 구성할 수 있습니다.사용자는 사용자별 액세스 목록에서 허용되는 작업만 수행할 수 있습니다.

다운로드 가능한 액세스 목록은 Cisco ACS(Secure Access Control Server)를 사용하여 각 사용자에게 적절한 액세스 목록을 제공할 때 가장 확장 가능한 방법입니다.다운로드 가능한 액세스 목록 기능 및 Cisco Secure ACS에 대한 자세한 내용은 다운로드 가능한 액세스 제어 목록 및 다운로드 가능한 IP ACL을 전송하도록 RADIUS 서버 구성을 참조하십시오.

ASA/PIX 8.x 참조:버전 8.2 이하의 Cisco ASA에서 동일한 컨피그레이션을 위한 CLI와 ASDM 컨피그레이션과 함께 다운로드 가능한 ACL을 사용하여 네트워크 액세스를 위한 ACS(Radius Authorization)

사전 요구 사항

요구 사항

이 문서에서는 ASA(Adaptive Security Appliance)가 완벽하게 작동하며 Cisco ASDM(Adaptive Security Device Manager) 또는 CLI에서 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

참고: ASDM 또는 SSH(Secure Shell)에서 디바이스를 원격으로 구성하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 소프트웨어 버전 8.3 이상
- Cisco ASDM 버전 6.3 이상
- Cisco VPN Client 버전 5.x 이상
- Cisco Secure ACS 5.x

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.

배경 정보

다운로드 가능한 IP ACL을 사용하여 여러 사용자 또는 사용자 그룹에 적용할 수 있는 ACL 정의 집합을 생성할 수 있습니다.이러한 ACL 정의 집합을 ACL 내용이라고 합니다.

다운로드 가능한 IP ACL은 다음과 같이 작동합니다.

1. ACS가 네트워크에 대한 사용자 액세스 권한을 부여할 때 ACS는 결과 섹션의 Authorization Profile(권한 부여 프로파일)에 다운로드 가능한 IP ACL이 할당되었는지 여부를 결정합니다.
2. ACS가 권한 부여 프로파일에 할당된 다운로드 가능한 IP ACL을 찾으면 ACS는 명명된 ACL을 지정하는 특성(사용자 세션의 일부로 RADIUS 액세스 수락 패킷에 있음)과 명명된 ACL의 버전을 전송합니다.

3. AAA 클라이언트가 캐시에 현재 버전의 ACL이 없다고 응답하면(즉, ACL이 신규 또는 변경됨) ACS는 디바이스에 ACL(신규 또는 업데이트)을 보냅니다.

다운로드 가능한 IP ACL은 각 사용자 또는 사용자 그룹의 RADIUS Cisco av-pair 특성 [26/9/1]에서 ACL의 구성에 대한 대안입니다.다운로드 가능한 IP ACL을 한 번 생성하고 이름을 지정한 다음 이름을 참조하는 경우 다운로드 가능한 IP ACL을 모든 권한 부여 프로파일에 할당할 수 있습니다.이 방법은 권한 부여 프로파일에 대해 RADIUS Cisco av 쌍 특성을 구성하는 경우보다 효율적입니다.

ACS 웹 인터페이스에 ACL 정의를 입력할 때 키워드 또는 이름 항목을 사용하지 마십시오.다른 모든 측면에서, 다운로드 가능한 IP ACL을 적용하려는 AAA 클라이언트에 표준 ACL 명령 구문 및 의미 체계를 사용합니다.ACS에 입력하는 ACL 정의는 하나 이상의 ACL 명령으로 구성됩니다.각 ACL 명령은 별도의 줄에 있어야 합니다.

ACS에서 여러 다운로드 가능한 IP ACL을 정의하고 다른 인증 프로파일에서 사용할 수 있습니다.Access Service Authorization 규칙의 조건에 따라 다운로드 가능한 IP ACL이 포함된 다른 권한 부여 프로파일을 다른 AAA 클라이언트로 보낼 수 있습니다.

또한 다운로드 가능한 IP ACL에서 ACL 내용의 순서를 변경할 수 있습니다.ACS는 테이블 상단부터 시작하여 ACL 내용을 검사하고, 발견한 첫 번째 ACL 콘텐츠를 다운로드합니다.주문을 설정할 때 가장 널리 적용되는 ACL 내용을 목록에서 더 높게 배치하면 시스템 효율성을 보장할 수 있습니다.

특정 AAA 클라이언트에서 다운로드 가능한 IP ACL을 사용하려면 AAA 클라이언트가 다음 규칙을 준수해야 합니다.

- 인증에 RADIUS 사용
- 다운로드 가능한 IP ACL 지원

다음은 다운로드 가능한 IP ACL을 지원하는 Cisco 디바이스의 예입니다.

- ASA
- IOS 버전 12.3(8)T 이상을 실행하는 Cisco 디바이스

다음은 ACL 정의 상자에 ASA ACL을 입력하기 위해 사용해야 하는 형식의 예입니다.

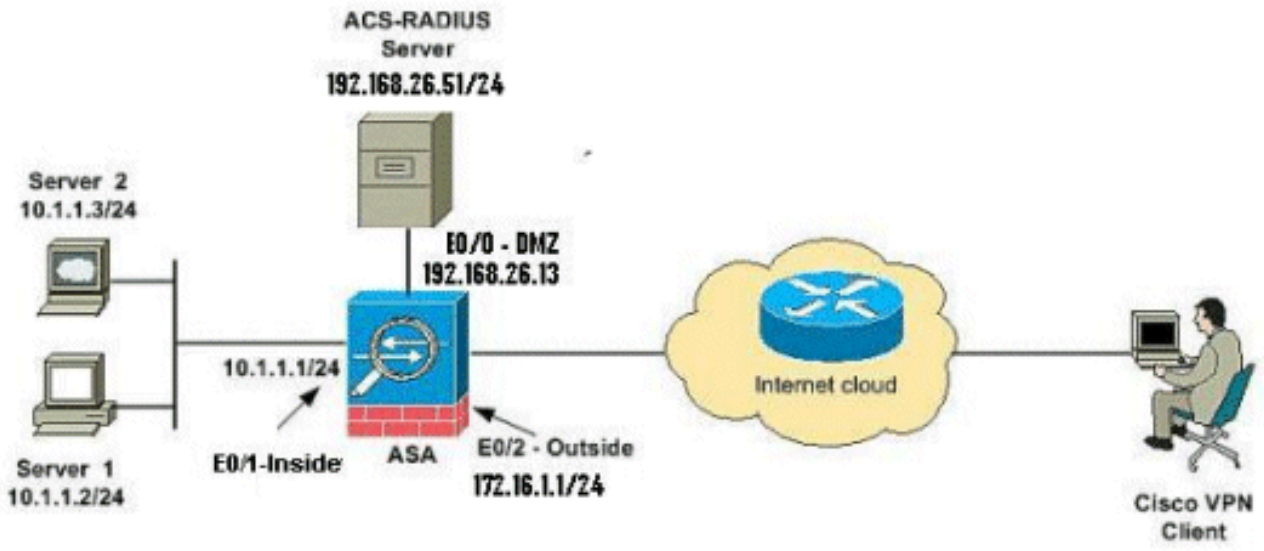
```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

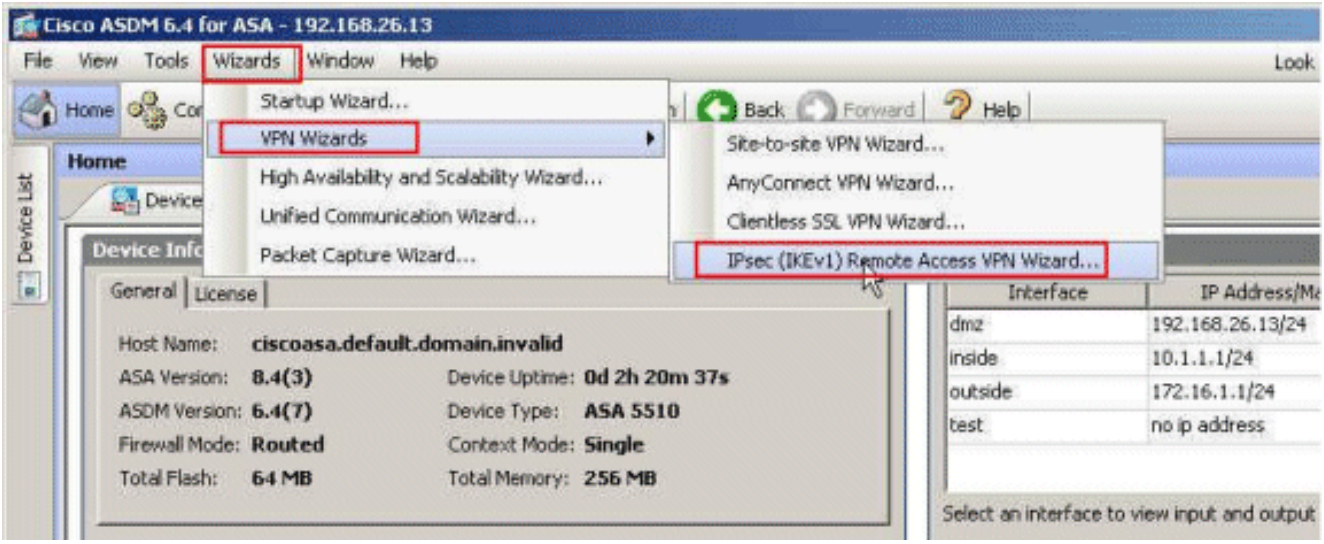
원격 액세스 VPN(IPsec) 구성

ASDM 절차

원격 액세스 VPN을 구성하려면 다음 단계를 완료합니다.

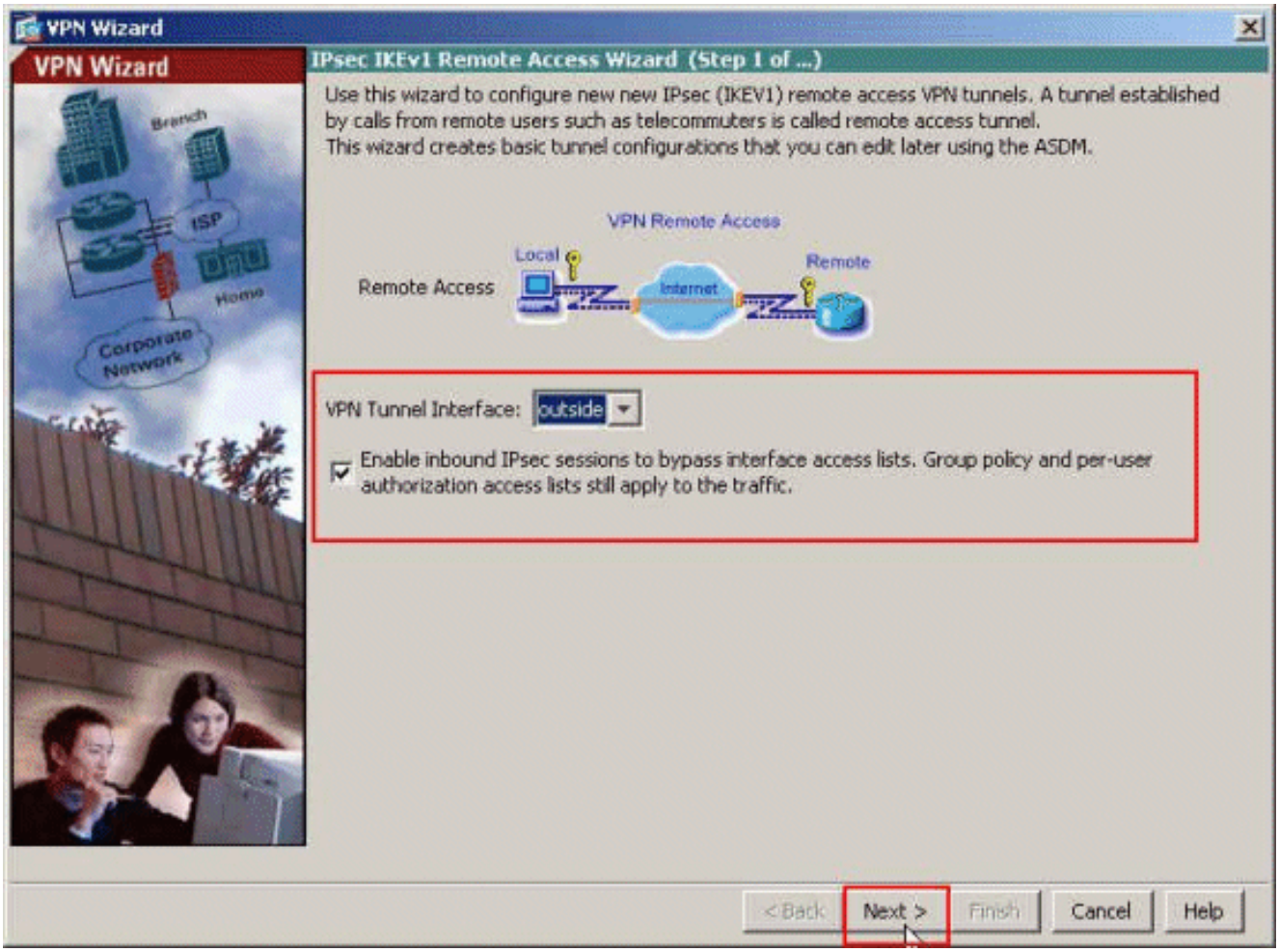
1. Wizards(**마법사**) > **VPN Wizards(VPN 마법사)** > **IPsec(IKEv1) Remote Access VPN Wizard(IPsec(IKEv1) 원격 액세스 VPN 마법사)**를 홈 창에서 선택합니다

.



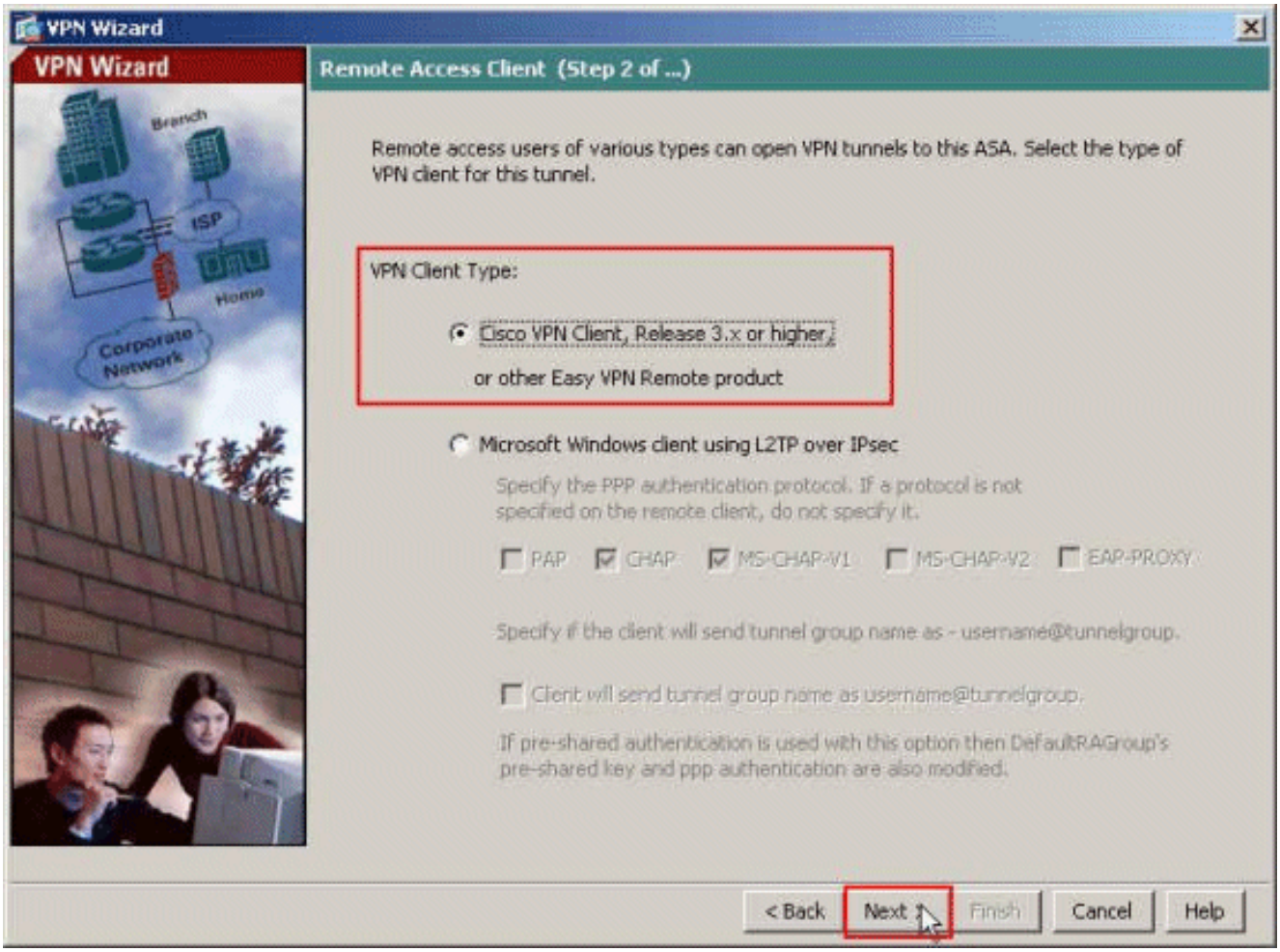
2. 필요에 따라 **VPN 터널 인터페이스(Outside**, 이 예에서는)를 선택하고 Enable inbound IPsec sessions to bypass interface access lists(**인터페이스 액세스 목록을 우회하도록 인바운드 IPsec 세션 활성화) 옆** 확인란이 선택되었는지 확인합니다

.



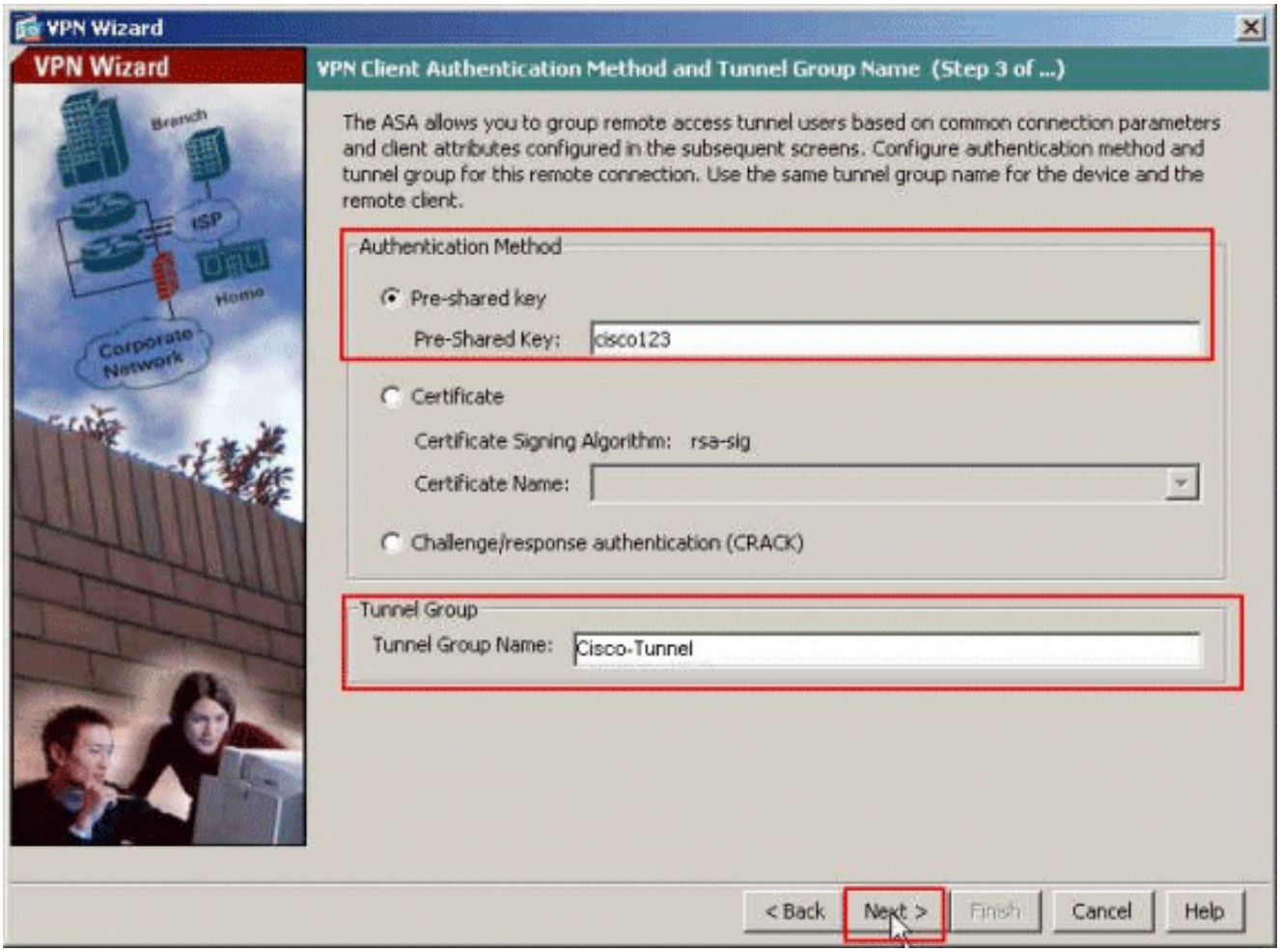
3. VPN Client Type(VPN 클라이언트 유형)을 **Cisco VPN Client, Release 3.x 이상으로 선택합니다**.Next(**다음)를 클릭합니다**

.



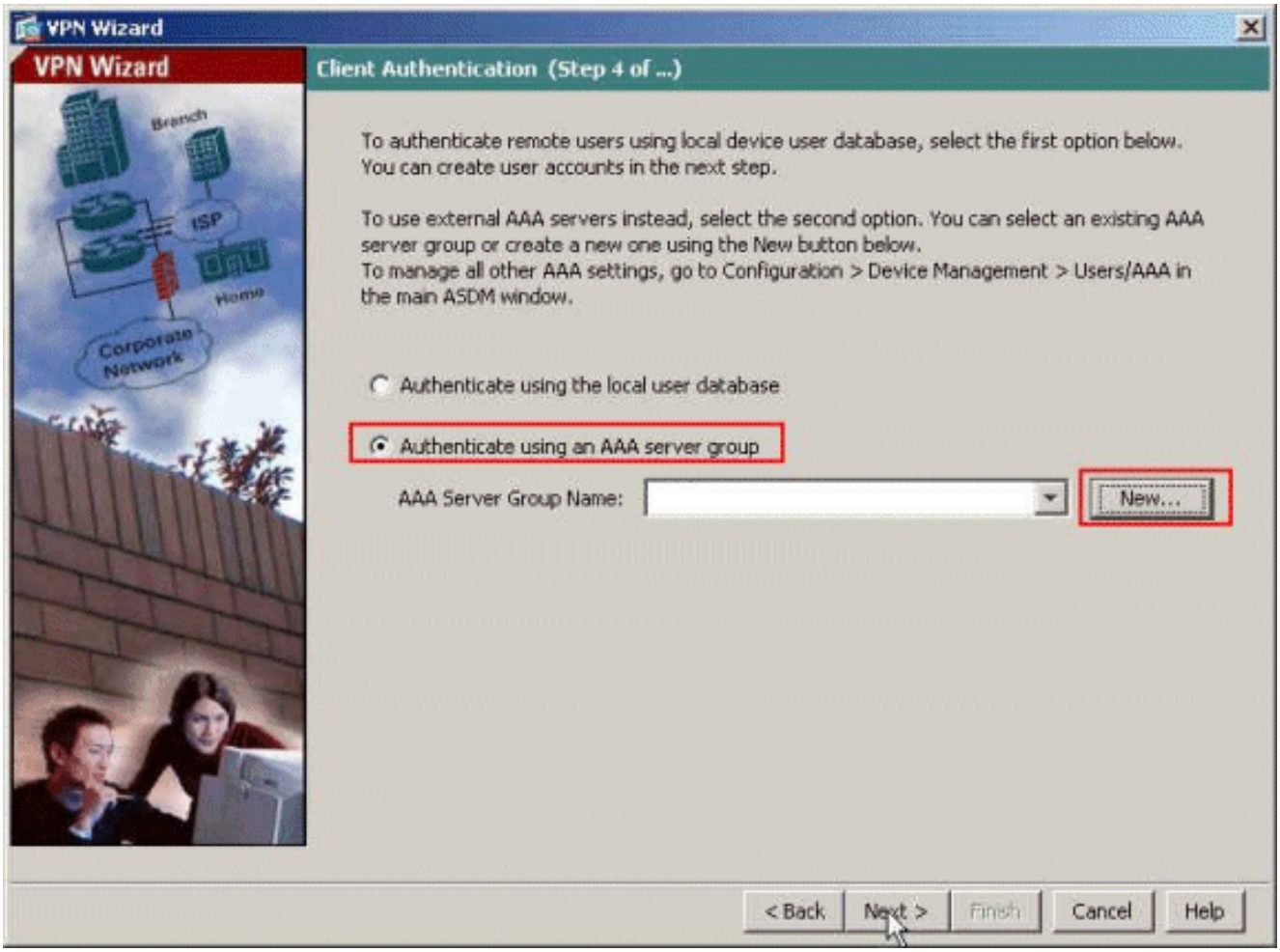
4. Authentication Method(**인증 방법**)를 선택하고 Authentication(인증) 정보를 제공합니다.여기서 사용되는 인증 방법은 **사전 공유 키입니다**.또한 제공된 공간에 **터널 그룹** 이름을 입력합니다.여기서 사용되는 **사전 공유 키**는 **cisco123**이고 여기에 사용된 **터널 그룹 이름**은 **Cisco-Tunnel입니다**.Next(**다음)를 클릭합니다**

.

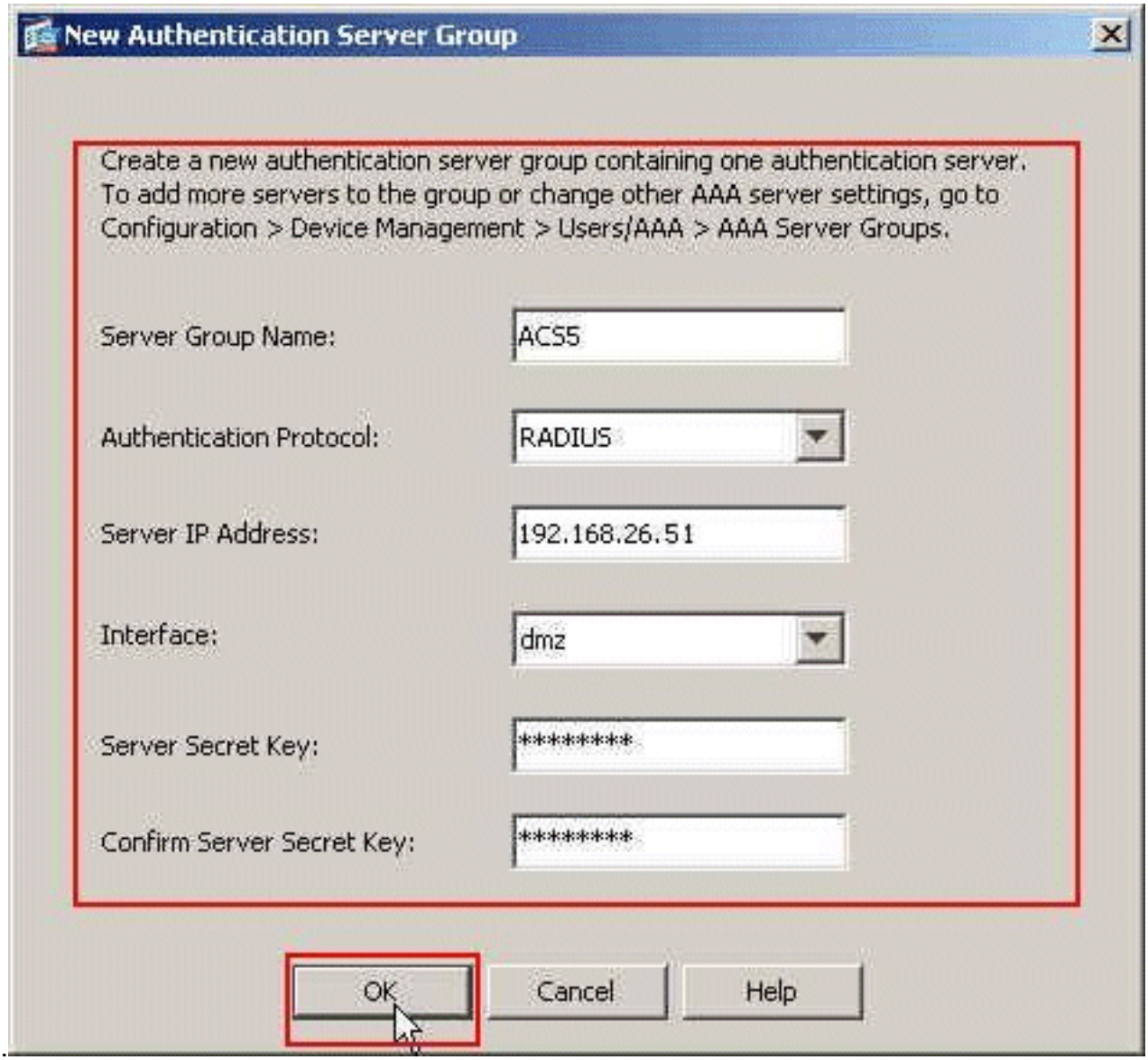


5. 원격 사용자를 로컬 사용자 데이터베이스에 인증할지 아니면 외부 AAA 서버 그룹에 인증할지를 선택합니다.여기서는 Authenticate using an **AAA server group**을 선택하겠습니다.새 AAA 서버 그룹 이름을 생성하려면 AAA Server Group Name(AAA 서버 그룹 이름) 필드 옆에 있는 **New**(새로 만들기)를 클릭합니다

.

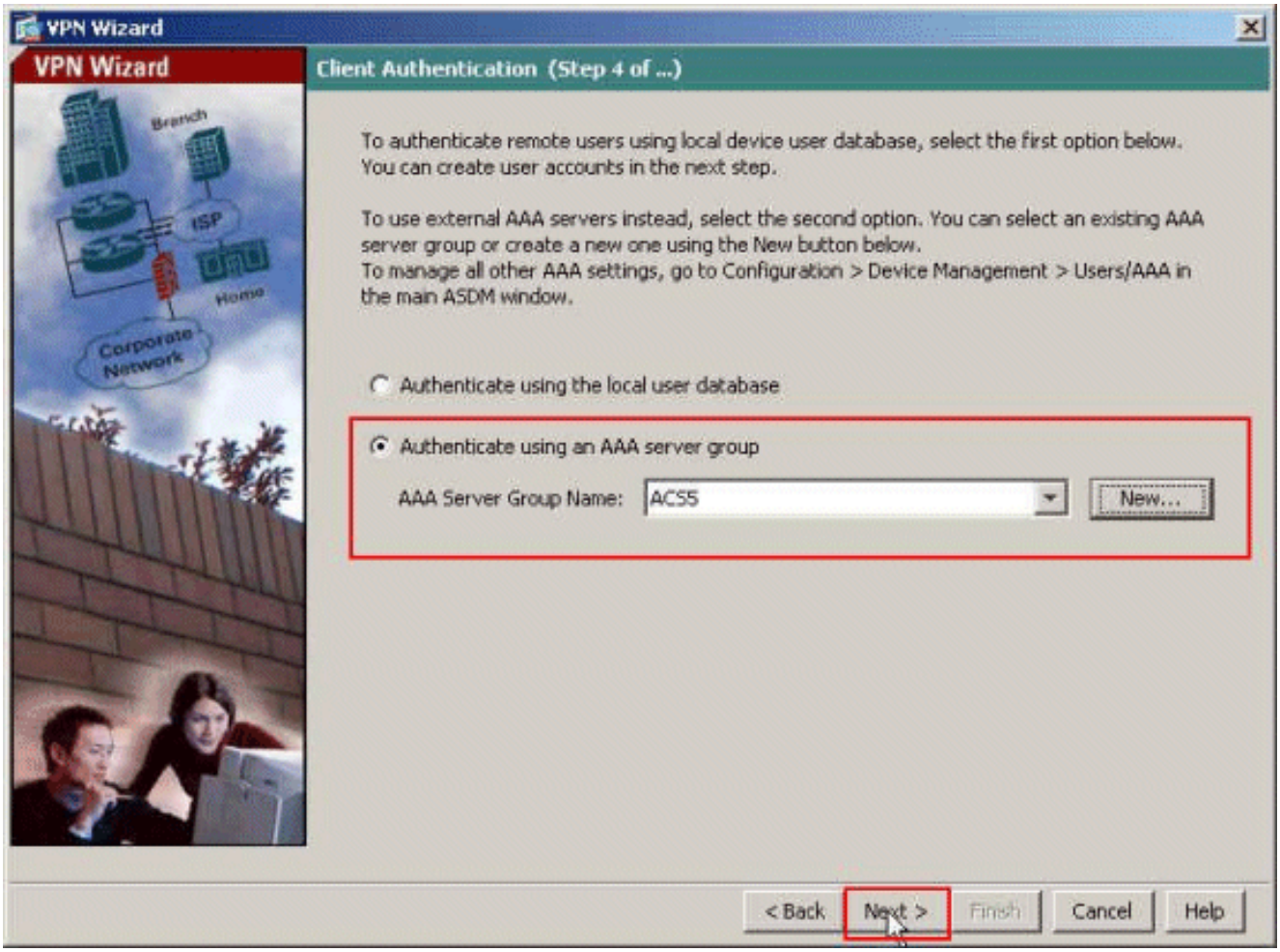


6. 제공된 각 공간에 서버 그룹 이름, 인증 프로토콜, 서버 IP 주소, 인터페이스 이름 및 서버 암호 키를 입력하고 **확인**을 클릭합니다



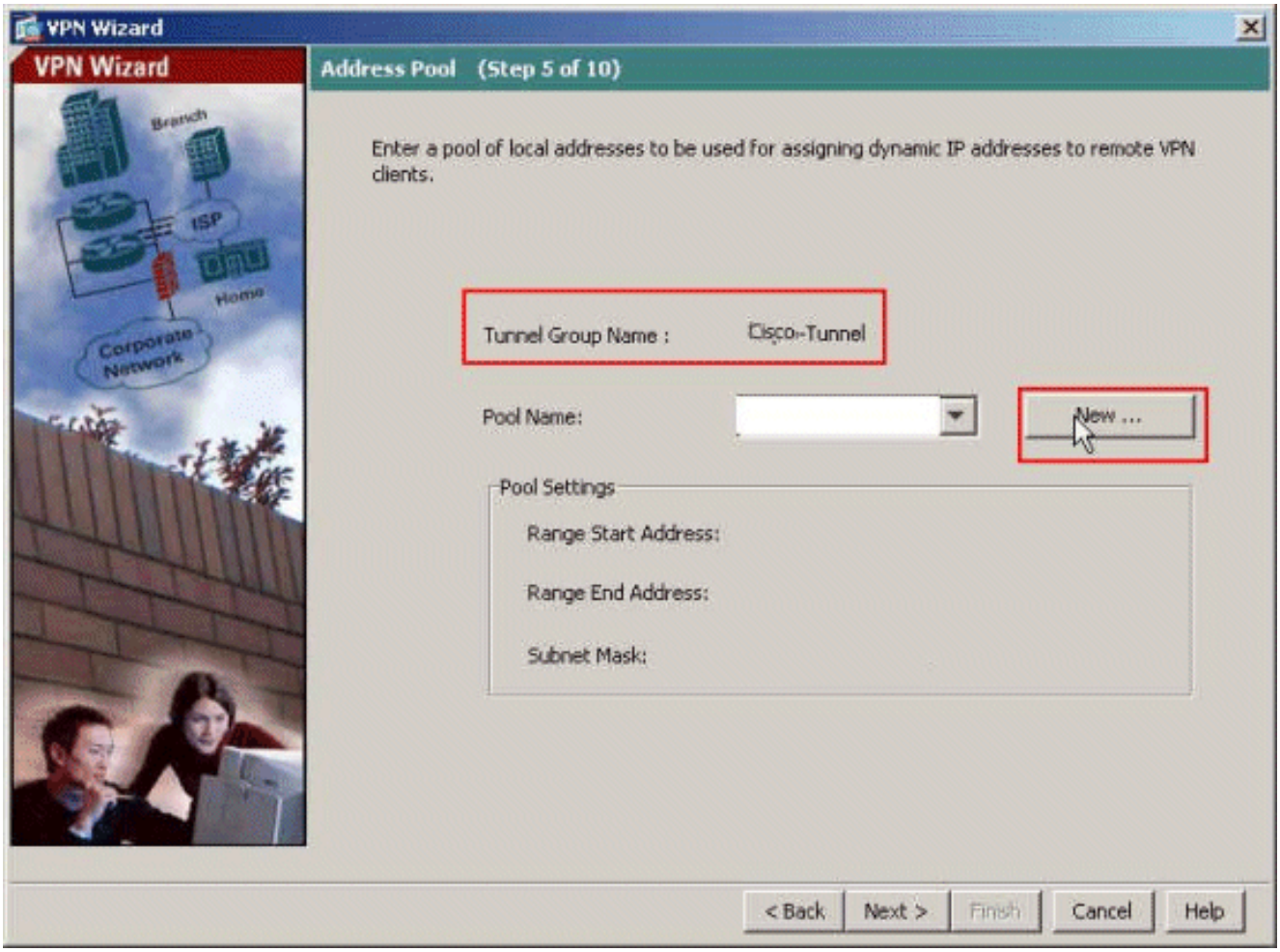
7. Next(다음)를 클릭합니다

.

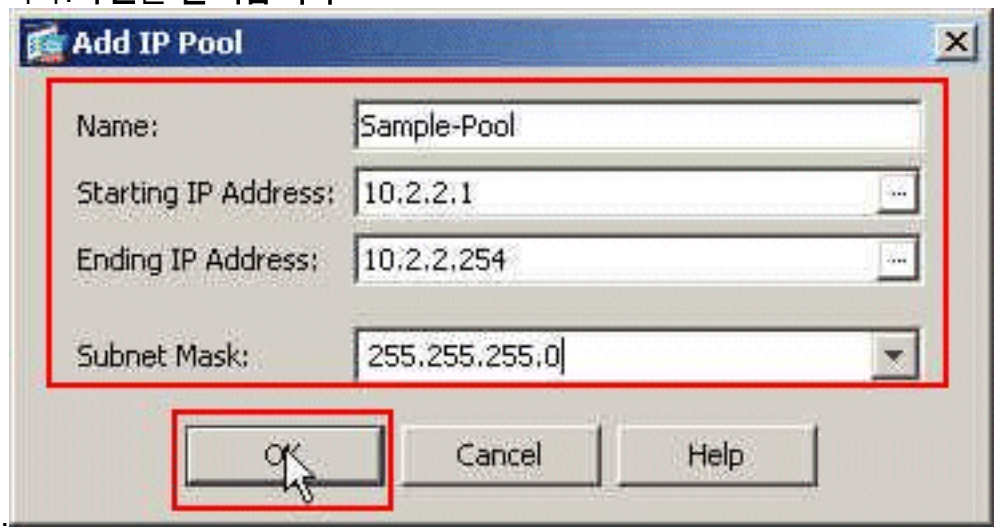


8. 연결할 때 원격 VPN 클라이언트에 동적으로 할당할 로컬 주소 풀을 정의합니다.새 로컬 주소 풀을 생성하려면 **New**를 클릭합니다

.



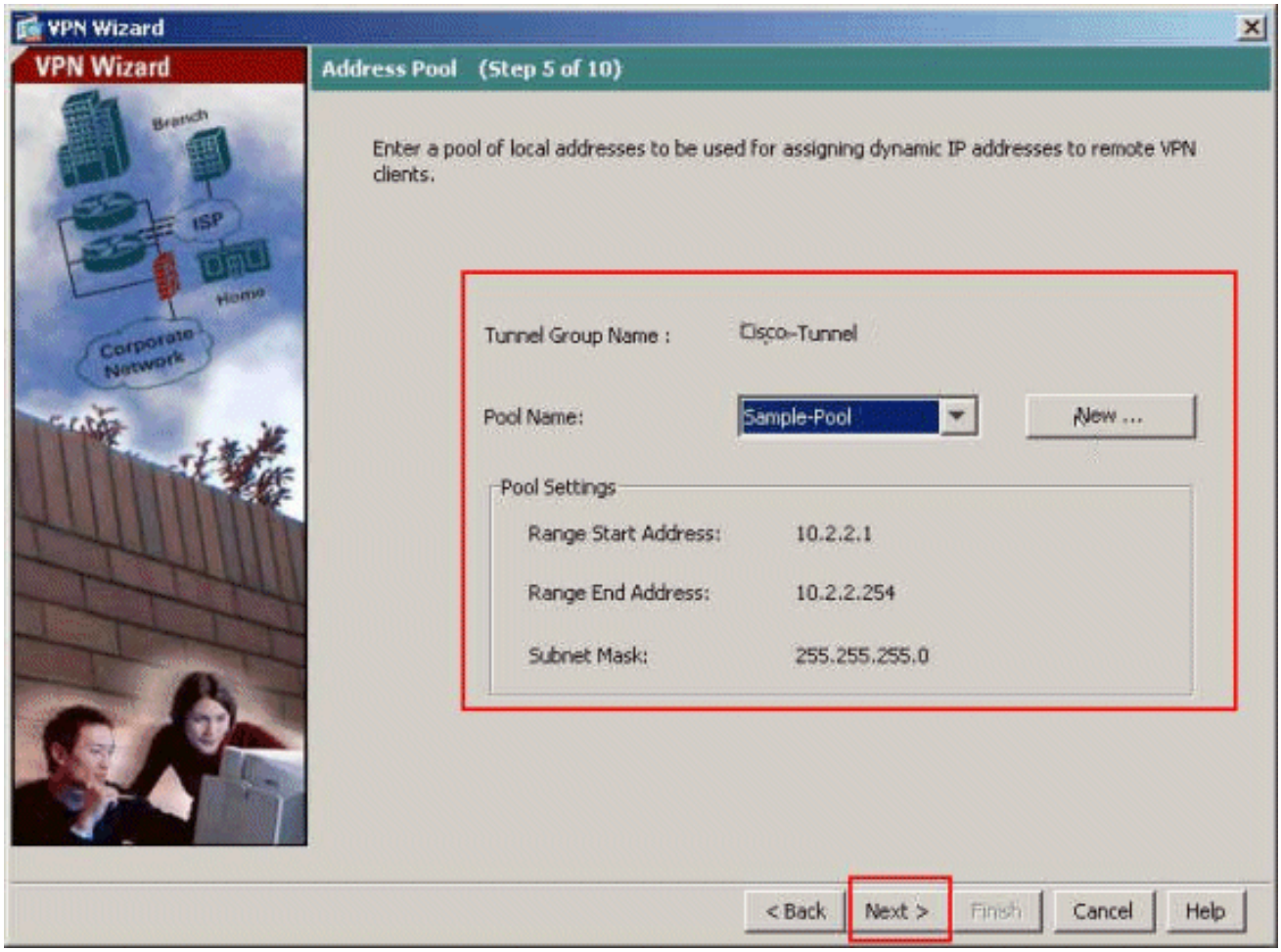
9. Add IP Pool(IP 풀 추가) 창에서 풀 이름, 시작 IP 주소, 끝 IP 주소 및 서브넷 마스크를 제공합니다.**확인**을 **클릭합니다**



.

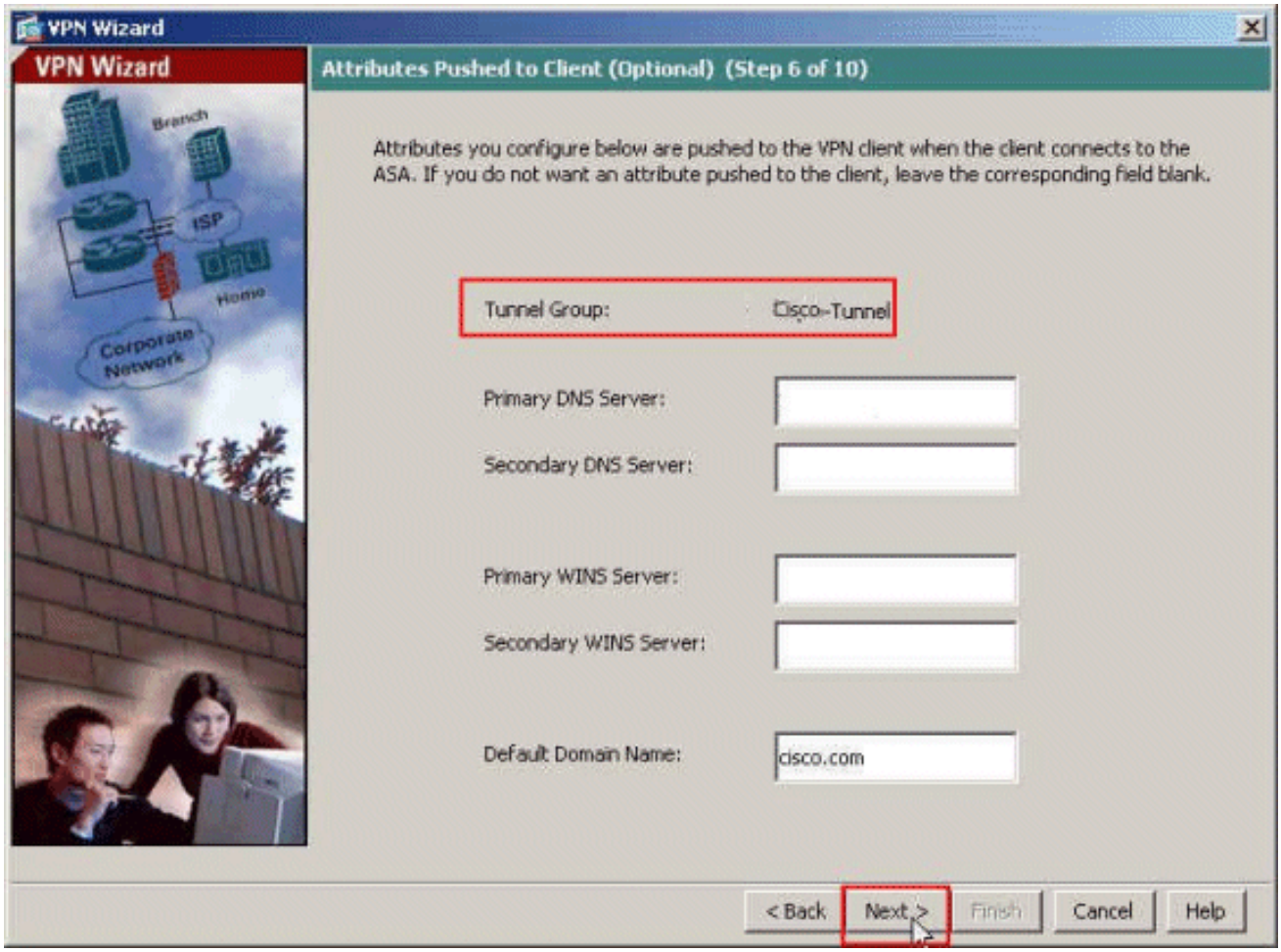
10. 드롭다운 목록에서 Pool Name(풀 이름)을 선택하고 Next(**다음**)를 클릭합니다.이 예제의 풀 이름은 9단계에서 생성한 Sample-**Pool**입니다

.

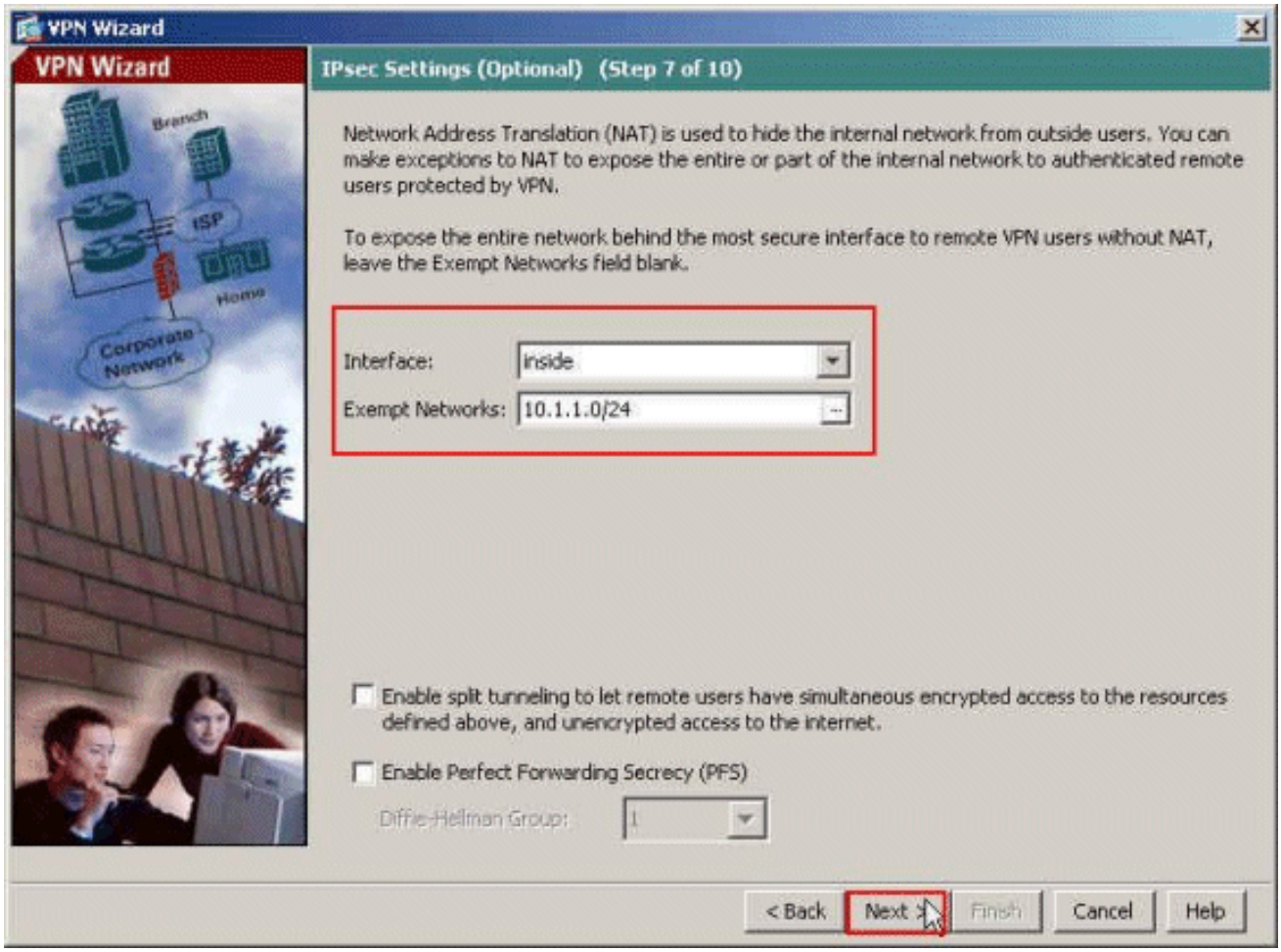


11. *선택 사항:*원격 VPN 클라이언트에 푸시할 DNS 및 WINS 서버 정보 및 기본 도메인 이름을 지정합니다

.

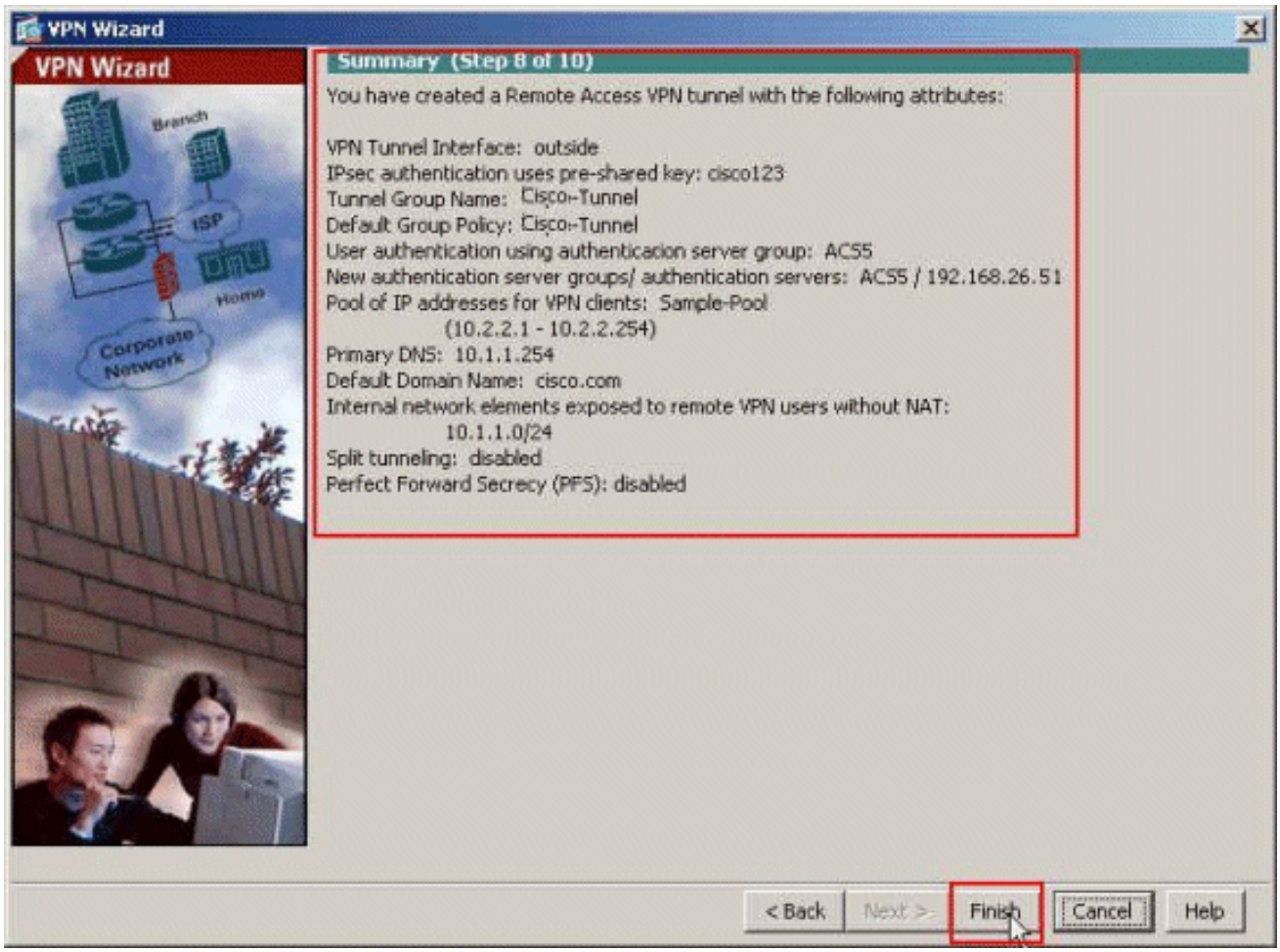


12. 내부 호스트 또는 네트워크가 원격 VPN 사용자에게 노출되어야 하는 경우 지정합니다 .Exempt **Networks**(제외 네트워크) 필드에 Interface name(인터페이스 이름)과 제외할 네트워크를 제공한 후 Next(다음)를 클릭합니다.이 목록을 비워 두면 원격 VPN 사용자가 ASA의 전체 내부 네트워크에 액세스할 수 있습니다.이 창에서 스플릿 터널링을 활성화할 수도 있습니다.스플릿 터널링은 이 절차의 앞부분에서 정의한 리소스로 트래픽을 암호화하고 해당 트래픽을 터널링하지 않음으로써 인터넷에 대한 암호화되지 않은 액세스를 제공합니다.스플릿 터널링이 *활성화되지 않으면* 원격 VPN 사용자의 모든 트래픽이 ASA로 터널링됩니다.이는 컨피그레이션에 따라 대역폭과 프로세서 집약적인 문제가 될 수 있습니다
.



13. 이 창에는 수행한 작업의 요약이 표시됩니다.구성에 만족하면 마침을 클릭합니다

.



CLI로 ASA 구성

다음은 CLI 컨피그레이션입니다.

ASA 디바이스에서 컨피그레이션 실행

```
ASA# sh run
ASA Version 8.4(3)
!
!--- Specify the hostname for the Security Appliance.
hostname ciscoasa enable password y.tvDXf6yFbMTAdD
encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! !---
Configure the outside and inside interfaces. interface
Ethernet0/0 nameif dmz security-level 50 ip address
192.168.26.13 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface Ethernet0/2 nameif outside
security-level 0 ip address 172.16.1.1 255.255.255.0 !
!--- Output is suppressed. boot system disk0:/asa843-
k8.bin ftp mode passive object network
NETWORK_OBJ_10.1.1.0_24 subnet 10.1.1.0 255.255.255.0
object network NETWORK_OBJ_10.2.2.0_24 subnet 10.2.2.0
255.255.255.0 access-list OUTIN extended permit icmp any
any !--- This is the Access-List whose name will be sent
by !--- RADIUS Server(ACS) in the Filter-ID attribute.
access-list new extended permit ip any host 10.1.1.2
access-list new extended deny ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500

ip local pool Sample-Pool 10.2.2.1-10.2.2.254 mask
255.255.255.0

no failover
icmp unreachable rate-limit 1 burst-size 1

!--- Specify the location of the ASDM image for ASA !---
to fetch the image for ASDM access. asdm image
disk0:/asdm-647.bin no asdm history enable arp timeout
14400 !--- Specify the NAT from internal network to the
Sample-Pool. nat (inside,outside) source static
NETWORK_OBJ_10.1.1.0_24 NETWORK_OBJ_10.1.1.0_24
destination static NETWORK_OBJ_10.2.2.0_24
NETWORK_OBJ_10.2.2.0_24 no-proxy-arp route-lookup
access-group OUTIN in interface outside !--- Create the
AAA server group "ACS5" and specify the protocol as
RADIUS. !--- Specify the ACS 5.x server as a member of
the "ACS5" group and provide the !--- location and key.
aaa-server ACS5 protocol radius
aaa-server ACS5 (dmz) host 192.168.26.51
timeout 5
key *****

aaa authentication http console LOCAL
http server enable 2003
http 0.0.0.0 0.0.0.0 inside
```

```
!--- PHASE 2 CONFIGURATION ---! !--- The encryption &
hashing types for Phase 2 are defined here. We are using
!--- all the permutations of the PHASE 2 parameters.
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-
aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-
aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-
aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-
aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes
esp-md5-hmac


!--- Defines a dynamic crypto map with !--- the
specified transform-sets created earlier. We are
specifying all the !--- transform-sets. crypto dynamic-
map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-
set
   ESP-AES-128-SHA ESP-AES-128-MD5
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-
256-MD5 ESP-3DES-SHA
   ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5

!--- Binds the dynamic map to the IPsec/ISAKMP process.
crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP

!--- Specifies the interface to be used with !--- the
settings defined in this configuration. crypto map
outside_map interface outside

!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policies defined with all the permutation !-
-- of the 5 ISAKMP parameters. The configuration
commands here define the !--- Phase 1 policy parameters
that are used. crypto ikev1 enable outside

crypto ikev1 policy 10
authentication crack
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
group 2
lifetime 86400
```

```
crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 40
authentication crack
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 70
authentication crack
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 90
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 100
authentication crack
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 110
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 120
```

```
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 130
authentication crack
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 140
authentication rsa-sig
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 150
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400


webvpn
group-policy Cisco-Tunnel internal
group-policy Cisco-Tunnel attributes
vpn-tunnel-protocol ikev1
default-domain value cisco.com
username admin password CdOTKv3uhDhHIw3A encrypted
privilege 15
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (ACS5) with the tunnel group. tunnel-group Cisco-
Tunnel type remote-access tunnel-group Cisco-Tunnel
general-attributes
address-pool Sample-Pool
authentication-server-group ACS5
default-group-policy Cisco-Tunnel

!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group Cisco-Tunnel ipsec-
attributes
ikev1 pre-shared-key *****

prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
: end
ASA#
```

개별 사용자에 대해 다운로드 가능한 ACL에 대한 ACS 구성

Cisco Secure ACS 5.x에서 다운로드 가능한 액세스 목록을 명명된 권한 개체로 구성한 다음 액세스 서비스 규칙의 결과 섹션에서 선택할 권한 부여 프로파일에 할당할 수 있습니다.

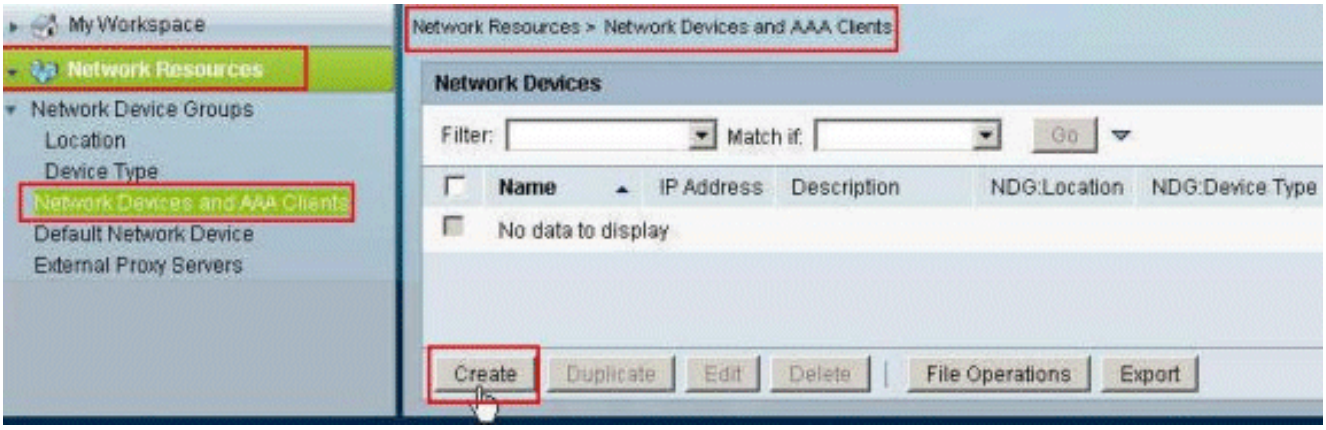
이 예에서 IPsec VPN 사용자 **cisco는** 성공적으로 인증하고 RADIUS 서버는 보안 어플라이언스에 다운로드 가능한 액세스 목록을 전송합니다."cisco" 사용자는 10.1.1.2 서버에만 액세스할 수 있으

며 다른 모든 액세스를 거부합니다.ACL을 확인하려면 Downloadable ACL for User/Group 섹션을 참조하십시오.

Cisco Secure ACS 5.x에서 RADIUS 클라이언트를 구성하려면 다음 단계를 완료합니다.

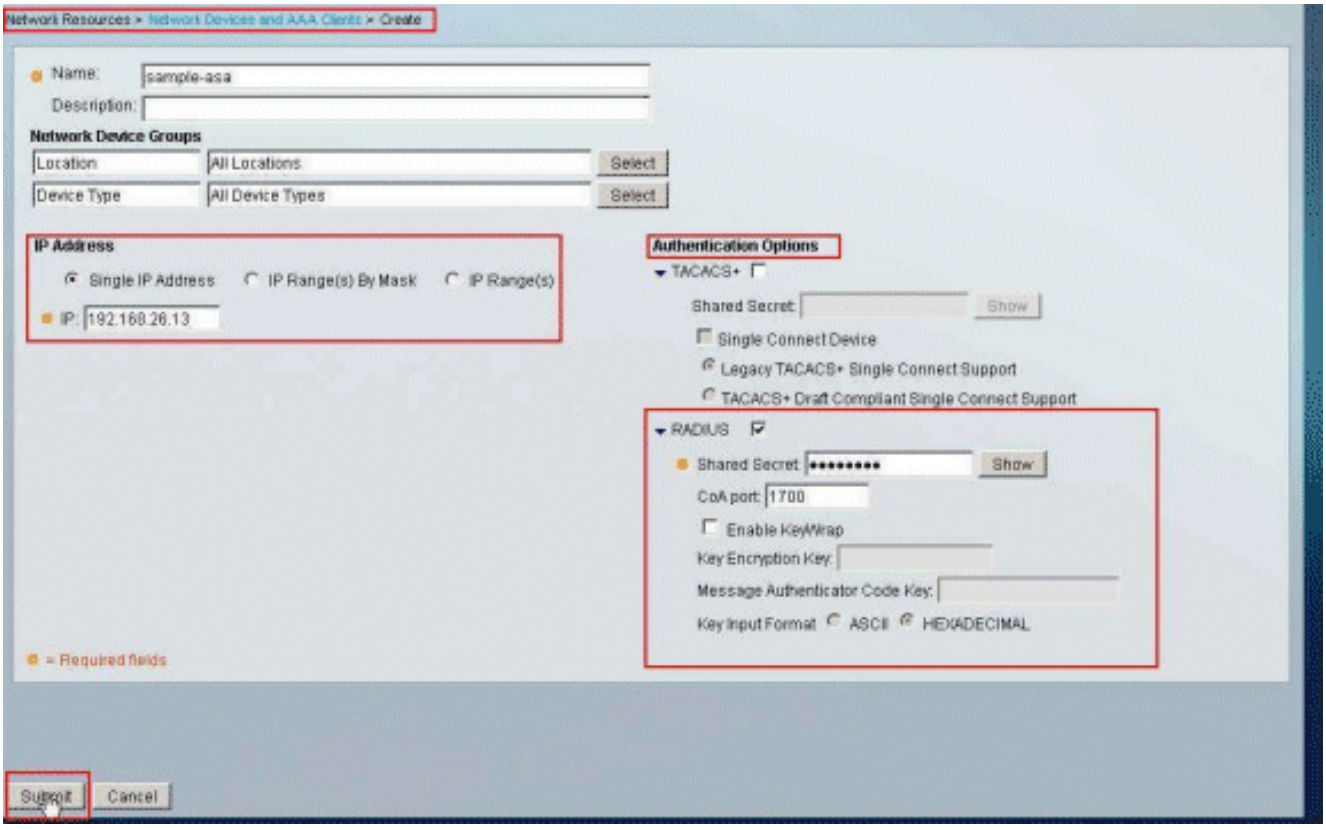
1. Network **Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)를** 선택하고 Create(생성)를 클릭하여 RADIUS 서버 데이터베이스에 ASA에 대한 항목을 추가합니다

.



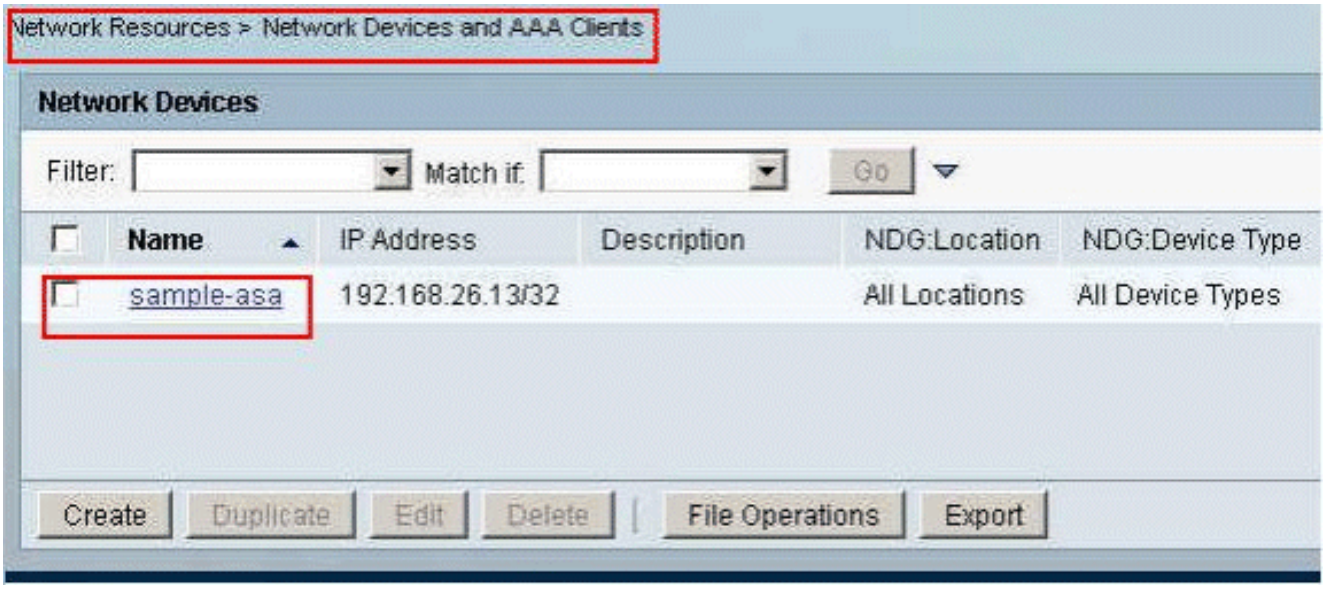
2. ASA의 로컬 유효 이름(이 예에서 **sample-asa**)을 입력한 다음 IP 주소 필드**에 192.168.26.13**을 입력합니다.Authentication Options(인증 옵션) 섹션에서 **RADIUS** 확인란을 선택하여 RADIUS를 선택하고 Shared Secret(공유 암호) 필드에 **cisco123**을 입력합니다.Submit(제출)**을 클릭합니다**

.



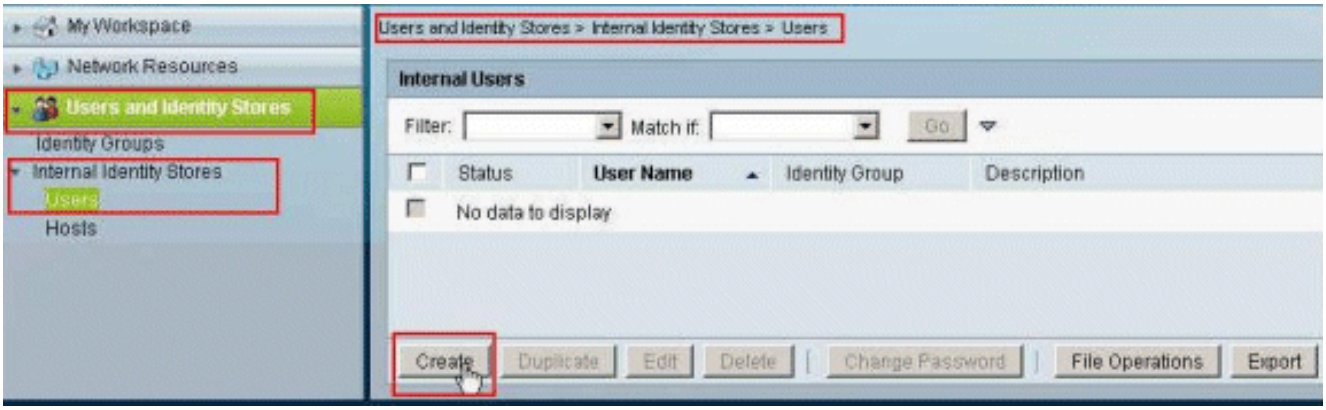
3. ASA가 RADIUS 서버(ACS) 데이터베이스에 성공적으로 추가되었습니다

.



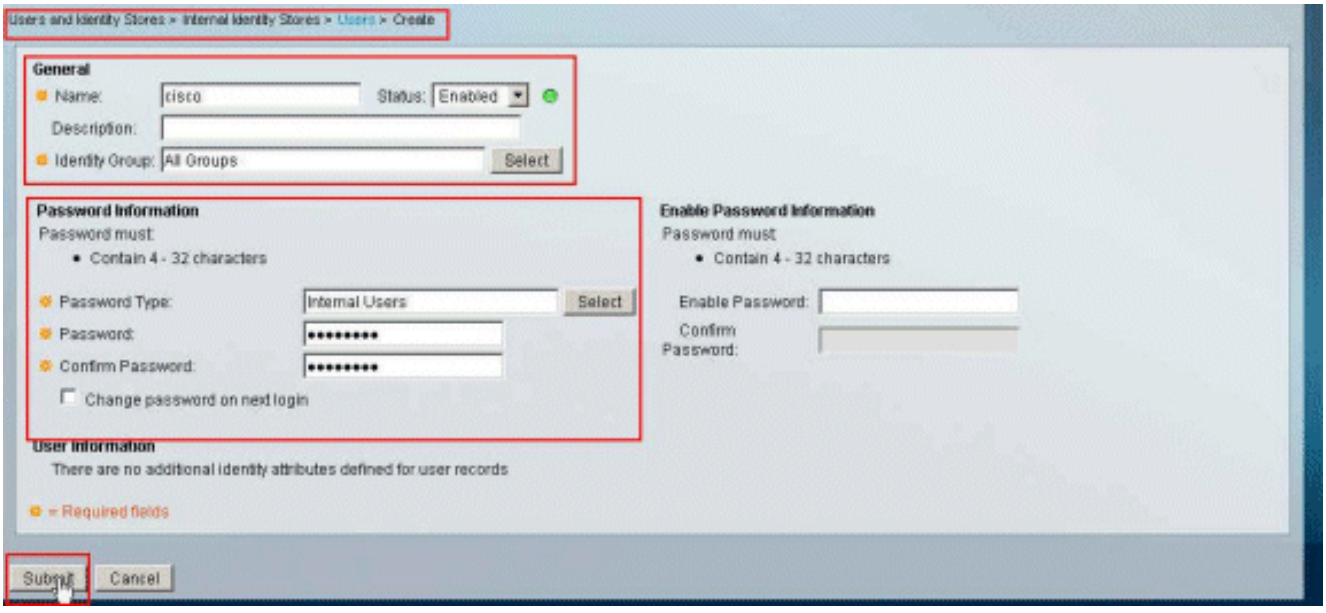
4. Users **and Identity Stores(사용자 및 ID 저장소) > Internal Identity Stores(내부 ID 저장소) > Users(사용자)를** 선택하고 **Create(생성)를** 클릭하여 VPN 인증을 위한 ACS의 로컬 데이터베이스에서 사용자를 생성합니다

.



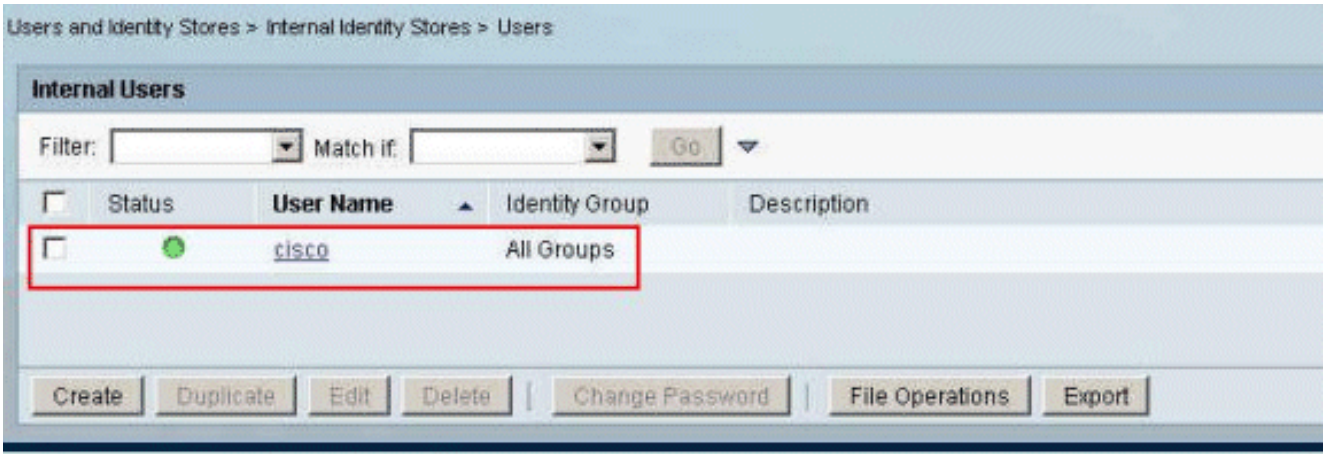
5. **cisco** 사용자 이름을 **입력합니다**.비밀번호 유형을 **내부 사용자**로 선택하고 비밀번호(**cisco123**, 이 예에서는)를 입력합니다. 비밀번호를 확인하고 Submit(제출)을 **클릭합니다**

.



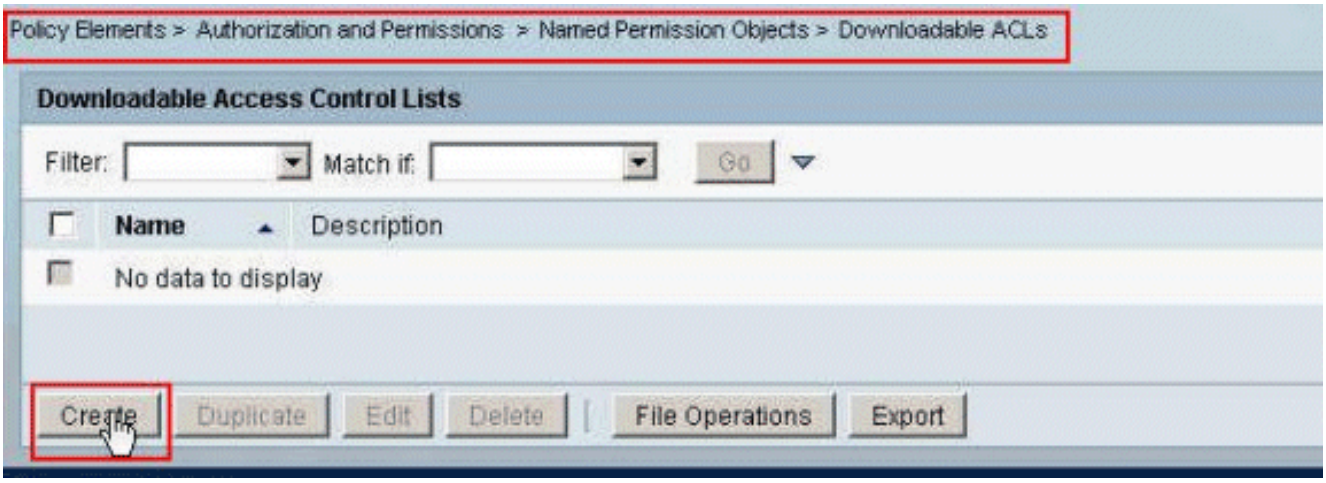
6. 사용자 **cisco**가 성공적으로 생성되었습니다

.



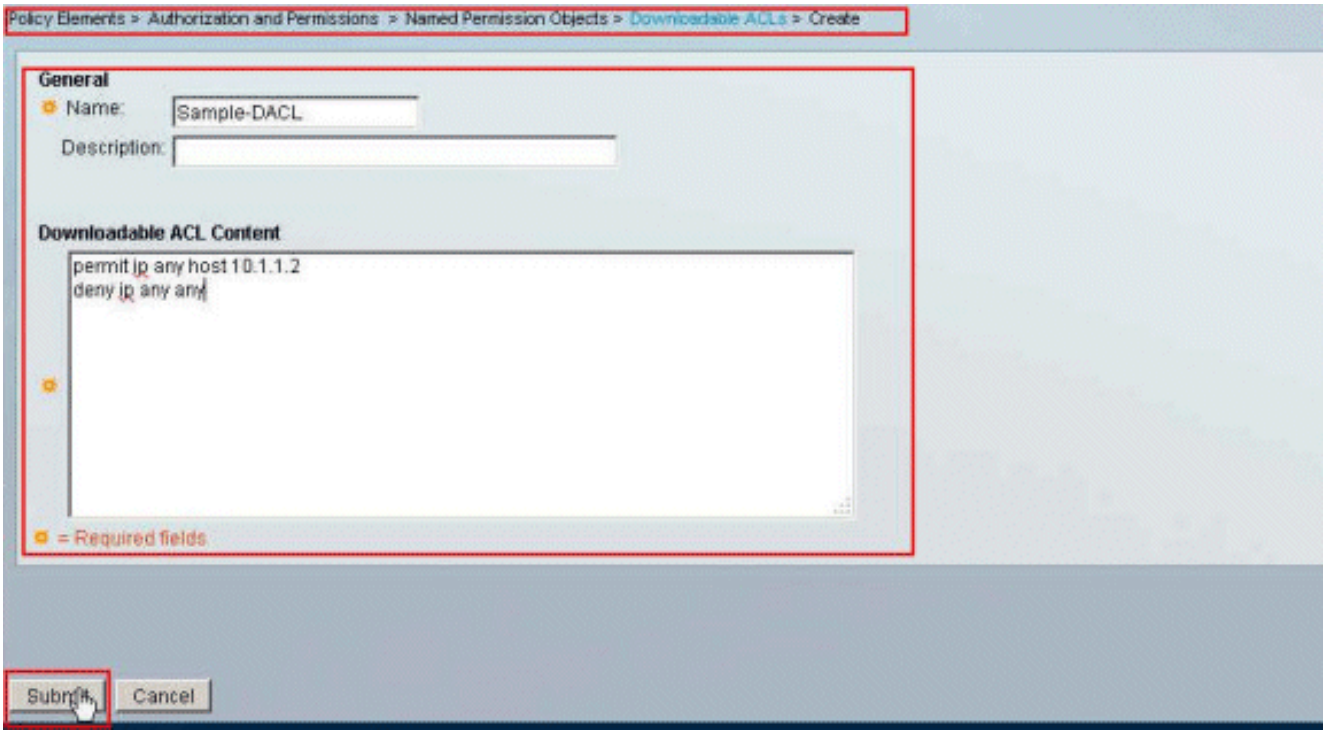
7. 다운로드 가능한 ACL을 만들려면 **Policy Elements(정책 요소)** > Authorization **and Permissions(권한 부여 및 권한)** > Named Permission Objects(명명된 권한 개체) > **Downloadable ACLs(다운로드 가능한 ACL)를** 선택하고 Create(생성)를 **클릭합니다**

.



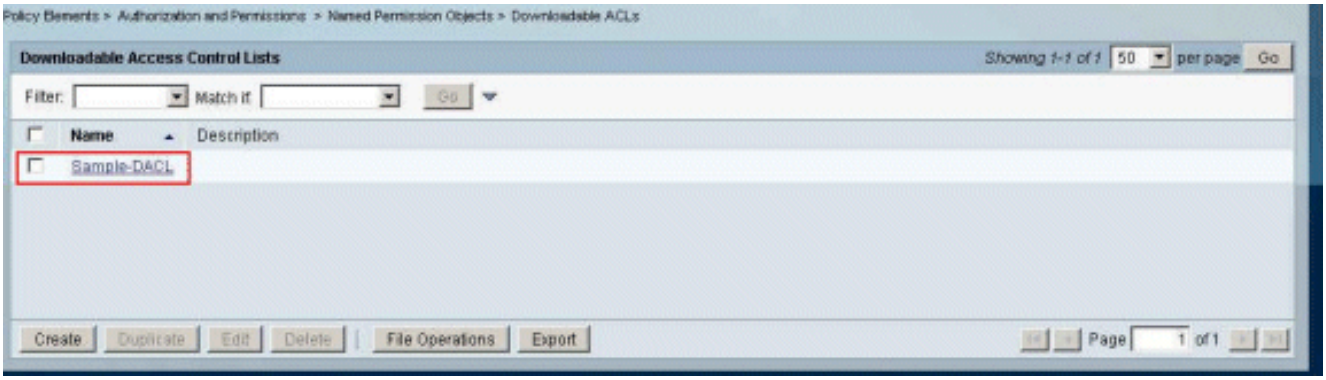
8. 다운로드 **가능한** ACL의 이름과 **ACL 콘텐츠를 제공합니다**.Submit(제출)**을 클릭합니다**

.



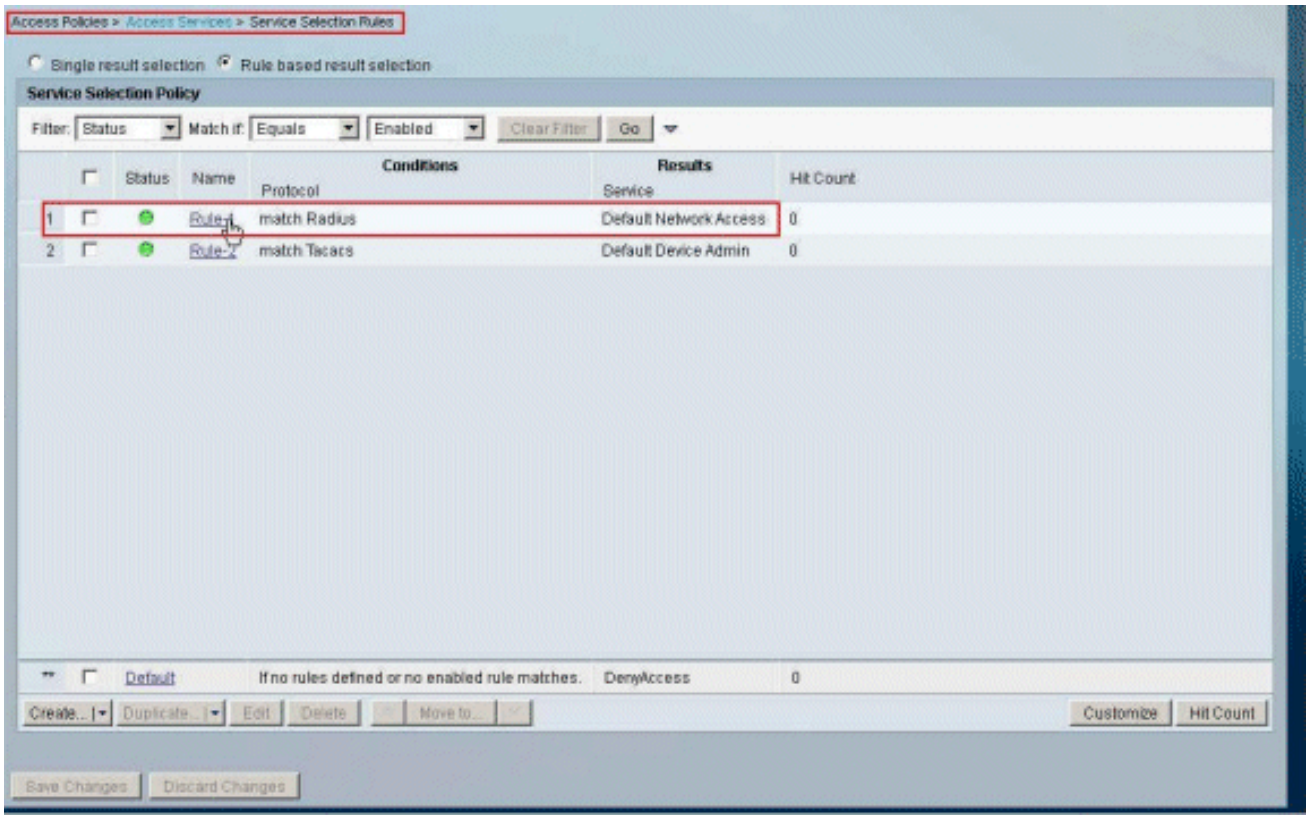
9. 다운로드 가능한 ACL **샘플-DACL**이 성공적으로 생성됩니다

.



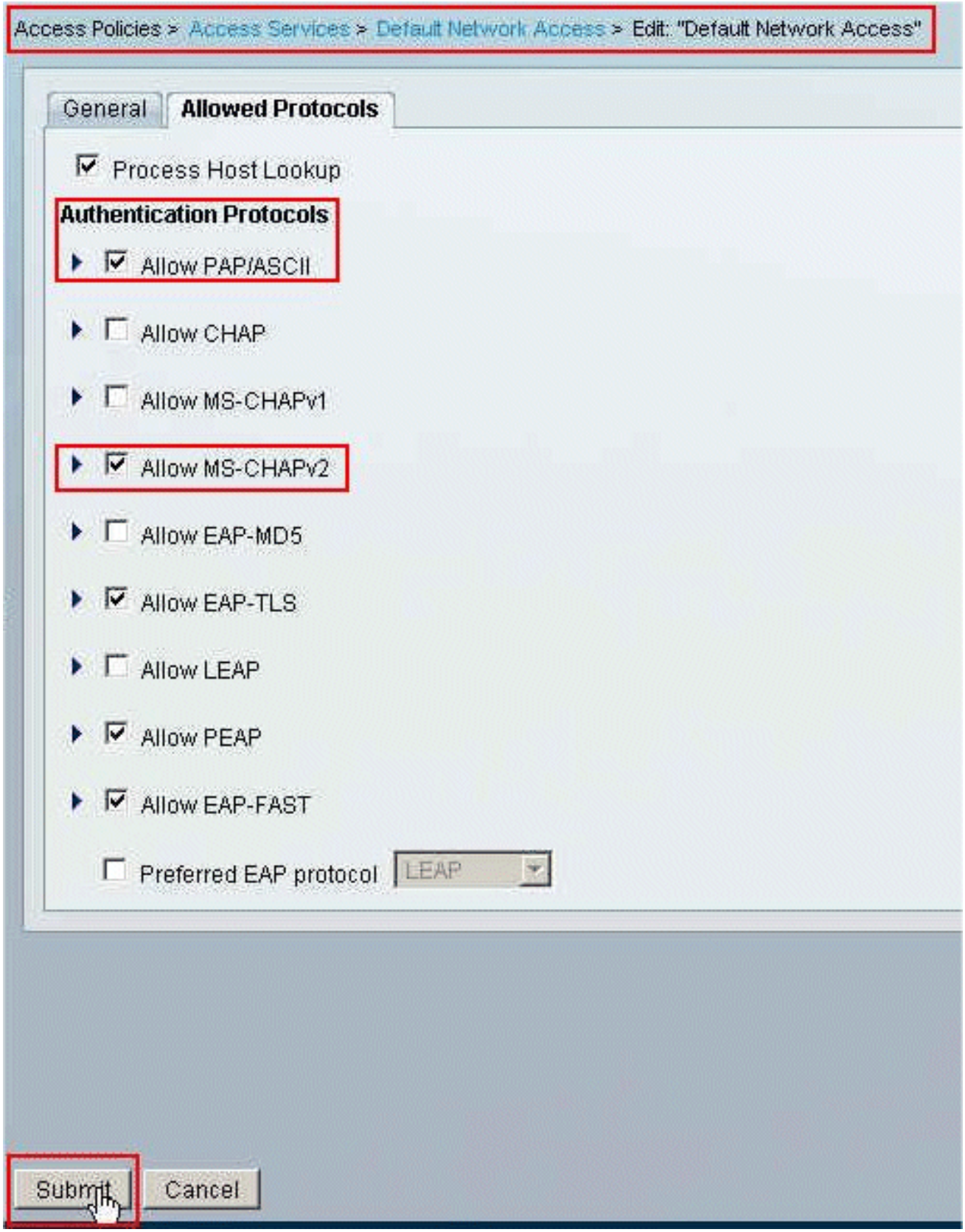
10. VPN 인증을 위한 액세스 정책을 구성하려면 **Access Policies(액세스 정책) > Access Services(액세스 서비스) > Service Selection Rules(서비스 선택 규칙)를** 선택하고 RADIUS 프로토콜에 적용할 서비스를 확인합니다.이 예에서 **Rule 1**은 **RADIUS**와 일치하고 Default Network Access는 RADIUS 요청에 대응합니다

.



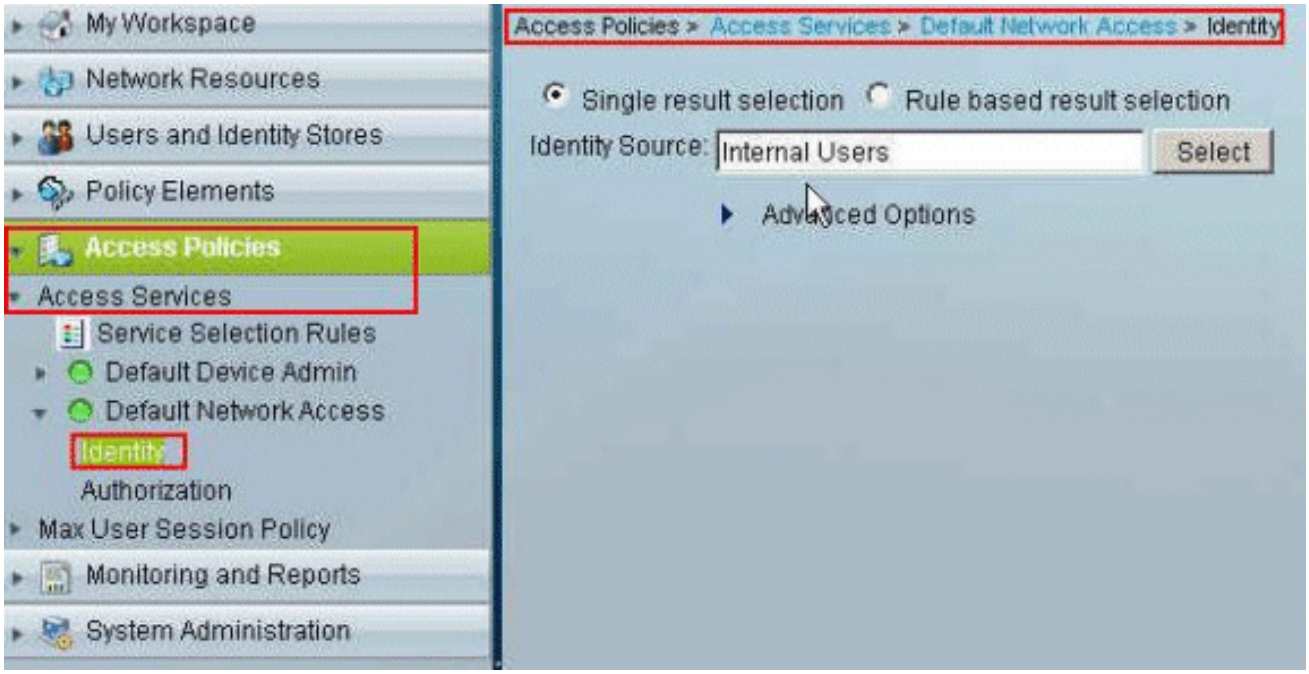
11. 10단계에서 결정된 **액세스 서비스**를 선택합니다. 이 예에서는 **기본 네트워크 액세스**가 사용됩니다.Allowed **Protocols(허용된 프로토콜)** 탭을 선택하고 Allow PAP**/ASCII(PAP/ASCII 허용)** 및 **Allow MS-CHAPv2(MS-CHAPv2 허용)가 선택되었는지** 확인합니다.Submit(제출)을 **클릭합니다**

.



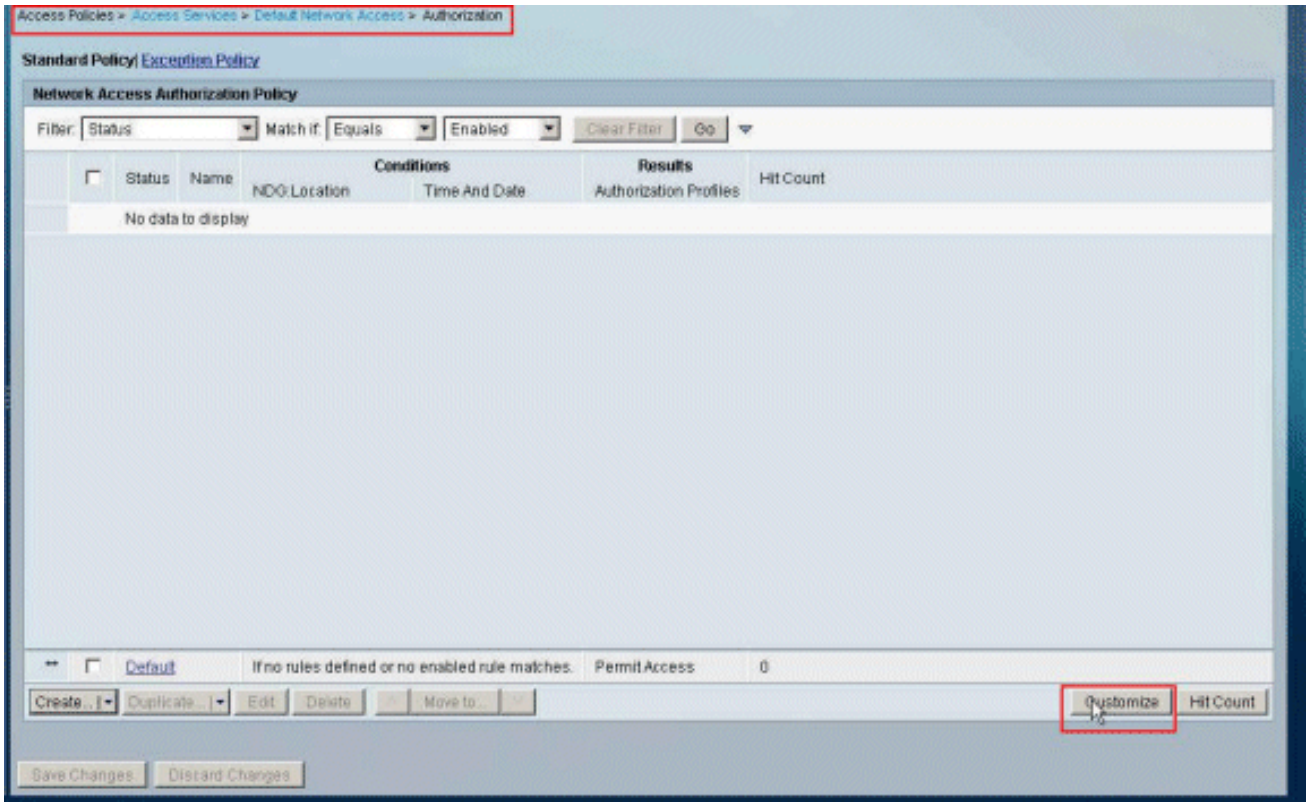
12. **Access Services**의 **Identity 섹션**을 클릭하고 **Internal Users(내부 사용자)**가 Identity Source(ID 소스)로 선택되었는지 확인합니다.이 예에서는 기본 네트워크 액세스를 사용했습니다

.



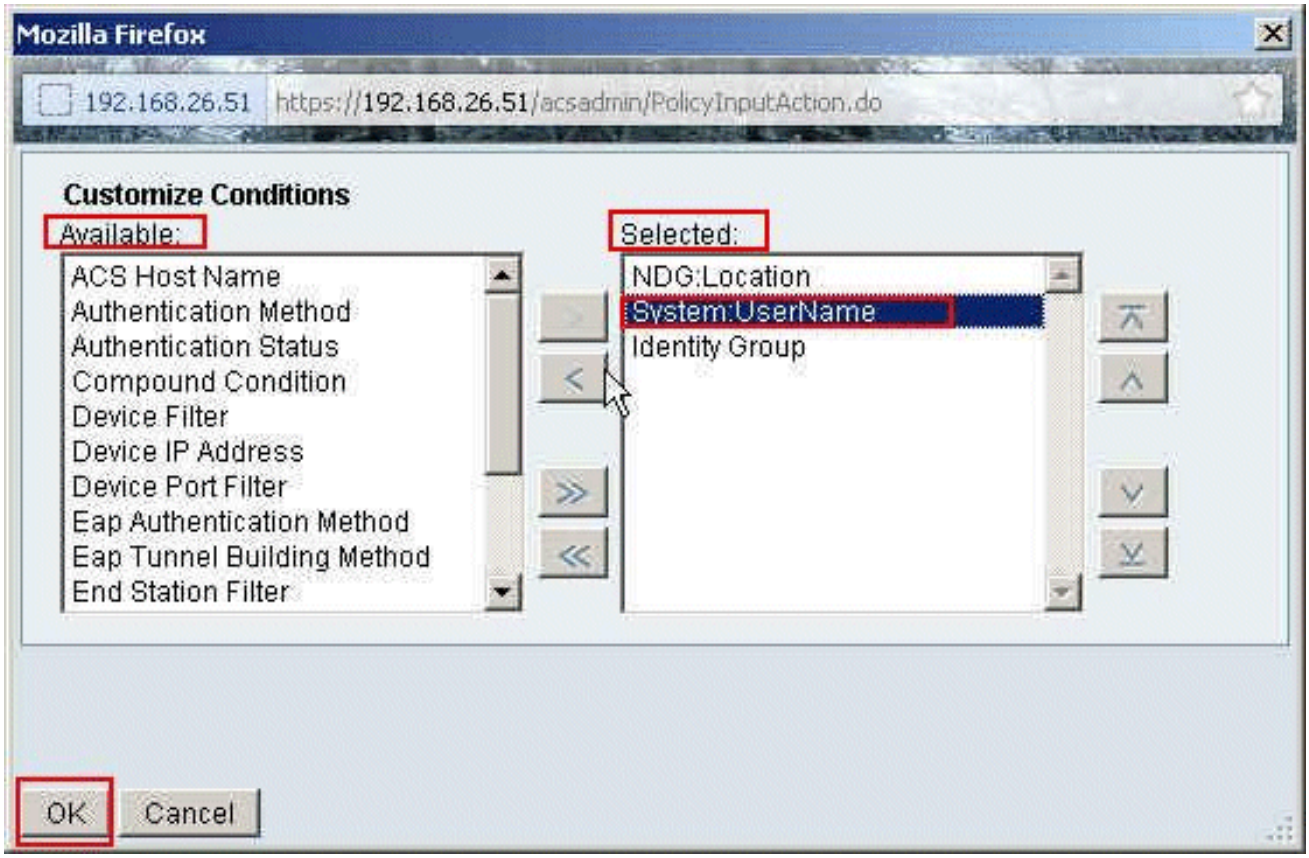
13. Access **Policies(액세스 정책)** > **Access Services(액세스 서비스)** > Default Network Access(**기본 네트워크 액세스**) > Authorization(권한 부여)을 선택하고 Customize(사용자 지정)를 **클릭합니다**

.



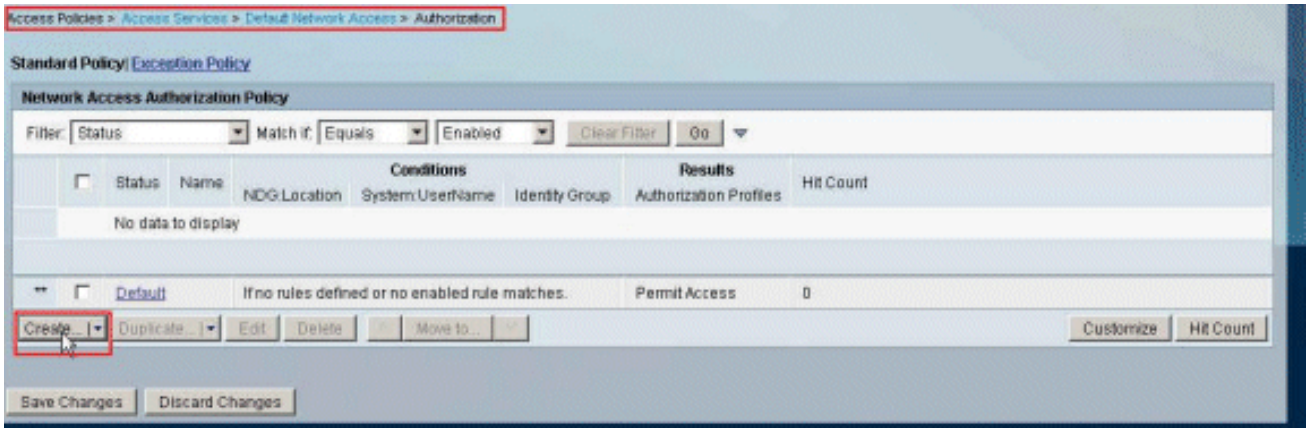
14. **System:UserName을 Available** 열에서 **Selected** 열로 **이동하고 OK**를 클릭합니다

.



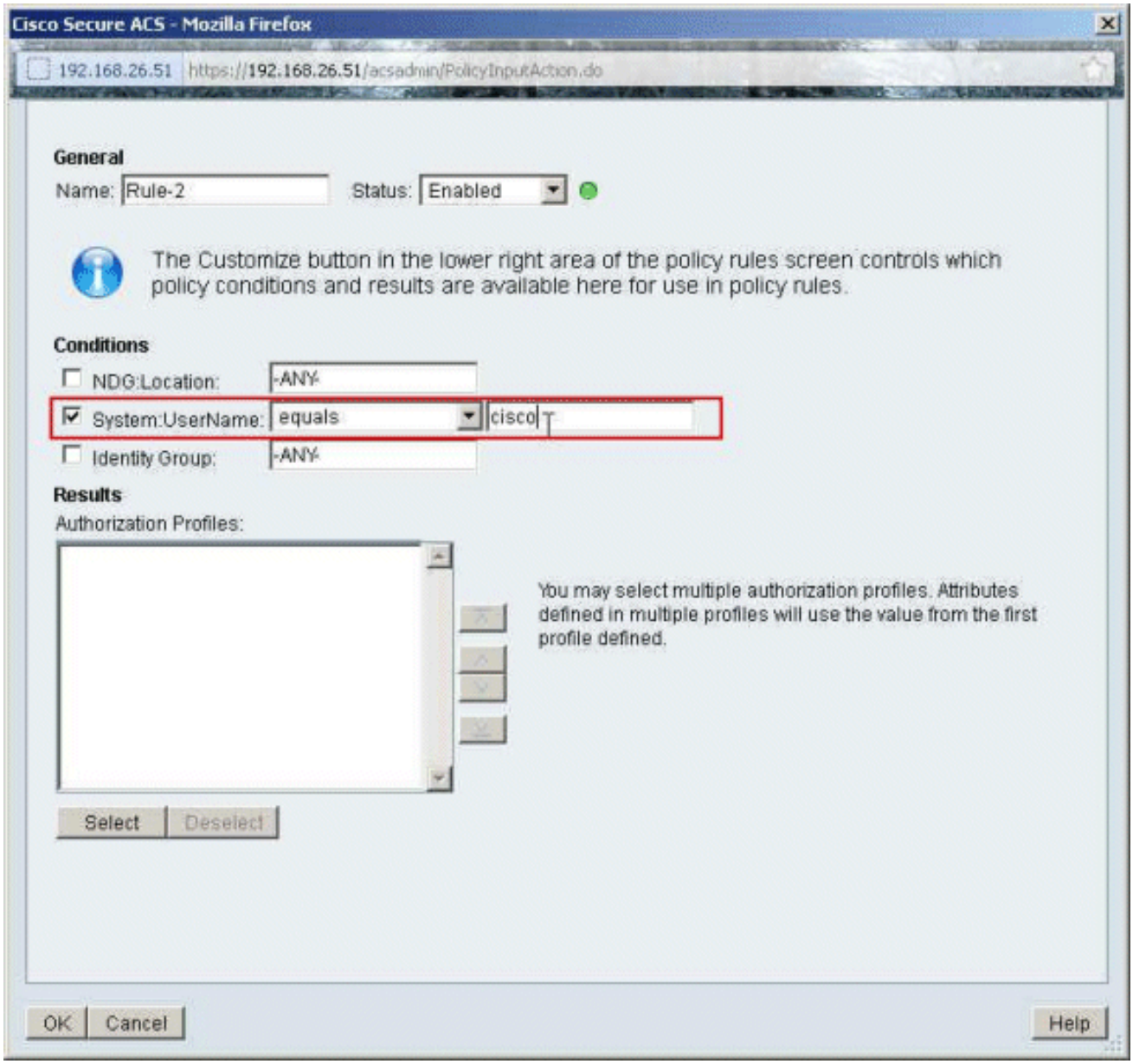
15. 새 규칙을 생성하려면 Create를 클릭합니다

.



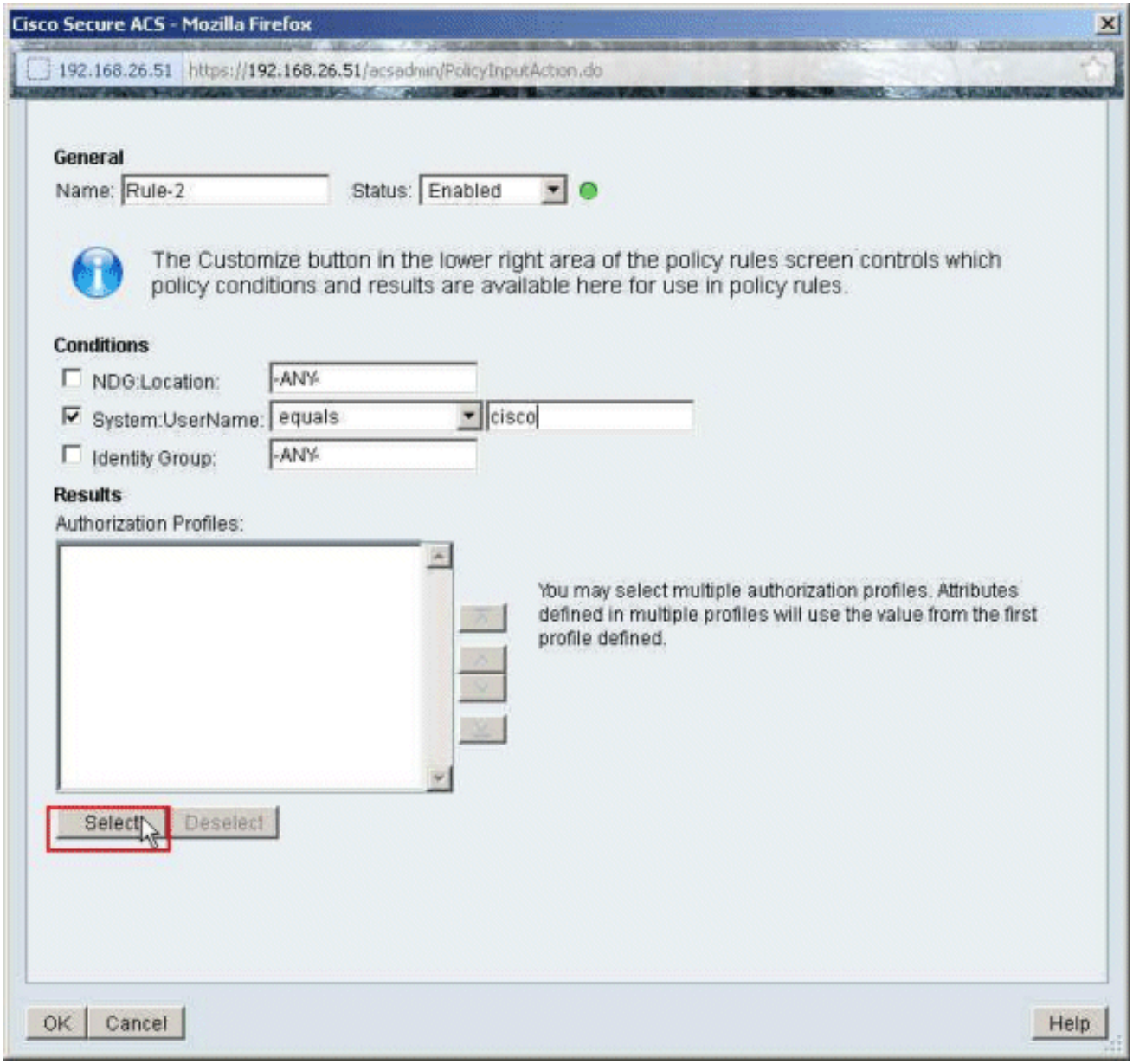
16. **System:UserName** 옆의 확인란이 선택되었는지 확인하고 드롭다운 목록에서 **등호**를 선택하고 **cisco** 사용자 이름을 **입력합니다**

.

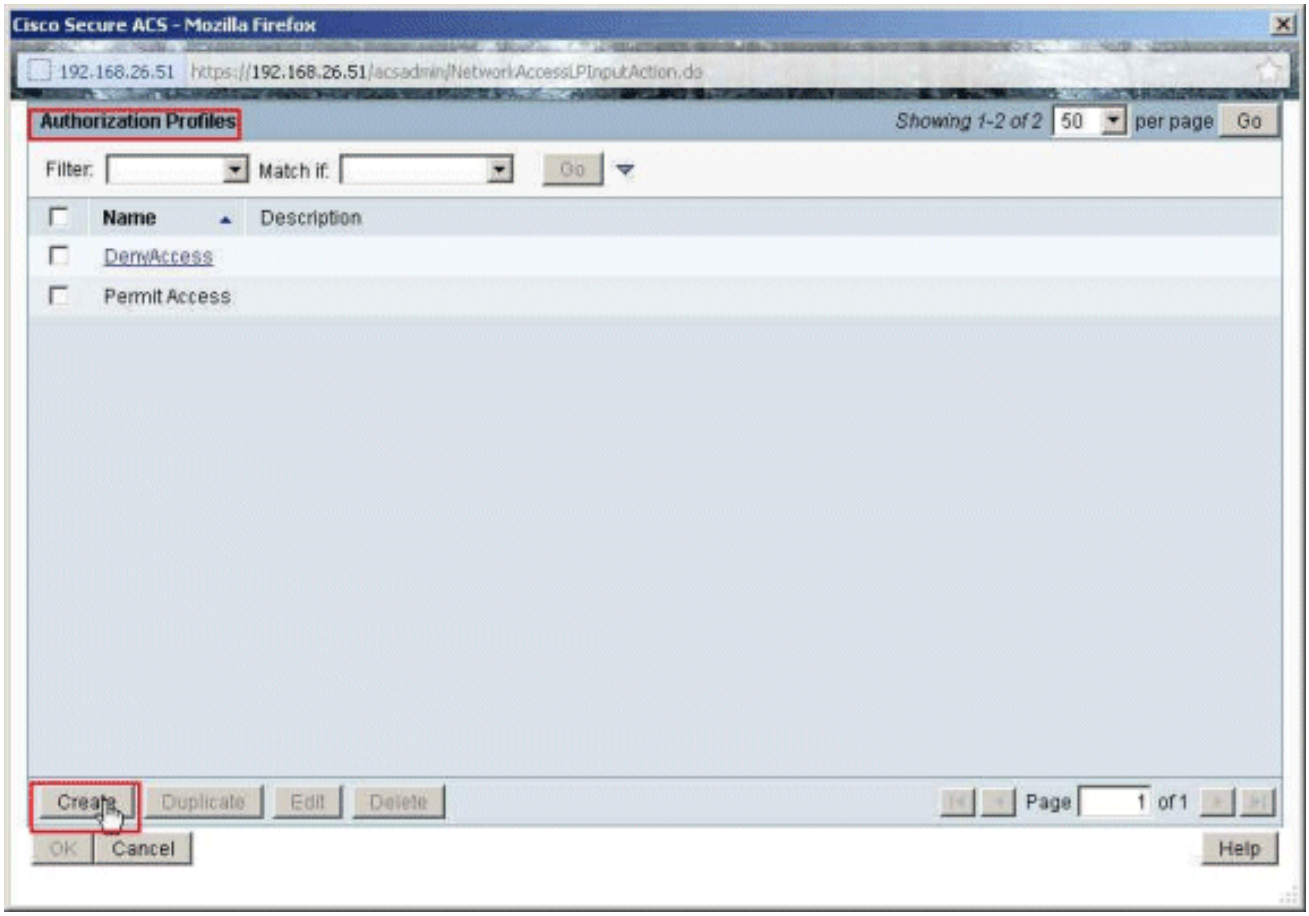

Cisco Secure ACS - Mozilla Firefox
192.168.26.51
https://192.168.26.51/acsadmin/PolicyInputAction.do
General
Name: Rule-2
Status: Enabled
The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.
Conditions
NDG:Location: -ANY-
System:UserName: equals cisco
Identity Group: -ANY-
Results
Authorization Profiles:
You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.
Select
Deselect
OK
Cancel
Help

17. 선택을 **클릭합니다**

.

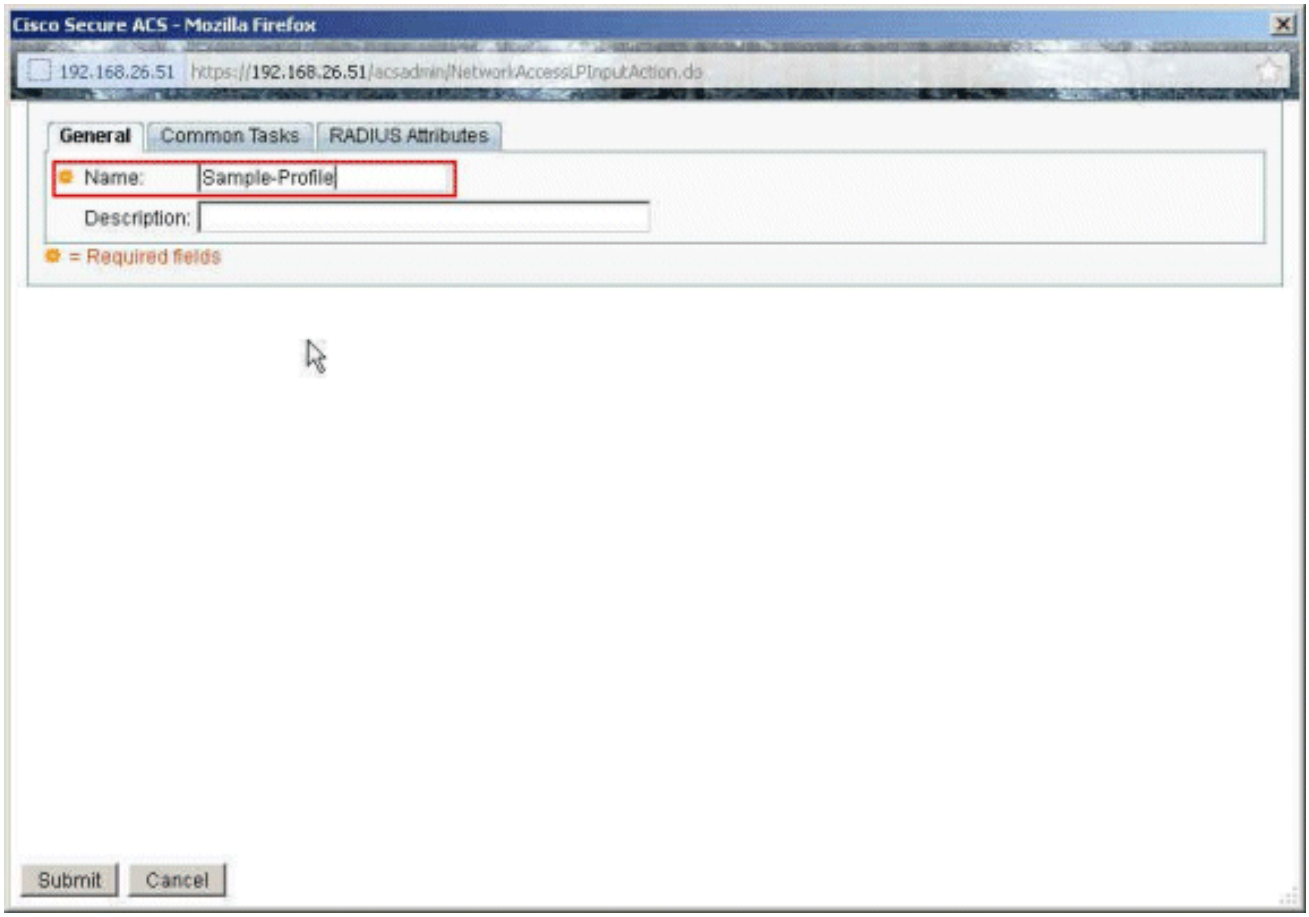


18. 새 권한 부여 프로파일을 생성하려면 Create를 클릭합니다
.



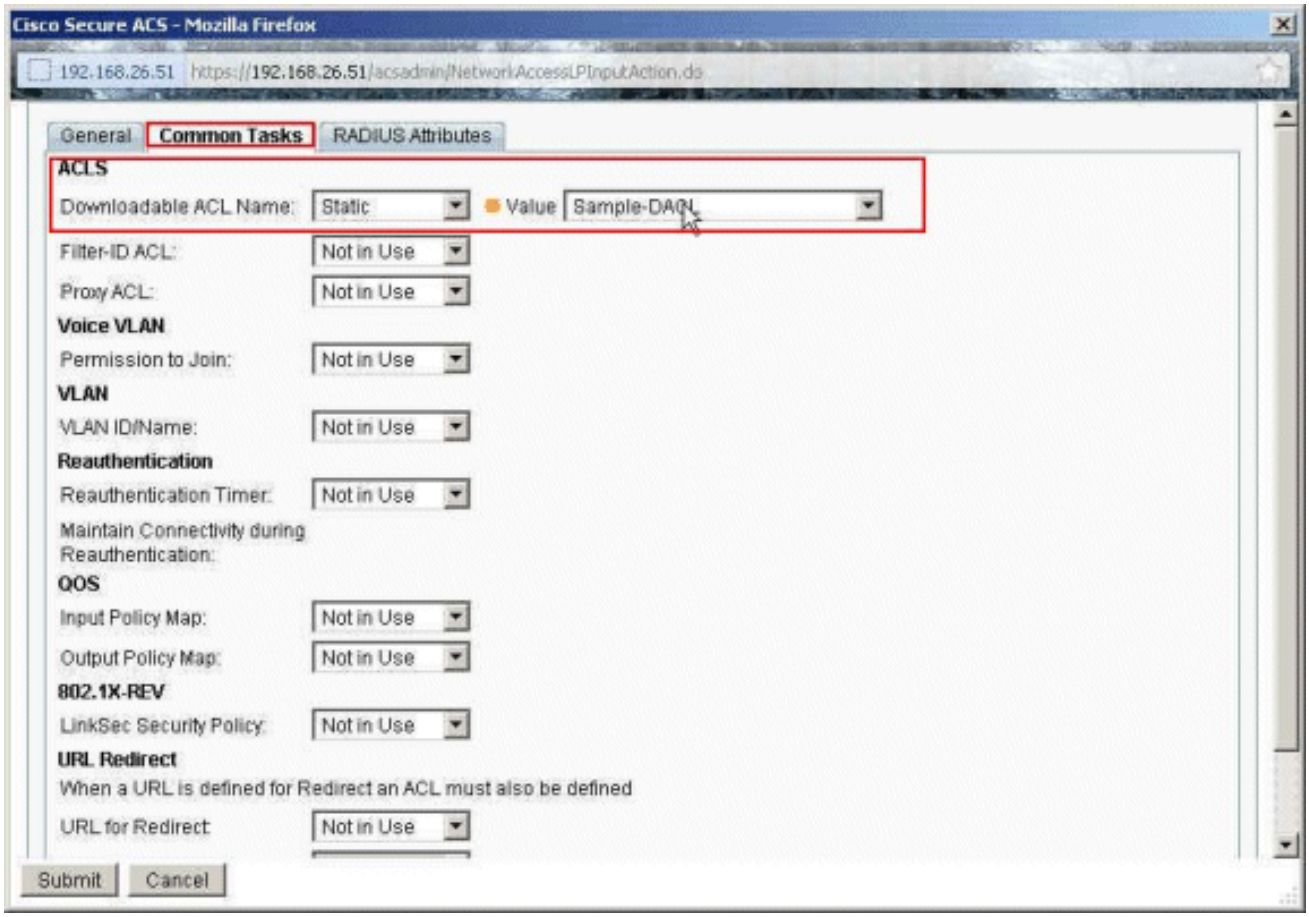
19. 권한 부여 프로파일의 이름을 **입력합니다.Sample-Profile**은 이 예에 사용됩니다

.



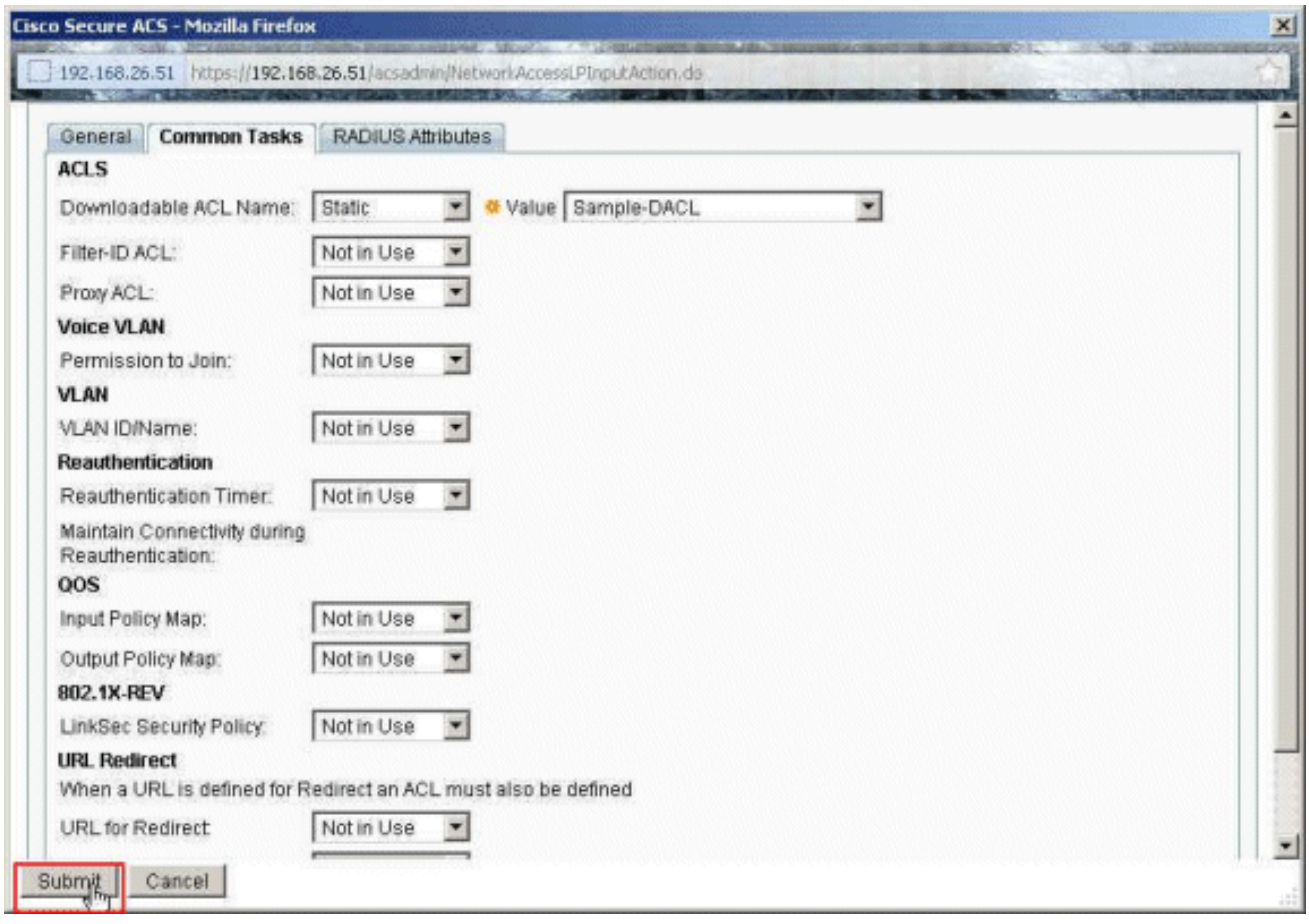
20. Common Tasks(**일반 작업**) 탭을 선택하고 **Downloadable ACL Name(다운로드 가능한 ACL 이름)**의 드롭다운 목록에서 Static(정적)을 **선택합니다**.새로 생성된 **DACL(Sample -DACL)**을 값 드롭다운 목록에서 선택합니다

.



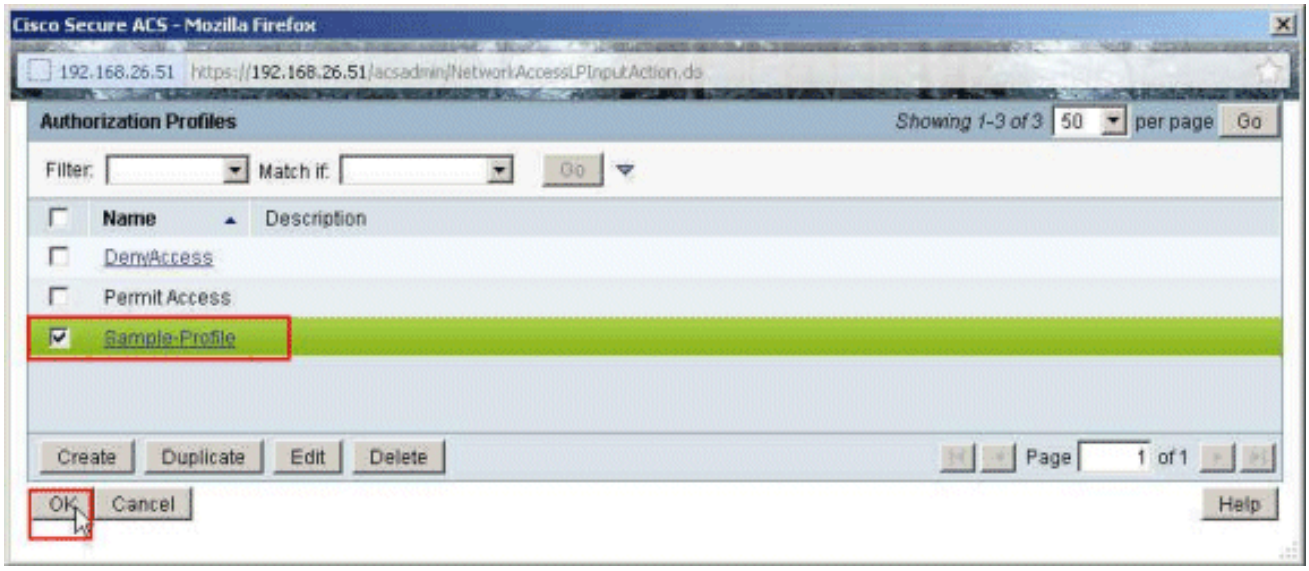
21. Submit(제출)을 클릭합니다

.



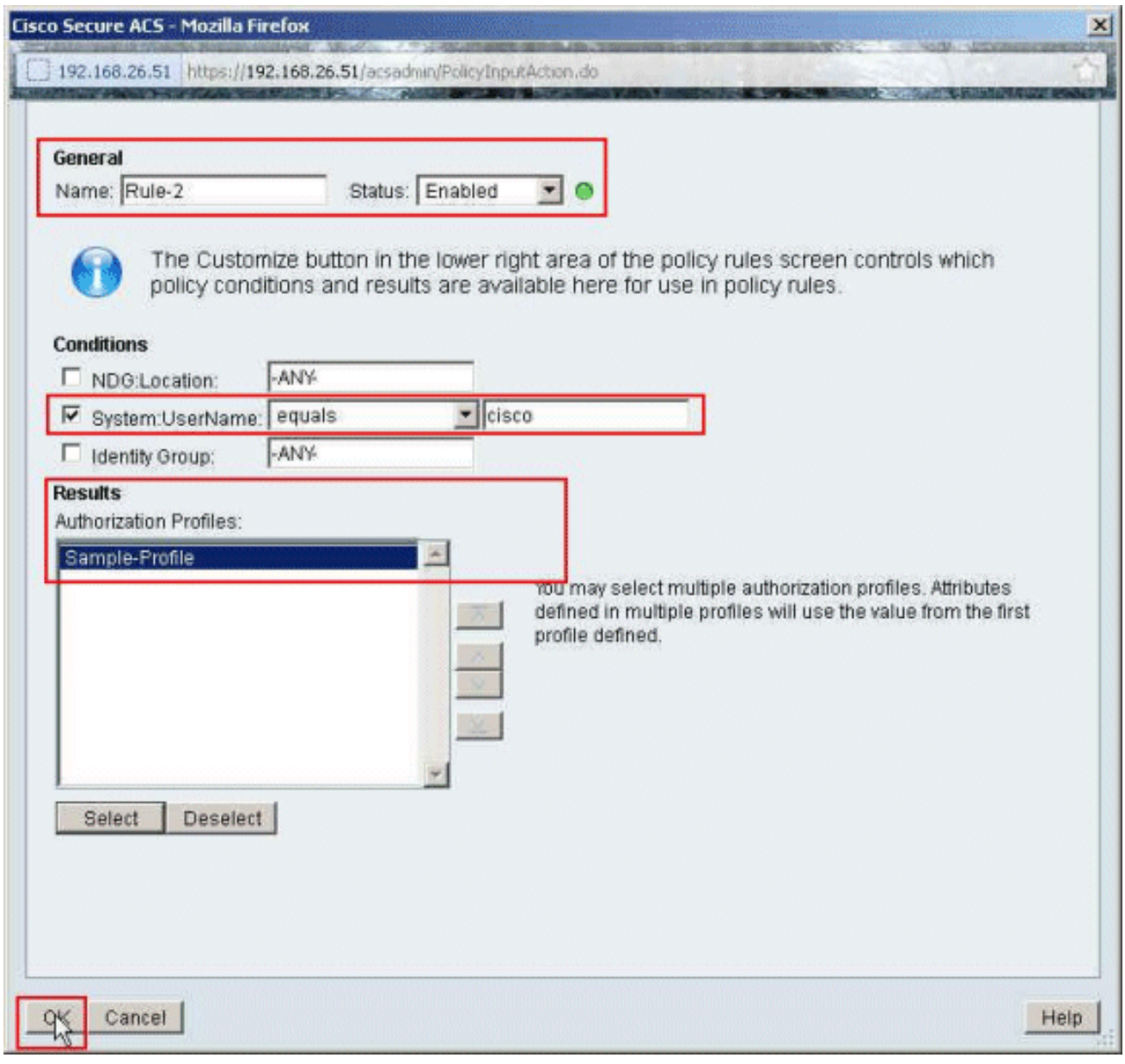
22. Sample-Profile(**Sample-Profile**(새로 생성된 Authorization Profile)) 옆의 확인란이 선택되었는지 확인하고 **OK**(확인)를 클릭합니다

.



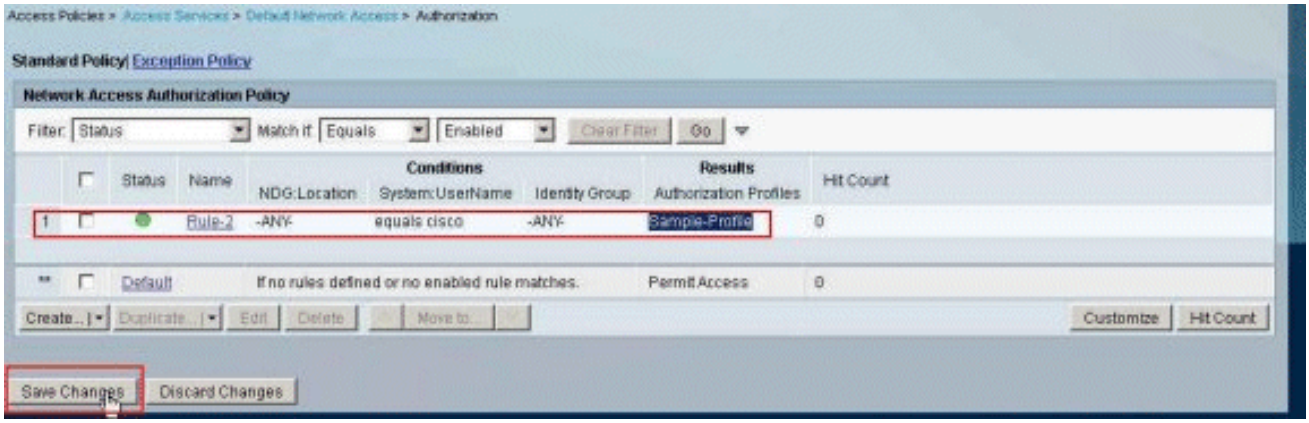
23. Authorization Profiles(권한 부여 프로파일) 필드에서 새로 생성된 **Sample-Profile**이 선택되었음을 확인했으면 **OK(확인)**를 클릭합니다

.



24. 새 규칙(**Rule-2**)이 System:UserName과 **cisco** 조건 및 **Sample-Profile**으로 생성되었는지 확인합니다.Save **Changes를 클릭합니다**.규칙 2가 생성되었습니다

.



그룹에 대해 다운로드 가능한 ACL을 위한 ACS 구성

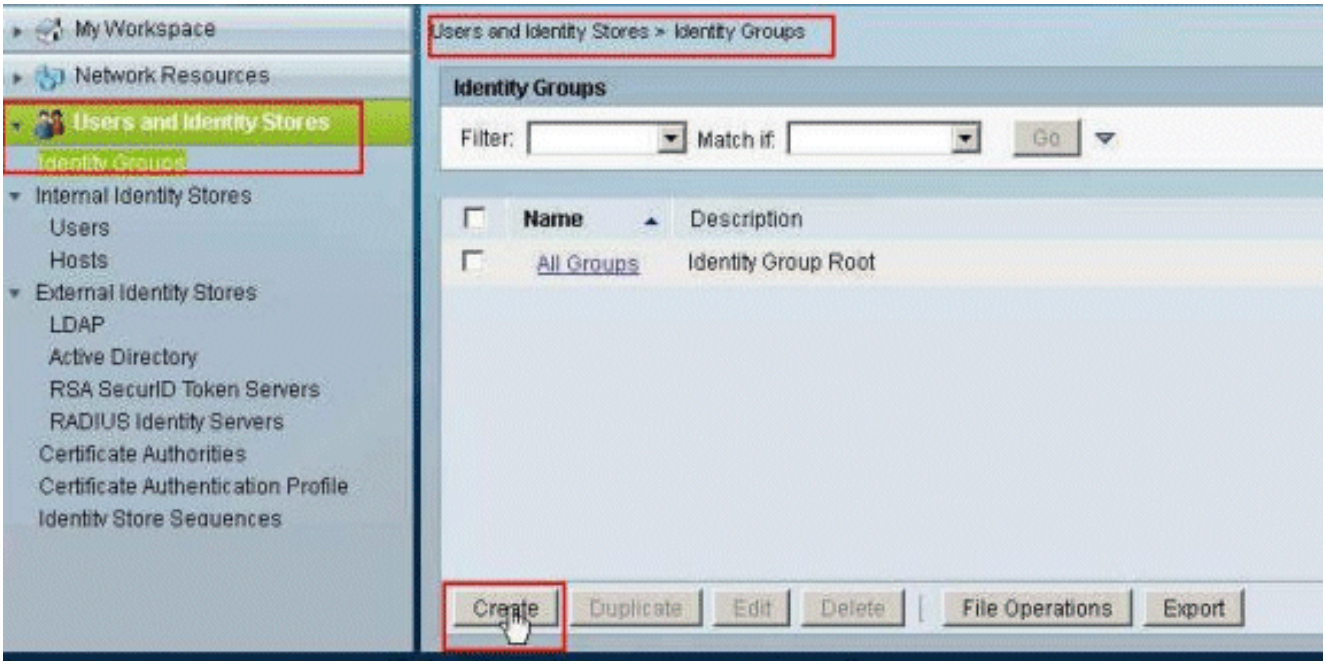
개별 사용자에 대해 다운로드 가능한 ACL을 위한 ACS 구성의 1~12단계를 완료하고 Cisco Secure ACS에서 그룹에 대해 다운로드 가능한 ACL을 구성하려면 다음 단계를 수행합니다.

이 예에서는 IPsec VPN 사용자 "cisco"가 **Sample-Group**에 **속합니다**.

Sample-Group 사용자 **cisco는** 성공적으로 인증하고 RADIUS 서버는 보안 어플라이언스에 다운로드 가능한 액세스 목록을 전송합니다."cisco" 사용자는 10.1.1.2 서버에만 액세스할 수 있으며 다른 모든 액세스를 거부합니다.ACL을 확인하려면 Downloadable ACL for User/Group 섹션을 참조하십시오.

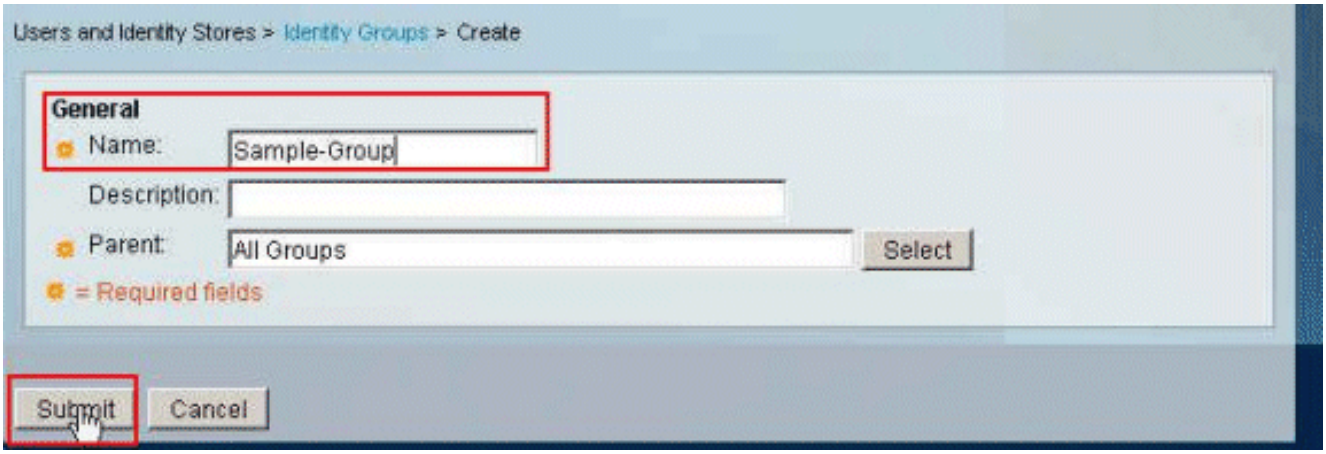
1. 탐색 모음에서 **Users and Identity Stores(사용자 및 ID 저장소) > Identity Groups(ID 그룹)**를 클릭하고 Create(생성)를 클릭하여 새 그룹을 생성합니다

.



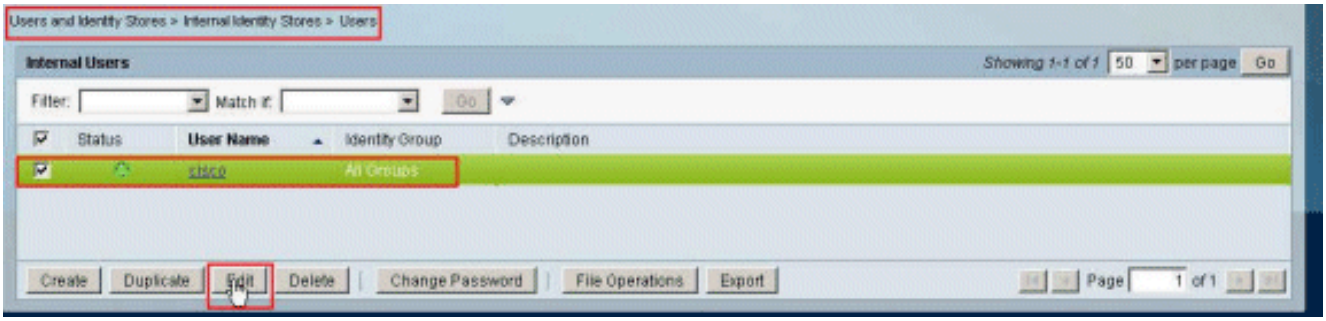
2. 그룹 이름(**Sample-Group**)을 입력하고 Submit(제출)을 **클릭합니다**

.



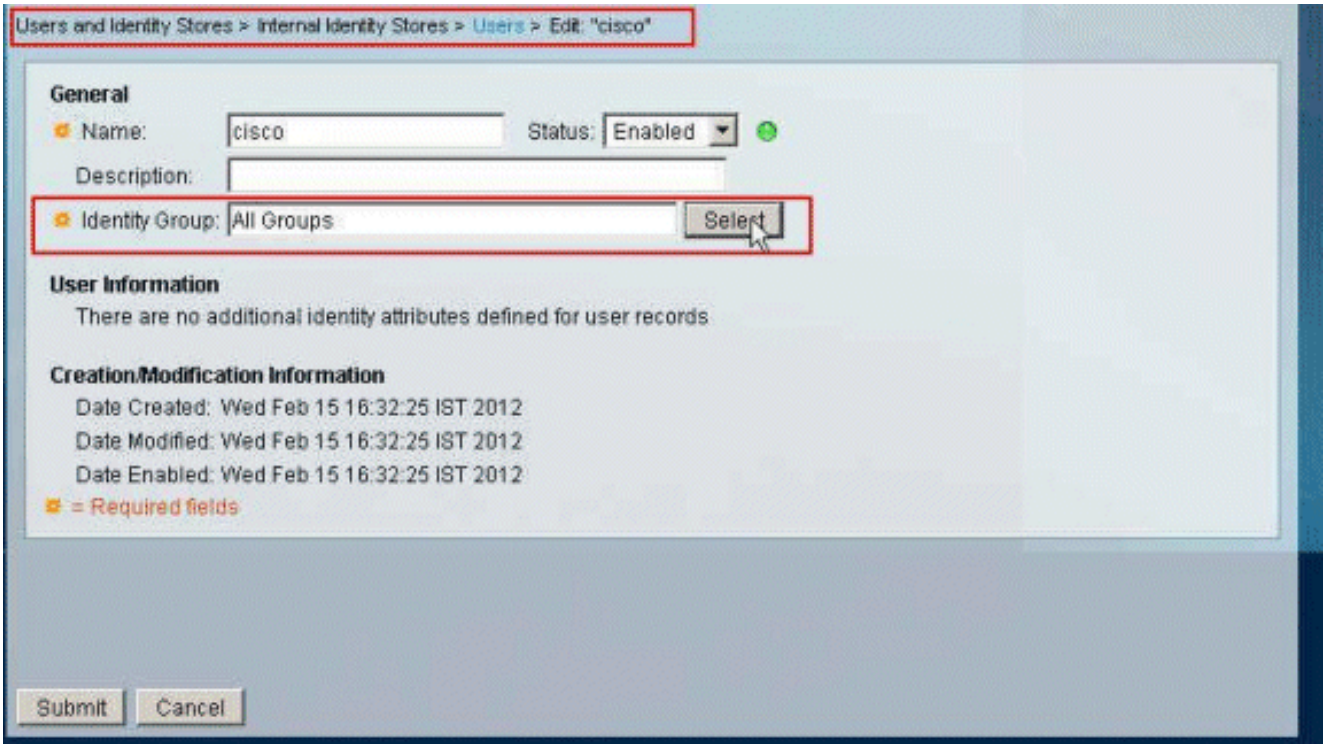
3. User **Identity Stores(사용자 ID 저장소) > Internal Identity Stores(내부 ID 저장소) > Users(사용자)를** 선택하고 **cisco** 사용자를 선택합니다.이 사용자의 그룹 구성원 자격을 변경하려면 Edit를 클릭합니다

.



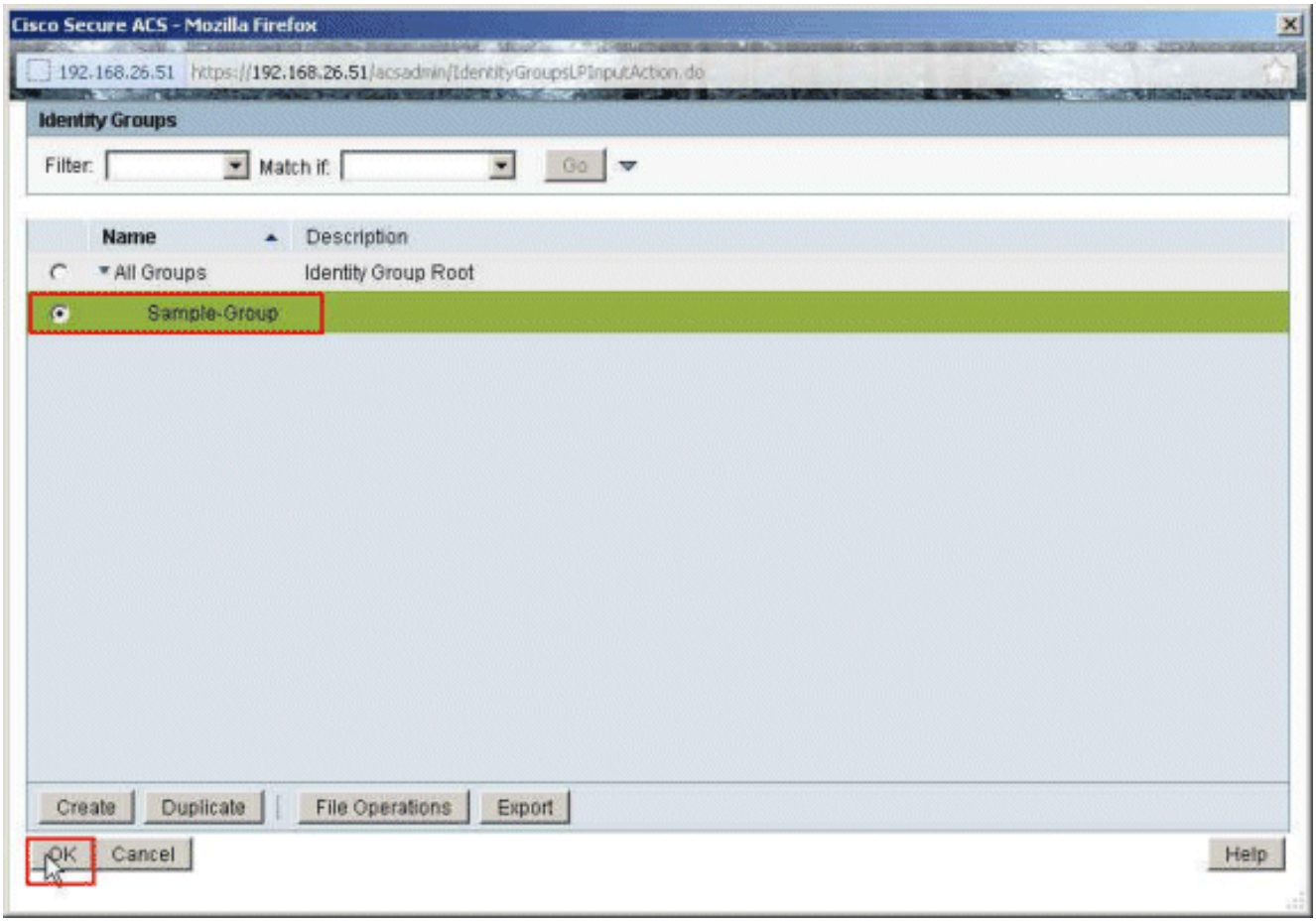
4. ID 그룹 옆에 있는 선택을 클릭합니다

.

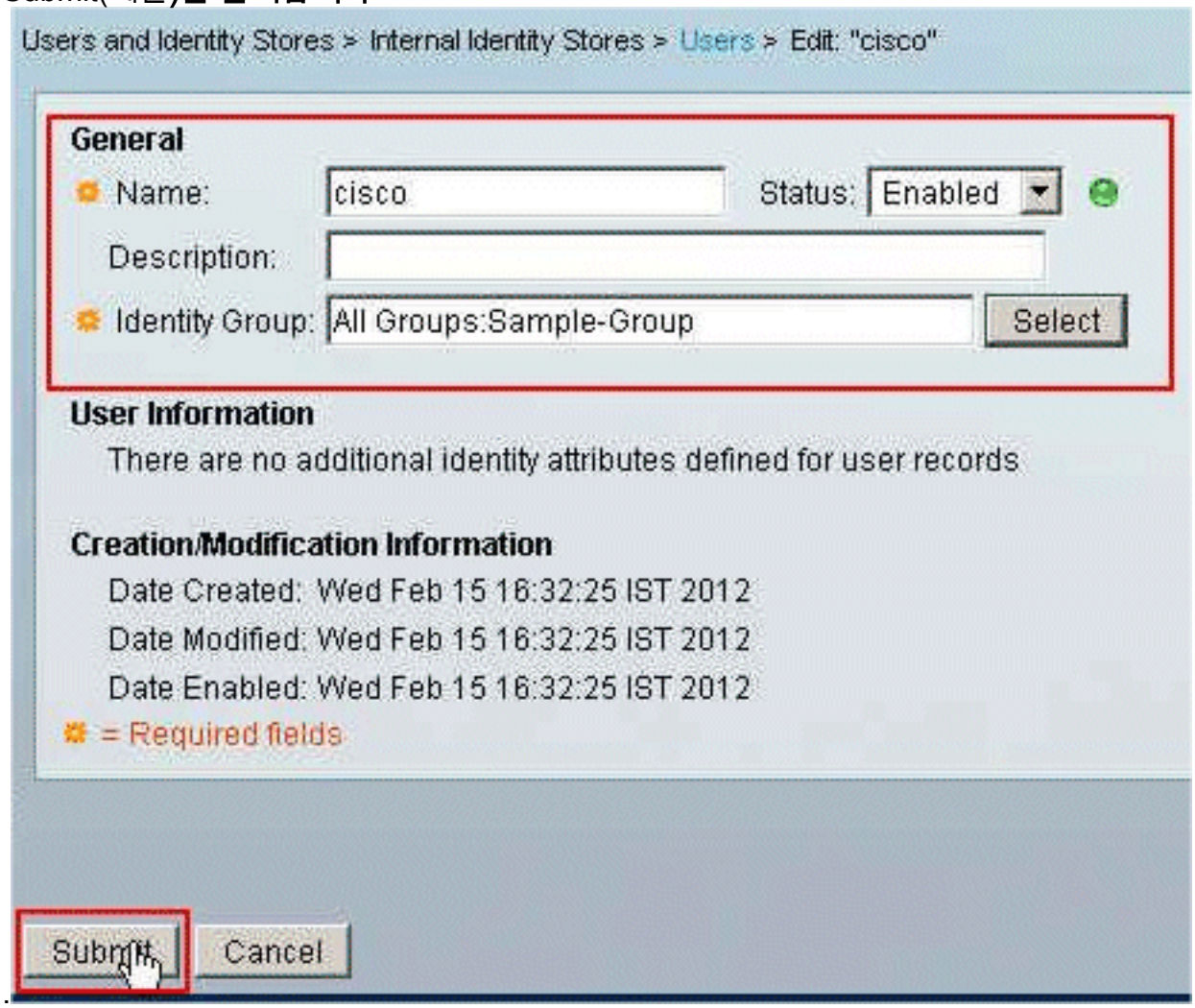


5. 새로 생성된 그룹(예: **Sample-Group**)을 선택하고 **OK**를 클릭합니다

.



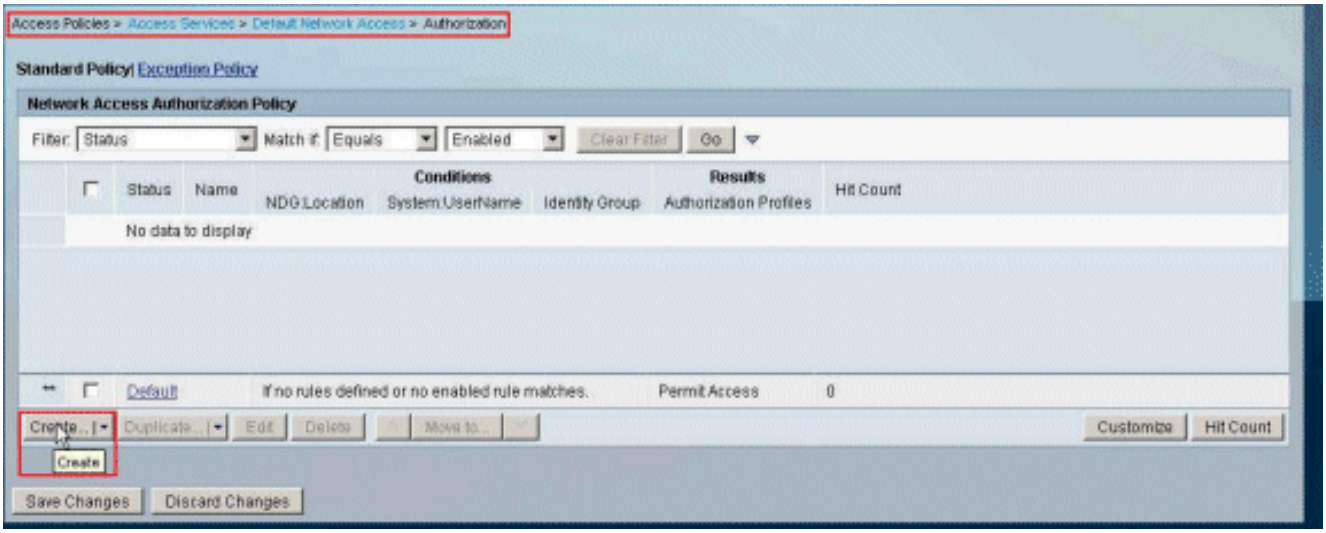
6. Submit(제출)을 클릭합니다



7. Access **Policies(액세스 정책)** > **Access Services(액세스 서비스)** > **Default Network**

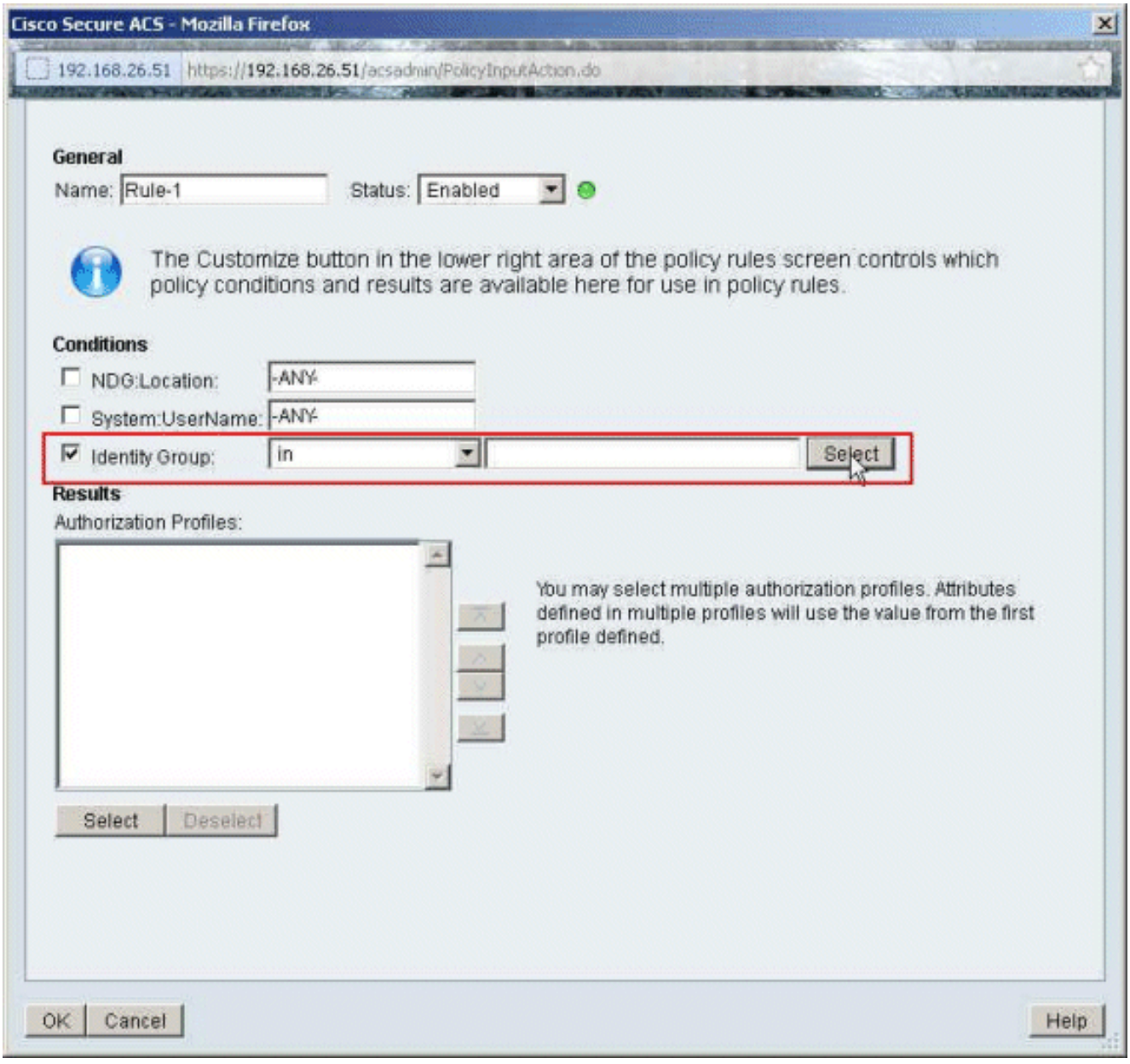
Access(기본 네트워크 액세스) > Authorization(권한 부여)을 선택하고 **Create(생성)를 클릭하여 새 규칙을 생성합니다**

.



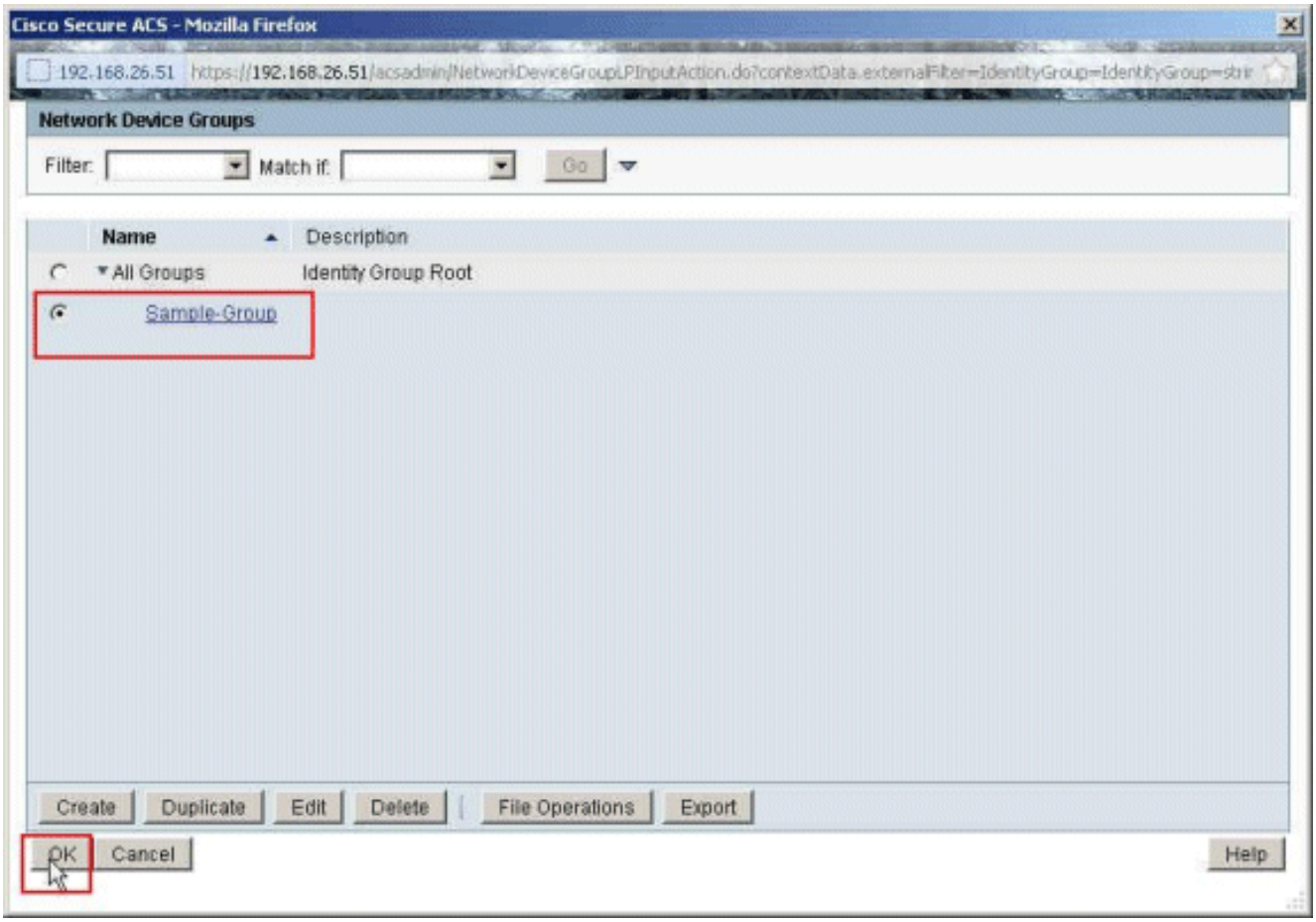
8. **Identity Group** 옆에 있는 확인란이 선택되었는지 확인하고 **선택**을 클릭합니다

.



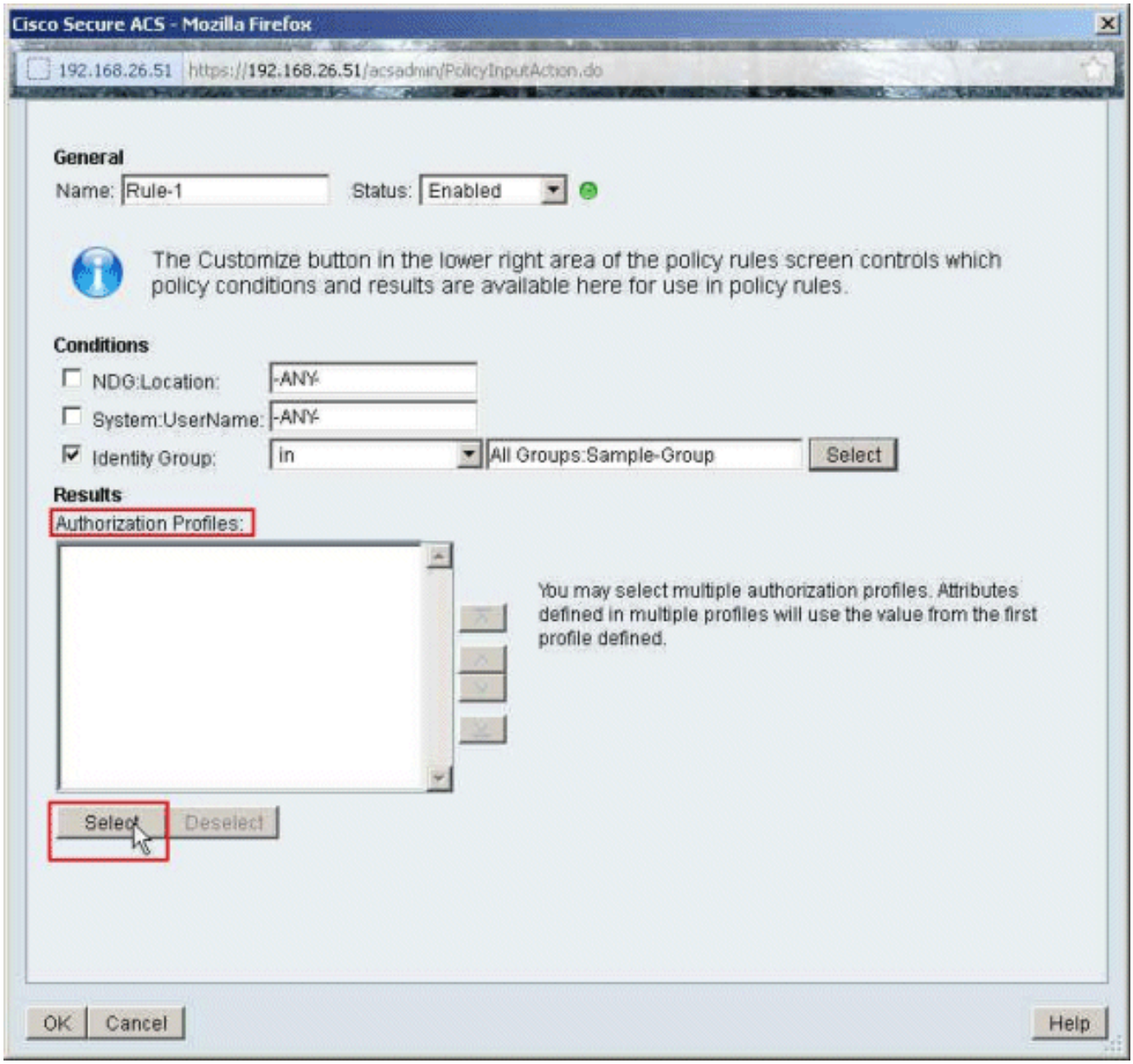
9. Sample-**Group을** 선택하고 **OK를** 클릭합니다

.

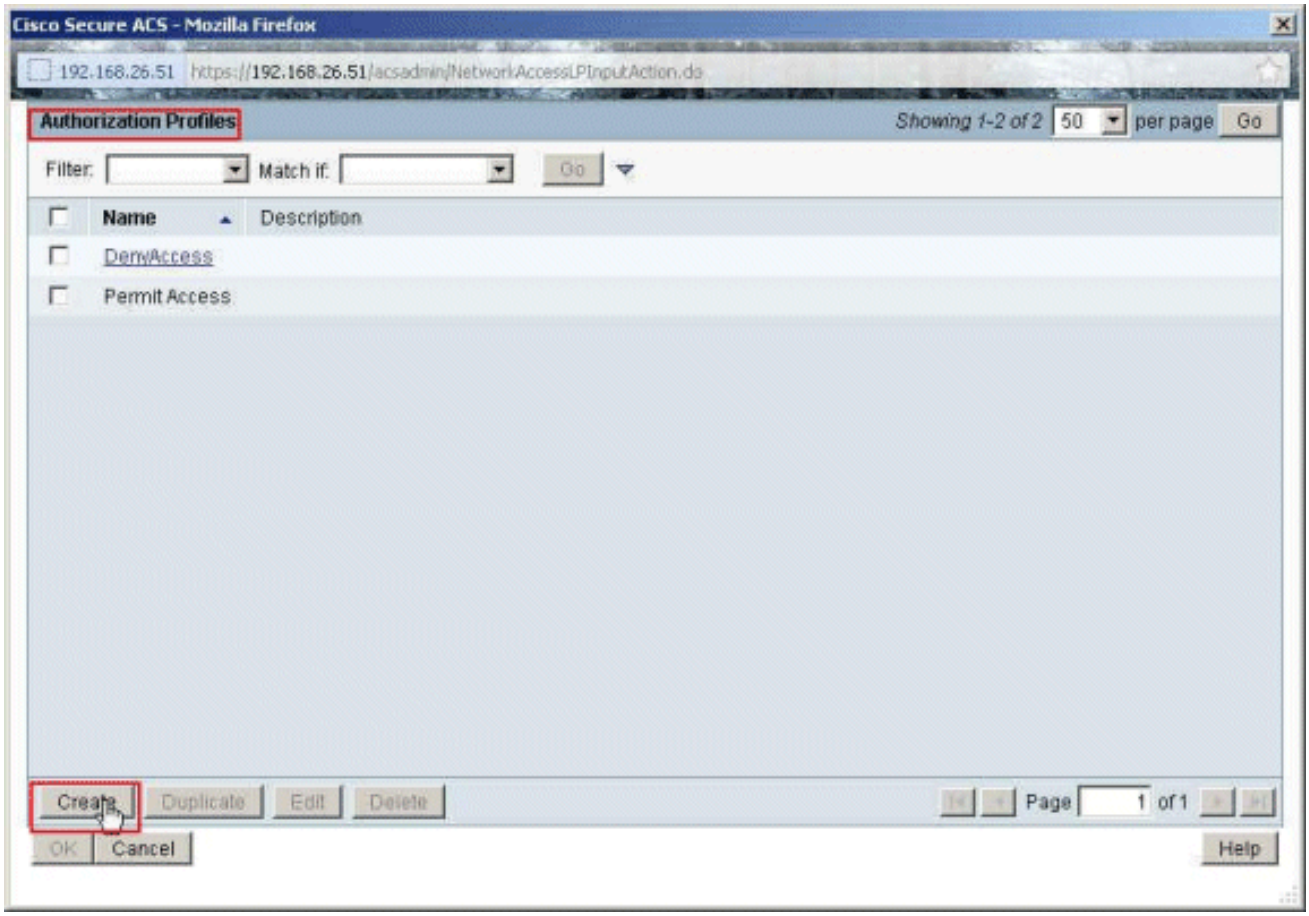


10. Authorization **Profiles** 섹션에서 Select(선택)를 클릭합니다

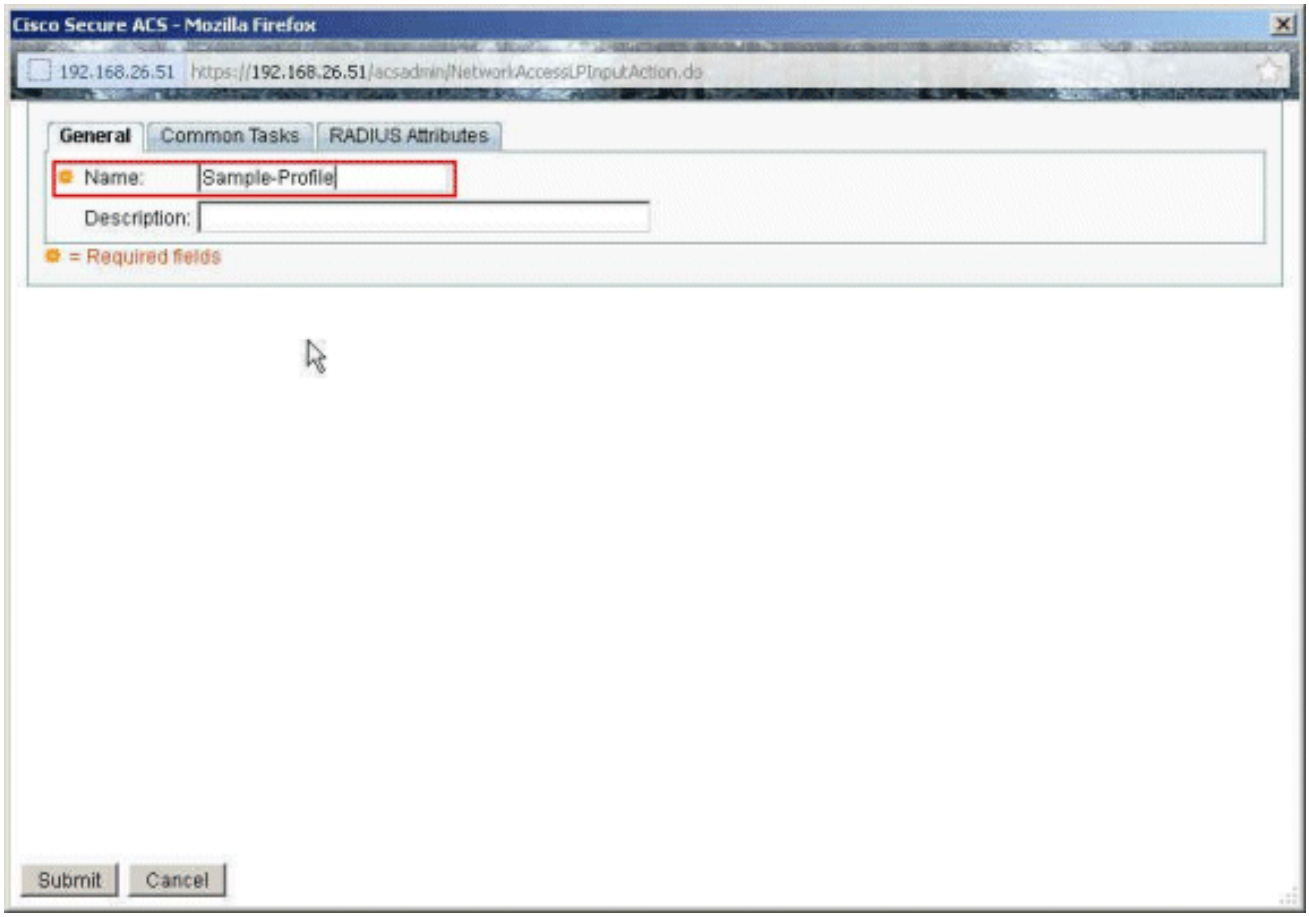
.



11. 새 권한 부여 프로파일을 생성하려면 Create를 클릭합니다
.

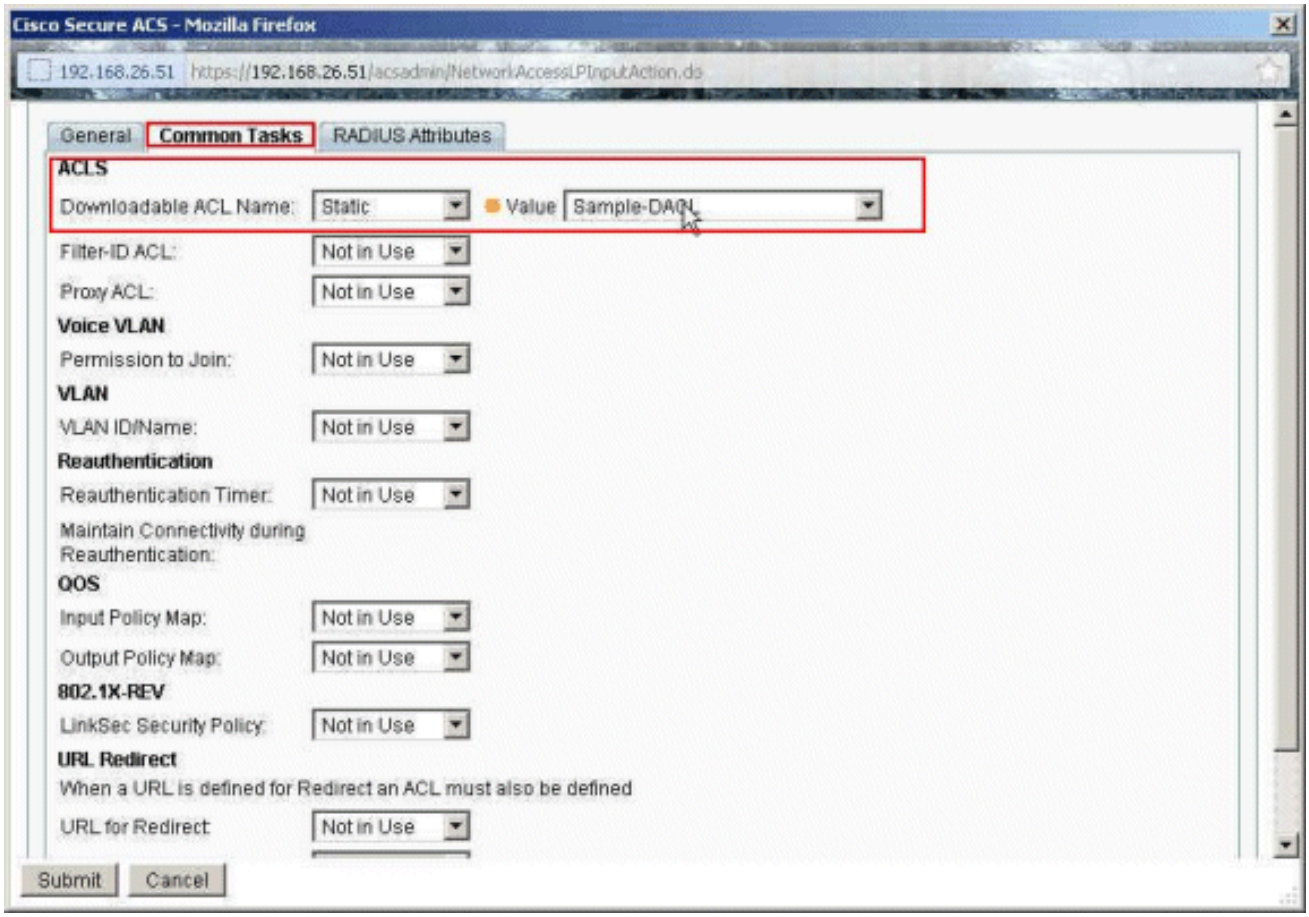


12. 권한 부여 **프로파일**의 이름을 **입력합니다**.**Sample-Profile**은 이 예에서 사용되는 이름입니다
.



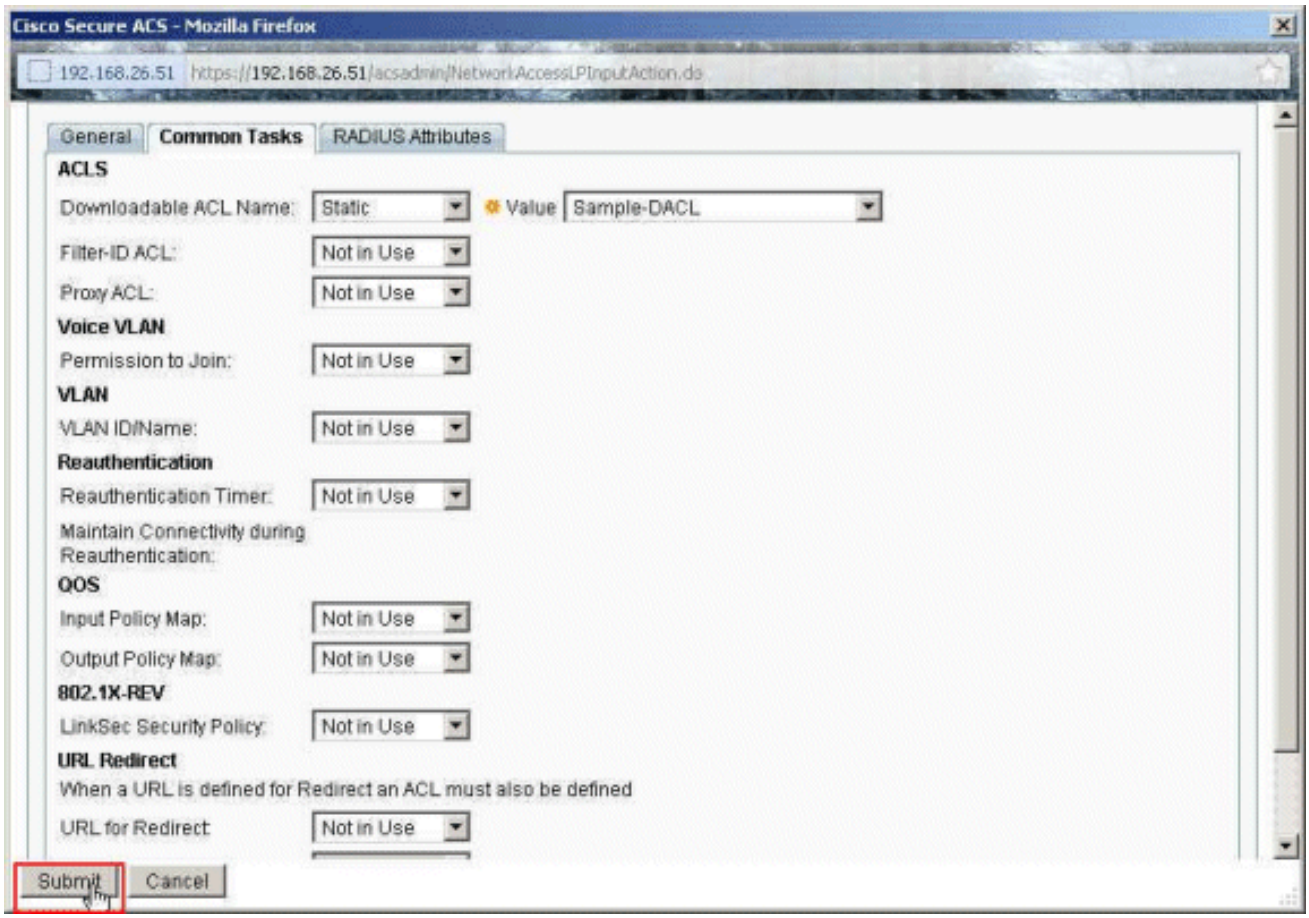
13. Common Tasks(**일반 작업**) 탭을 선택하고 **Downloadable ACL Name(다운로드 가능한 ACL 이름)**의 드롭다운 목록에서 Static(정적)을 **선택합니다**.Value 드롭다운 목록에서 새로 생성된 **DACL(Sample -DACL)**을 선택합니다

.



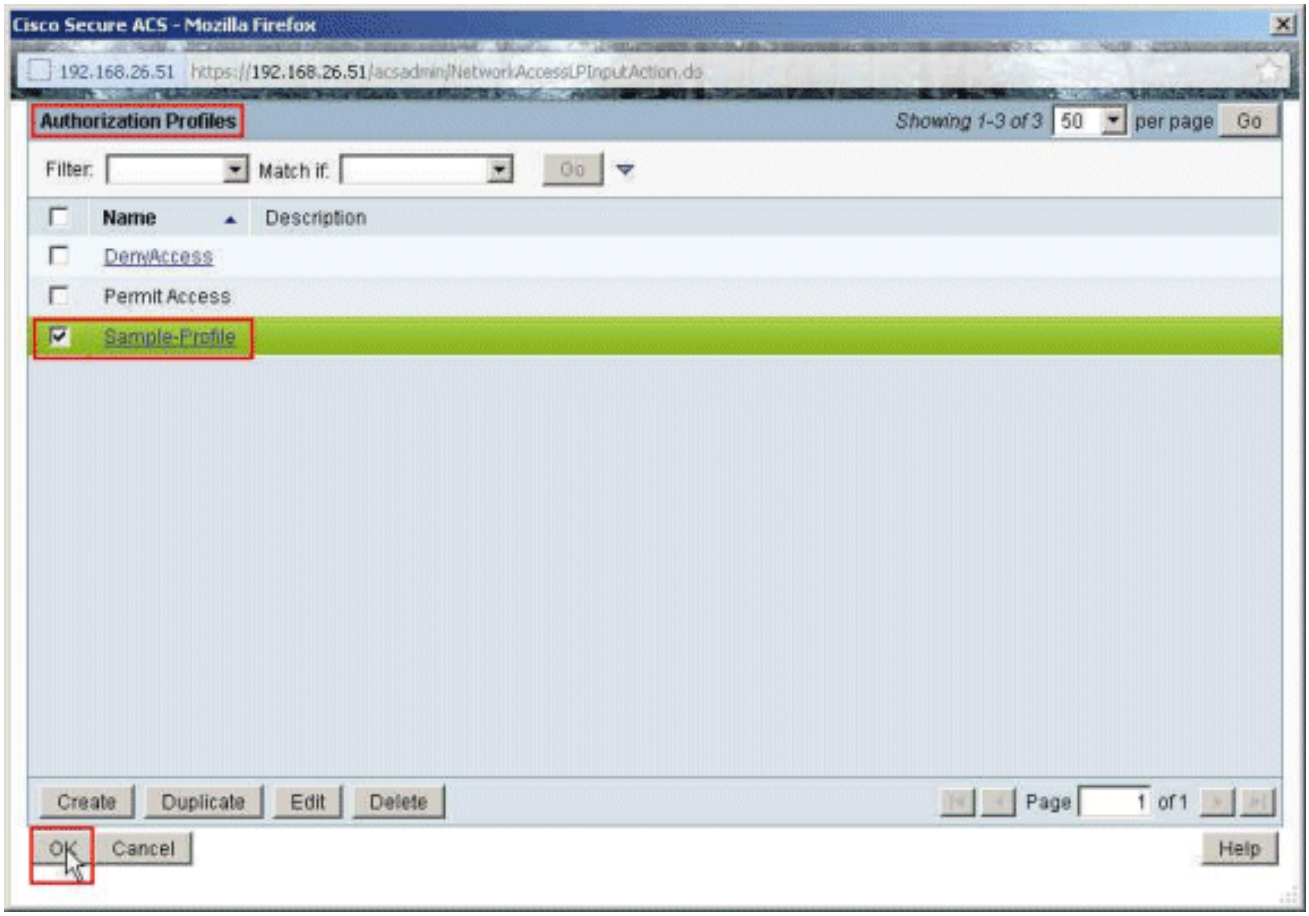
14. Submit(제출)을 클릭합니다

.



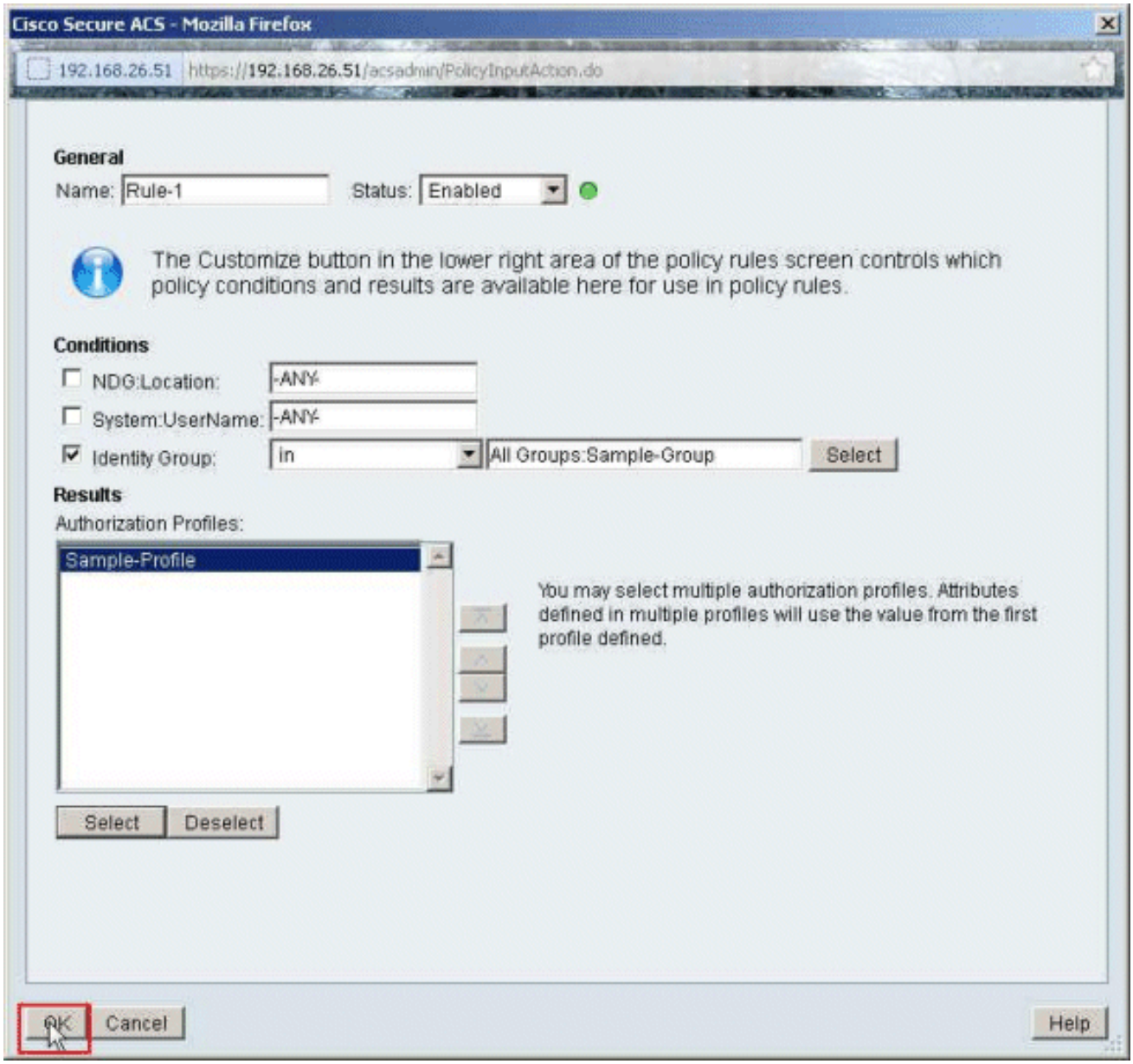
15. 앞서 생성한 Authorization Profile **Sample-Profile**을 선택하고 **OK**를 클릭합니다

.


Cisco Secure ACS - Mozilla Firefox
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do
Authorization Profiles
Showing 1-3 of 3 50 per page Go
Filter: Match if: Go
Name Description
DenyAccess
Permit Access
Sample-Profile
Create Duplicate Edit Delete
Page 1 of 1
OK Cancel
Help

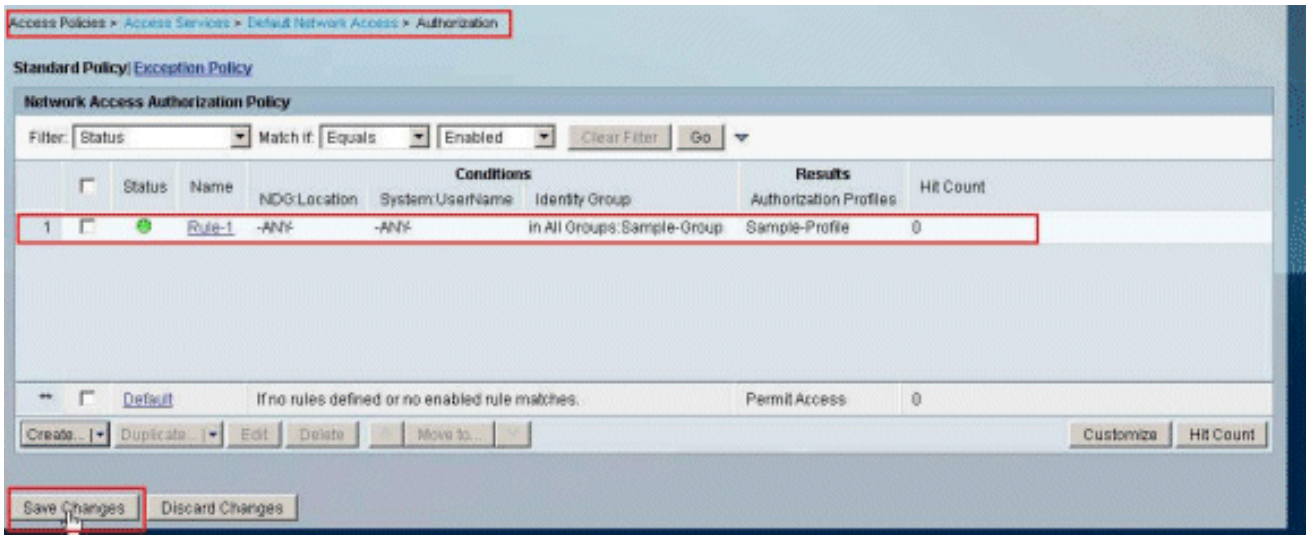
16. **확인을 클릭합니다**

.



17. ID 그룹 **샘플 그룹**을 조건으로 하고 **Sample-Profile**을 Result로 사용하여 **Rule-1**이 생성되었는지 확인합니다.Save **Changes를 클릭합니다**

.



네트워크 장치 그룹에 대해 다운로드 가능한 ACL에 대한 ACS 구성

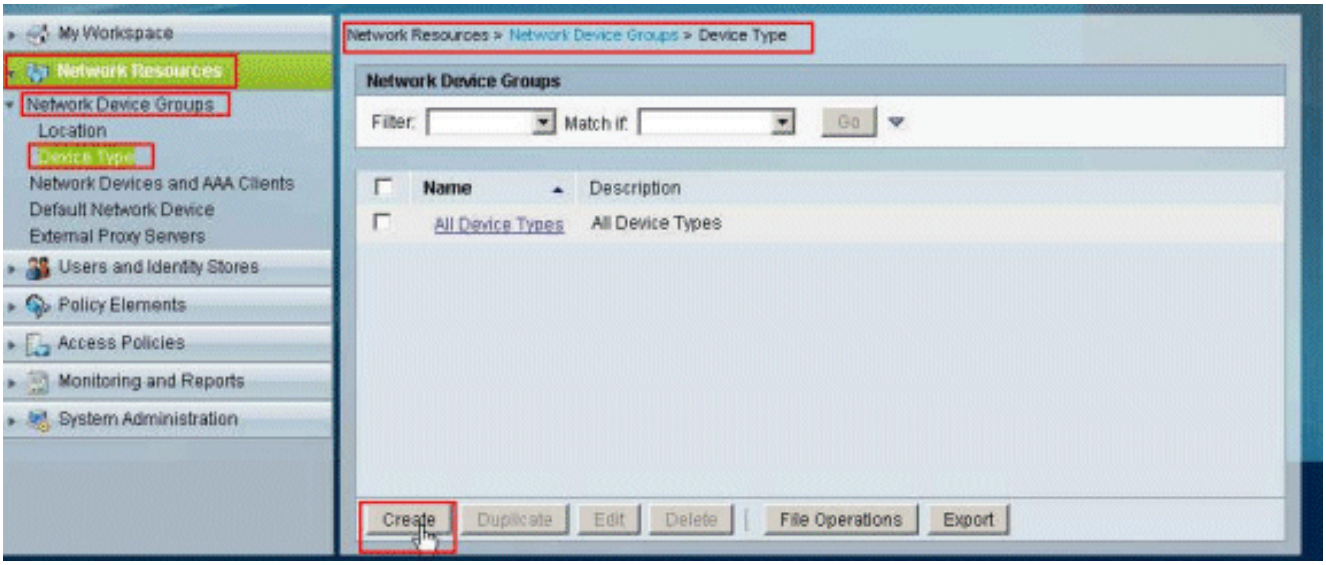
Configure ACS for Downloadable ACL for Individual User(개별 사용자에 대해 다운로드 가능한

ACL을 위한 ACS 구성)의 1~12단계를 완료하고 Cisco Secure ACS에서 네트워크 장치 그룹에 대해 다운로드 가능한 ACL을 구성하려면 다음 단계를 수행합니다.

이 예에서 ASA(RADIUS Client)는 네트워크 디바이스 그룹 **VPN-Gateways**에 속합니다.사용자 "cisco"에 대해 ASA에서 오는 VPN 인증 요청이 성공적으로 인증되고 RADIUS 서버가 다운로드 가능한 액세스 목록을 보안 어플라이언스에 전송합니다."cisco" 사용자는 10.1.1.2 서버에만 액세스할 수 있으며 다른 모든 액세스를 거부합니다.ACL을 확인하려면 Downloadable ACL for User/Group 섹션을 참조하십시오.

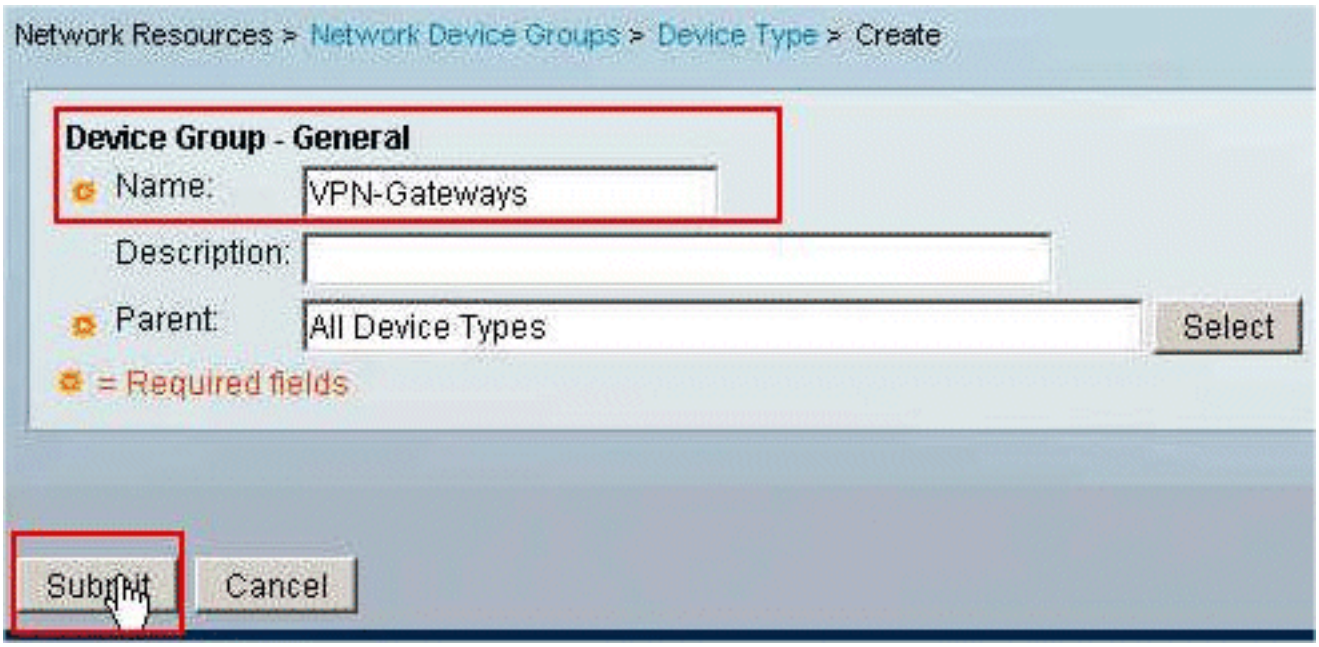
1. Network Resources(**네트워크 리소스**) > **Network Device Groups(네트워크 디바이스 그룹)** > Device Type(**디바이스 유형)을** 선택하고 **Create(생성)를** 클릭하여 새 네트워크 디바이스 그룹을 생성합니다

.



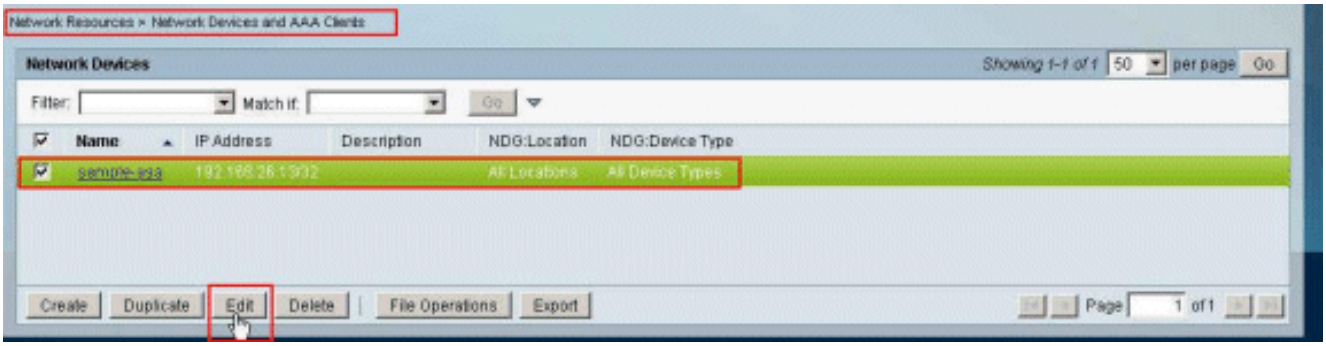
2. 네트워크 **장치 그룹** 이름(**VPN-Gateways**의 경우)을 입력하고 Submit(제출)을 **클릭합니다**

.



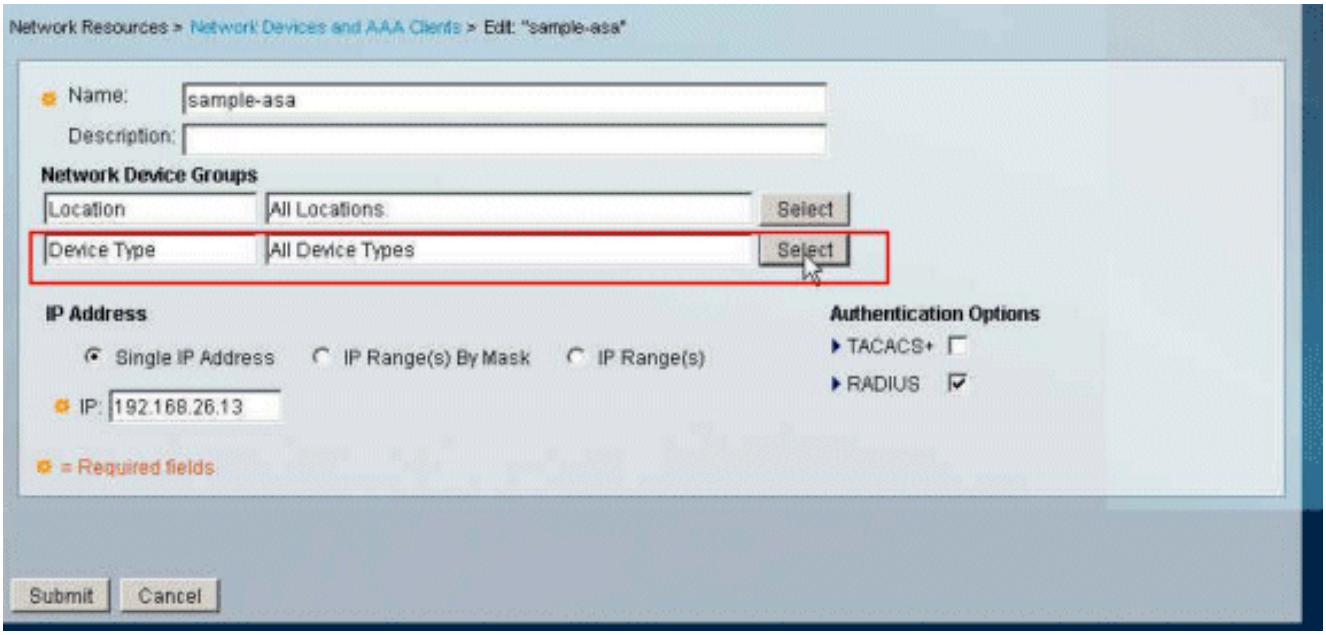
3. Network **Resources(네트워크 리소스)** > **Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)**를 선택하고 앞서 생성한 **RADIUS** Client **sample-asa를** 선택합니다 .Edit(**편집**)를 클릭하여 이 RADIUS 클라이언트(asa)의 **Network Device Group** 멤버십을 변경합니다

.



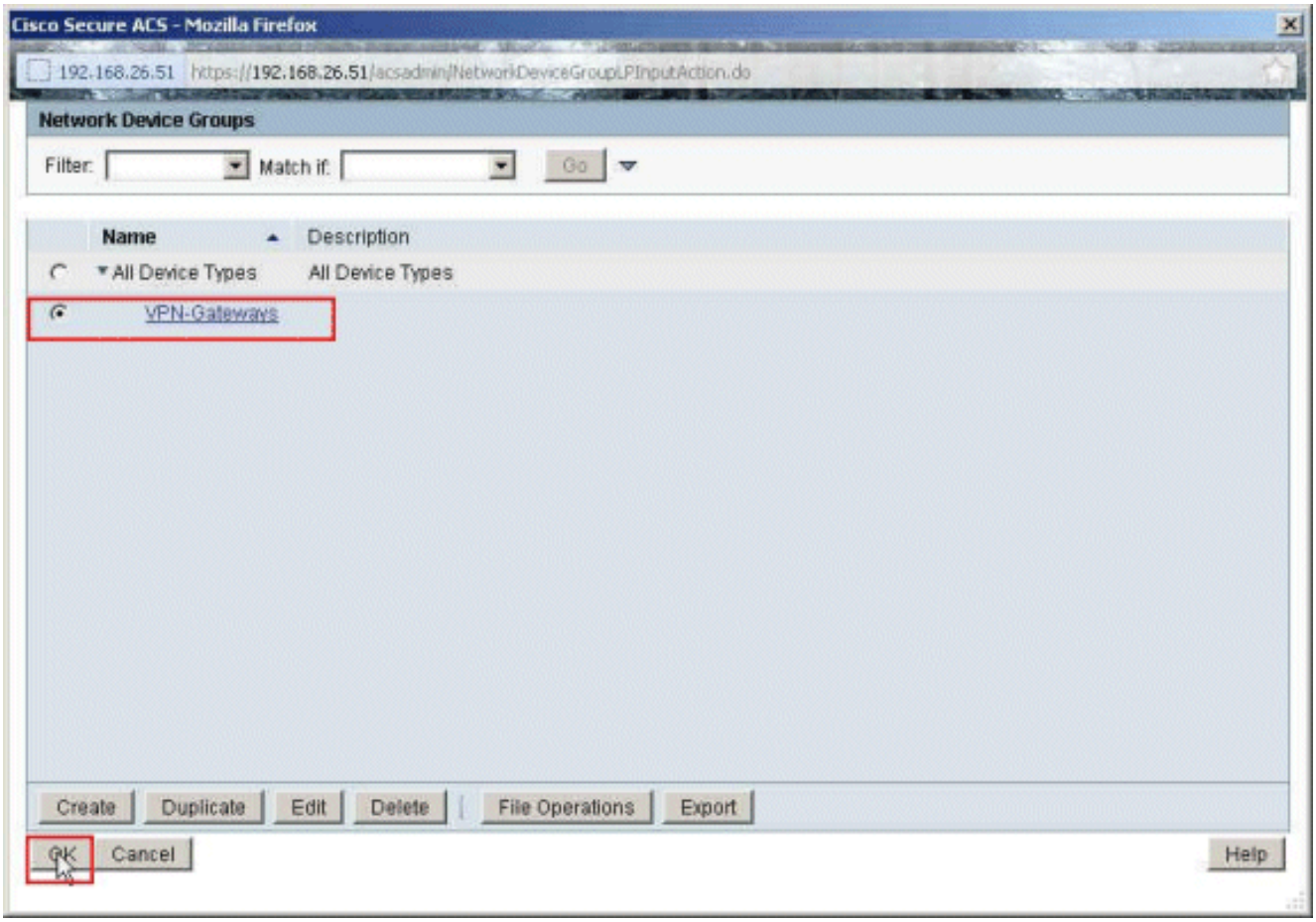
4. Device Type 옆에 있는 Select를 클릭합니다

.



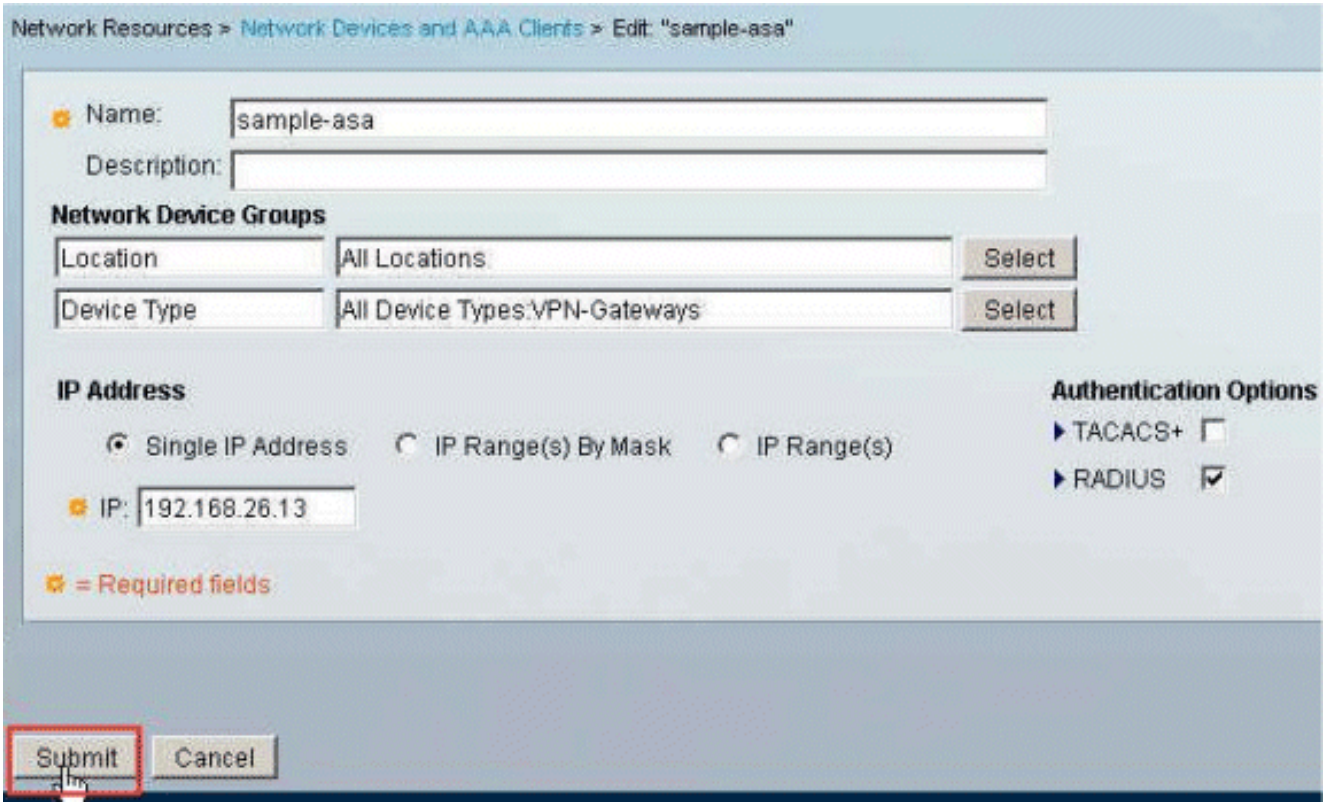
5. 새로 생성된 네트워크 디바이스 그룹(**VPN-Gateways**)을 선택하고 **OK**(확인)를 클릭합니다

.



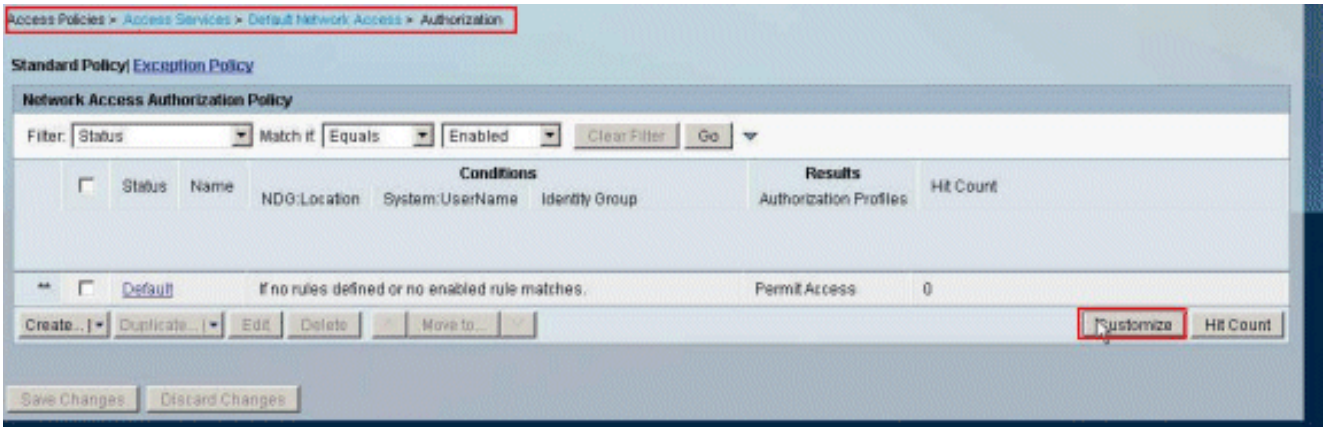
6. Submit(제출)을 클릭합니다

.



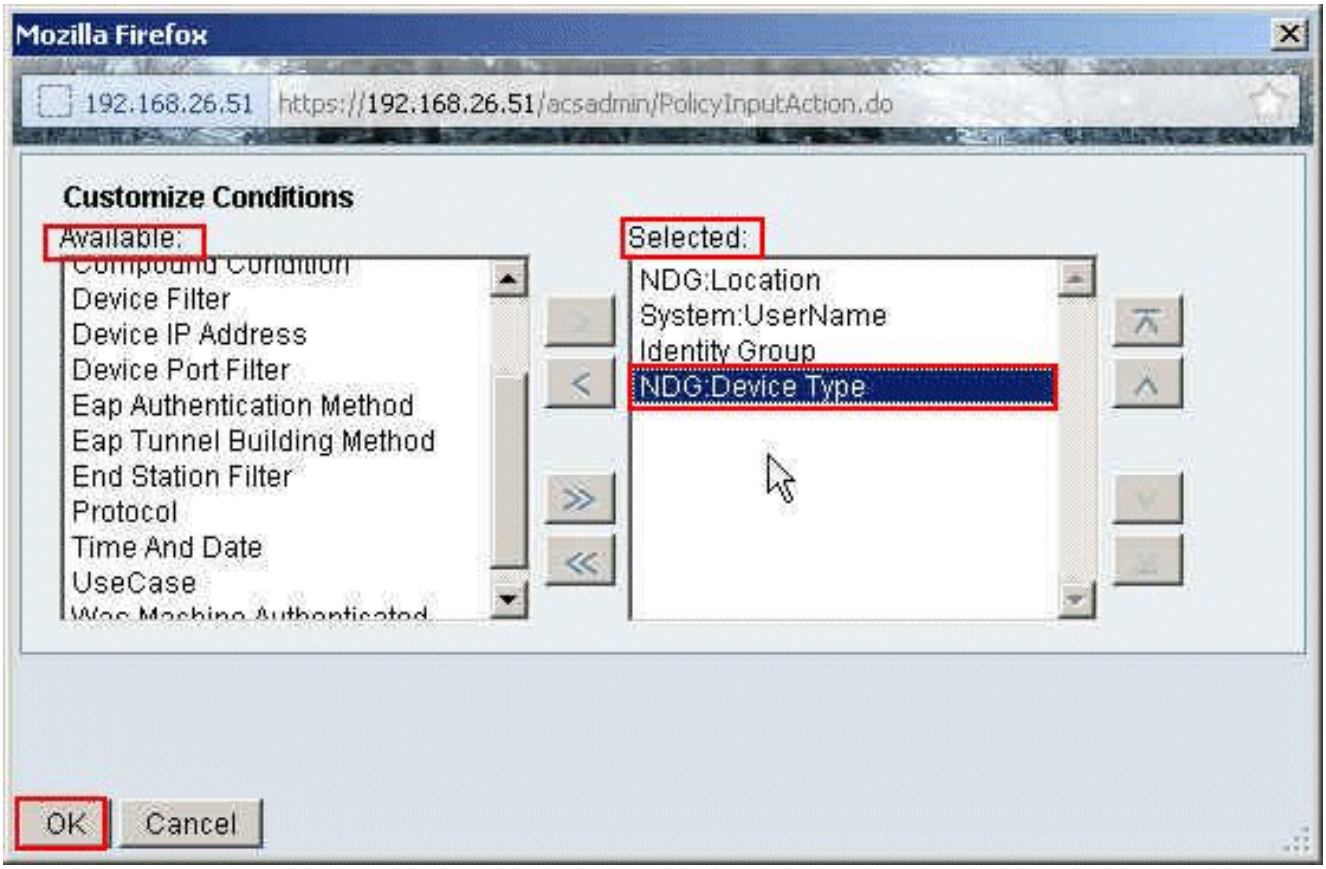
7. Access **Policies(액세스 정책)** > **Access Services(액세스 서비스)** > Default Network Access(**기본 네트워크 액세스**) > Authorization(권한 부여)을 선택하고 Customize(사용자 지정)를 **클릭합니다**

.



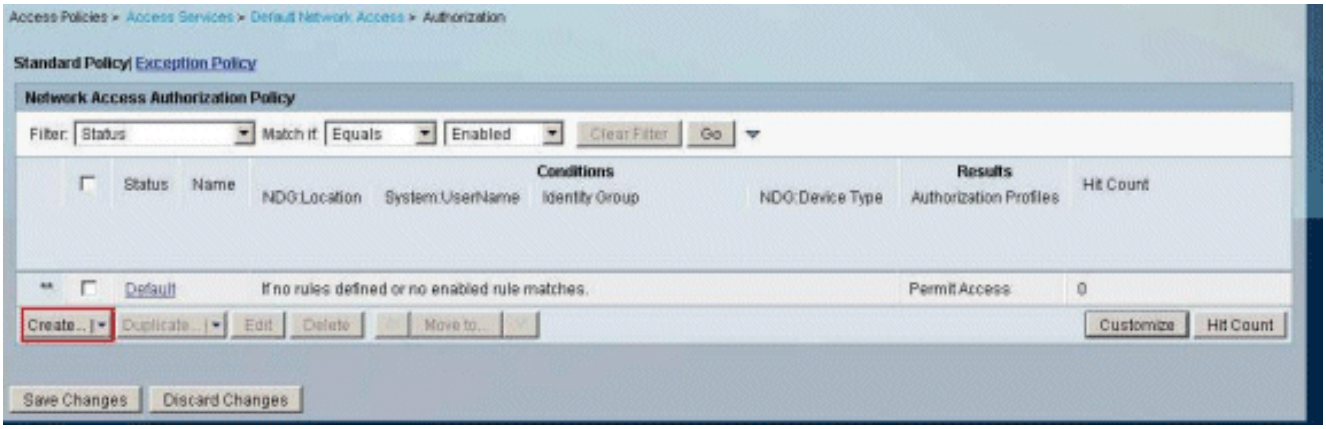
8. NDG:**Device Type(NDG:디바이스 유형)**을 **Available** 섹션에서 **Selected(선택됨)** 섹션으로 이동하고 **OK(확인)를 클릭합니다**

.



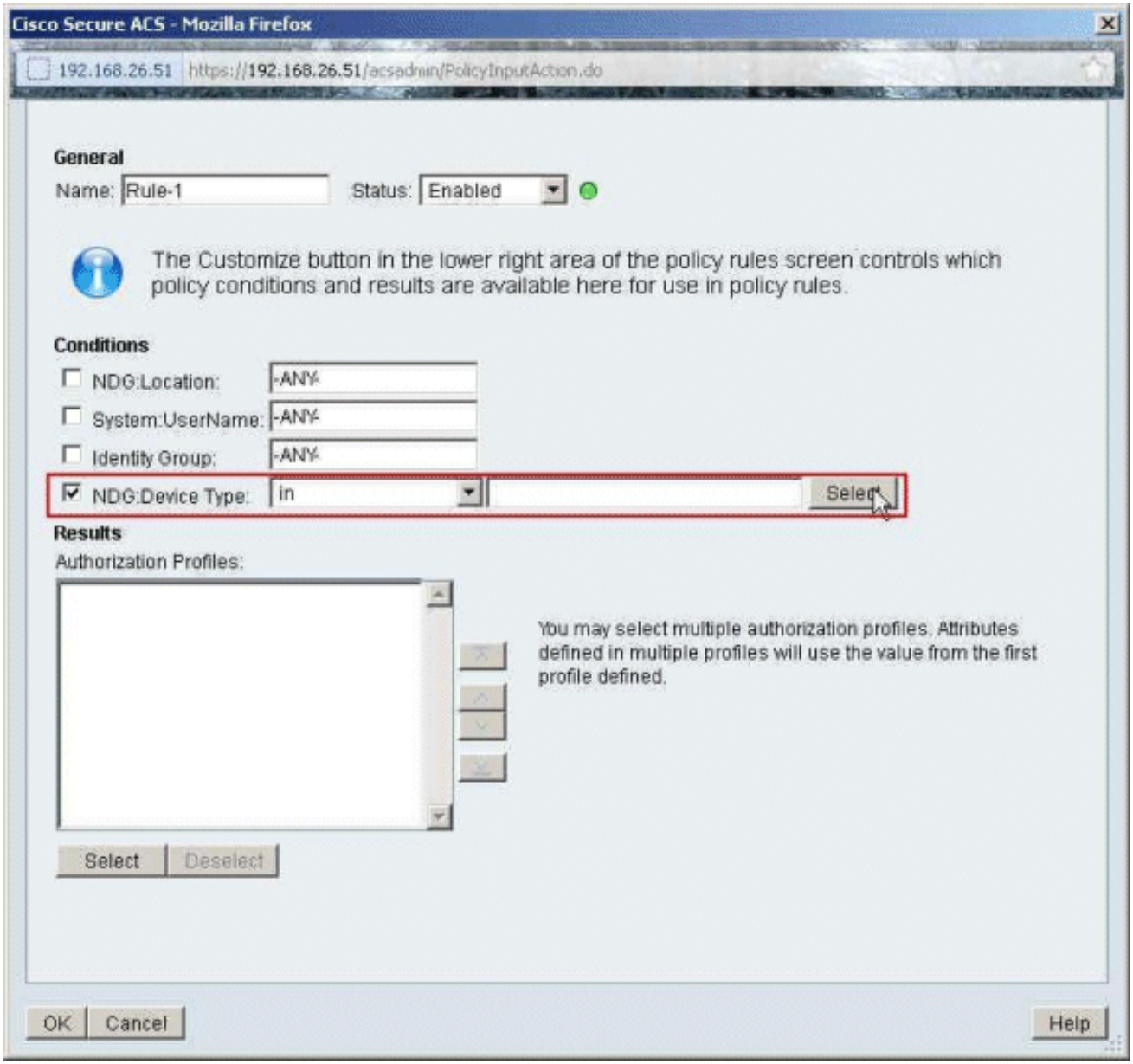
9. 새 규칙을 생성하려면 Create를 클릭합니다

.



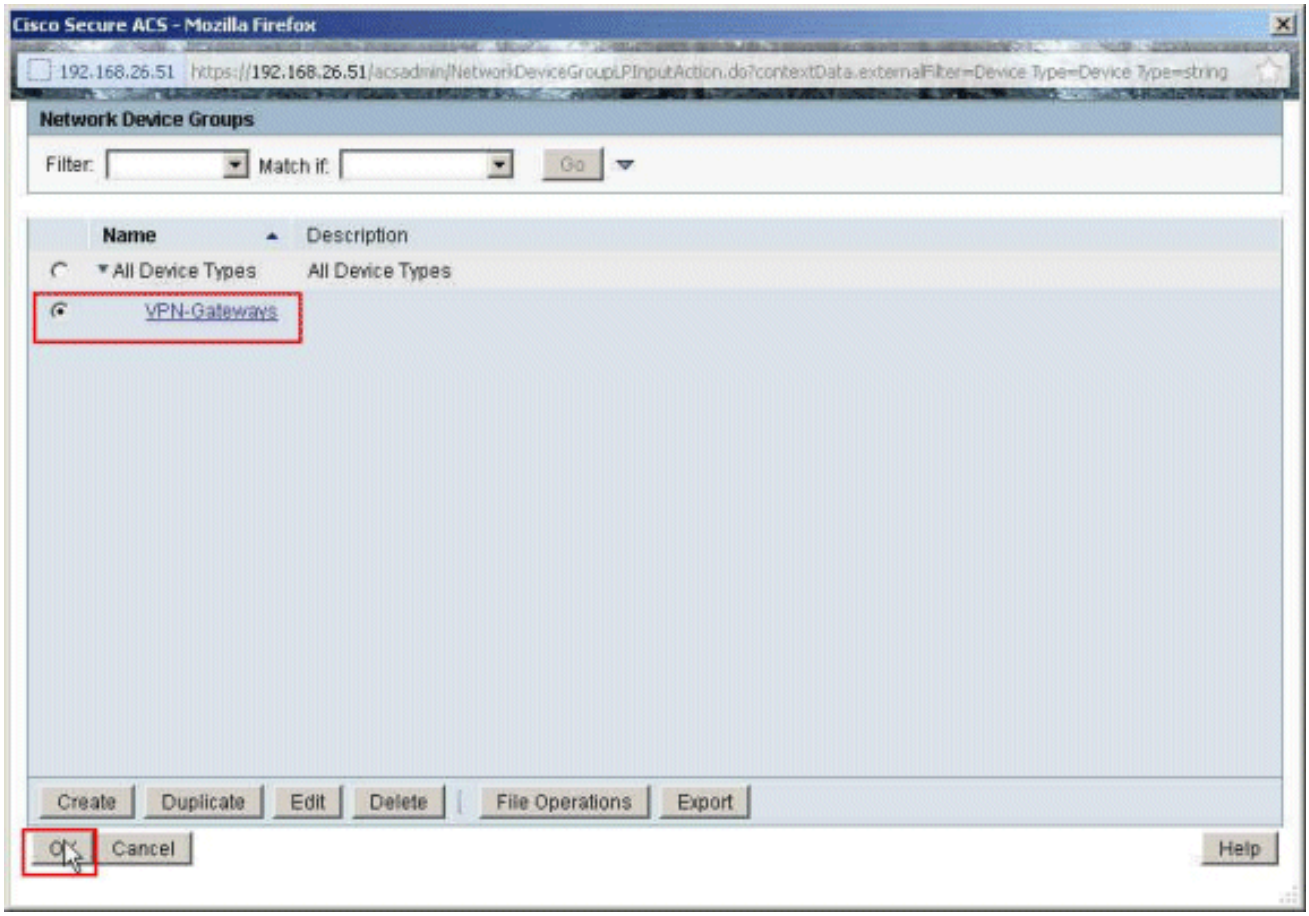
10. NDG:Device **Type**(NDG:**디바이스 유형**) 옆의 확인란이 선택되었는지 확인하고 드롭다운 목록에서 **in(인)**을 선택합니다.선택을 **클릭합니다**

.



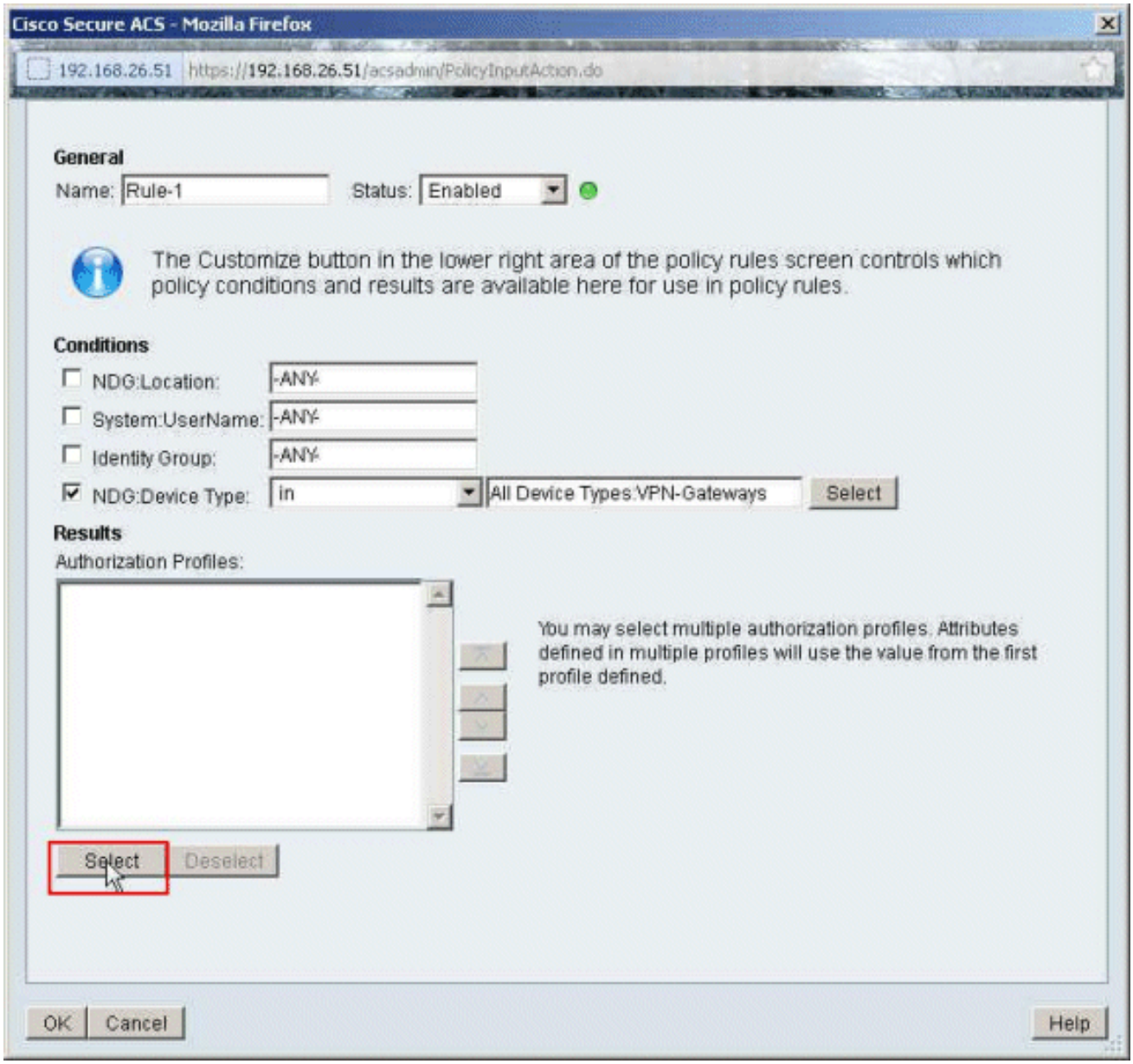
11. 앞서 생성한 네트워크 디바이스 그룹 **VPN-Gateway**를 선택하고 **OK**(확인)를 클릭합니다

.

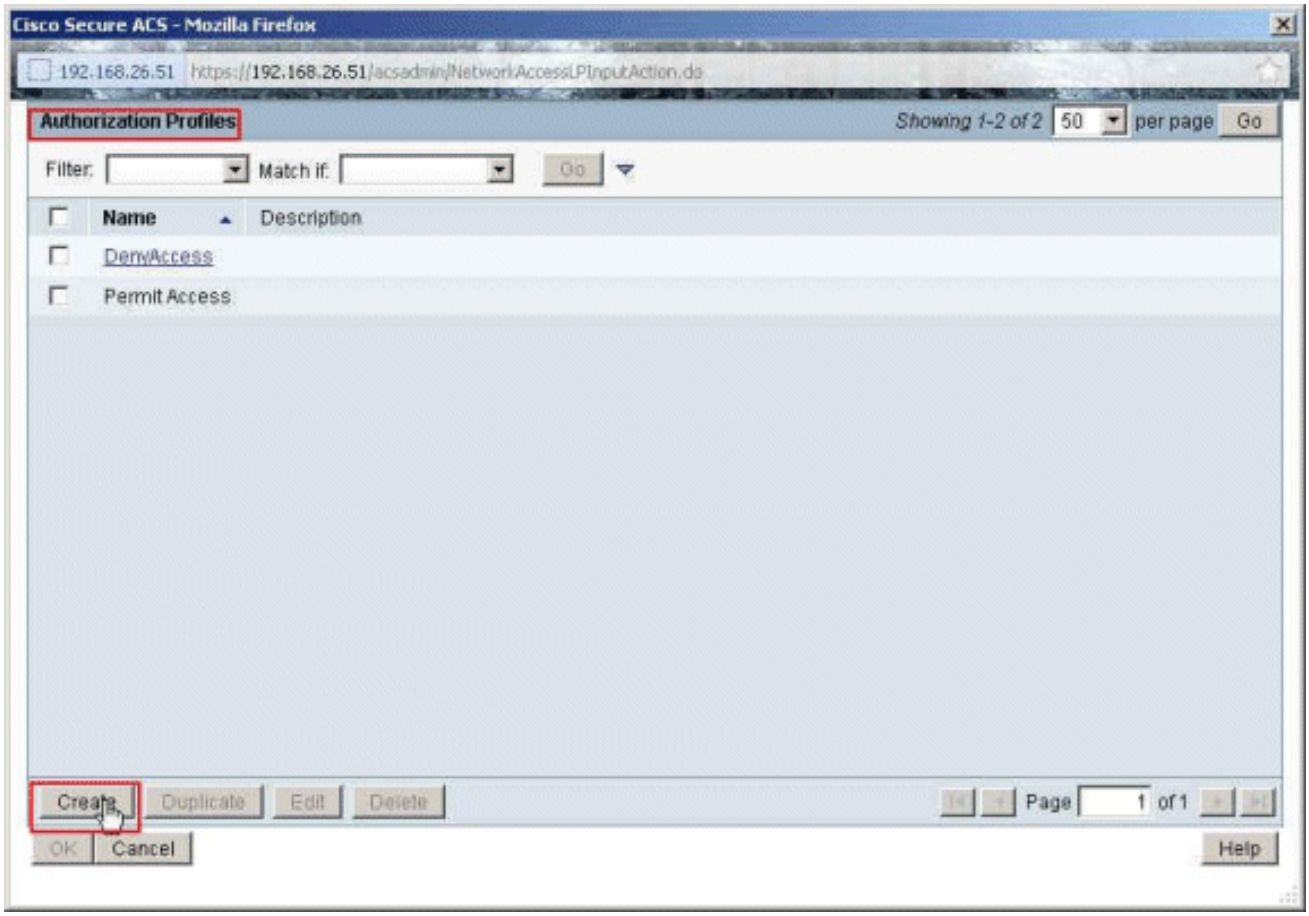

Cisco Secure ACS - Mozilla Firefox
192.168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do?contextData.externalFilter=Device Type=Device Type=string
Network Device Groups
Filter:
Match if:
Go
Name
Description
All Device Types
All Device Types
VPN-Gateways
Create
Duplicate
Edit
Delete
File Operations
Export
OK
Cancel
Help

12. 선택을 **클릭합니다**

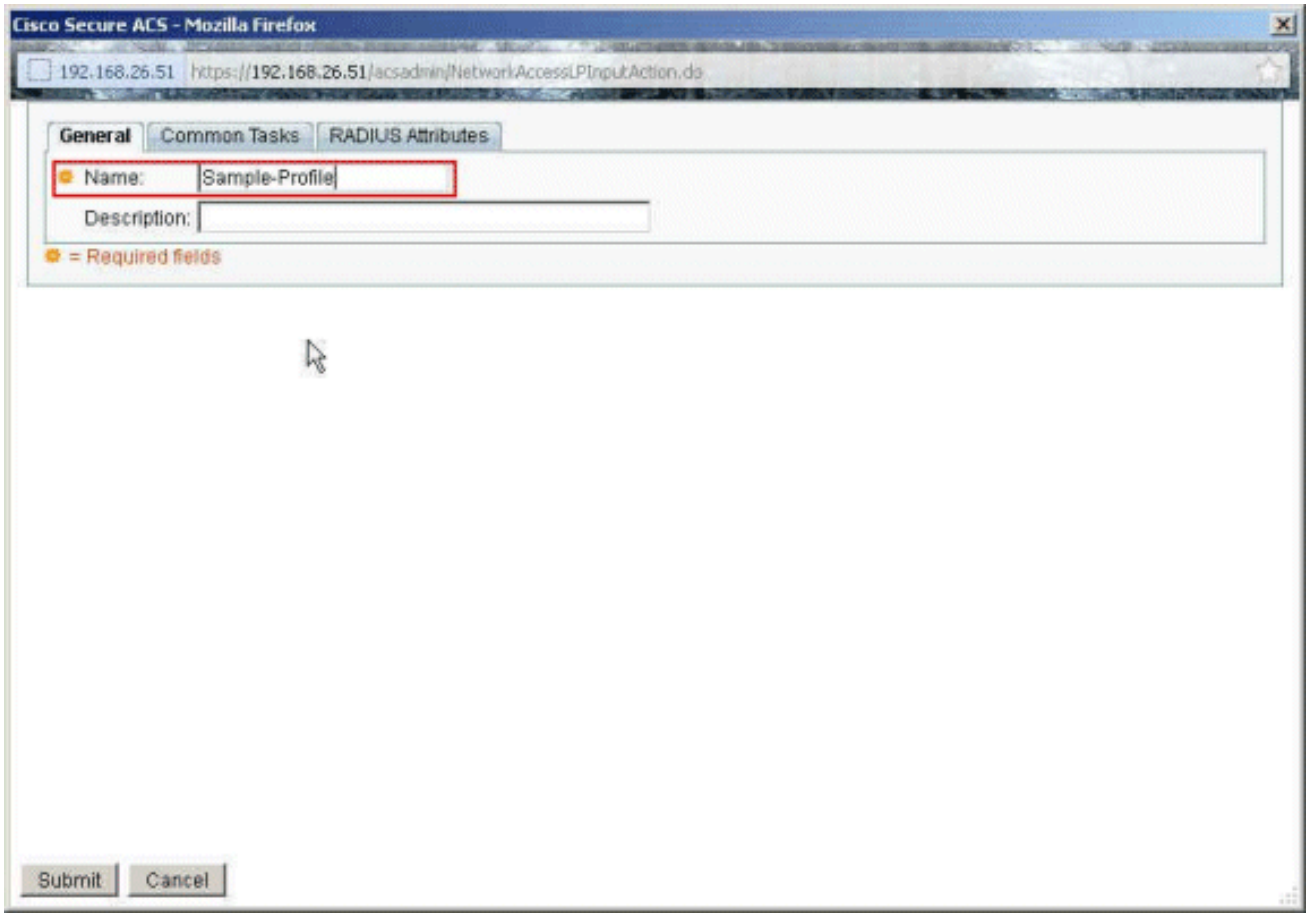
.



13. 새 권한 부여 프로파일을 생성하려면 Create를 클릭합니다
.

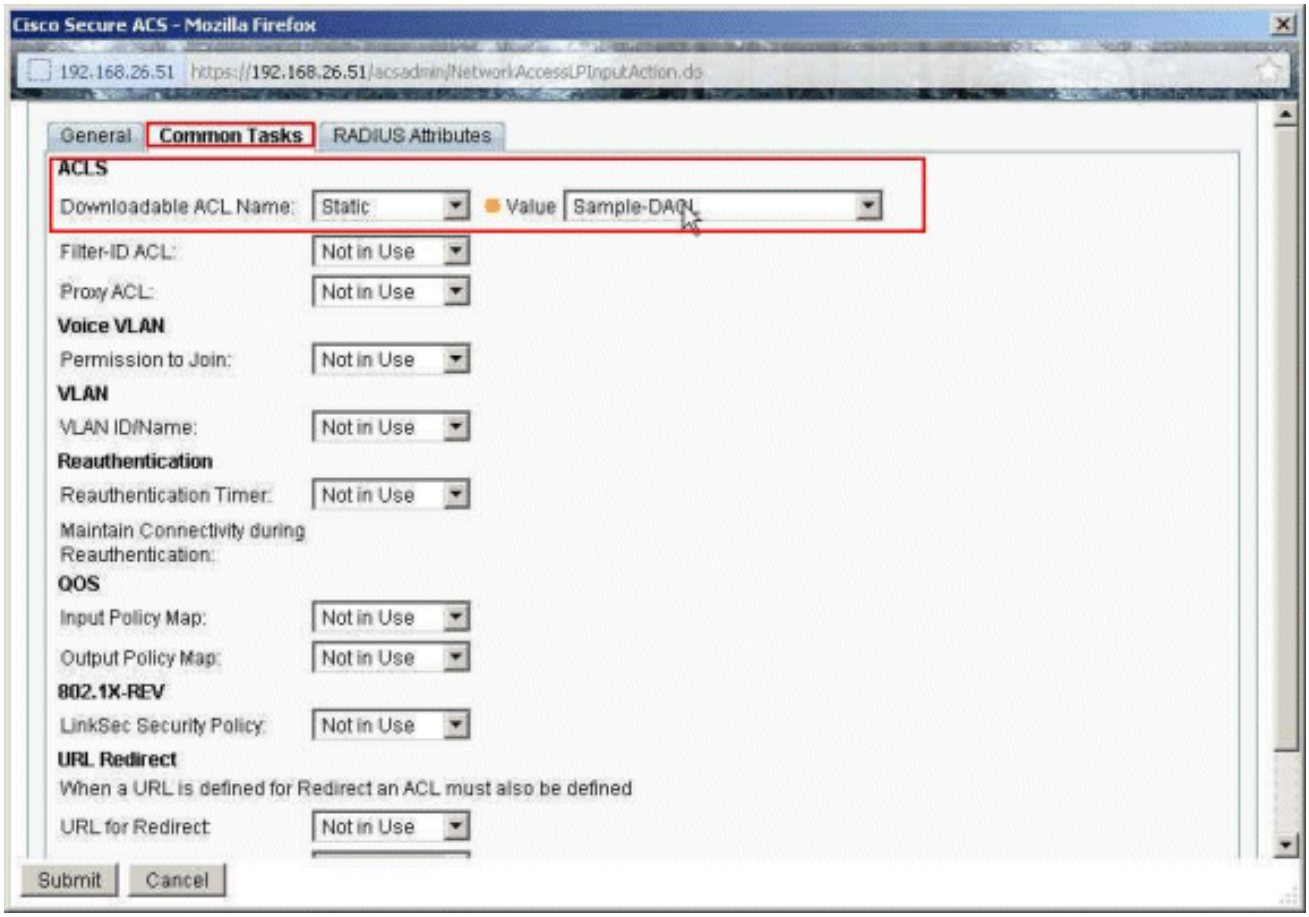


14. 권한 부여 프로파일의 이름을 **입력합니다**.**Sample-Profile**은 이 예에서 사용되는 이름입니다
.



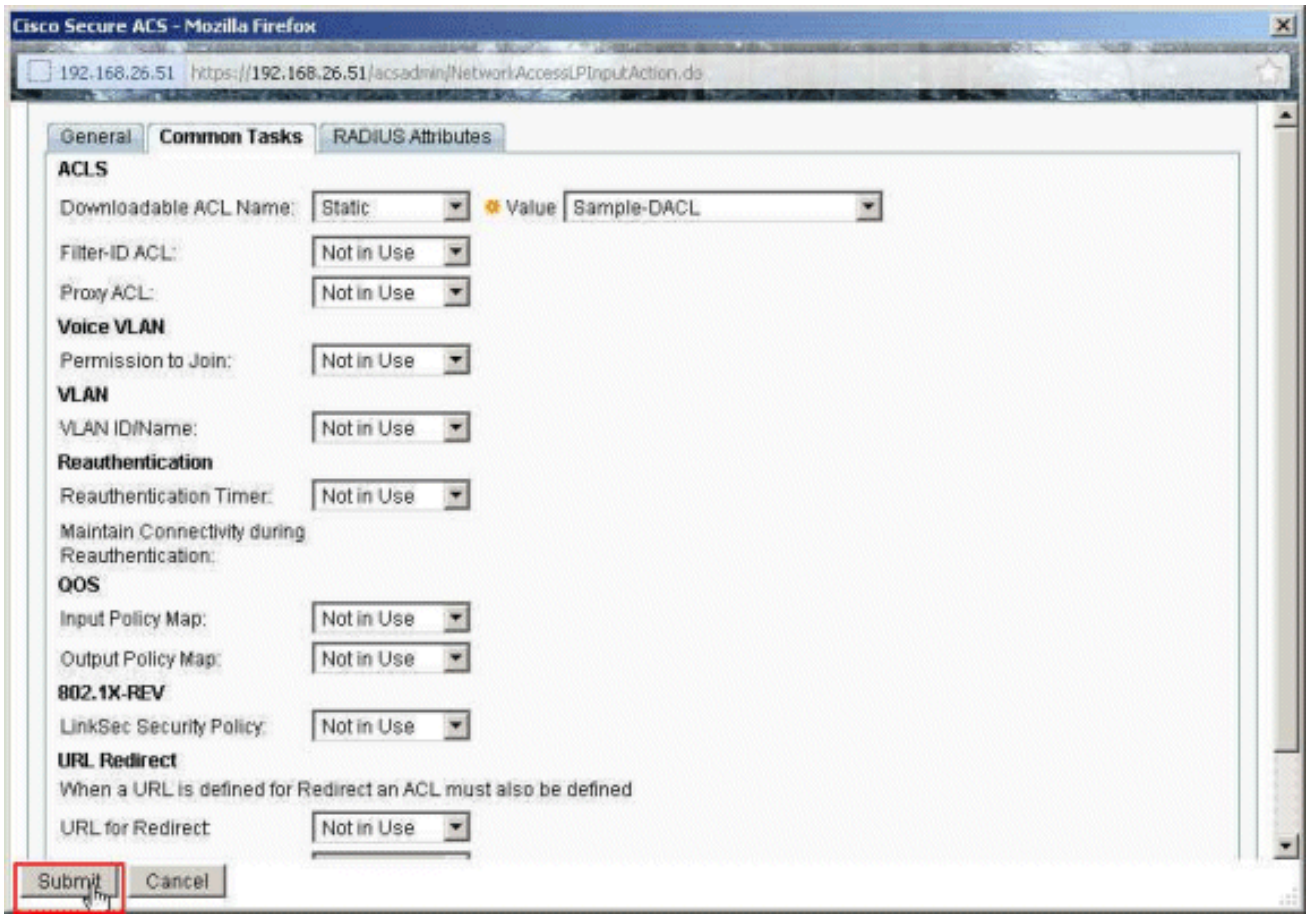
15. Common **Tasks(공통 작업)** 탭을 선택하고 다운로드 가능한 ACL 이름에 대한 드롭다운 목록에서 Static을 선택합니다.값 드롭다운 목록에서 새로 생성된 **DACL(Sample-DACL)**을 선택합니다

.



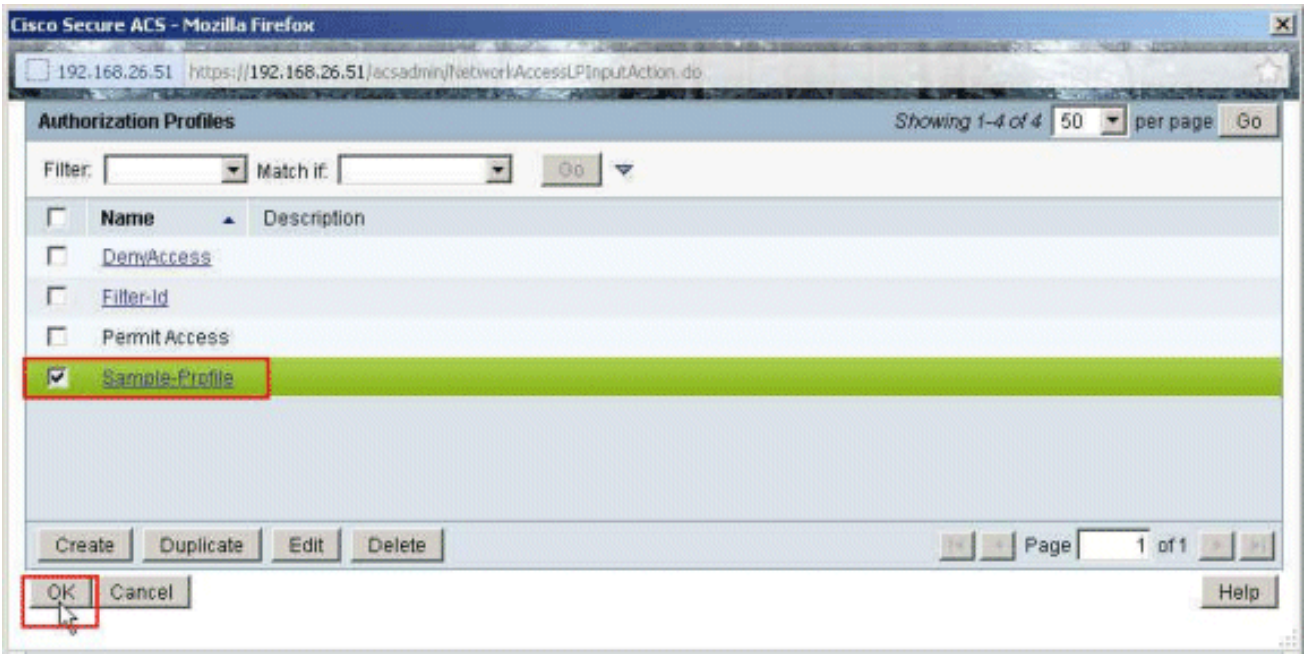
16. Submit(제출)**을 클릭합니다**

.



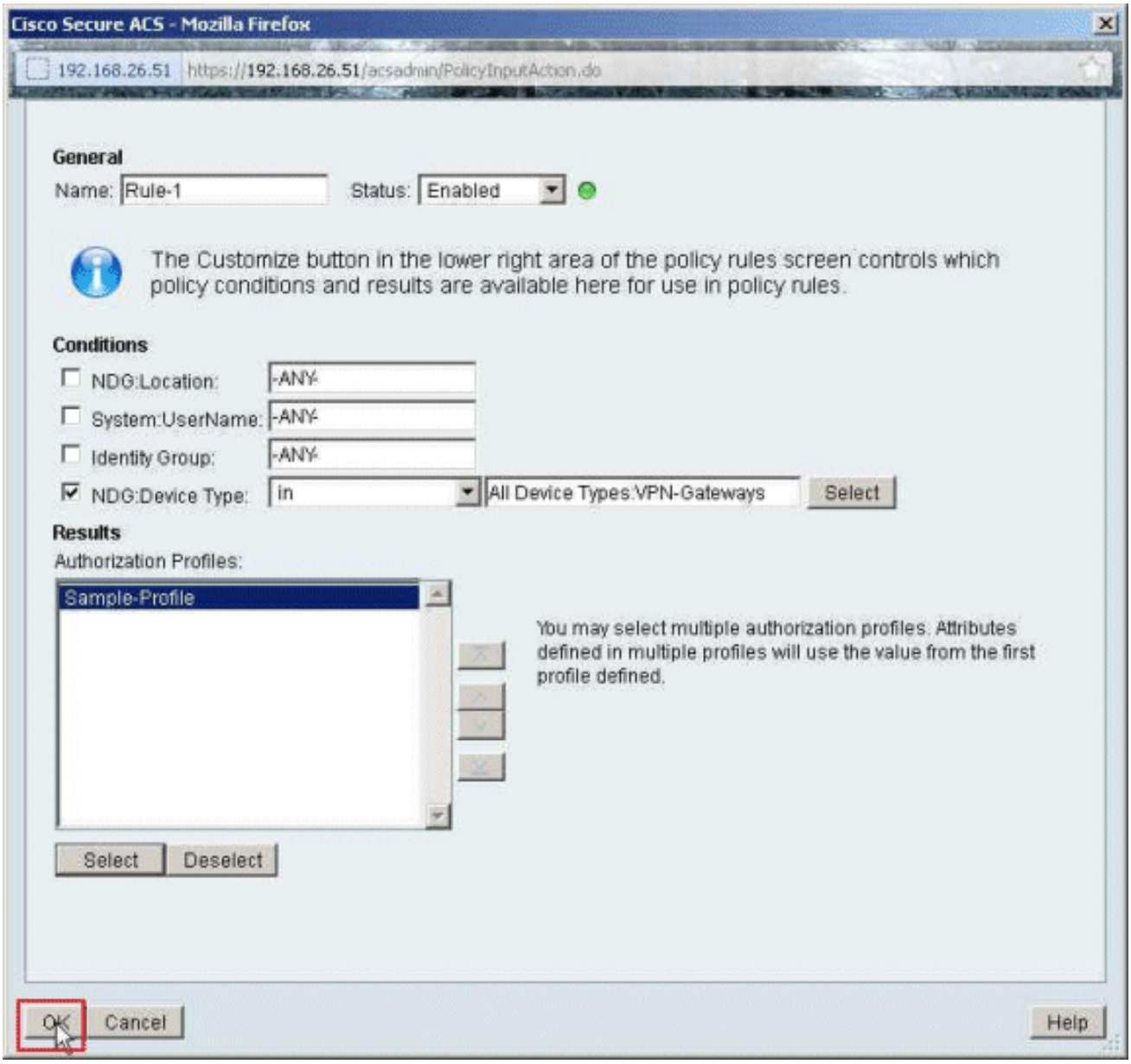
17. 이전에 **생성된 샘플 프로파일을** 선택하고 확인을 **클릭합니다**

.



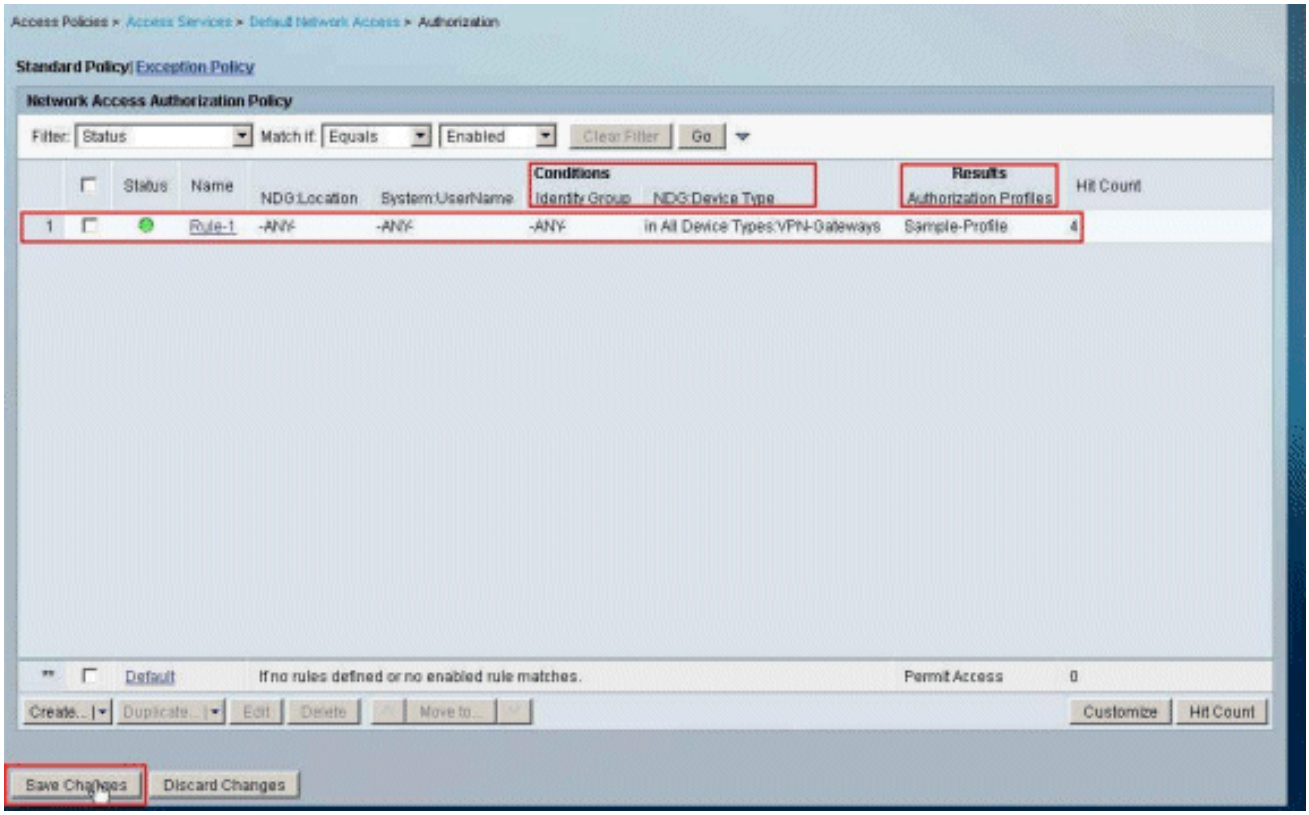
18. **확인**을 **클릭합니다**

.



19. Rule **-1**이 NDG:Device Type as condition 및 **Sample-Profile**로 VPN**-Gateways**를 사용하여 생성되었는지 확인합니다.Save **Changes**를 **클릭합니다**

.



사용자 그룹에 대한 IETF RADIUS 설정 구성

사용자가 인증할 때 RADIUS 서버에서 보안 어플라이언스에 이미 생성한 액세스 목록의 이름을 다운로드하려면 IETF RADIUS filter-id 특성(특성 번호 11)을 구성합니다.

```
filter-id=acl_name
```

Sample-Group **usercisco는** 성공적으로 인증되며 RADIUS 서버는 보안 어플라이언스에 이미 생성한 액세스 목록에 대한 ACL 이름(새 이름)을 다운로드합니다."cisco" 사용자는 10.1.1.2 서버를 **제외한** ASA 네트워크 내부에 있는 모든 디바이스에 액세스할 수 있습니다.ACL을 확인하려면 Filter-Id ACL 섹션을 참조하십시오.

예와 같이 **new**라는 ACL이 ASA에서 필터링하도록 구성됩니다.

```
access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

이러한 매개변수는 true인 경우에만 나타납니다.다음을 구성했습니다.

- 네트워크 컨피그레이션에서 RADIUS 프로토콜 중 하나를 사용하는 AAA 클라이언트
- RADIUS(IETF) Filter-Id가 있는 권한 부여 프로파일이 Access-Service 규칙의 결과 섹션 아래에서 선택됩니다.

RADIUS 특성은 ACS에서 요청 AAA 클라이언트로 각 사용자에 대한 프로필로 전송됩니다.

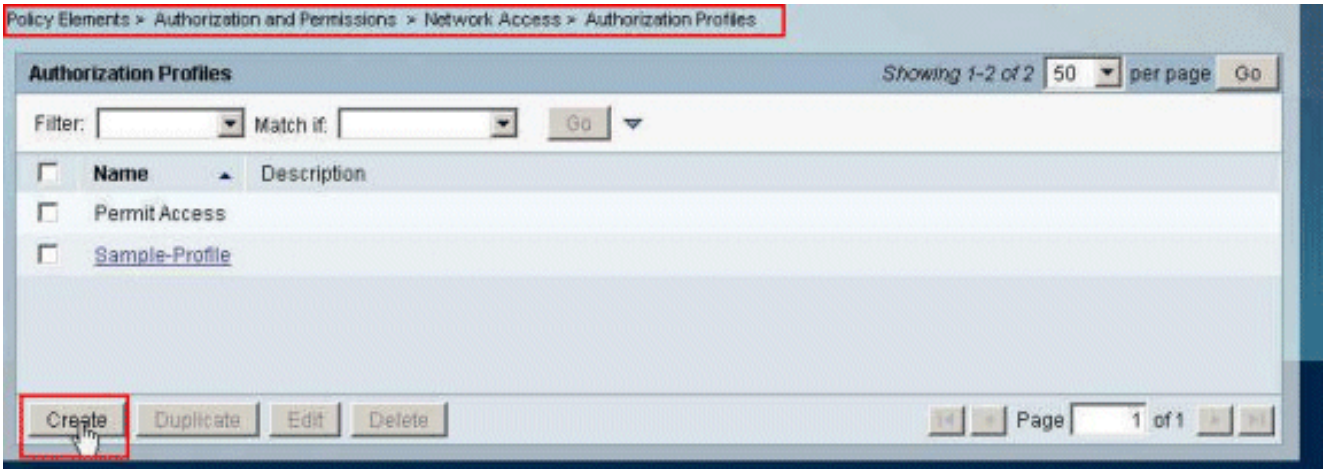
개별 사용자에 대해 다운로드 가능한 ACL을 위한 ACS 구성의 1~6단계 및 10~12단계를 완료하고,

Configure ACS for Downloadable ACL for Group(그룹에 대해 다운로드 가능한 ACL에 대해 ACS 구성)의 1~6단계를 수행하고, Cisco Secure ACS에서 Filter-ID를 구성하려면 이 섹션에서 다음 단계를 수행합니다.

권한 부여 프로파일에 따라 적용할 IETF **RADIUS** 특성 설정을 구성하려면 다음 단계를 수행합니다.

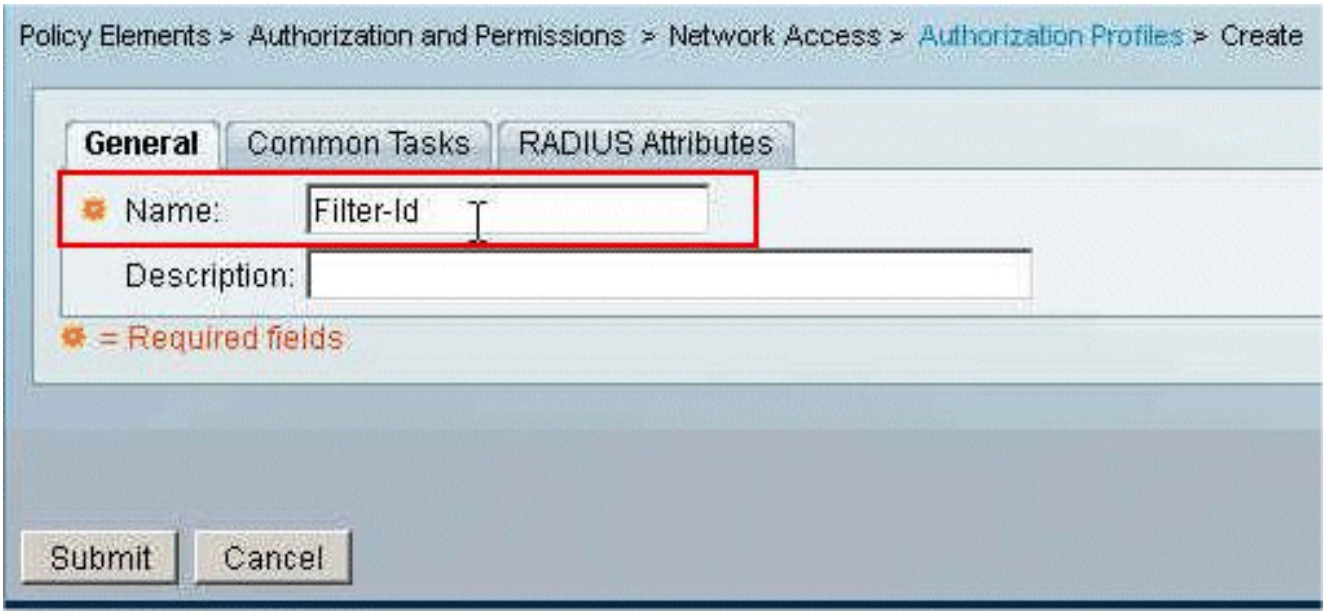
1. Policy **Elements(정책 요소)** > Authorization and **Permissions(권한 부여 및 권한)** > **Network Access(네트워크 액세스)** > **Authorization Profiles(권한 부여 프로파일)를** 선택하고 Create(생성)를 클릭하여 **새 권한 부여 프로파일을 생성합니다**

.



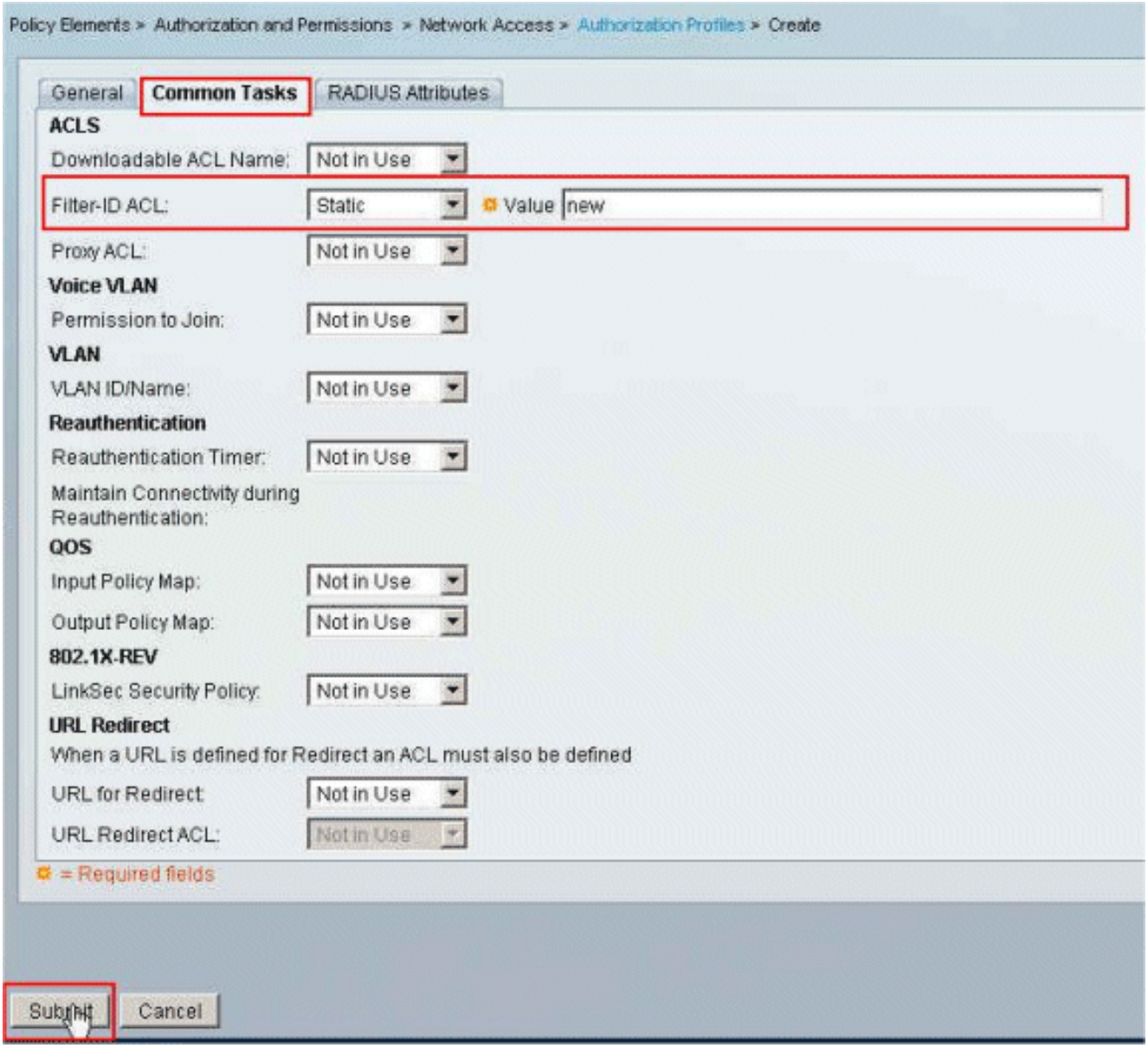
2. 권한 부여 프로파일의 이름을 **입력합니다.Filter-Id**는 이 예에서는 단순성을 위해 선택한 권한 부여 프로파일 이름입니다

.



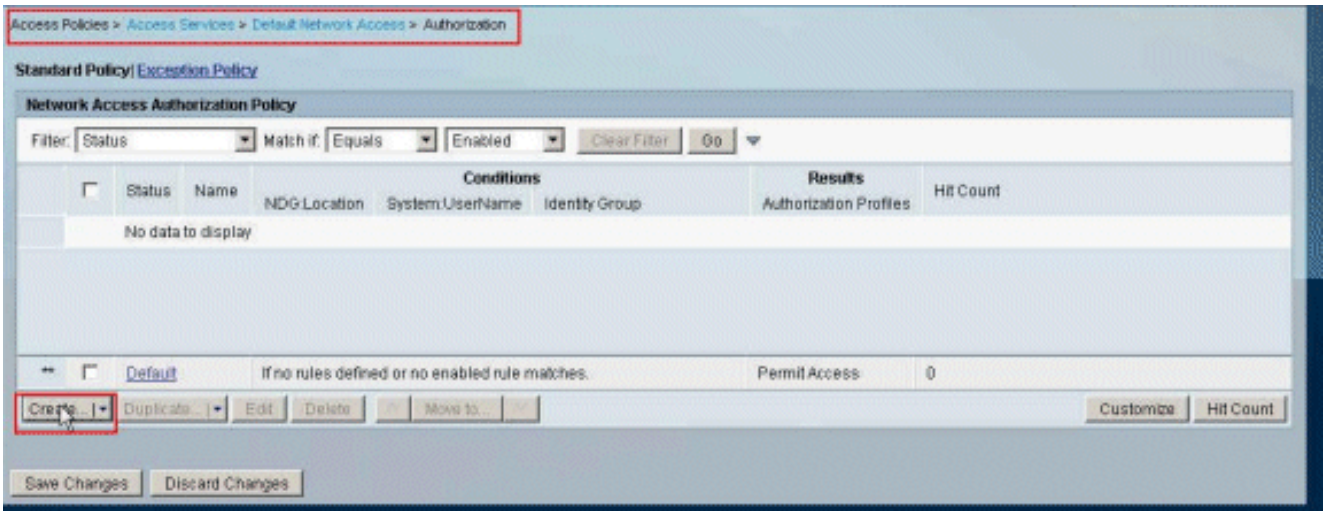
3. Common **Tasks(공통 작업)** 탭을 클릭하고 **Filter-ID ACL**에 대한 드롭다운 목록에서 Static(고정)을 **선택합니다.**Value(값) 필드에 액세스 목록 이름을 **new**로 입력하고 Submit(제출)을 **클릭합니다**

.



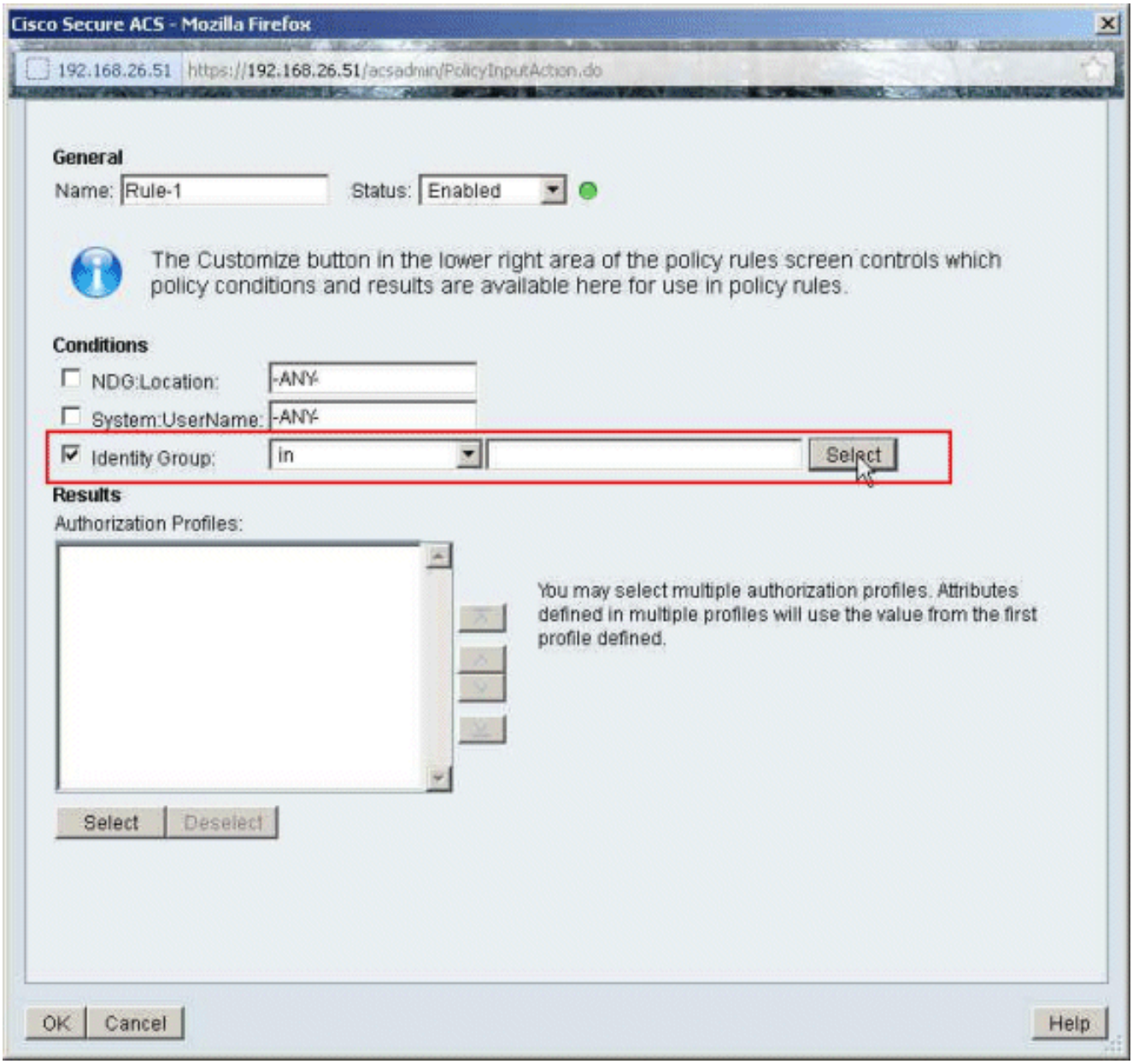
4. Access **Policies(액세스 정책) > Access Services(액세스 서비스) > Default Network Access(기본 네트워크 액세스) > Authorization(권한 부여)을** 선택하고 **Create(생성)를 클릭하여 새 규칙을 생성합니다**

.



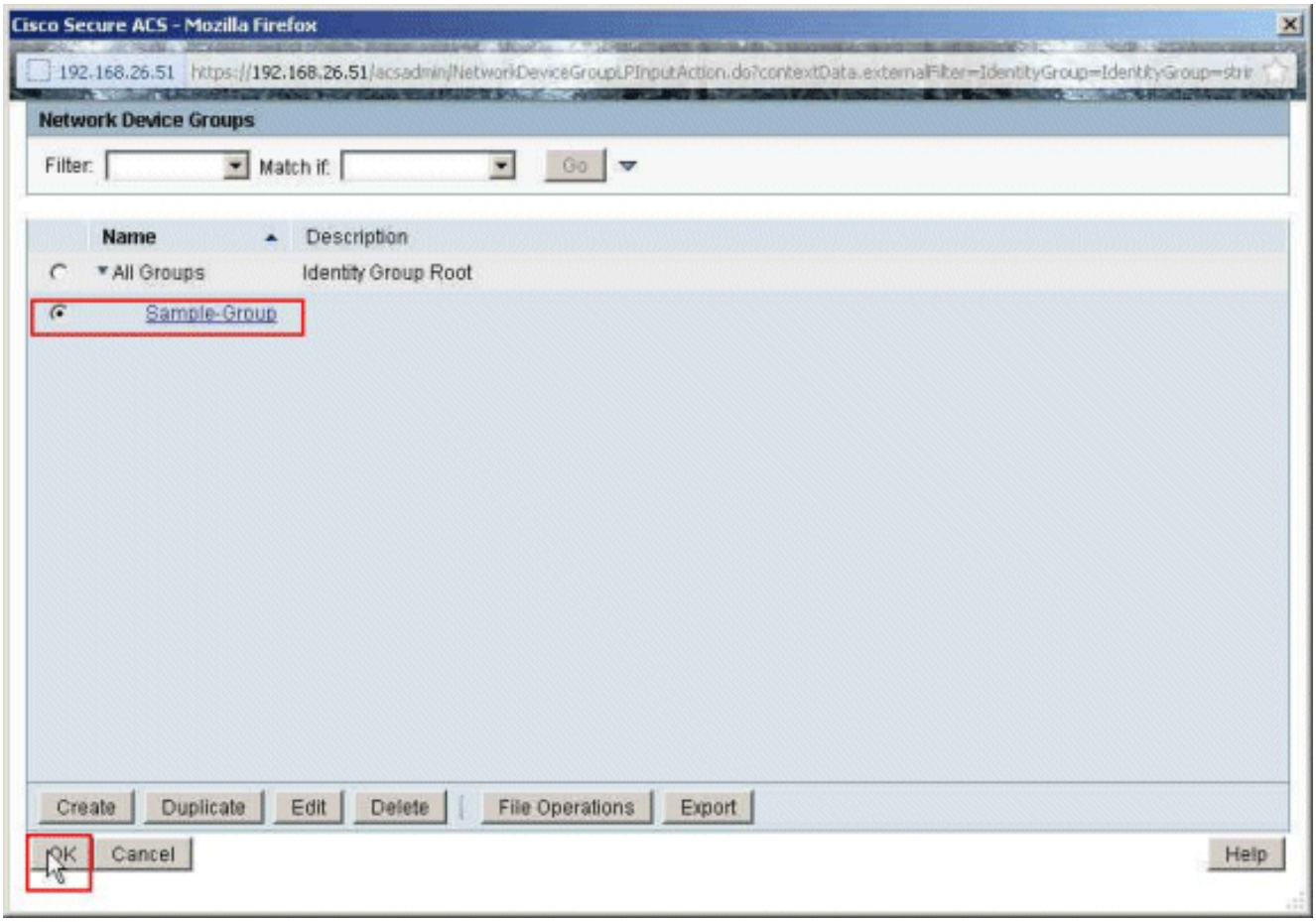
5. **Identity Group** 옆에 있는 확인란이 선택되었는지 확인하고 **선택**을 클릭합니다

.



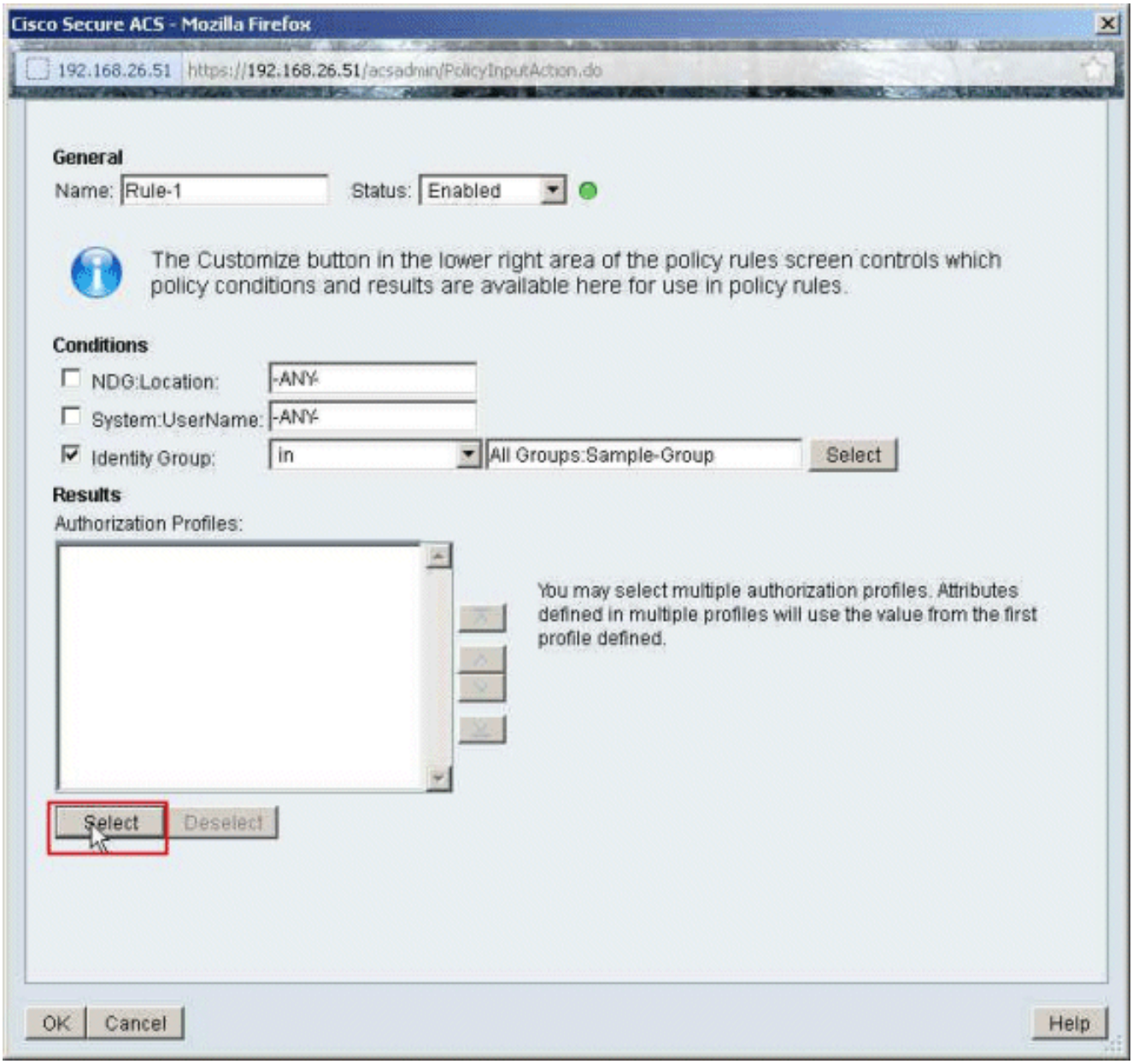
6. Sample-**Group**을 선택하고 **OK**를 클릭합니다

.

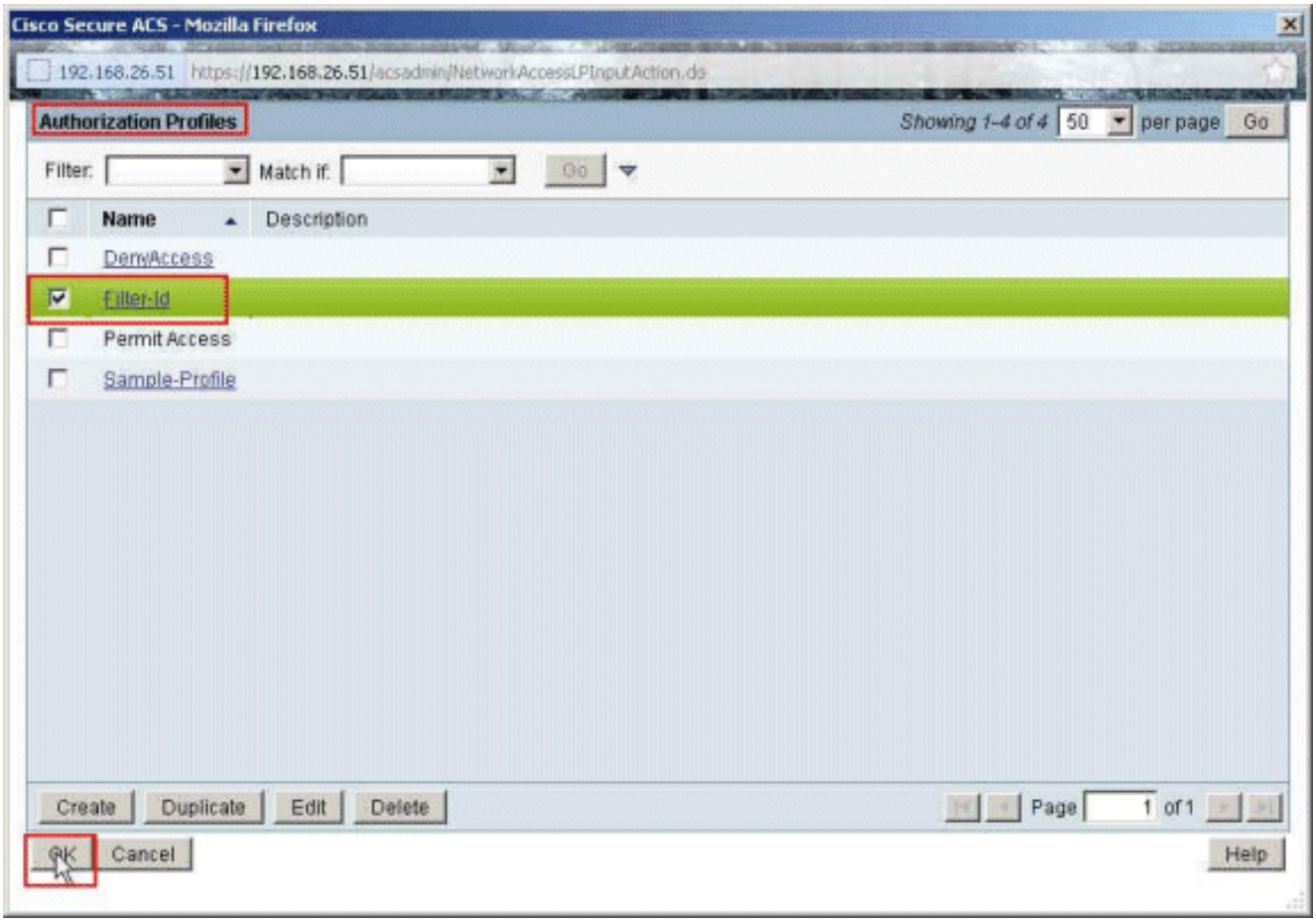


7. Authorization **Profiles** 섹션에서 Select를 클릭합니다

.

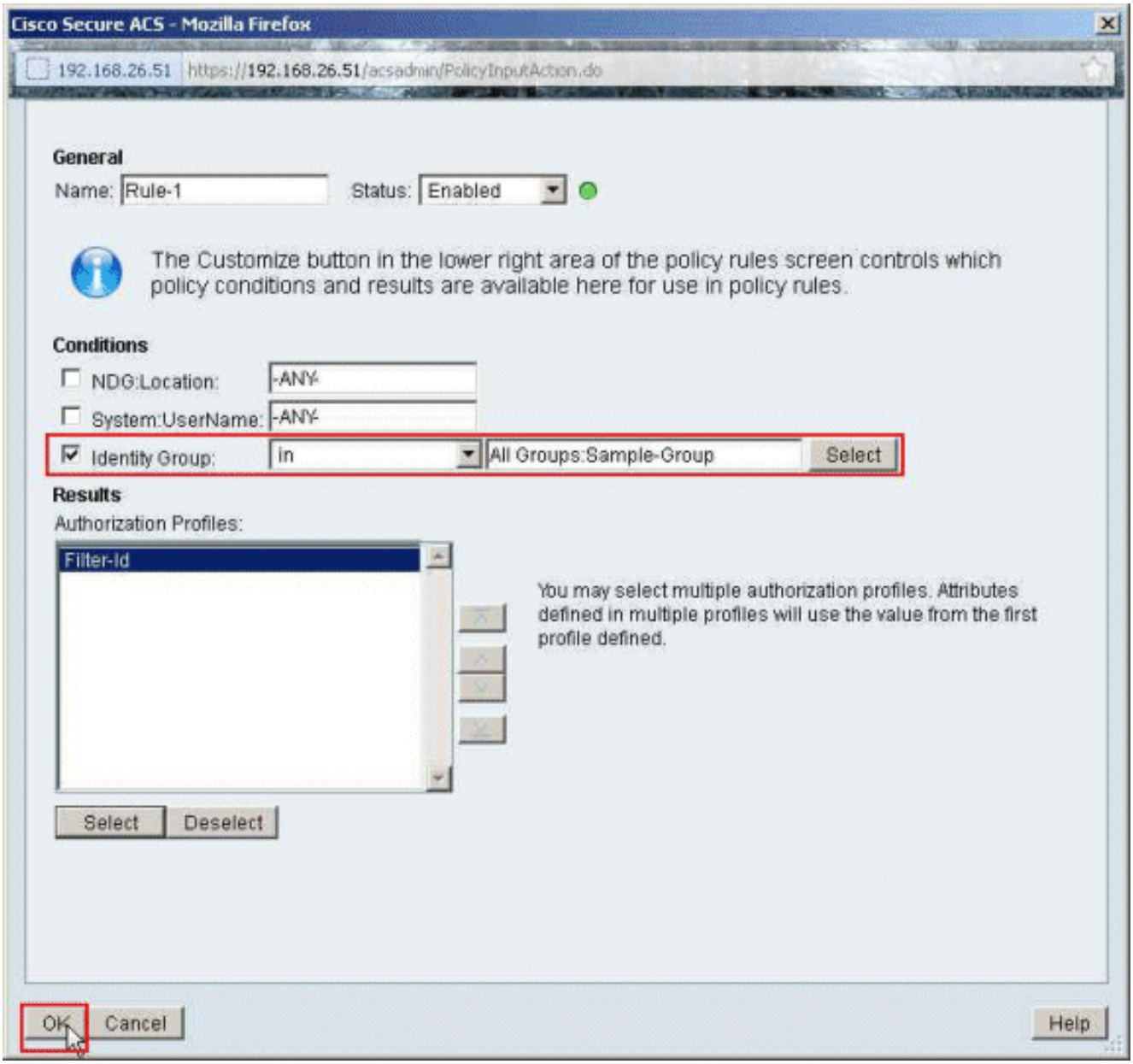


8. 이전에 생성된 Authorization Profile **Filter-Id**를 선택하고 **OK**(확인)를 클릭합니다
.


Cisco Secure ACS - Mozilla Firefox
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do
Authorization Profiles
Showing 1-4 of 4 50 per page Go
Filter: Match if: Go
Name Description
DenyAccess
Filter-Id
Permit Access
Sample-Profile
Create Duplicate Edit Delete
Page 1 of 1
OK Cancel
Help

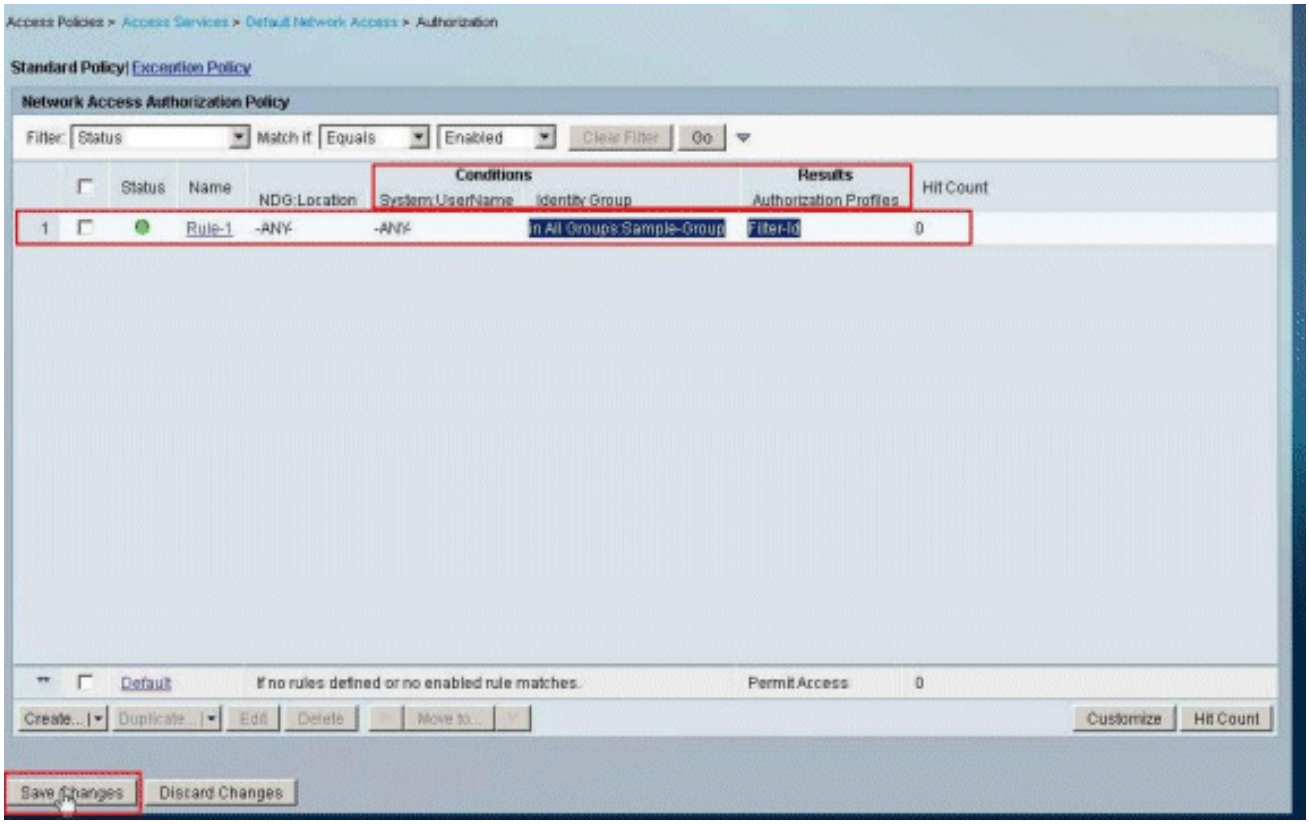
9. **확인을 클릭합니다**

.



10. ID 그룹 **Sample-Group**을 조건으로 하고 **Filter-Id**를 Result로 사용하여 Rule-**1**이 생성되었는지 확인합니다.Save **Changes**를 **클릭합니다**

.

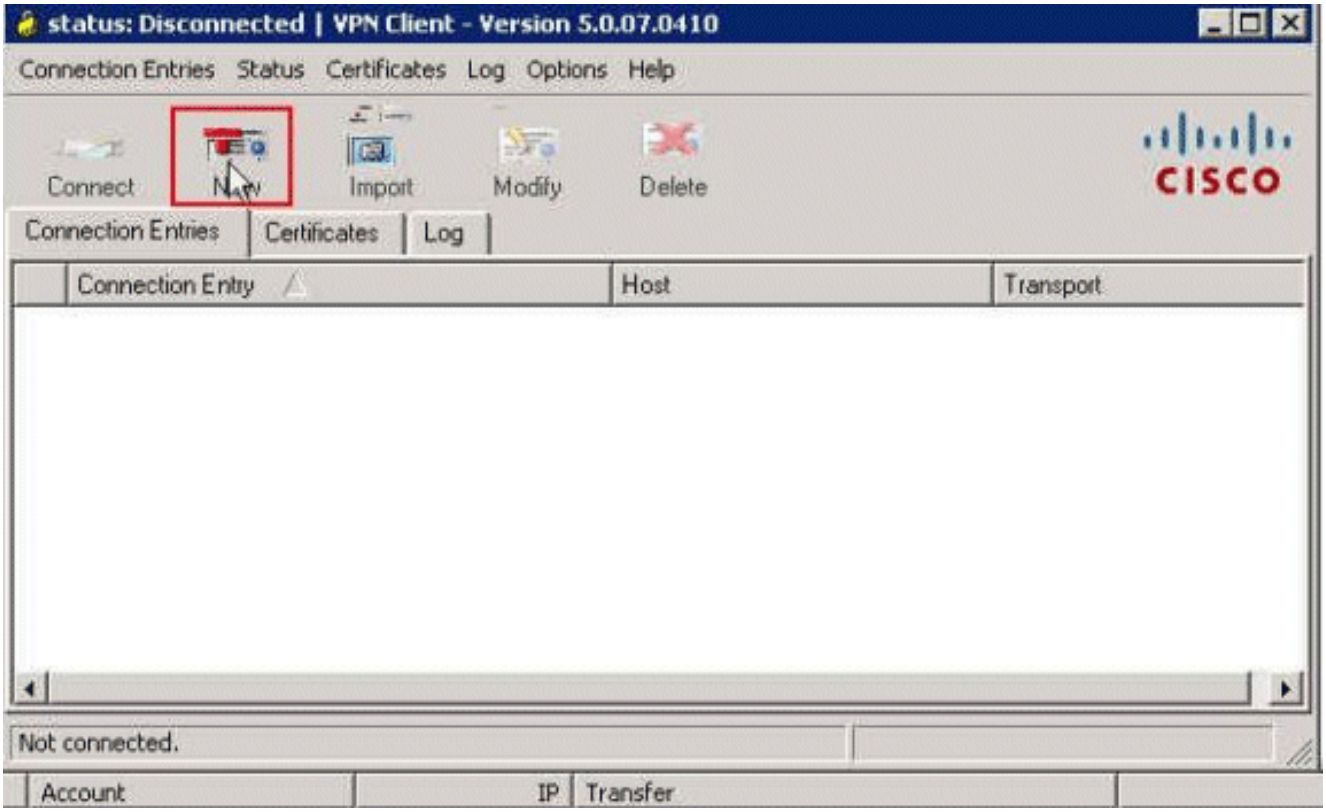


Cisco VPN 클라이언트 컨피그레이션

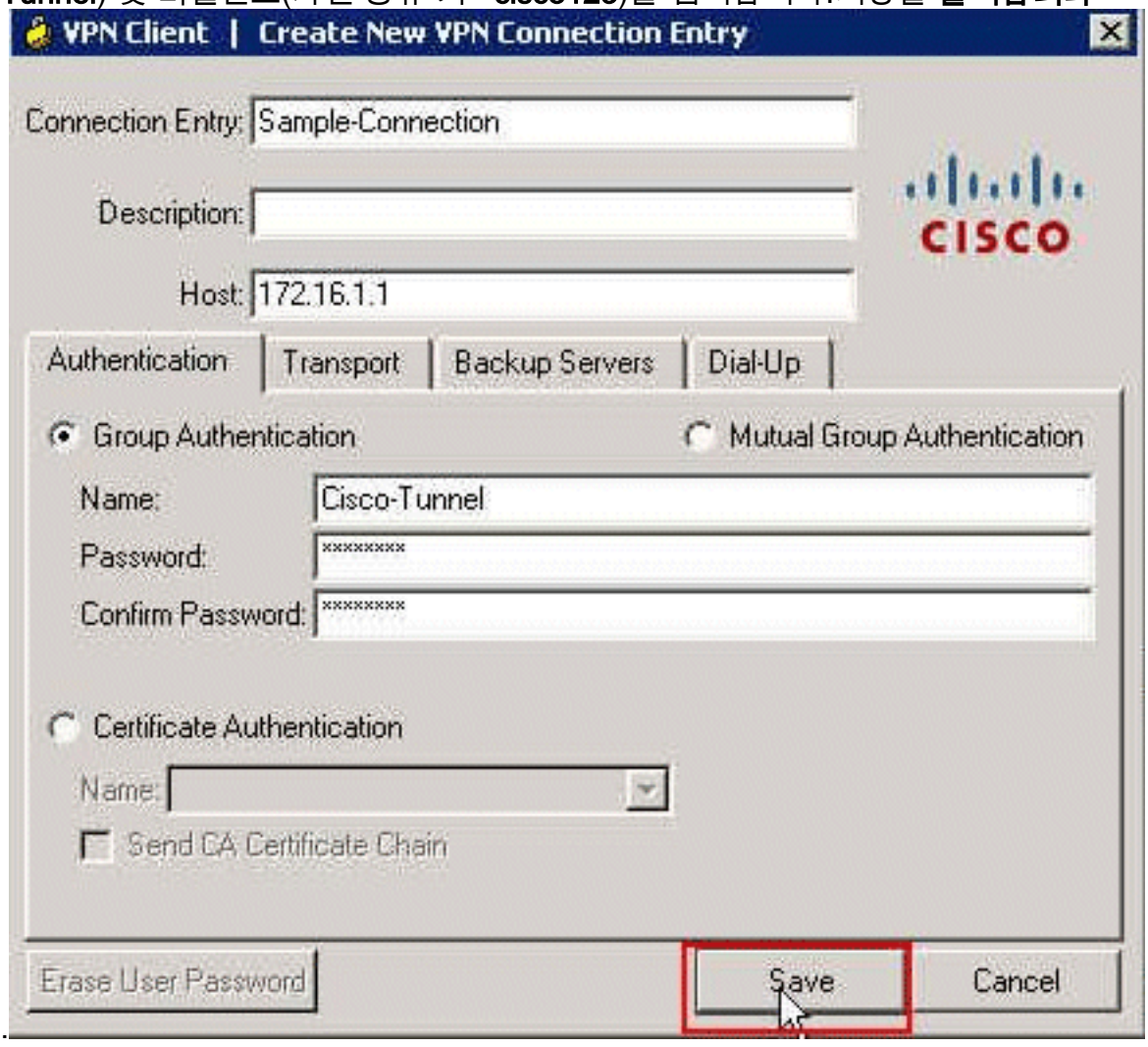
ASA가 성공적으로 구성되었는지 확인하려면 Cisco VPN Client를 사용하여 Cisco ASA에 연결합니다.

다음 단계를 완료하십시오.

1. Start(**시작**) > **Programs(프로그램)** > **Cisco Systems VPN Client(Cisco Systems VPN 클라이언트)** > **VPN Client(VPN 클라이언트)**를 선택합니다.
2. Create New VPN Connection Entry(새 VPN 연결 항목 생성) 창을 시작하려면 New(새로 만들기)를 클릭합니다
.

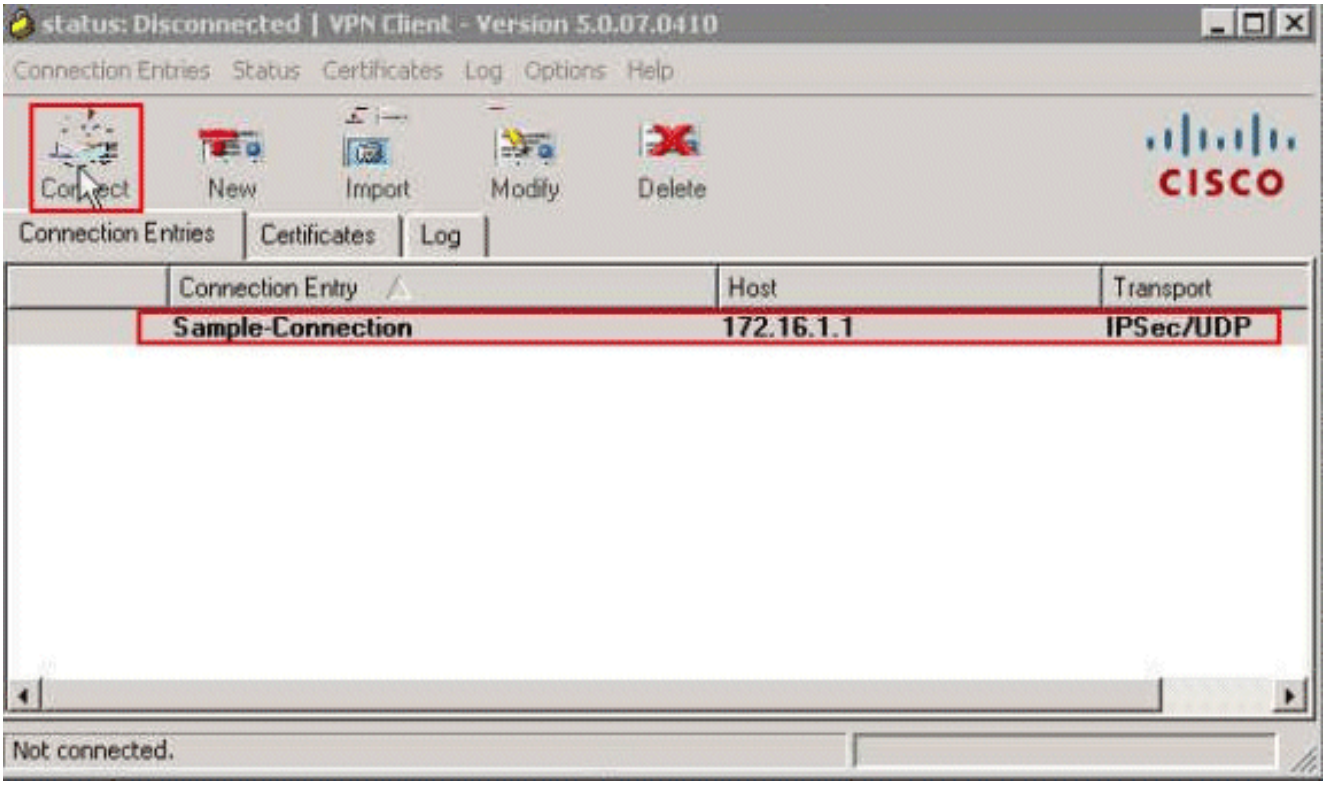


3. 새 연결의 세부 정보를 입력합니다.설명과 함께 연결 항목의 이름을 입력합니다.Host(호스트) 상자**에 ASA의 외부 IP 주소**를 입력합니다.ASA에 구성된 대로 VPN 터널 그룹 이름(**Cisco-Tunnel**) 및 비밀번호(사전 공유 키 - **cisco123**)를 입력합니다.저장을 **클릭합니다**



4. 사용할 연결을 클릭하고 VPN Client 주 창에서 **Connect(연결)**를 클릭합니다

.

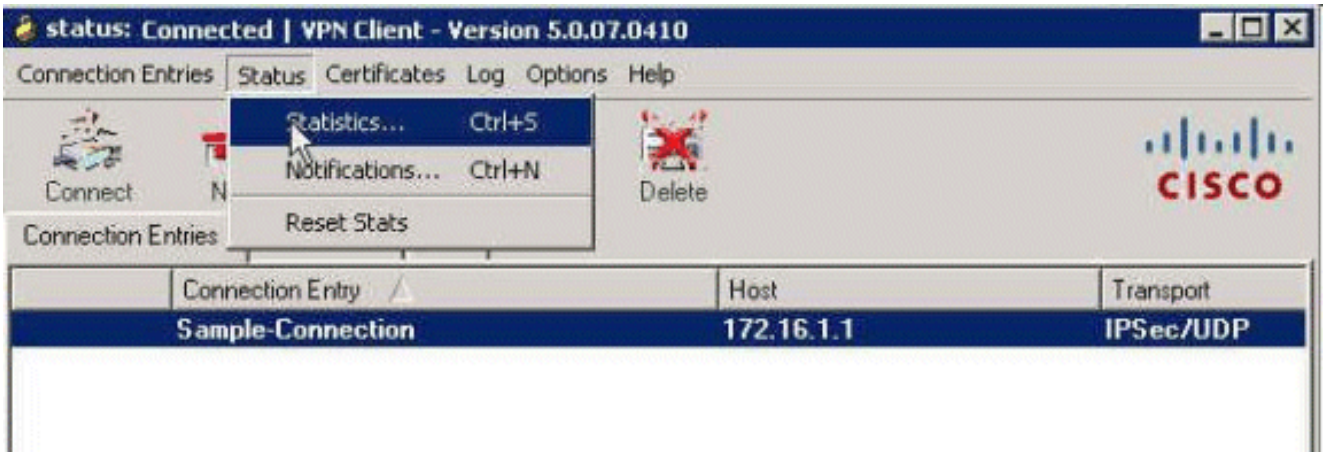


5. 프롬프트가 표시되면 ASA에서 인증을 위해 구성한 대로 **cisco** 사용자 이름 및 비밀번호 **cisco123**을 입력하고 **OK**를 클릭하여 원격 네트워크에 연결합니다

.

6. 연결이 성공적으로 설정되면 Status 메뉴에서 Statistics를 선택하여 터널의 세부 정보를 확인합니다

.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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

암호화 명령 표시

- **show crypto isakmp sa** - 피어의 현재 IKE SA(Security Associations)를 모두 표시합니다.

```
ciscoasa# sh crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.16.1.50
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
ciscoasa#
```

- **show crypto ipsec sa** - 현재 SA에서 사용하는 설정을 표시합니다.

```
ciscoasa# sh crypto ipsec sa
interface: outside
    Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr:
       172.16.1.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
      current_peer: 172.16.1.50, username: cisco
      dynamic allocated peer ip: 10.2.2.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
      #pkts decaps: 333, #pkts decrypt: 333, #pkts verify: 333
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly:
        0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.1.50/0
      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 9A06E834
      current inbound spi : FA372121

    inbound esp sas:
      spi: 0xFA372121 (4197916961)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28678
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x9A06E834 (2584143924)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28678
```

```
            IV size: 16 bytes
            replay detection support: Y
            Anti replay bitmap:
             0x00000000 0x00000001
```

사용자/그룹에 대해 다운로드 가능한 ACL

사용자 Cisco에 대해 다운로드 가능한 ACL을 확인합니다.ACL은 CSACS에서 다운로드됩니다.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list #ACSACL#-IP-Sample-DACL-4f3b9117; 2 elements; name hash: 0x3c878038
   (dynamic)
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 1 extended permit ip any host
   10.1.1.2 (hitcnt=0) 0x5e896ac3
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 2 extended deny ip any any
   (hitcnt=130) 0x19b3b8f5
```

필터 ID ACL

[011] Filter-Id가 Group - Sample-Group에 적용되었으며, 그룹의 사용자는 ASA에 정의된 ACL(신규)에 따라 필터링됩니다.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list new; 2 elements; name hash: 0xa39433d3
access-list new line 1 extended permit ip any host 10.1.1.2 (hitcnt=4)
   0x58a3ea12
access-list new line 2 extended deny ip any any (hitcnt=27) 0x61f918cd
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.샘플 **디버그** 출력도 표시됩니다.

참고: 원격 액세스 IPsec VPN 문제 해결에 대한 자세한 내용은 가장 일반적인 L2L 및 원격 액세스 IPsec VPN 문제 해결 솔루션을 참조하십시오.

보안 연결 지우기

문제를 해결할 때 변경한 후 기존 SA를 지우십시오.PIX의 특권 모드에서 다음 명령을 사용합니다.

- **clear [crypto] ipsec sa** - 활성 IPsec SA를 삭제합니다.crypto 키워드는 선택 사항입니다.
- **clear [crypto] isakmp sa** - 활성 IKE SA를 삭제합니다.crypto 키워드는 선택 사항입니다.

문제 해결 명령

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.

- **debug crypto ipsec 7** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp 7** - 1단계의 ISAKMP 협상을 표시합니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliances 지원 페이지
- Cisco ASA 5500 Series Adaptive Security Appliances 명령 참조
- Cisco Adaptive Security Device Manager
- IPsec 협상/IKE 프로토콜 지원 페이지
- Cisco VPN 클라이언트 지원 페이지
- Cisco Secure Access Control System
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems