ASA 8.3 及更高版本：使用带CLI和ASDM的可下载ACL的VPN访问的RADIUS授权(ACS 5.x)配置示例

目录

简介

本文档将说明如何配置安全设备针对网络访问对用户进行身份验证。由于您可以隐式启用RADIUS授权，因此本文档不包含有关安全设备上RADIUS授权配置的信息。本部分提供的是有关安全设备如何处理从 RADIUS 服务器接收的访问列表信息的信息。

可以将 RADIUS 服务器配置为下载访问列表到安全设备或在身份验证时下载访问列表名称。用户获得授权仅可执行用户特定访问列表中所允许的操作。

当您使用思科安全访问控制服务器(ACS)为每个用户提供适当的访问列表时，可下载的访问列表是最可扩展的方式。有关可下载访问列表功能和 Cisco Secure ACS 的详细信息，请参阅将 RADIUS

服务器配置为发送可下载访问控制列表和可下载 IP ACL。

请参阅ASA/PIX 8.x:使用带CLI和ASDM的可下载ACL的网络访问的RADIUS授权(ACS)配置示例，用于8.2版及更低版本的Cisco ASA上的相同配置。

先决条件

要求

本文档假设自适应安全设备(ASA)已完全运行，且已配置为允许思科自适应安全设备管理器(ASDM)或CLI进行配置更改。

注意：请参阅允许ASDM的HTTPS访问，以便允许ASDM或安全外壳(SSH)远程配置设备。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA软件版本8.3及更高版本
- Cisco ASDM版本6.3及更高版本
- Cisco VPN客户端5.x版及更高版本
- 思科安全ACS 5.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

您可以使用可下载的IP ACL来创建可应用于许多用户或用户组的ACL定义集。这些 ACL 定义集称为 ACL 内容。

可下载 IP ACL 的运行方式如下：

1. 当ACS授予用户网络访问权限时，ACS将确定是否将可下载的IP ACL分配给结果部分的授权配置文件。
2. 如果ACS找到分配给授权配置文件的可下载IP ACL,ACS会发送一个属性（作为用户会话的一部分，在RADIUS access-accept数据包中），指定命名ACL和命名ACL的版本。
3. 如果AAA客户端响应其缓存中没有当前版本的ACL（即，ACL是新的或已更改），则ACS会将ACL（新的或已更新的）发送到设备。

可下载 IP ACL 是每个用户或用户组的 RADIUS Cisco cisco-av-pair 属性 [26/9/1] 中的替代 ACL 配置。您可以创建一次可下载的IP ACL，为其指定名称，然后将可下载的IP ACL分配给任何授权配置文件（如果您引用了其名称）。此方法比为授权配置文件配置RADIUS Cisco-av-pair属性时更有效。

在 ACS Web 界面中输入 ACL 定义时，请勿使用关键字或名称条目；在其他所有方面，请对计划应

用可下载 IP ACL 的 AAA 客户端使用标准 ACL 命令语法和语义。输入 ACS 中的 ACL 定义包含一个或多个 ACL 命令。每个 ACL 命令必须独占一行。

在ACS中，您可以定义多个可下载IP ACL，并在不同的授权配置文件中使用它们。根据访问服务授权规则中的条件，您可以将包含可下载IP ACL的不同授权配置文件发送到不同的AAA客户端。

此外，您还可以更改可下载IP ACL中ACL内容的顺序。ACS从表顶部开始检查ACL内容，并下载它找到的第一个ACL内容。在设置顺序时，如果将适用范围最广的 ACL 内容置于列表中的较高位置，则可以确保系统效率。

要在特定AAA客户端上使用可下载的IP ACL,AAA客户端必须遵守以下规则：

- 使用 RADIUS 进行身份验证
- 支持可下载 IP ACL

以下是支持可下载 IP ACL 的 Cisco 设备示例：

- ASA
- 运行IOS版本12.3(8)T及更高版本的思科设备

以下是在ACL Definitions框中输入ASA ACL所必须使用的格式示例：

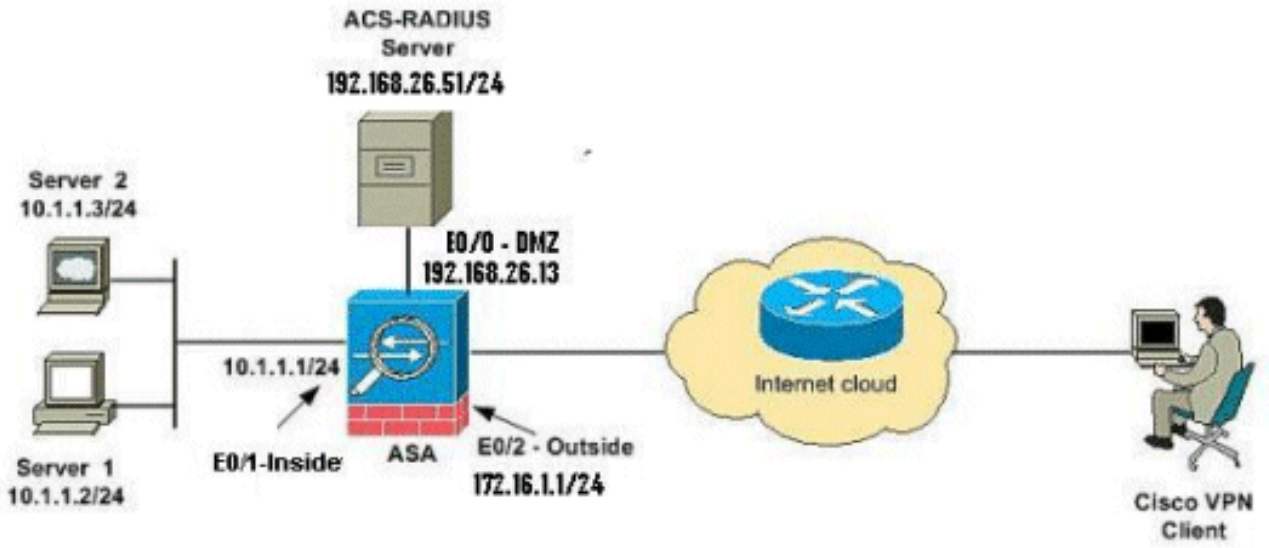
```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 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
```

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：



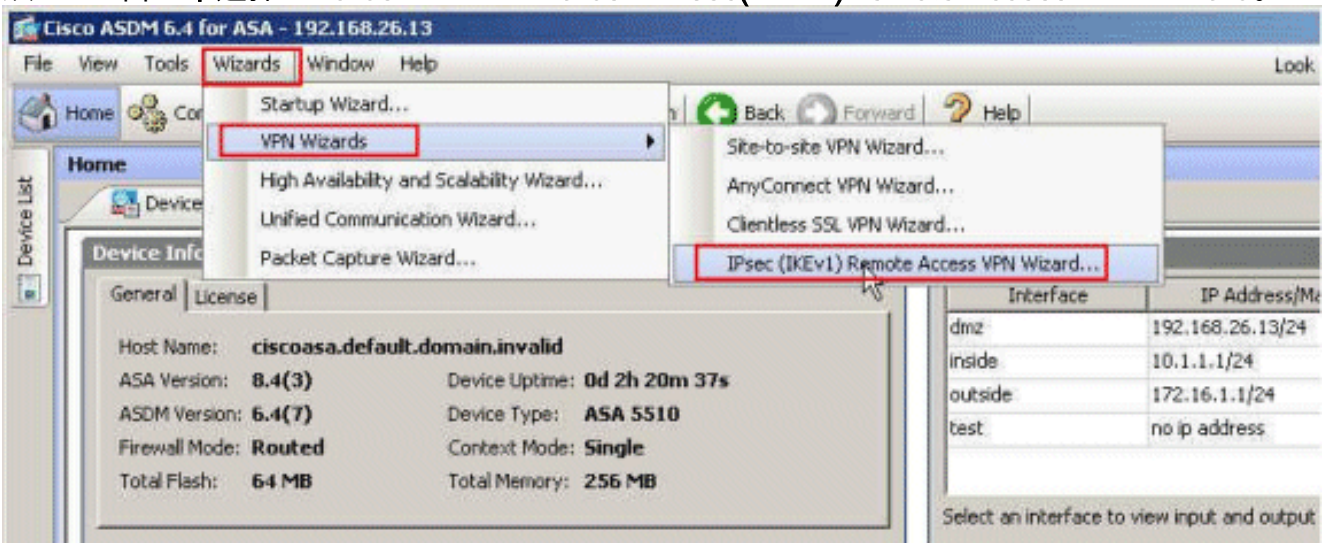
注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的RFC 1918 地址。

配置远程访问VPN(IPsec)

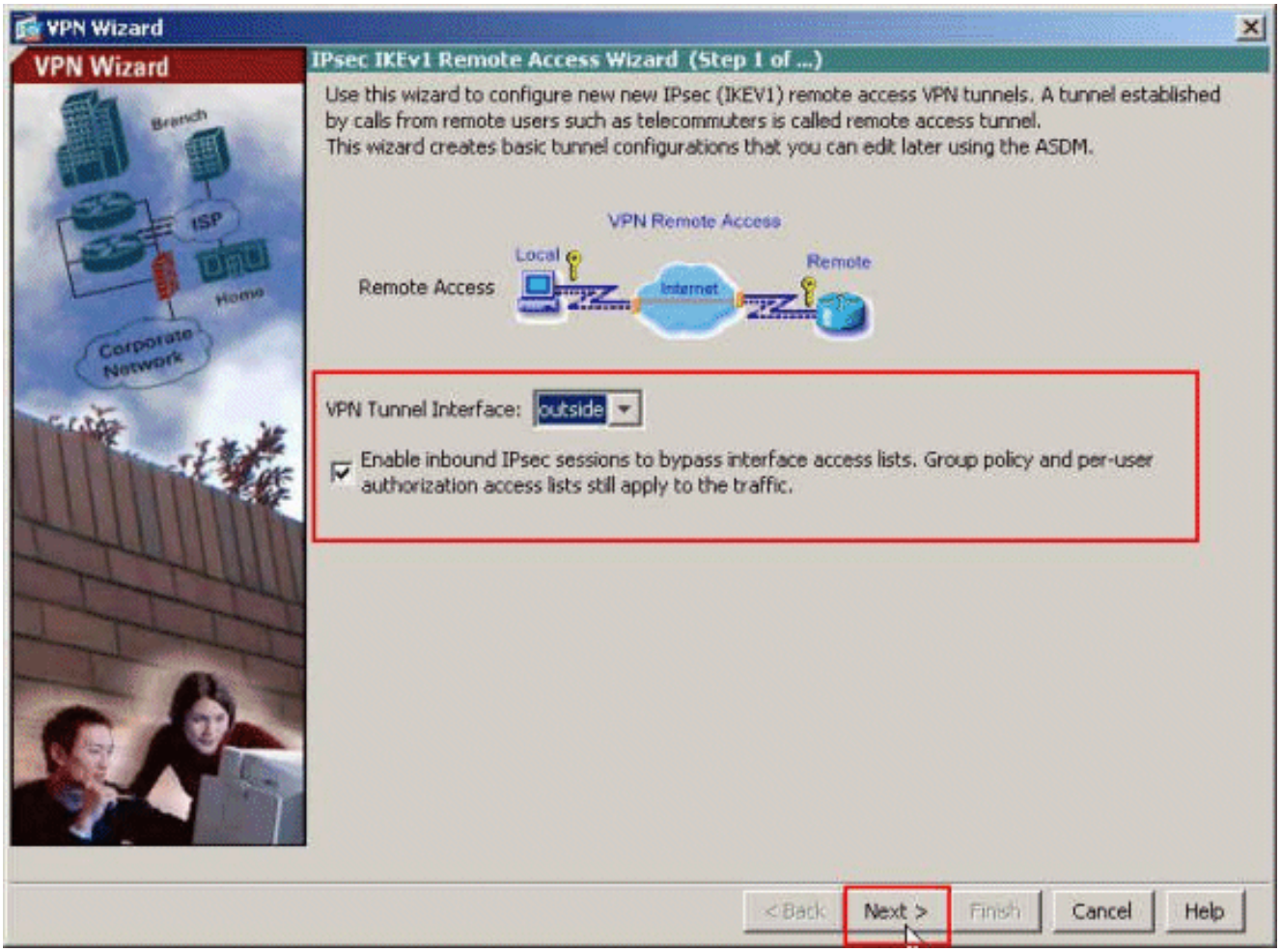
ASDM 步骤

执行下列步骤以配置远程访问 VPN：

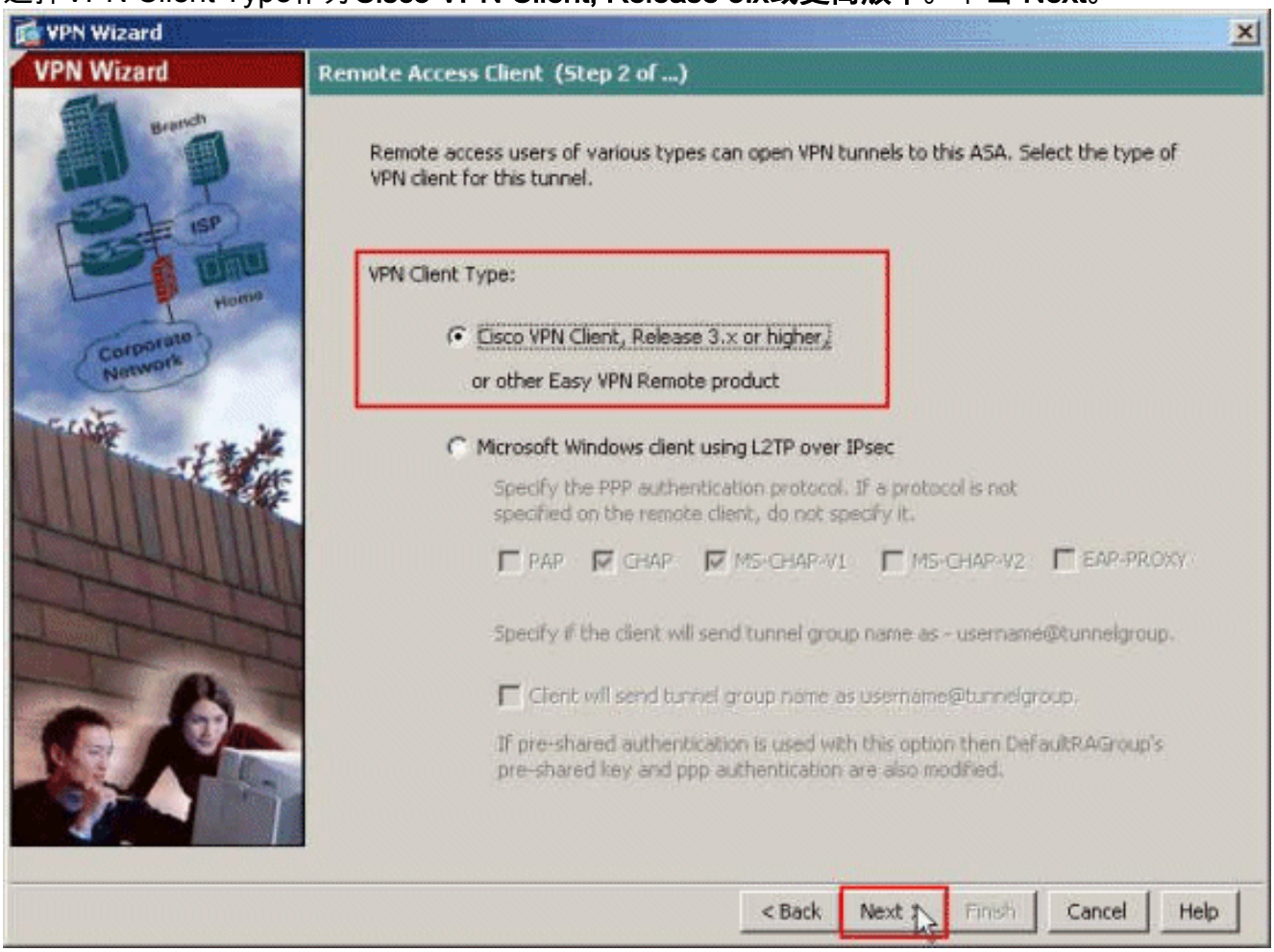
1. 从Home窗口**中选择Wizards > VPN Wizards > IPsec(IKEv1)Remote Access VPN Wizard**。



2. 根据需要**选择VPN Tunnel Interface**(本例中为**Outside**)，并确保选中**Enable inbound IPsec sessions to bypass interface access lists**旁边的复选框。

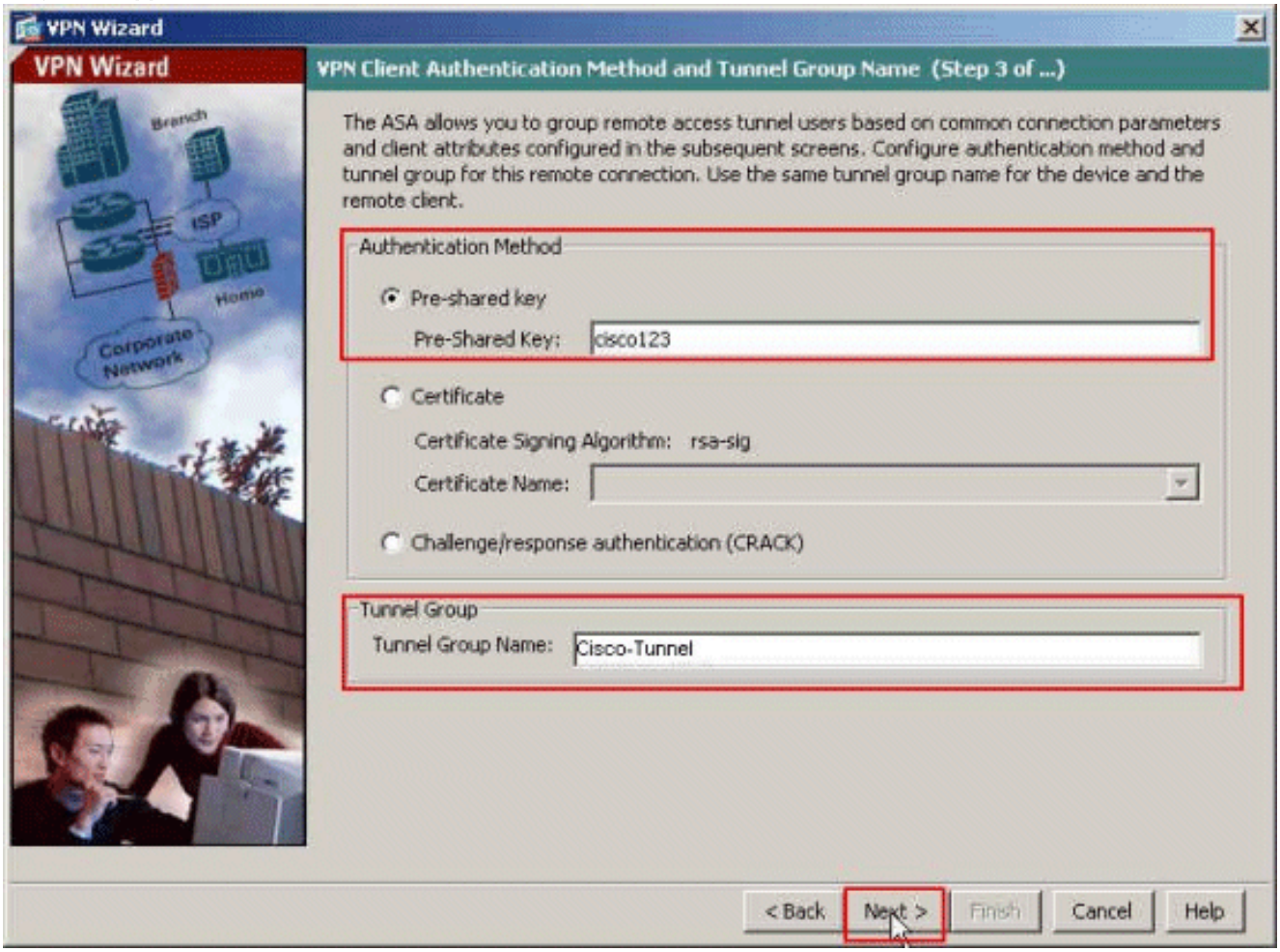


3. 选择VPN Client Type作为**Cisco VPN Client, Release 3.x或更高版本**。单击 **Next**。

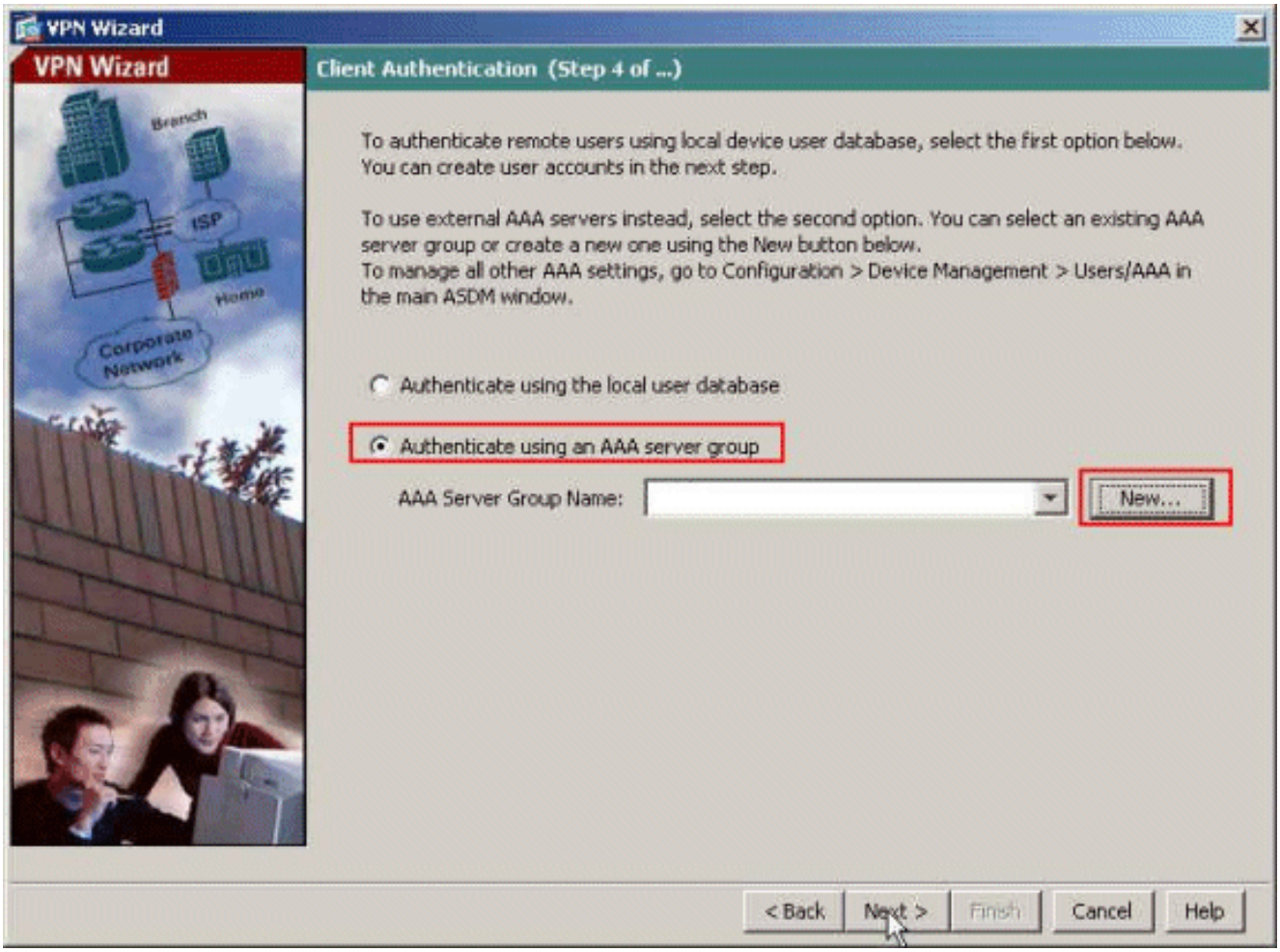


4. 选择“**Authentication Method**”并提供“Authentication”信息。此处使用的身份验证方**法是预共享**

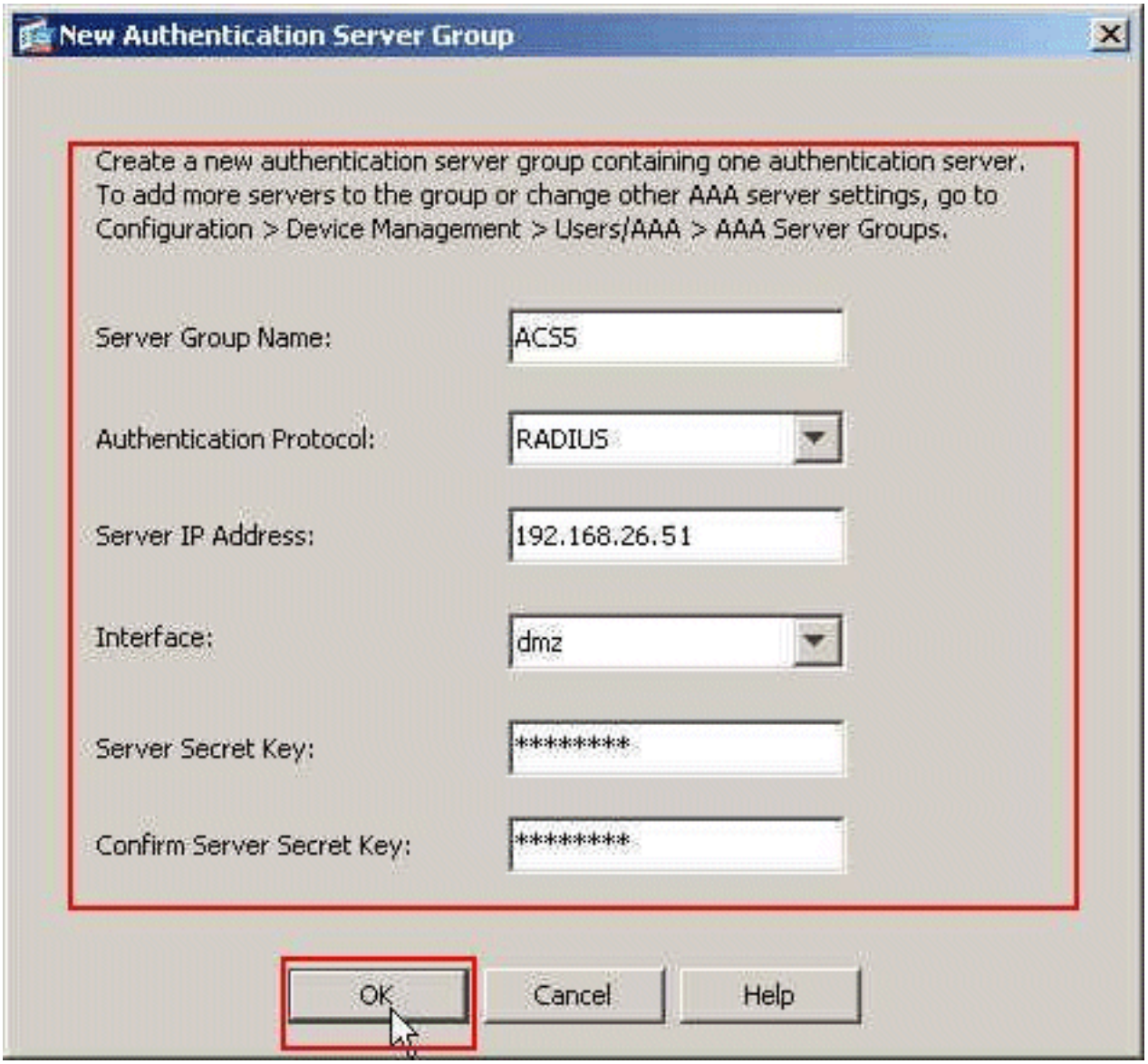
密钥。此外，在提供的空间中提供隧道组名称。此处使用的预共享密钥是cisco123，此处使用的隧道组名称是Cisco-Tunnel。单击 Next。



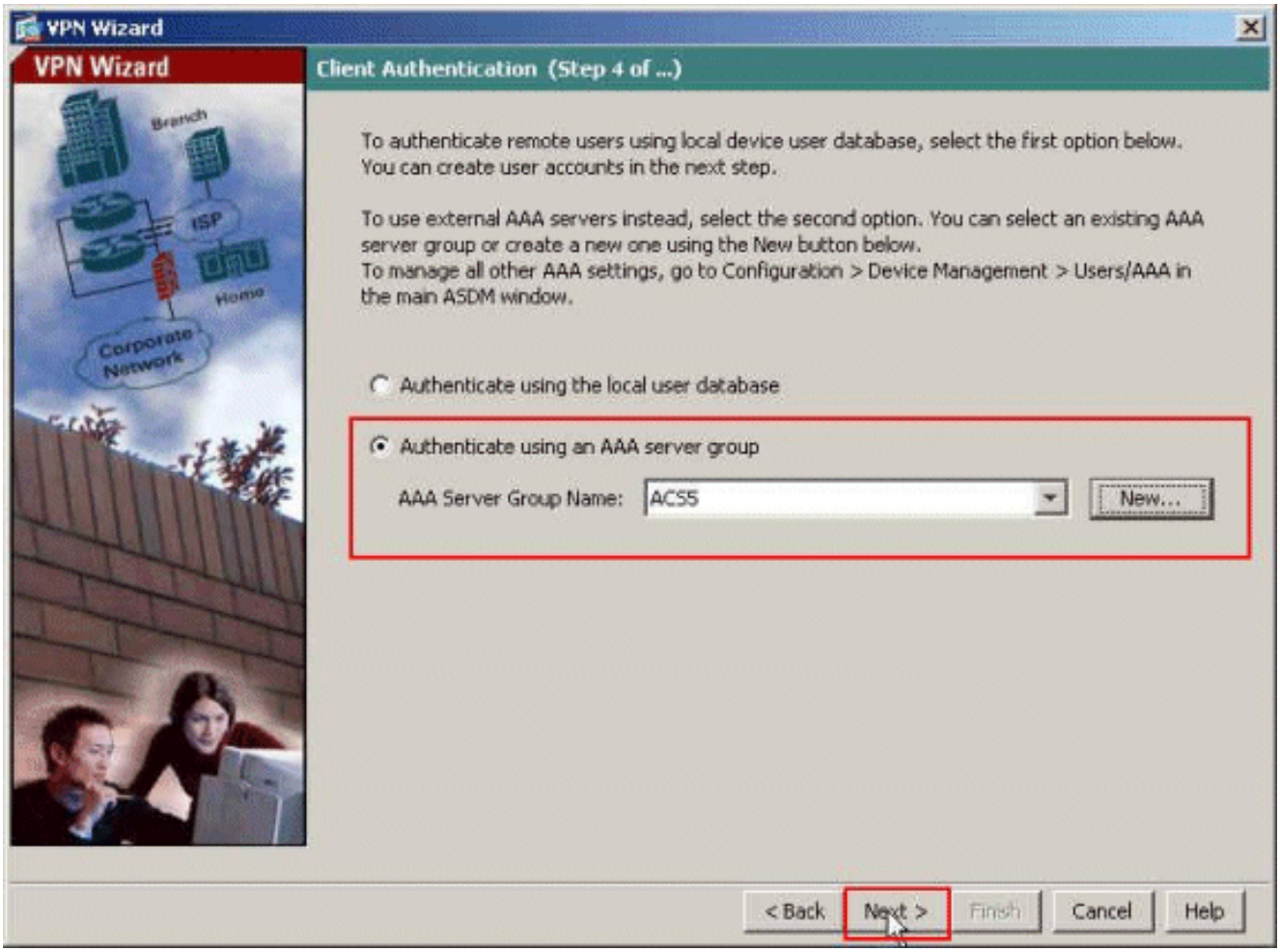
5. 选择是希望使用本地用户数据库对远程用户进行身份验证，还是希望使用外部 AAA 服务器组对远程用户进行身份验证。此处，我们选择**使用AAA服务器组进行身份验证**。单击AAA Server Group Name字段旁边的**New**以创建新的AAA Server Group Name。



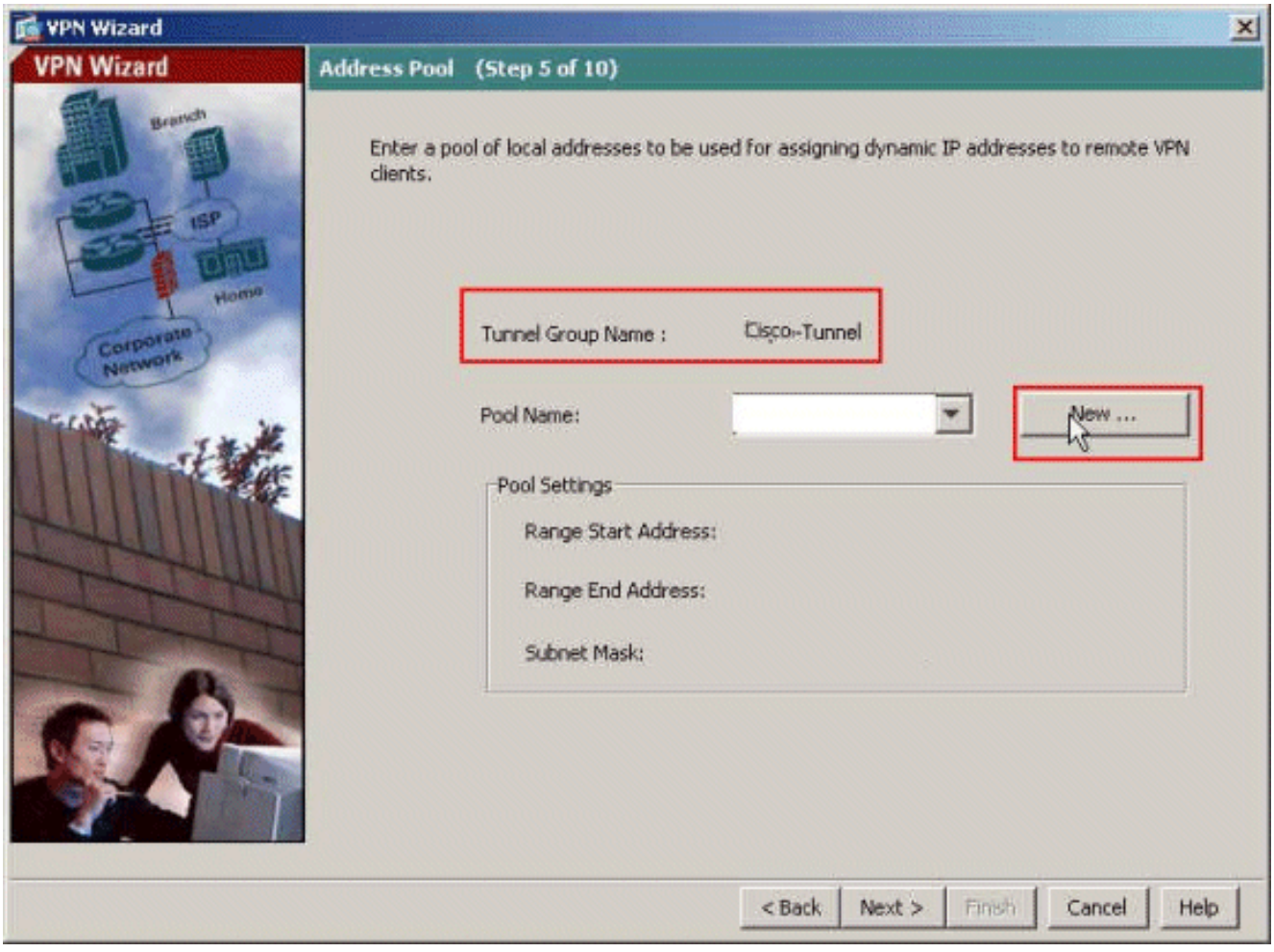
6. 在提供的相应空格中提供服务器组名称、身份验证协议、服务器IP地址、接口名称和服务器密钥，然后单击**确定**。


New Authentication Server Group
Create a new authentication server group containing one authentication server.
To add more servers to the group or change other AAA server settings, go to
Configuration > Device Management > Users/AAA > AAA Server Groups.
Server Group Name:
ACS5
Authentication Protocol:
RADIUS
Server IP Address:
192.168.26.51
Interface:
dmz
Server Secret Key:
****
Confirm Server Secret Key:
****
OK
Cancel
Help

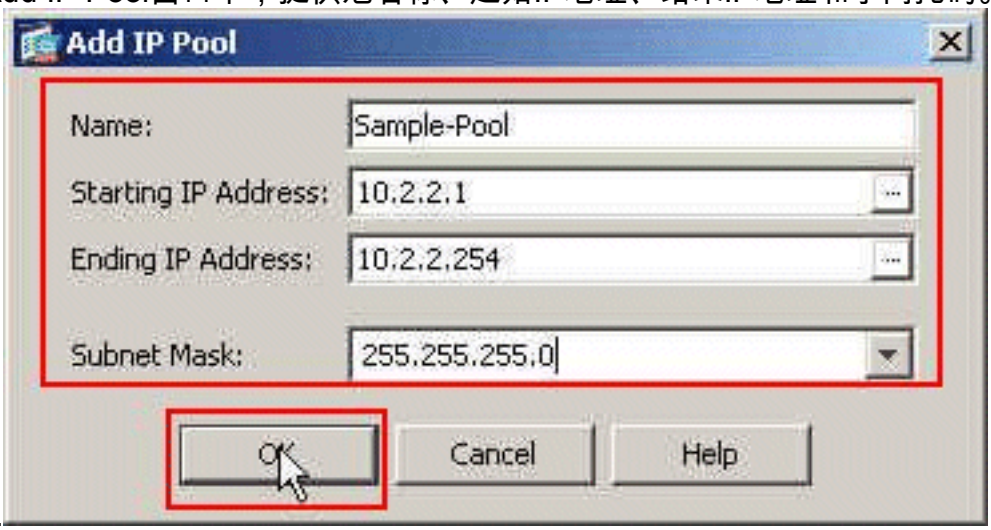
7. 单击 **Next**。



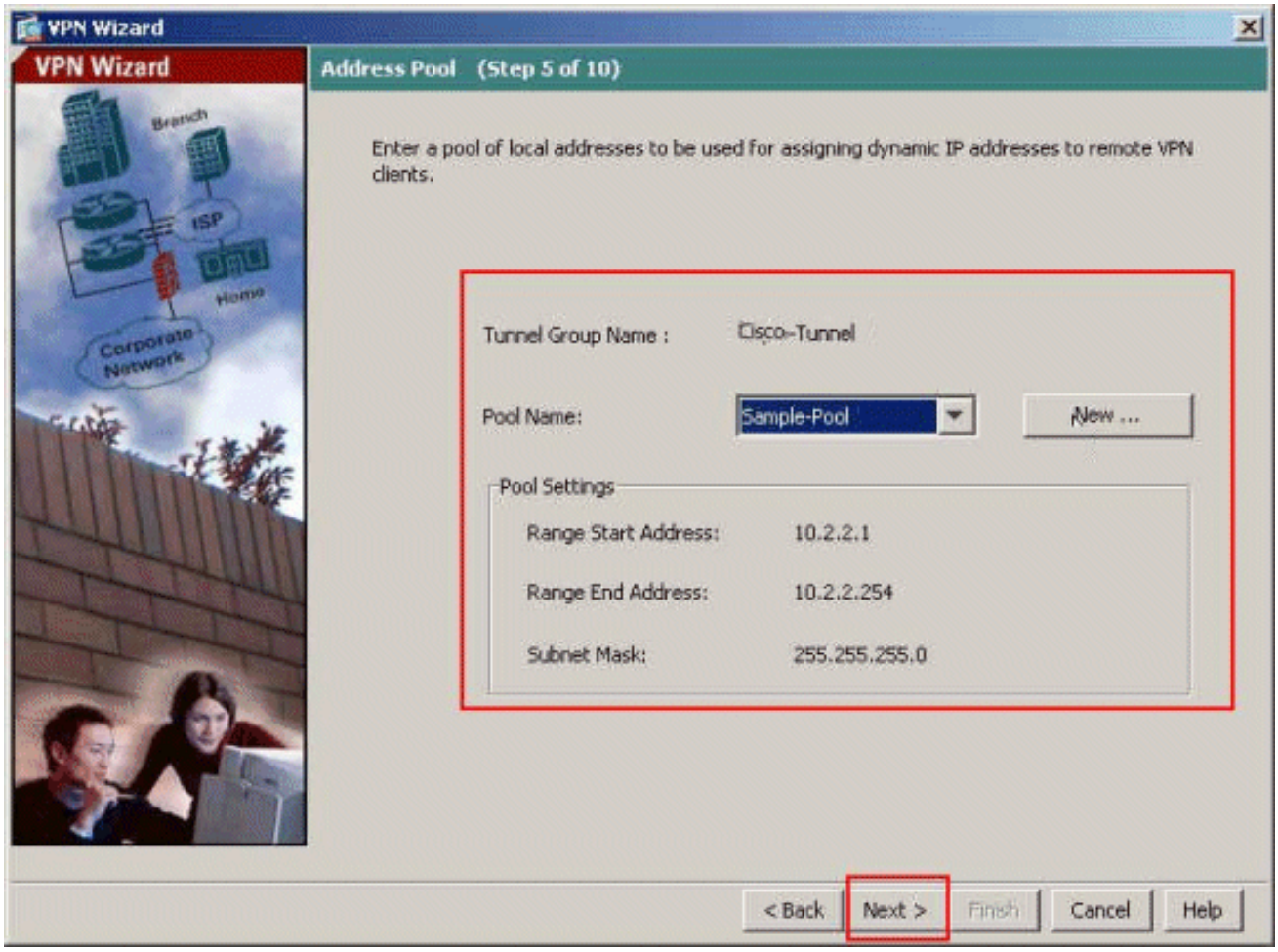
8. 定义一个要在远程 VPN 客户端进行连接时动态分配给它们的本地地址池。单击**New**以创建新的本地地址池。



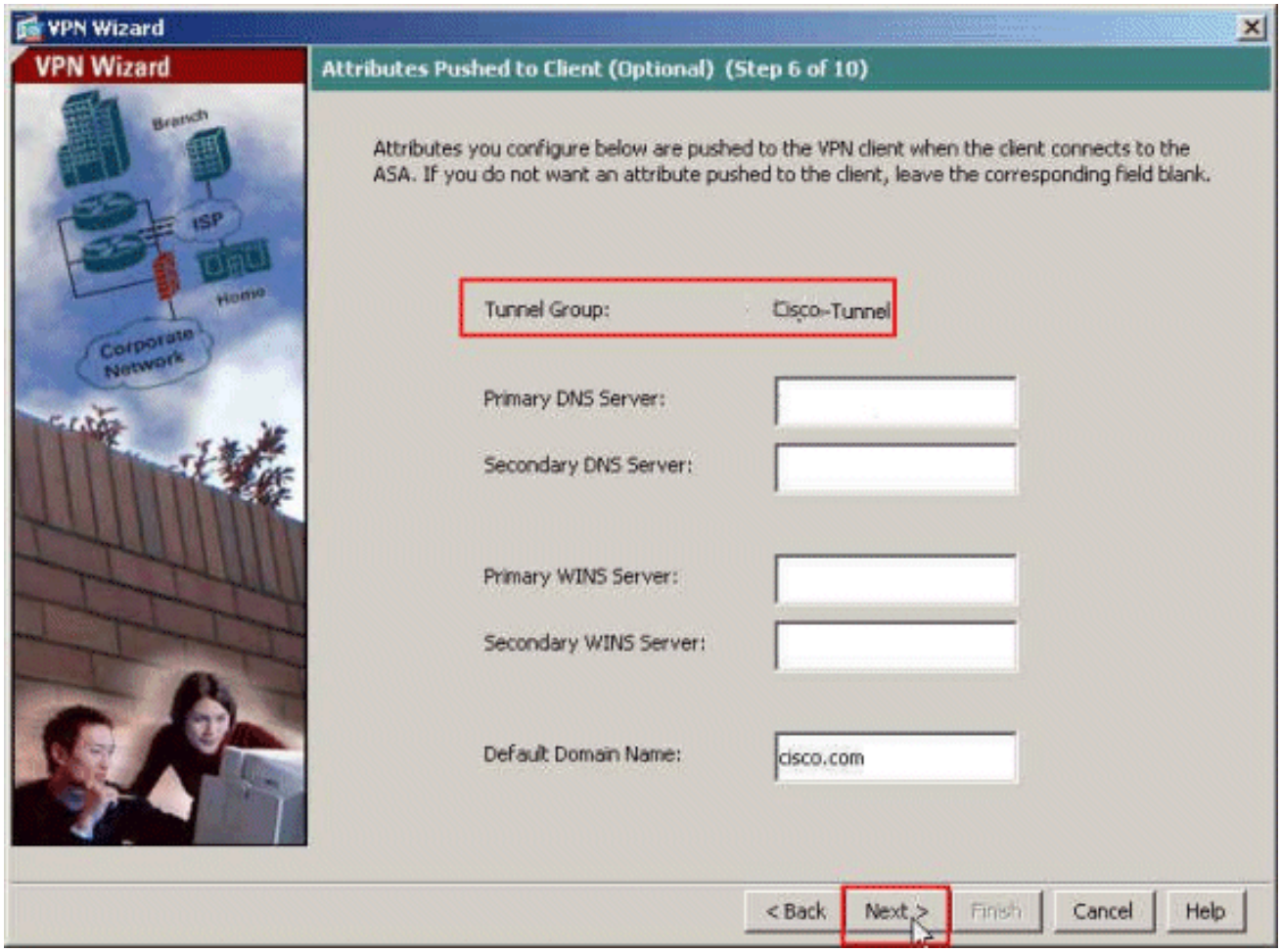
9. 在Add IP Pool窗口中，提供池名称、起始IP地址、结束IP地址和子网掩码。Click OK.



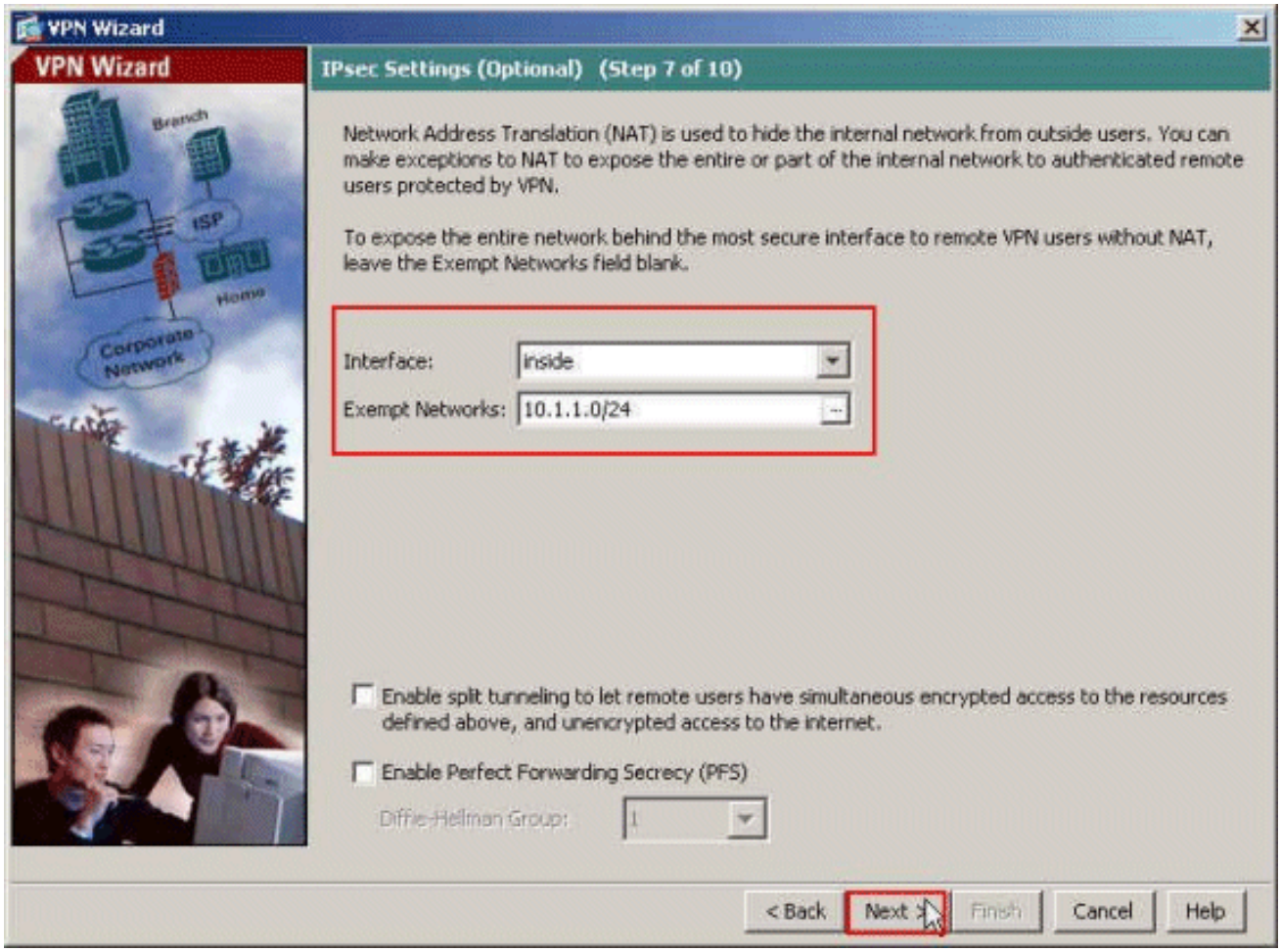
10. 从下拉列表中选择池名称，然后单击“下**一步”**。此示例的池名称是**在步骤**9中创建的Sample-Pool。



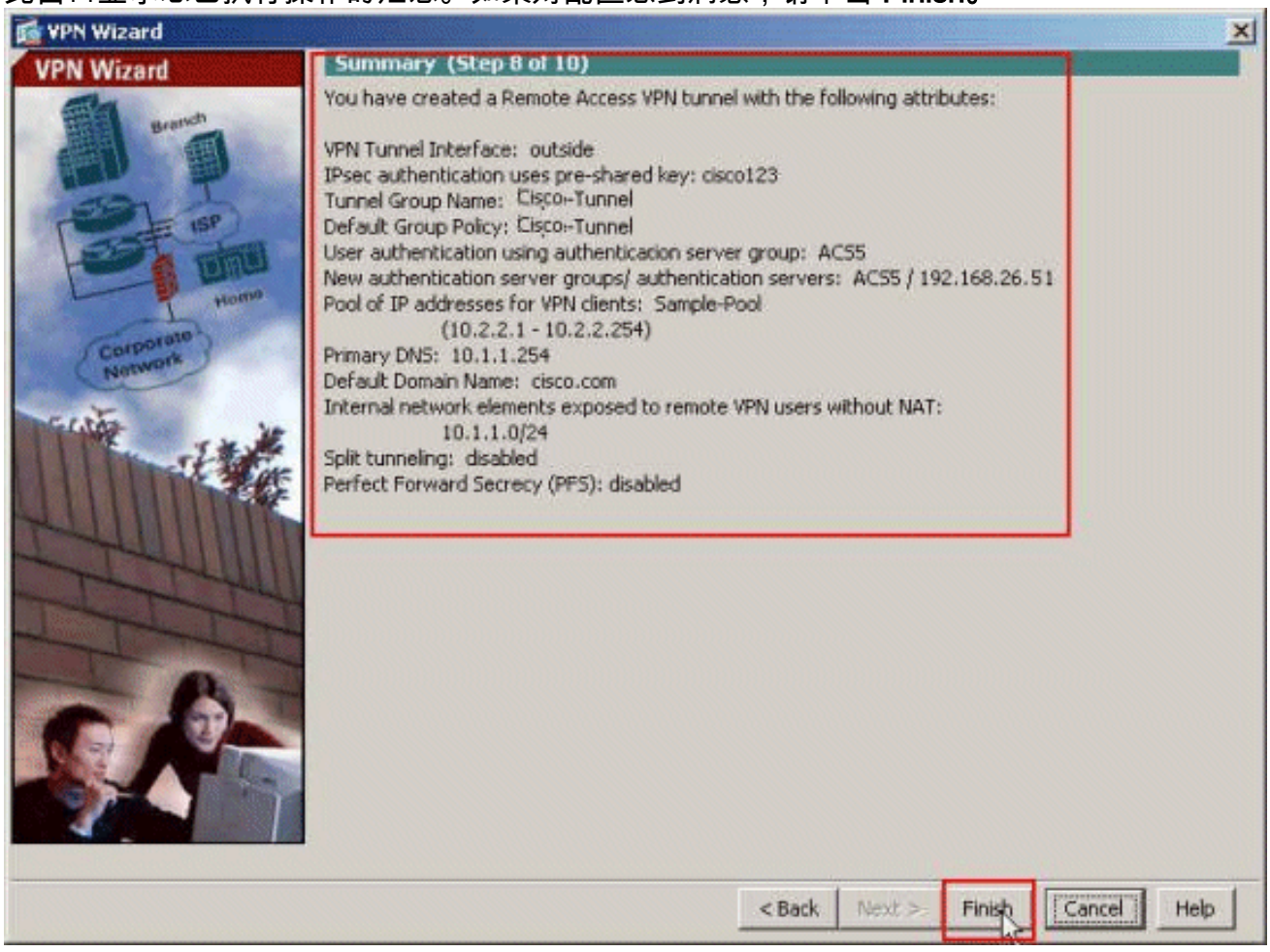
11. *可选：*指定 DNS 和 WINS 服务器信息以及将被推送到远程 VPN 客户端的默认域名。



12. 指定哪些内部主机或网络（如果有）应向远程 VPN 用户公开。在Exempt Networks字段中提供接口名称和要免除的网络后，单击**Next**。如果将此列表留空，则将允许远程 VPN 用户访问 ASA 的整个内部网络。您还可以在此窗口上启用分割隧道。分割隧道对发往本过程中前面所定义的资源的数据流进行加密，并通过不以隧道形式传输该数据流提供对整个 Internet 的未加密访问。如果*未启用分割隧道，则来自远程 VPN 用户的所有数据流将通过隧道传输到 ASA*。这可能导致很高的带宽和处理器使用率，具体取决于您的配置。



13. 此窗口显示您已执行操作的汇总。如果对配置感到满意，请单击 **Finish**。



使用CLI配置ASA

以下是CLI配置：

ASA 设备上的运行配置

```
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#
```

为适用于个人用户的可下载 ACL 配置 ACS

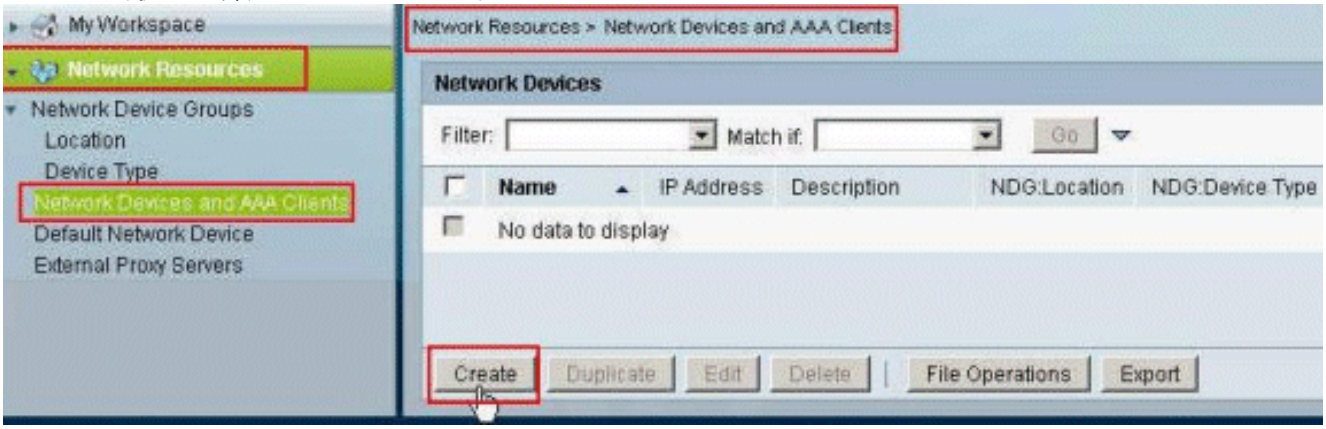
您可以将Cisco Secure ACS 5.x上的可下载访问列表配置为命名权限对象，然后将其分配给授权配置文件，该配置文件将在访问服务中规则的结果部分中选择。

在本示例中，IPsec VPN用户**cisco**成功进行身份验证，并且RADIUS服务器向安全设备发送可下载的访问列表。用户“cisco”只能访问 10.1.1.2 服务器，拒绝其他所有访问。要检验ACL，请参阅

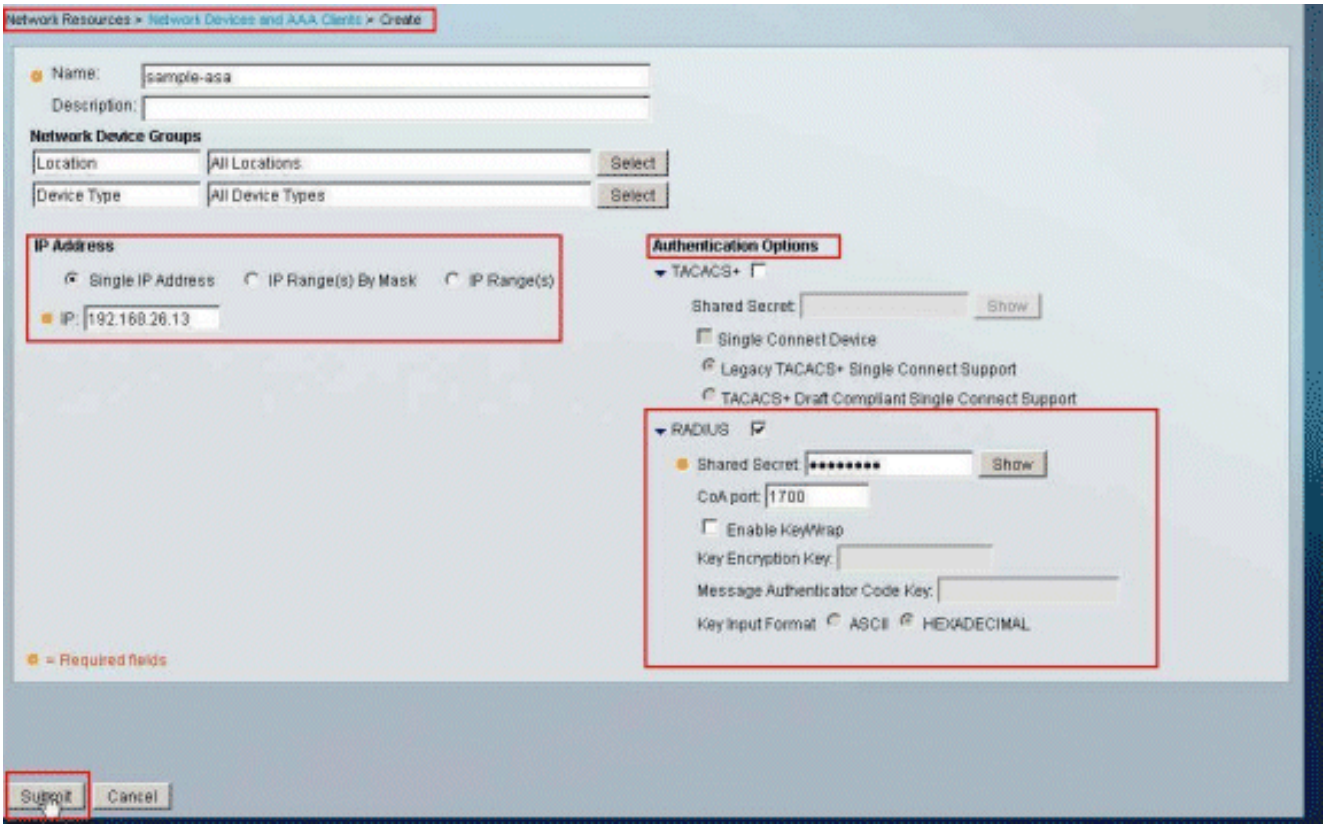
User/Group的Downloadable ACL部分。

要在思科安全ACS 5.x中配置RADIUS客户端，请完成以下步骤：

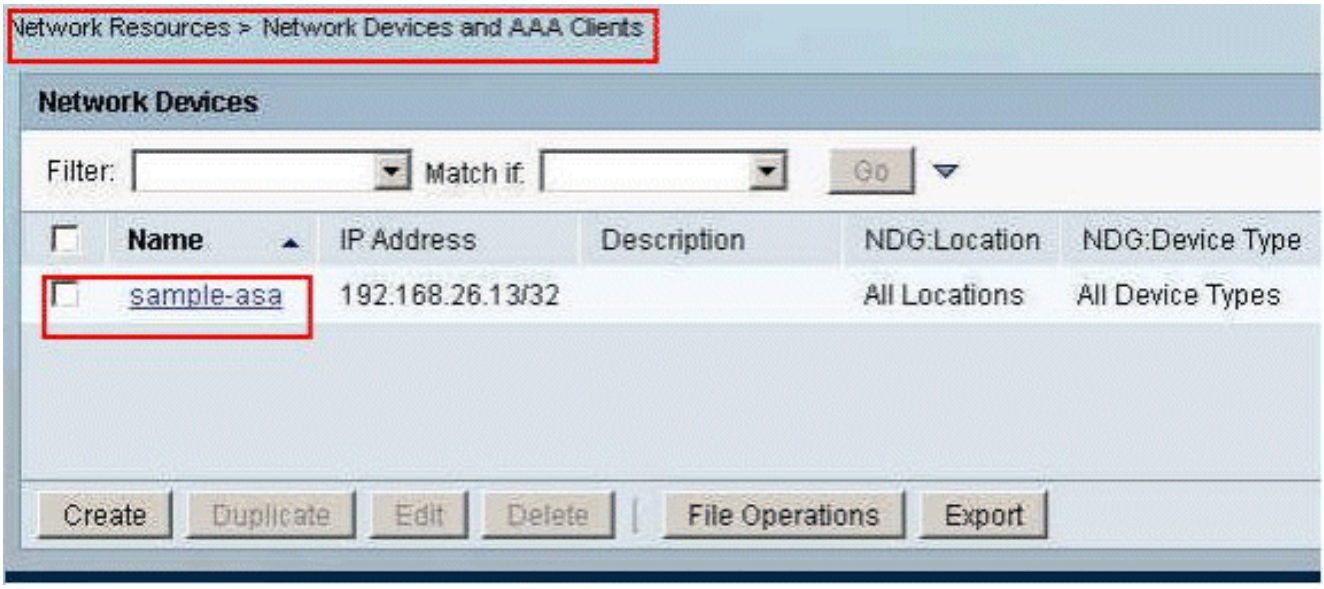
1. 选择**Network Resources > Network Devices and AAA Clients**，然后单击**Create**以在RADIUS服务器数据库中为ASA添加条目。



2. 输入ASA的本地有效名称(**示例 — asa**，在本例中)，然后在**IP address字段中**输入192.168.26.13。通过选中**RADIUS**复选框在“身份验证选项”部分选择**RADIUS**，并在“共享密钥”字段中输入**cisco123**。单击“Submit”。

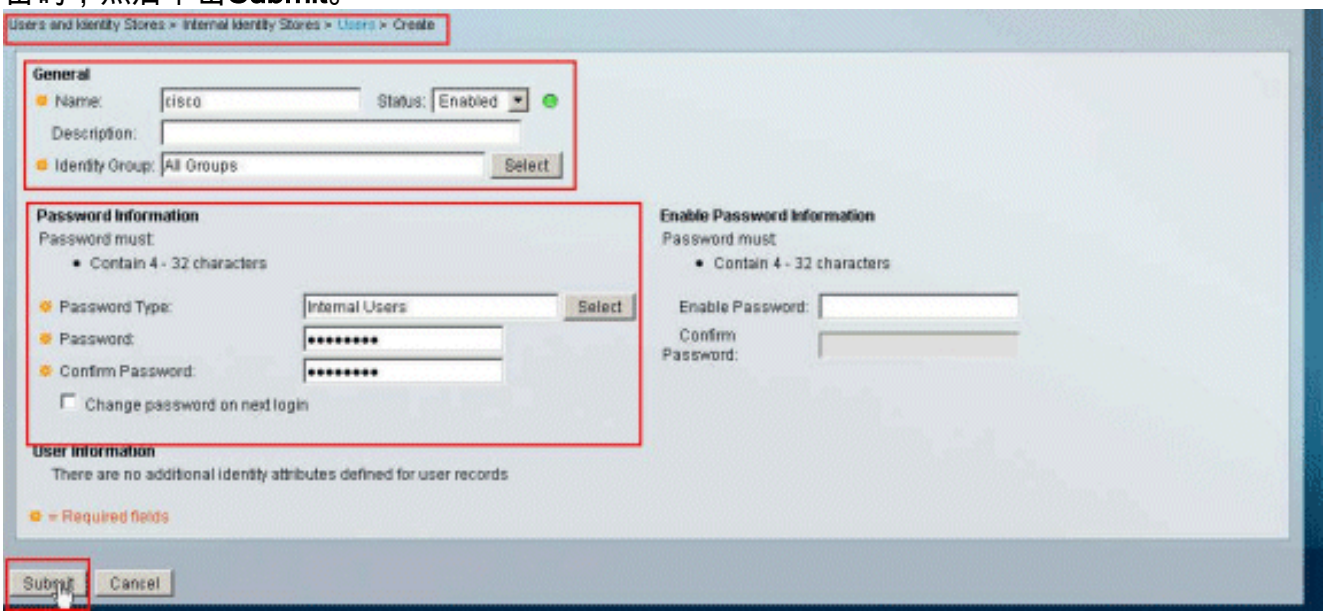


3. ASA已成功添加到RADIUS服务器(ACS)数据库。

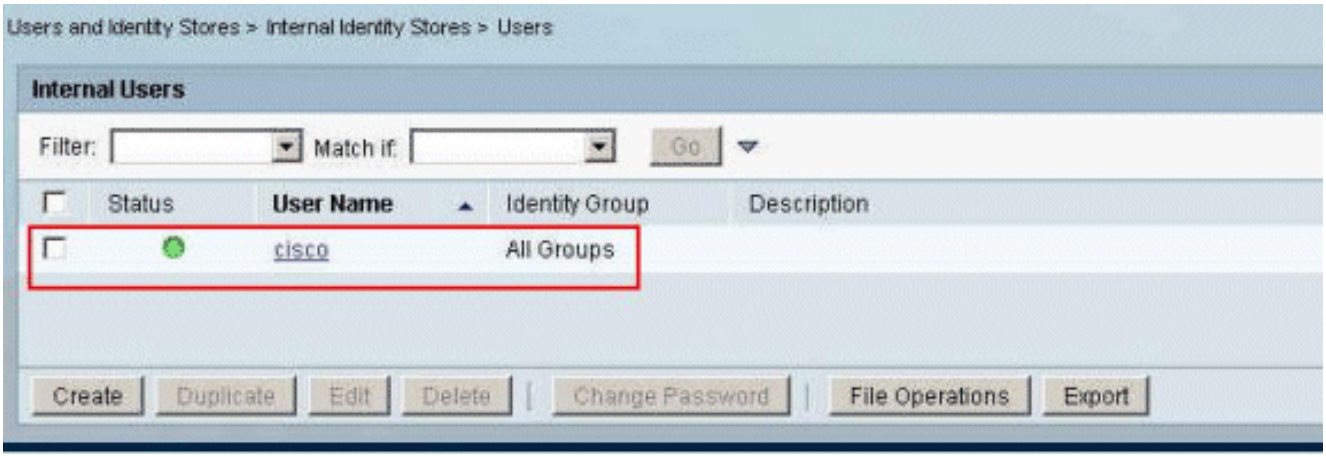


4. 选择**Users and Identity Stores > Internal Identity Stores > Users**，然后单击**Create**，以便在ACS的本地数据库中创建用户以进行VPN身份验证。

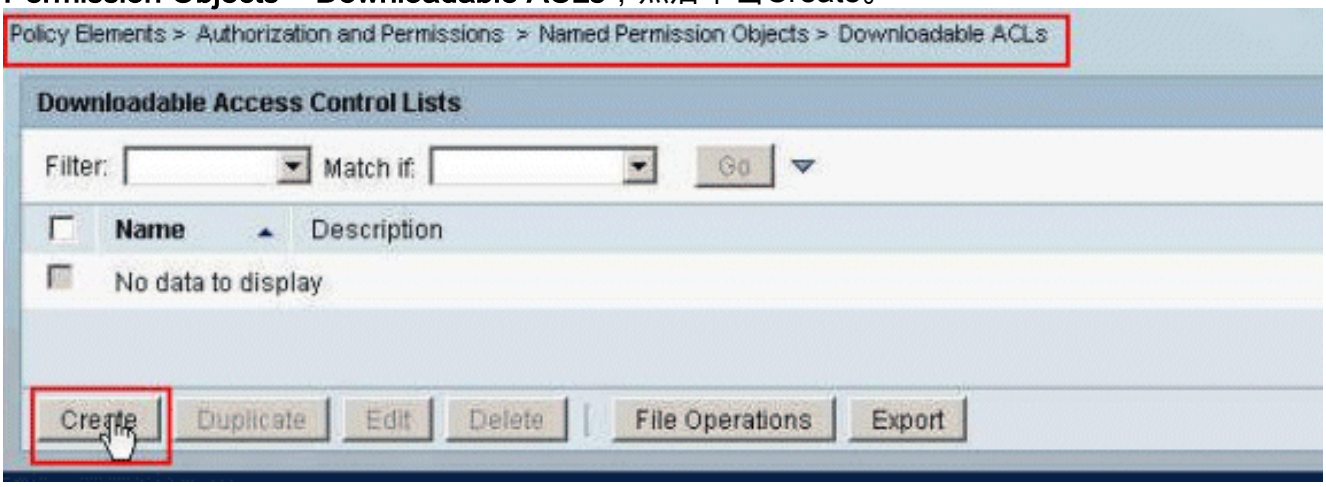
5. 输入用户名**cisco**。选择密码类型**为Internal Users**，然后输入密码(**本例中**为cisco123)。 确认密码，然后单击**Submit**。



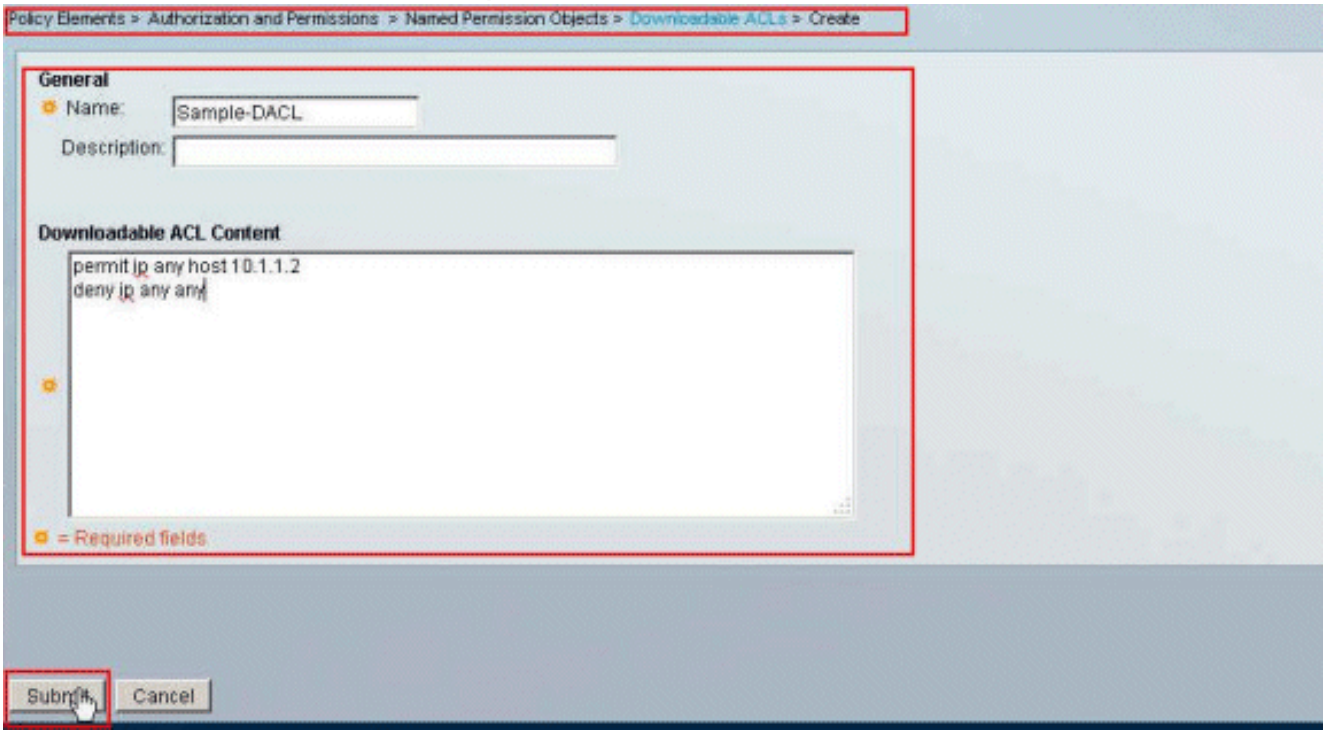
6. 已成功**创**建用户cisco。



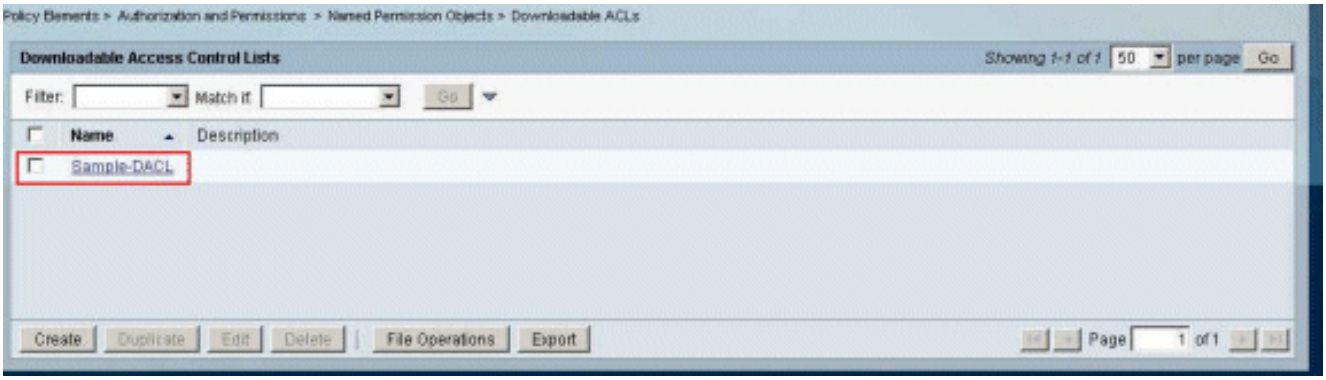
7. 要创建可下载ACL，请选择**Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs**，然后单击Create。



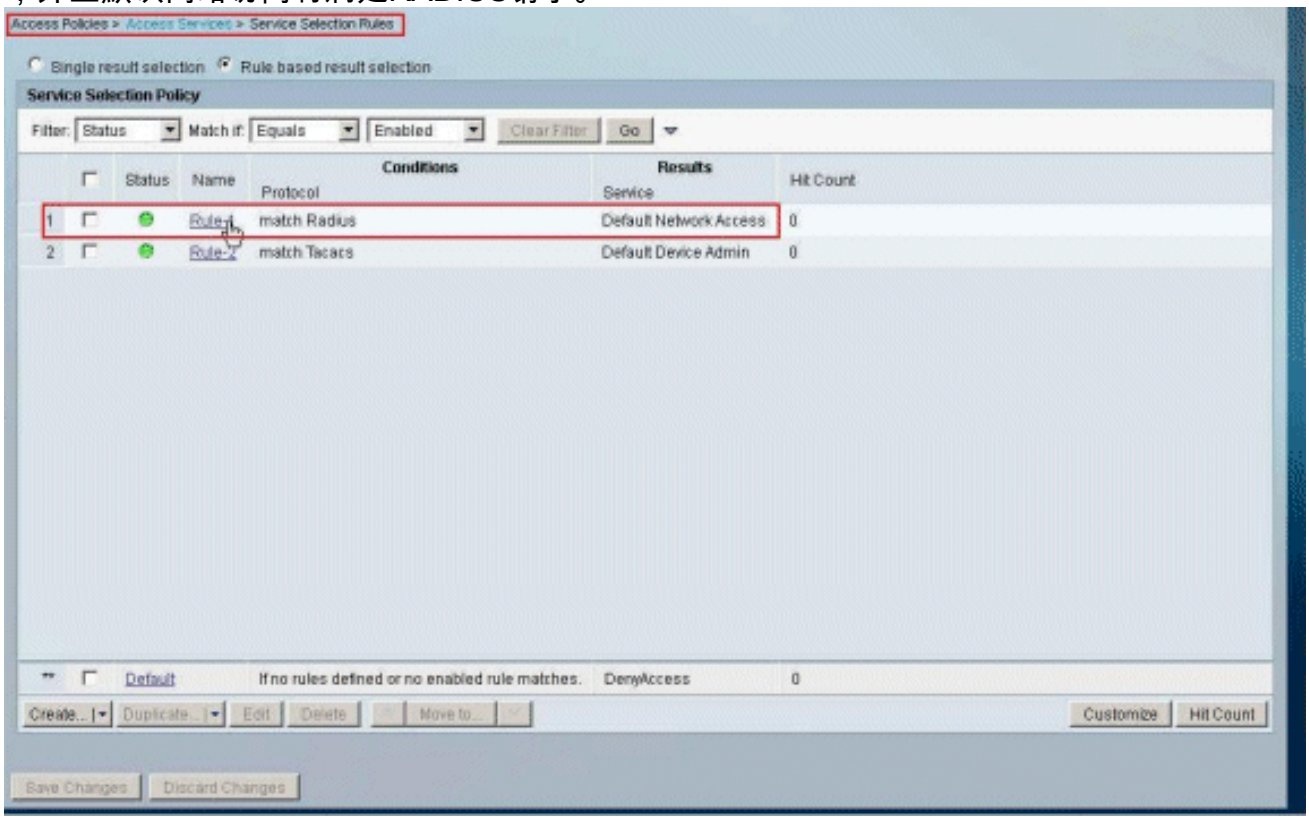
8. 提供**可下**载ACL的名称以及ACL**内容**。单击“Submit”。



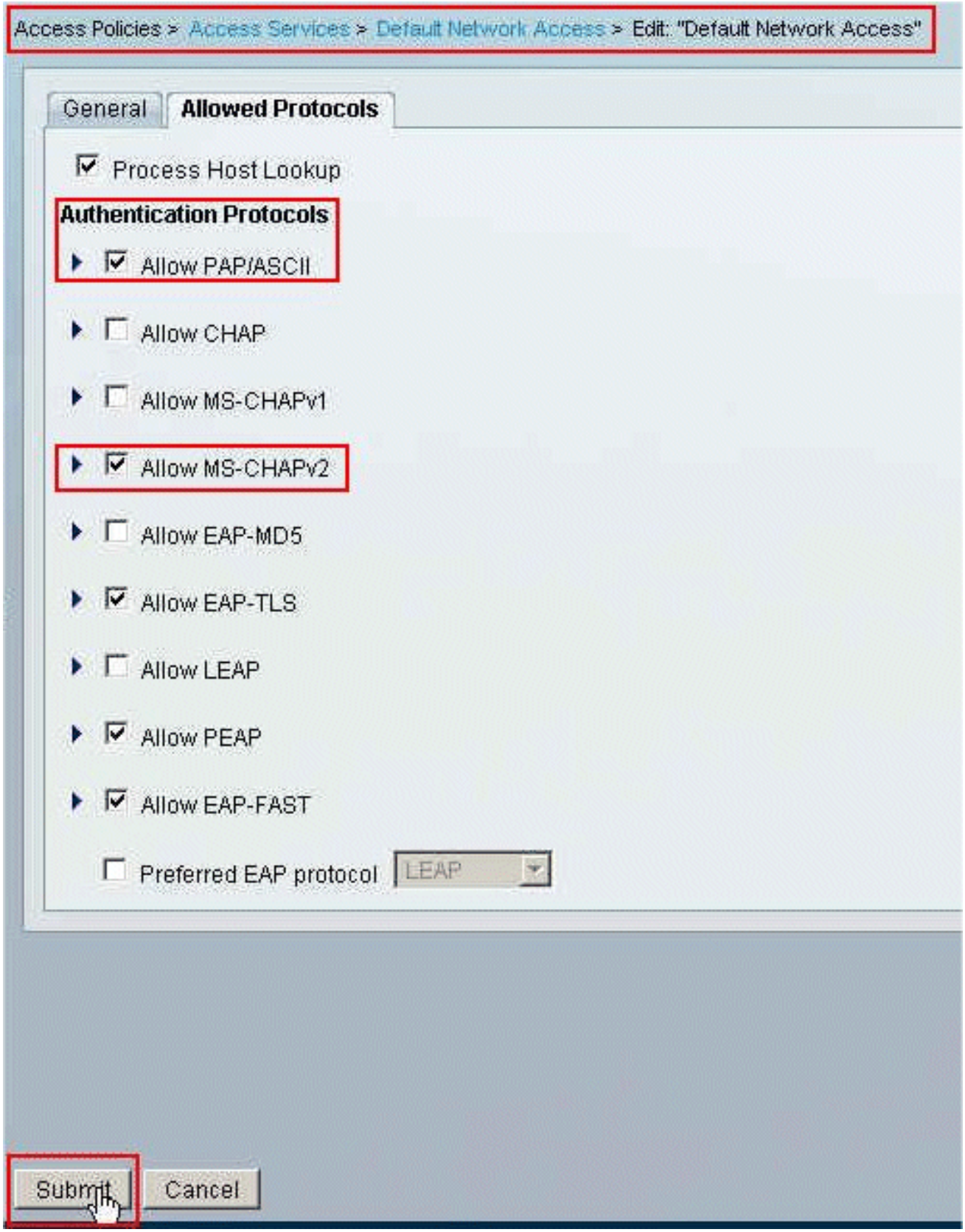
9. 已成功创**建可下载**ACL Sample-DACL。



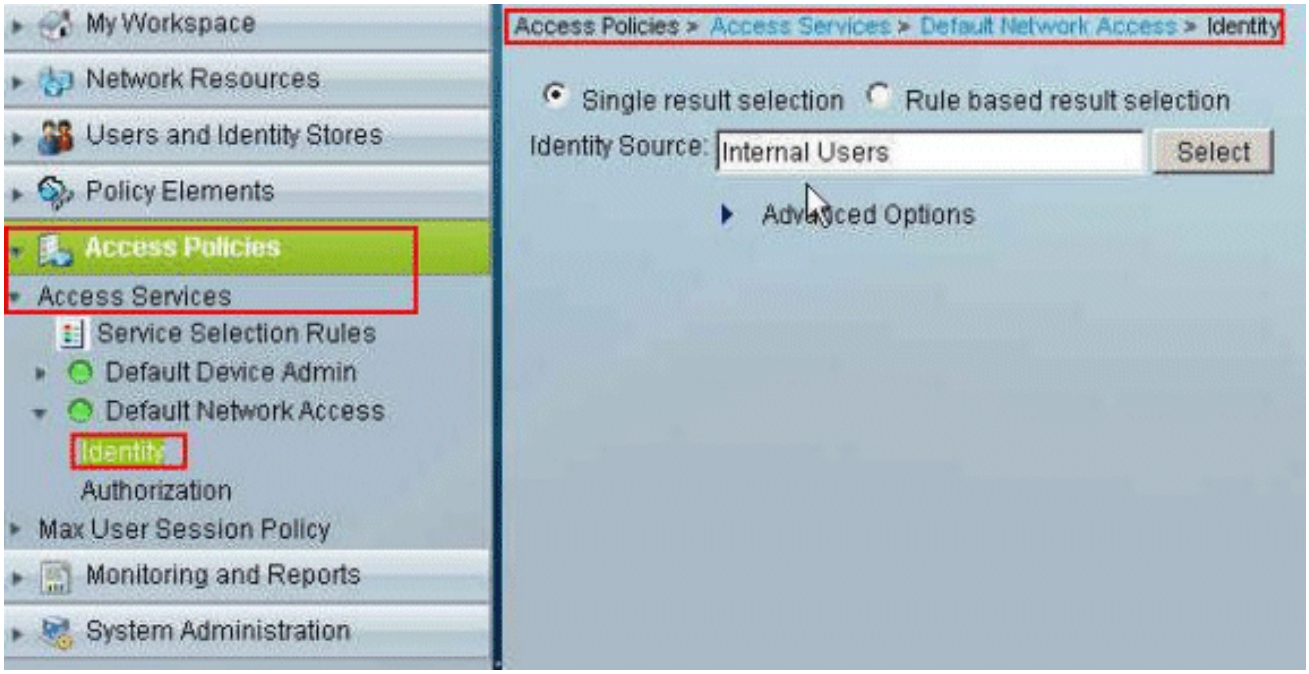
10. 要配置VPN身份验证的访问策略，请选择**Access Policies > Access Services > Service Selection Rules**，并确定哪个服务符合RADIUS协议。在本示例中，**规则1与RADIUS匹配**，并且默认网络访问将满足RADIUS请求。



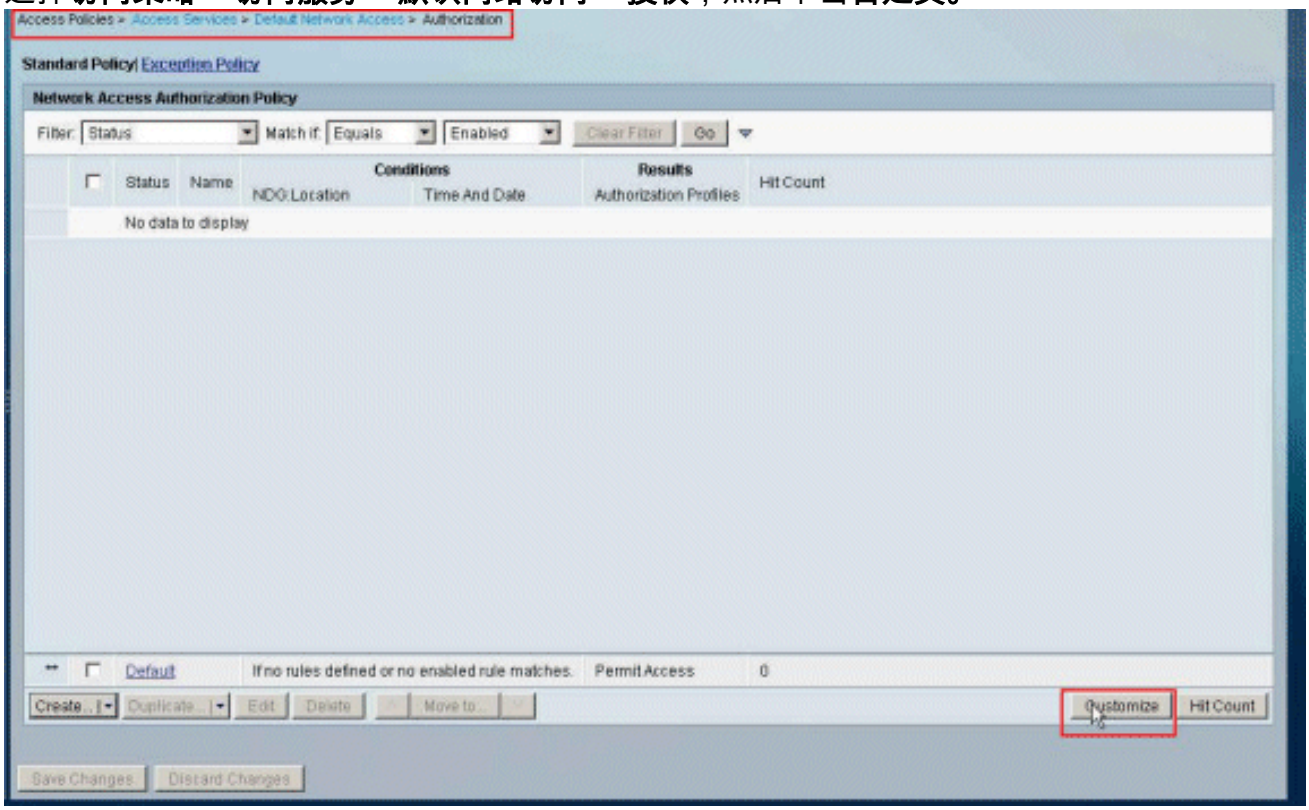
11. 选择步**骤10**中确定的访问服务。在本例中，**使用默认**网络访问。选择“**允许的协**议”选项卡，并确**保选择“允许PAP/ASCII”和“允许MS-CHAPv2”。单击“提交”**。



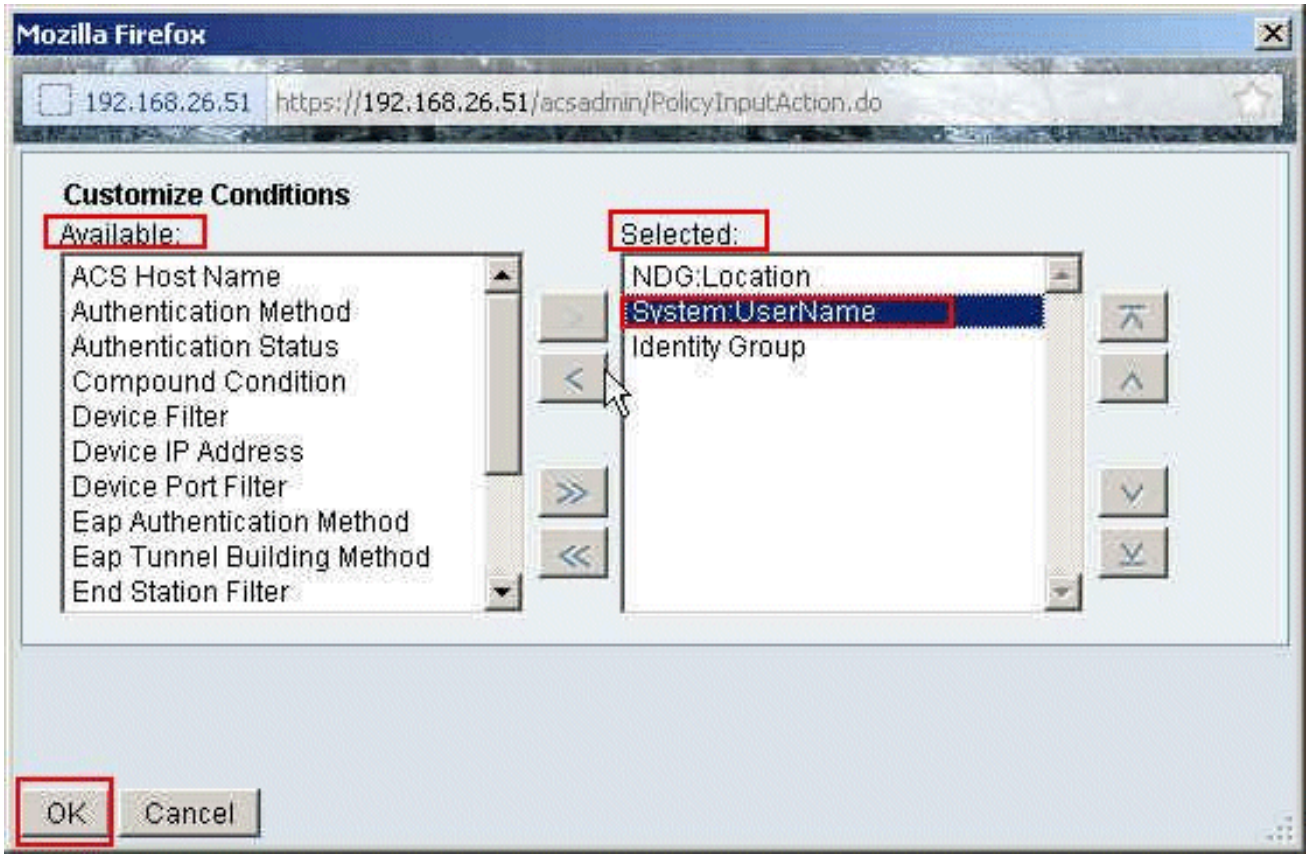
12. 单击访**问服务**的“身**份”部**分，并确保已选**择“内部用户**”作为身份源。在本例中，我们采用了默认网络访问。



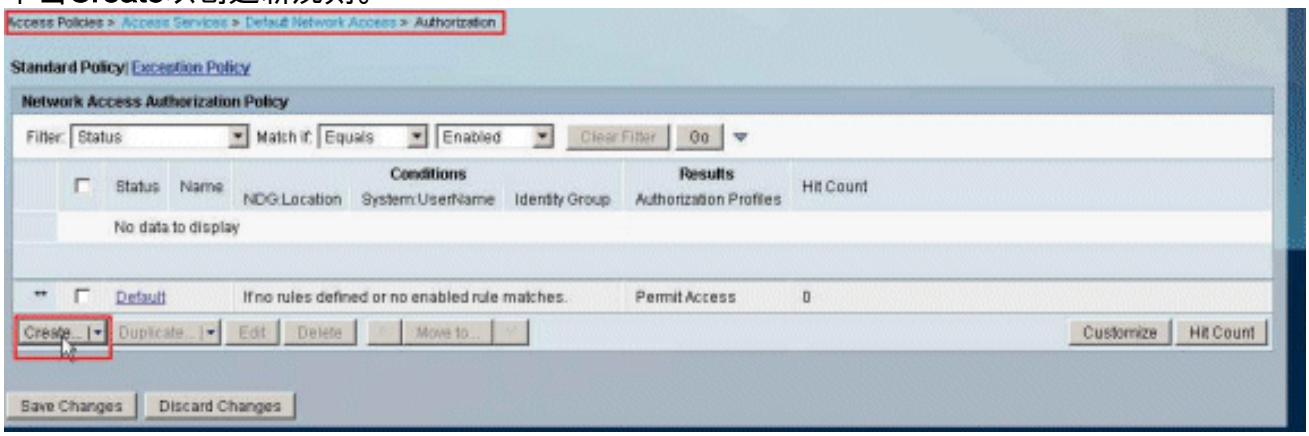
13. 选择**访问策略 > 访问服务 > 默认网络访问 > 授权**，然后单击**自定义。**



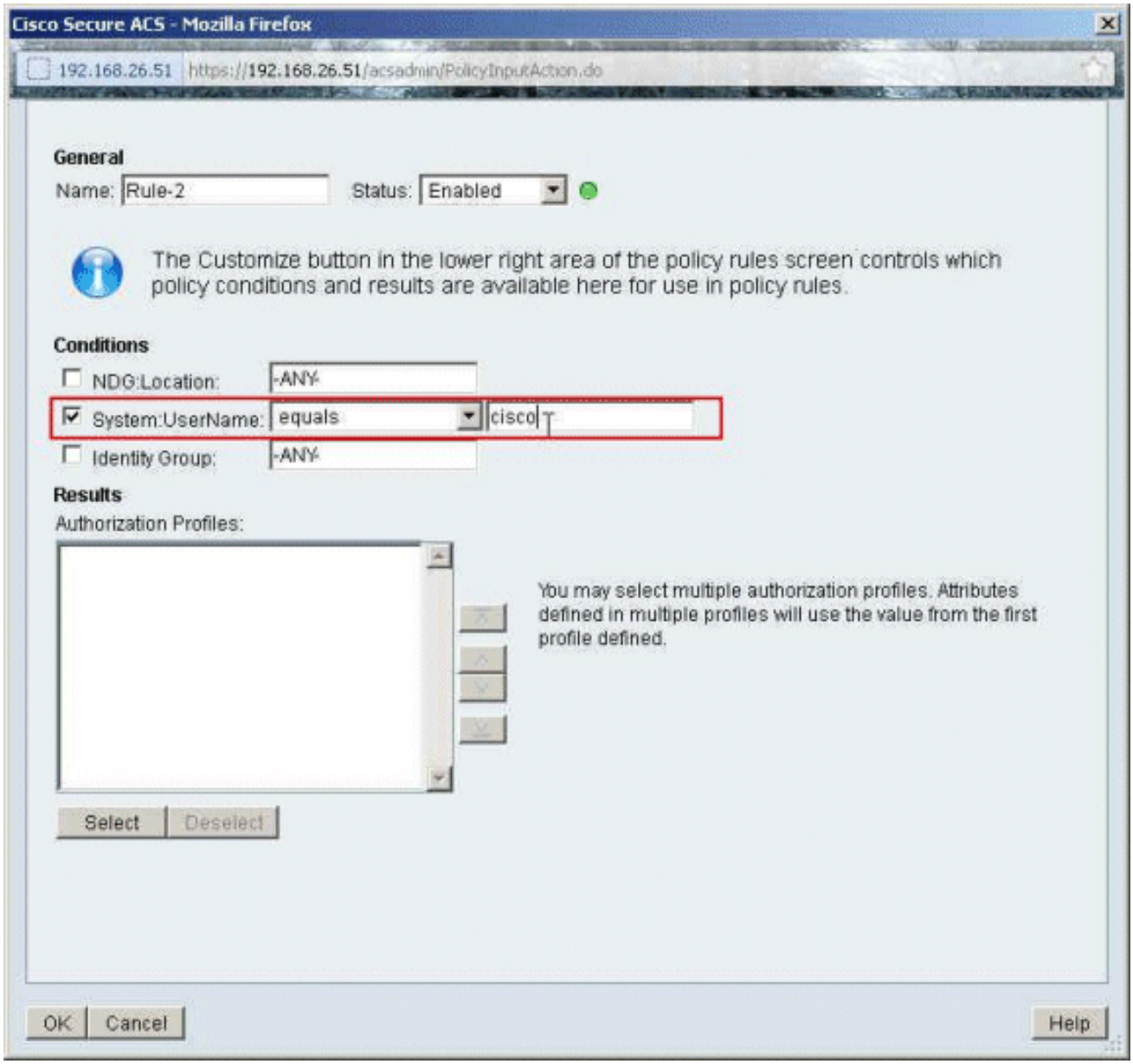
14. 将**System:UserName**从“**Available**”**列移**到“Selected”列，然后单击**“OK”。**



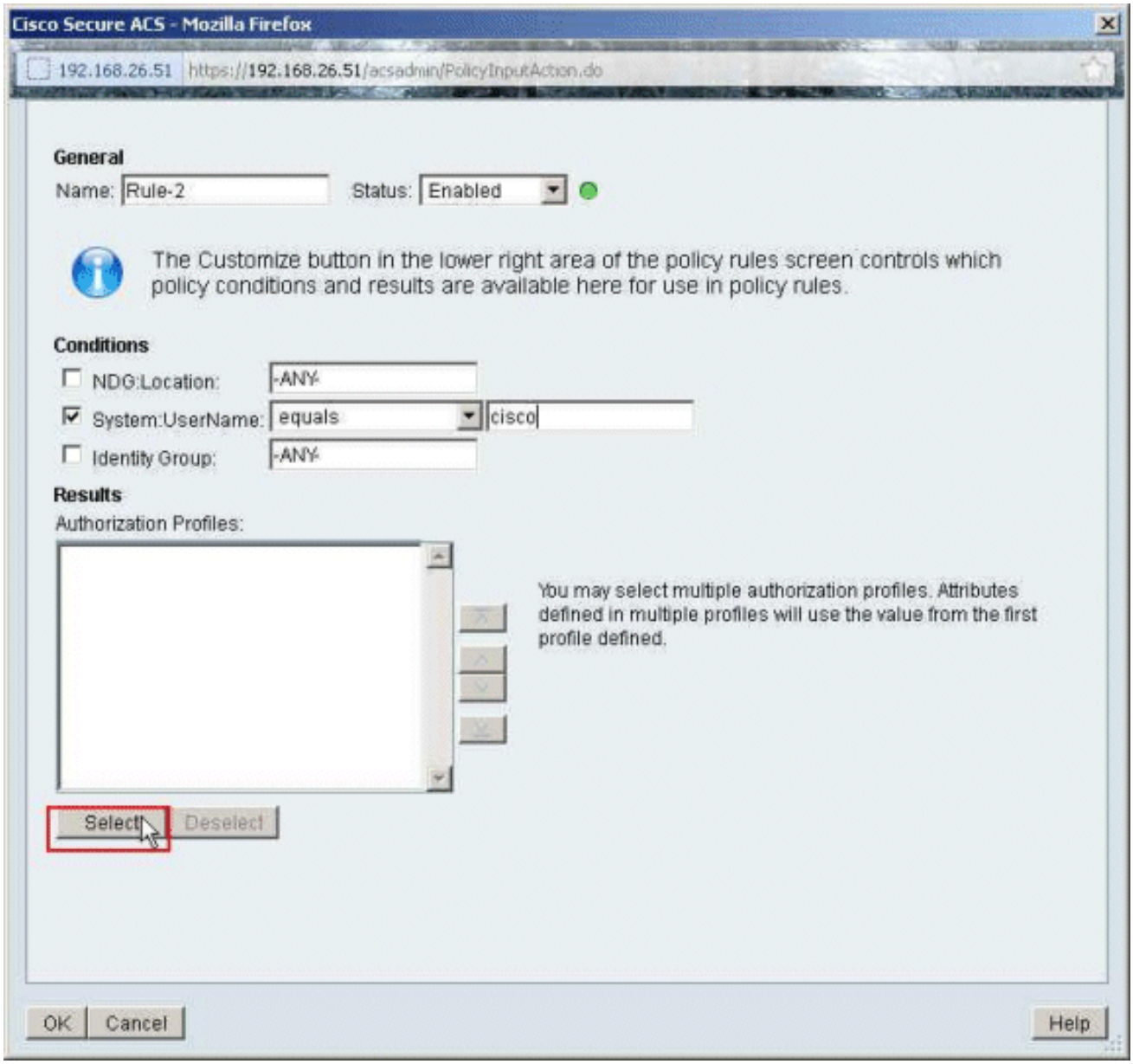
15. 单击**Create**以创建新规则。



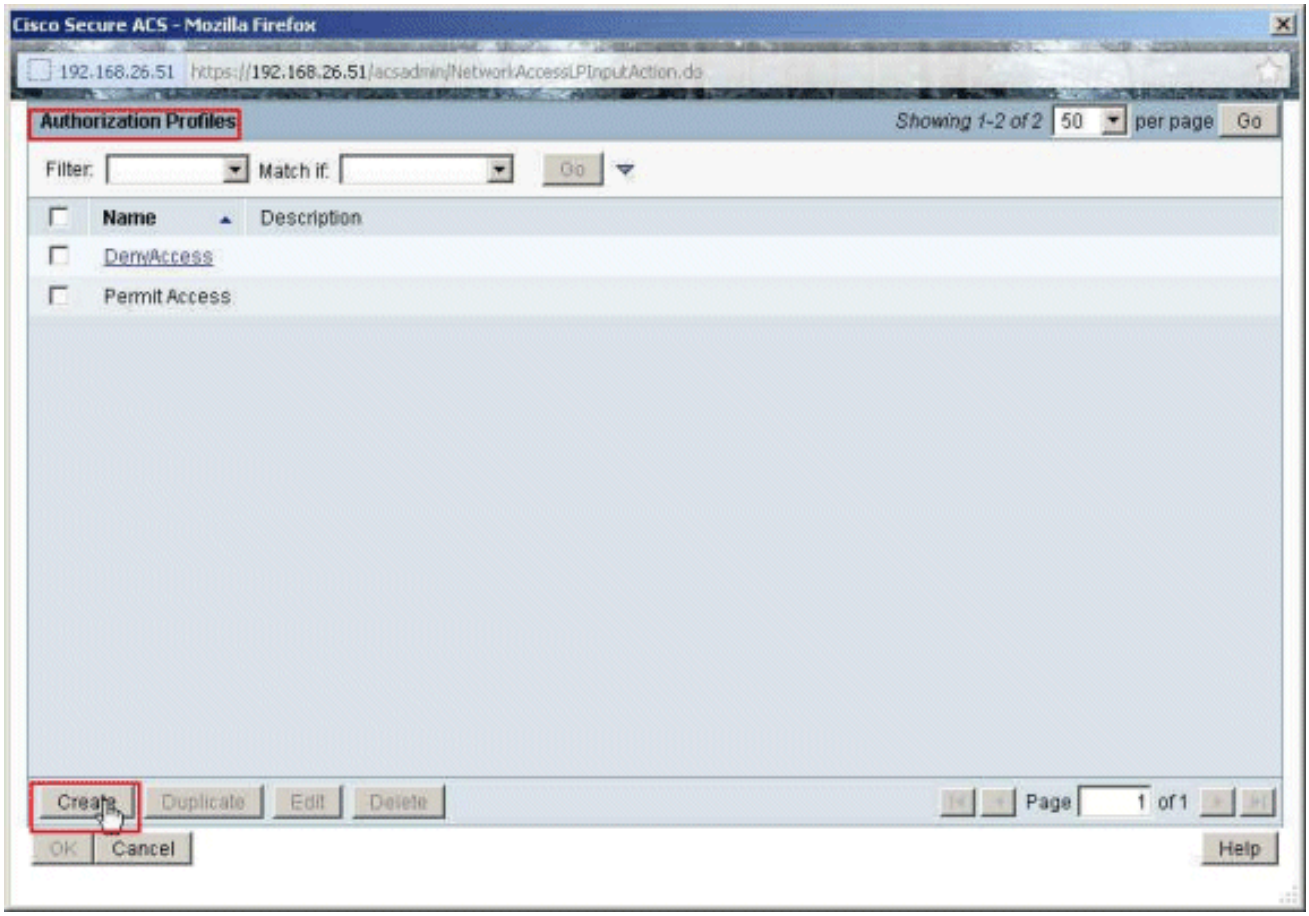
16. 确保选中“System:UserName（**系统：用户名**）”旁边的复选框，从下拉列表中选择**equals**，然后输入用户名**cisco**。


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

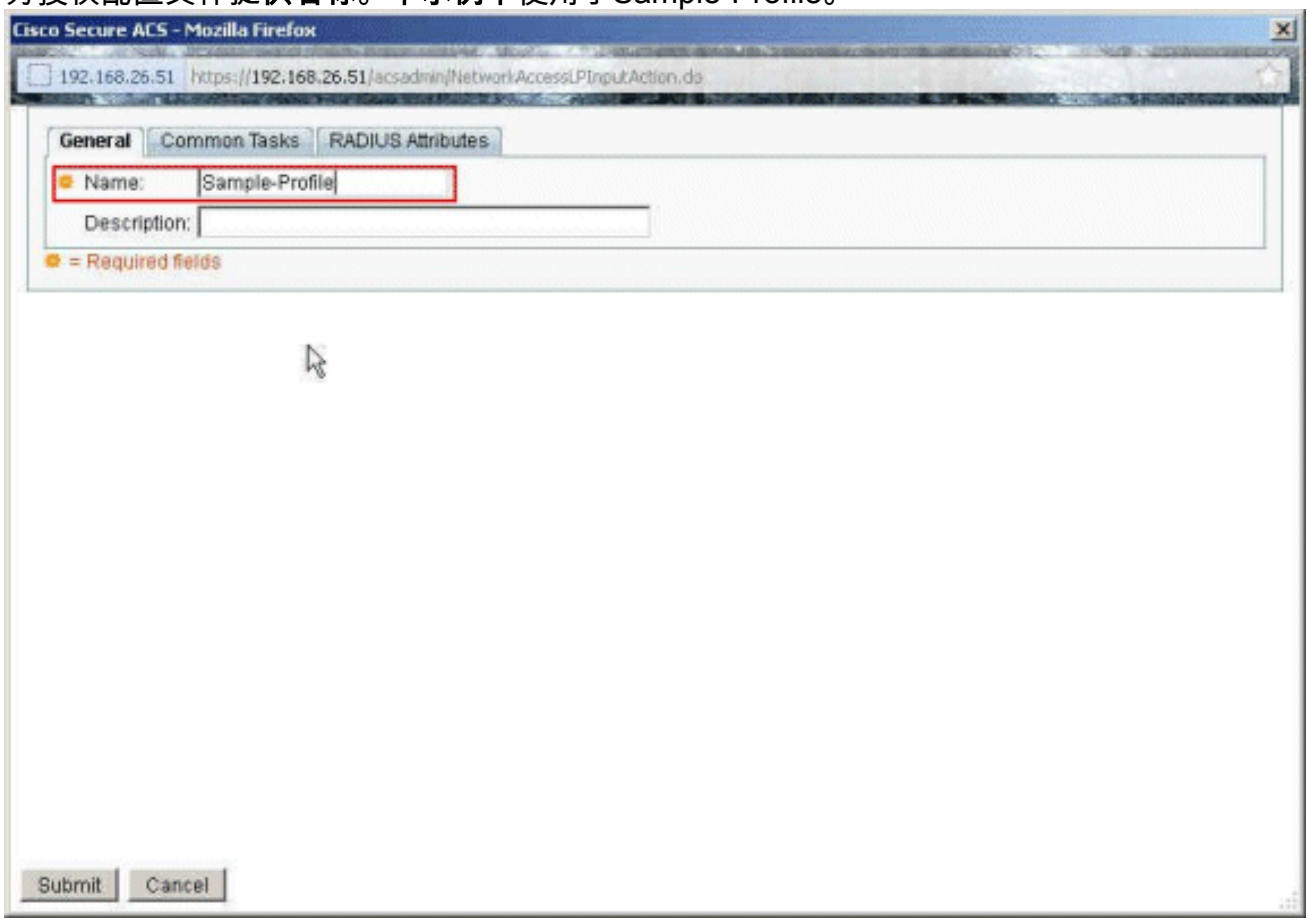
17. 单击**选择**。



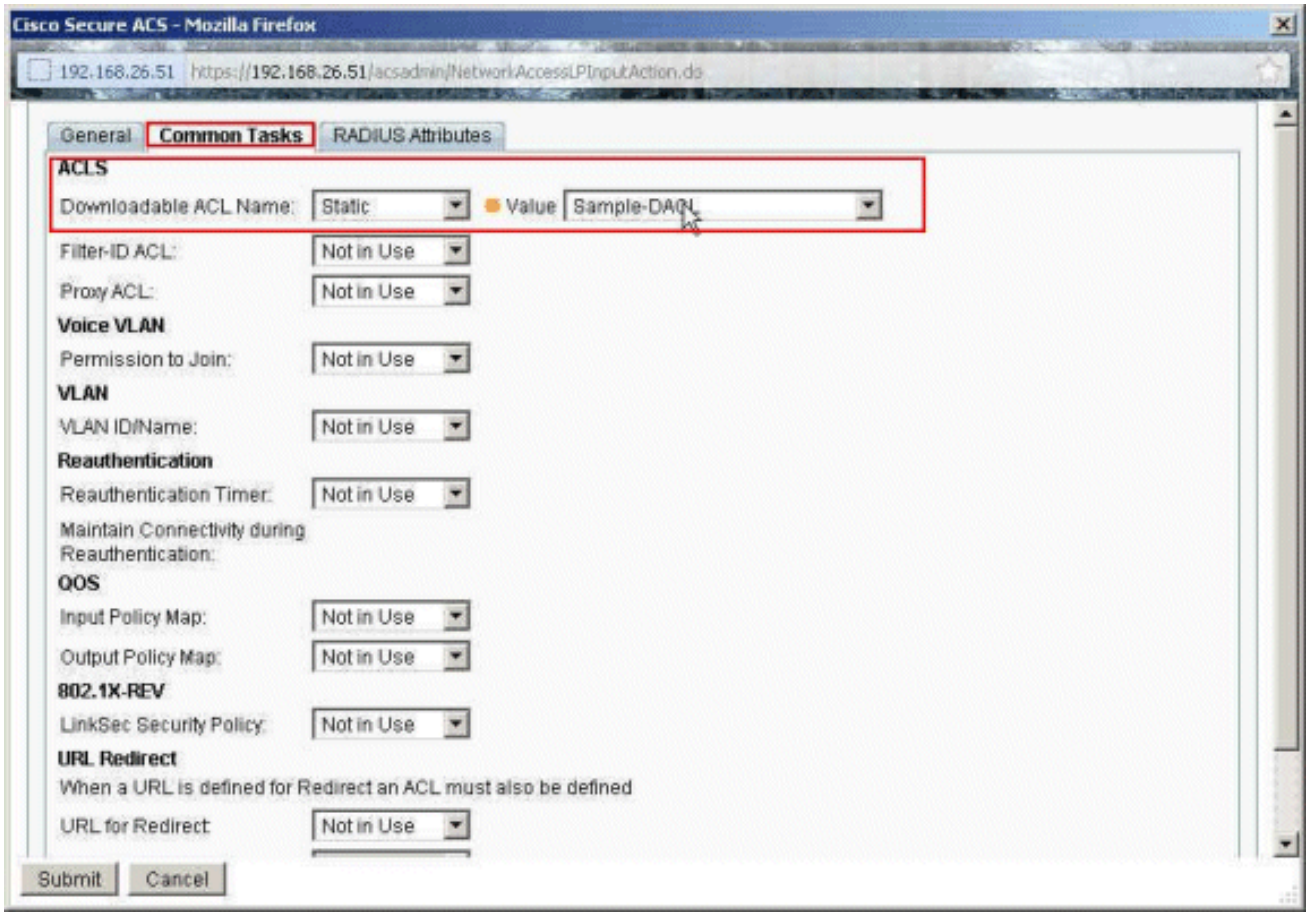
18. 单击**Create**以创建新的授权配置文件。



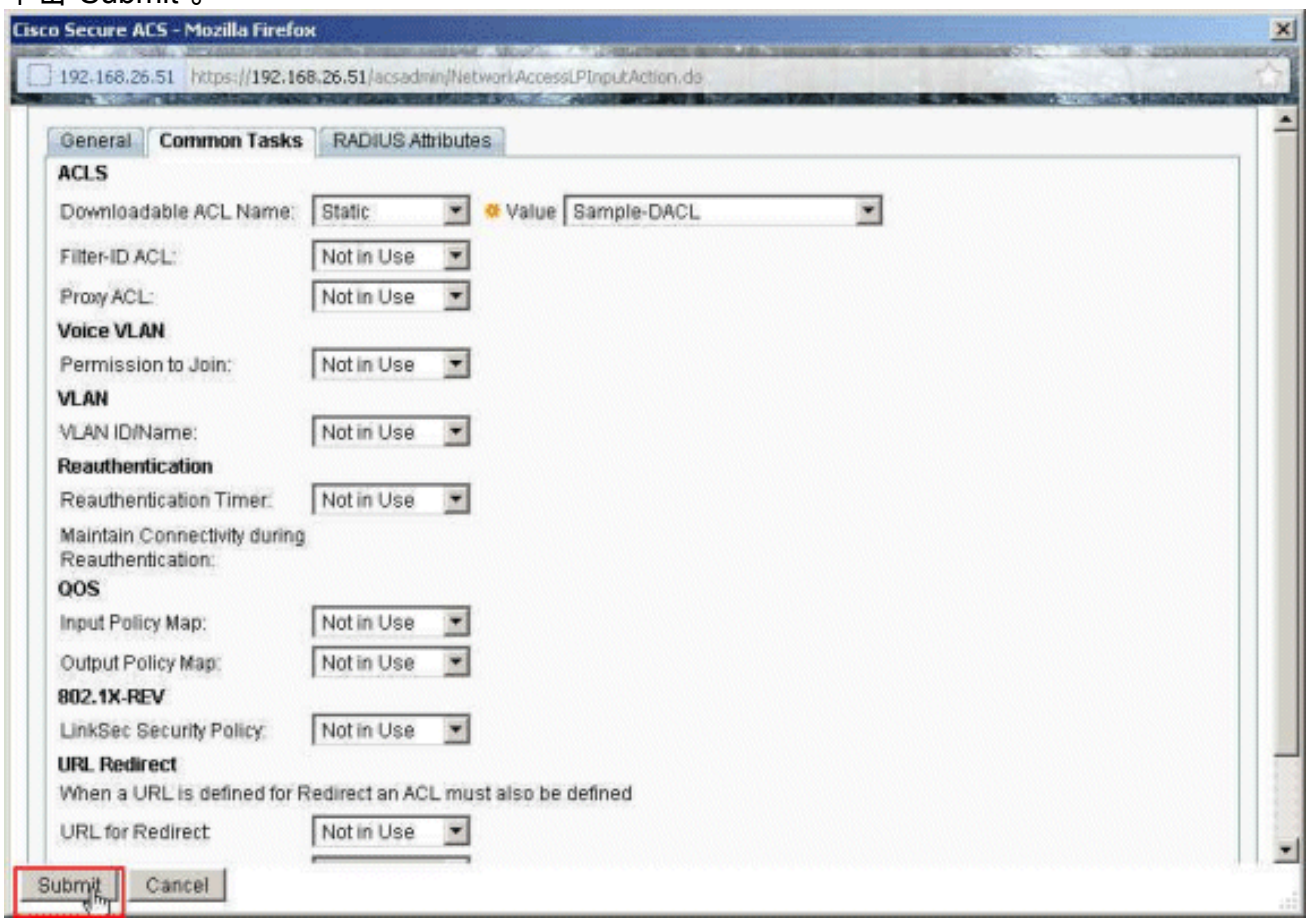
19. 为授权配置文件提**供名称。本示例中**使用了Sample-Profile。



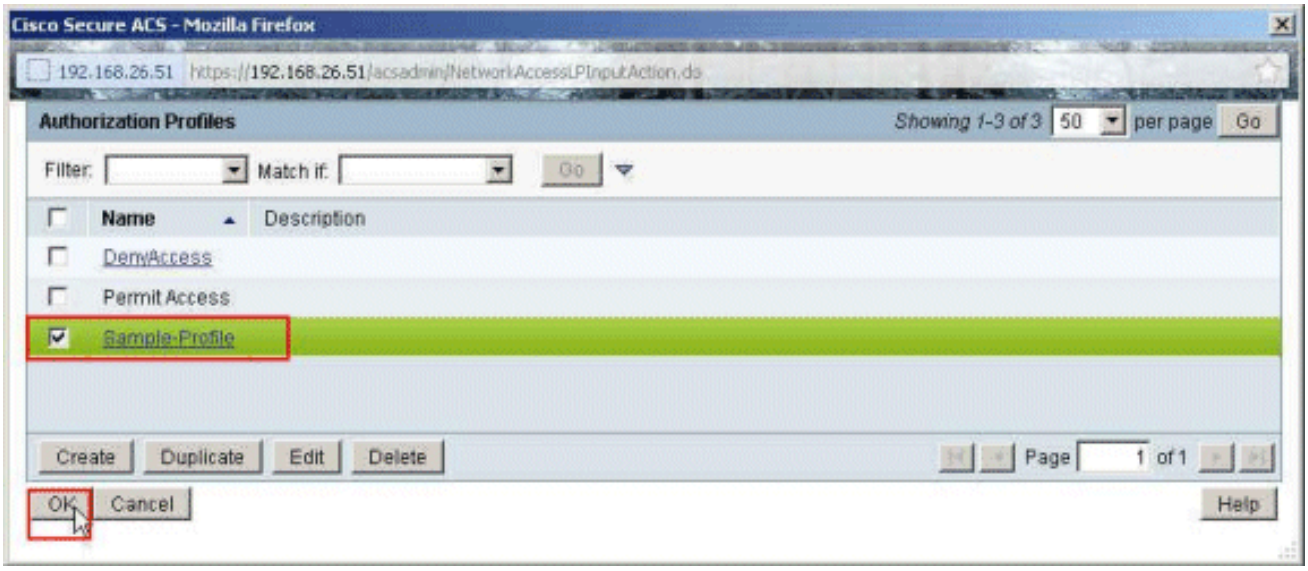
20. 选择**Common Tasks**选项卡，并从Downloadable ACL Name下拉列**表**中选择**Static**。从value下拉列**表中选择新**创建的DACL（示例 — DACL）。



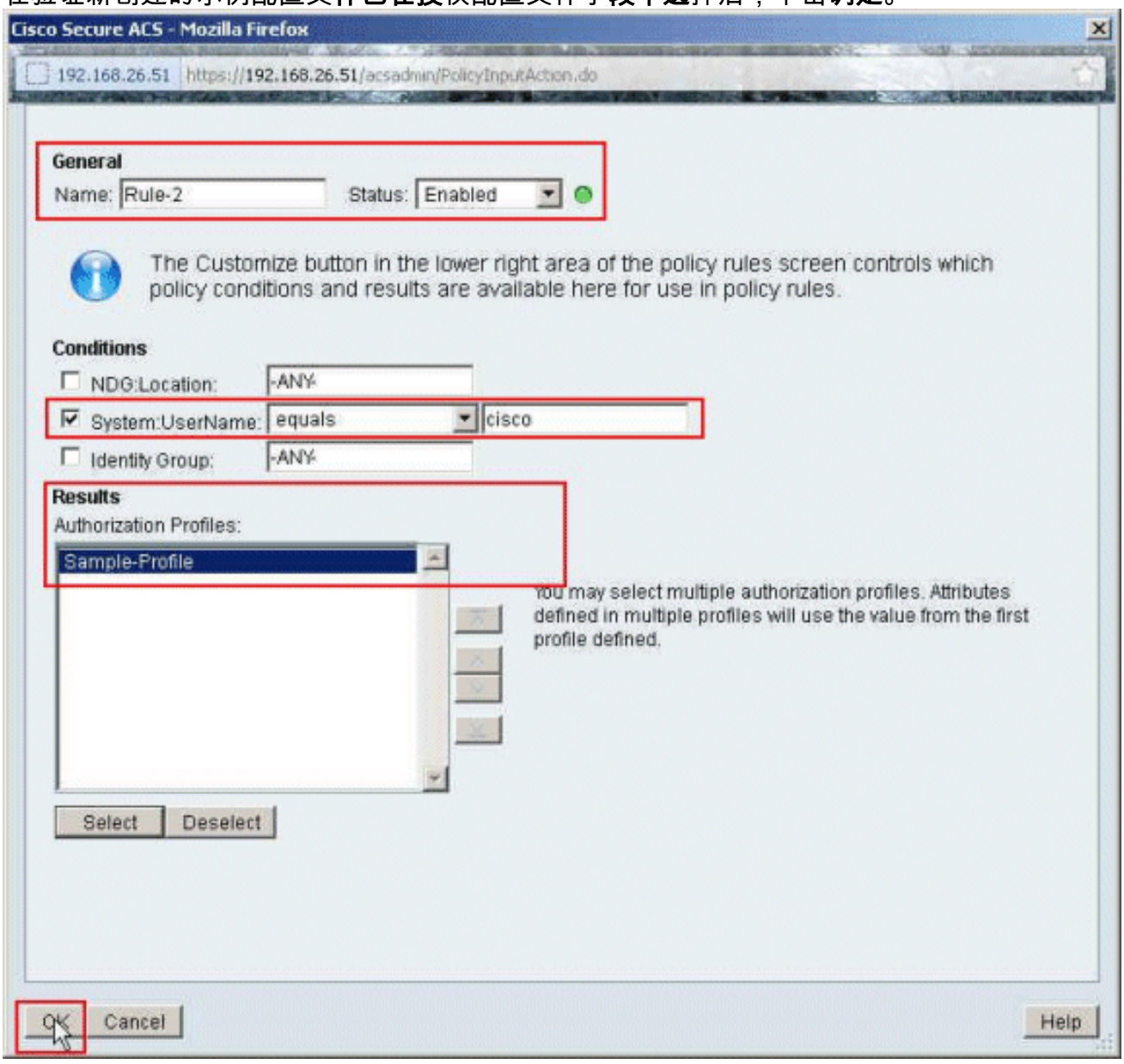
21. 单击“Submit”。



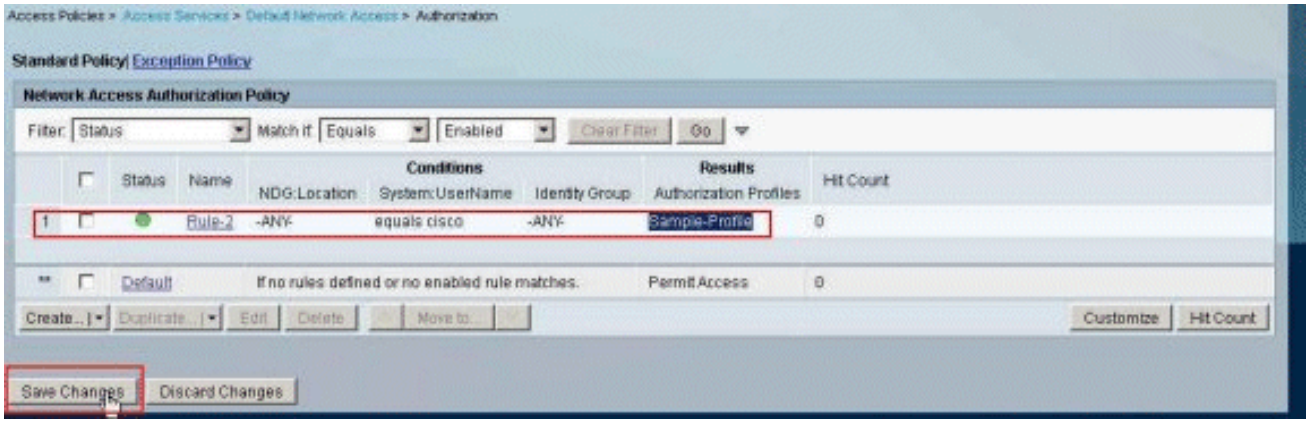
22. 确保选中Sample-Profile(新创**建的授**权配置文件)旁边的复选框，然后单击**OK**。



23. 在验证新创建的示例配置文**件已在授**权配置文件字**段中选**择后，单击**确定**。



24. 验证新规则(**规则–2**)是否使用System:UserName **equals cisco conditions** 和**Sample-Profile** 作为结果创建的。点击**Save Changes**。已成功创建规则2。



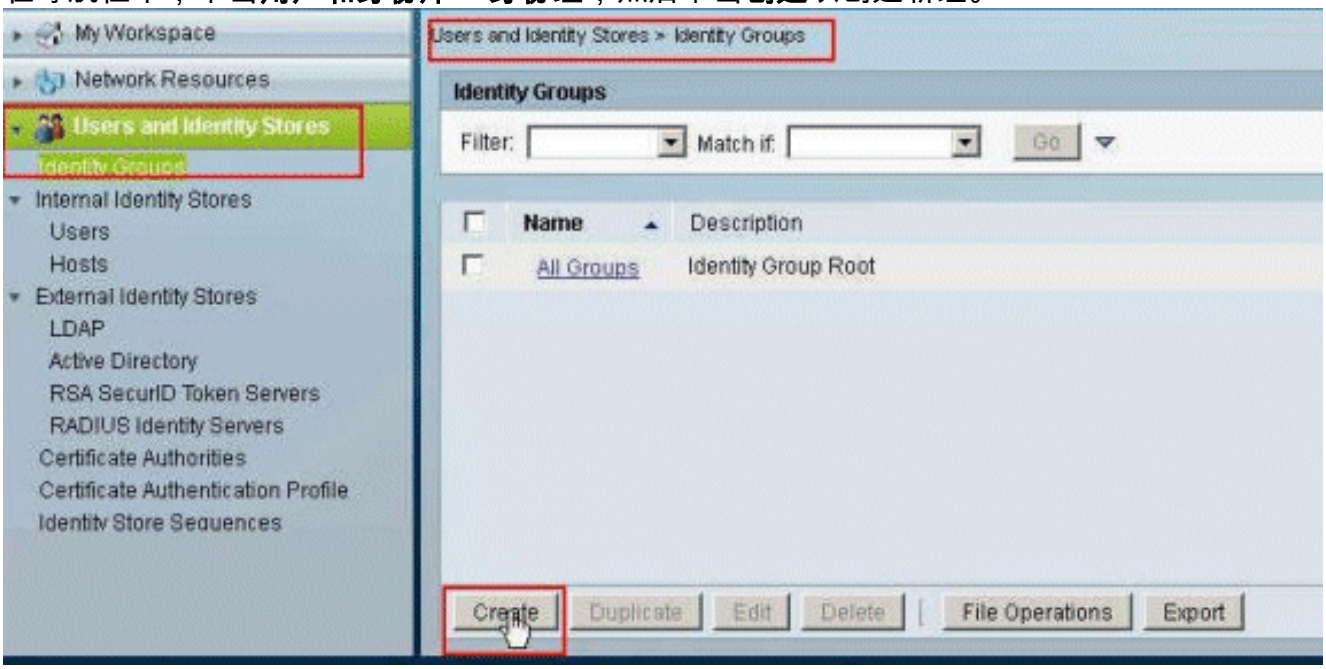
为适用于组的可下载 ACL 配置 ACS

完成为单个用户的可下载ACL配置ACS的步骤1至步骤12，然后执行这些步骤以在思科安全ACS中为组配置可下载ACL。

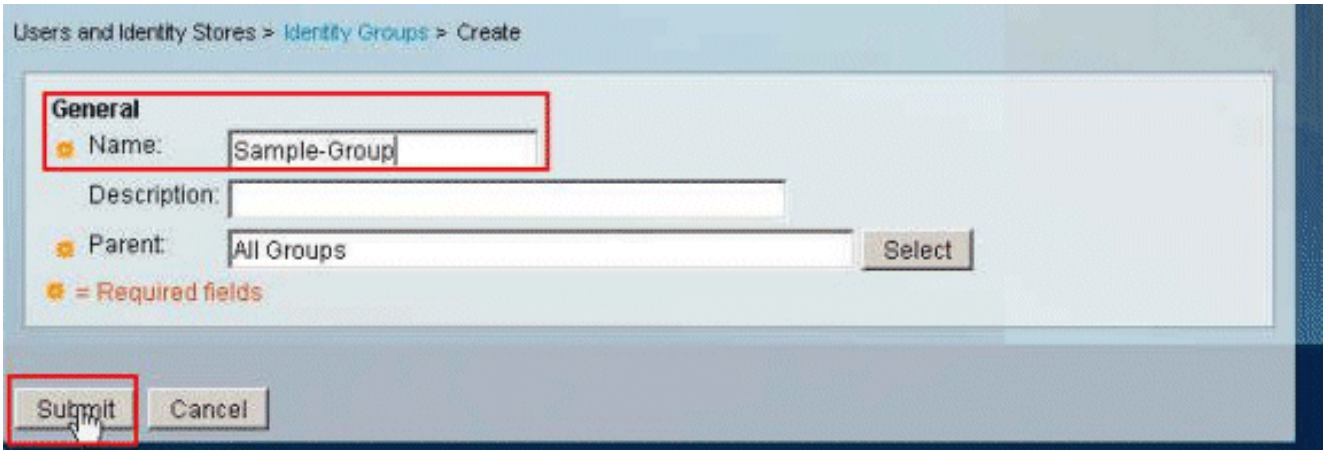
在本示例中，IPsec VPN用户“cisco”属于**Sample-Group**。

Sample-Group用户cisco成功进行身份验证，RADIUS服务器向安全设备发送可下载访问列表。用户“cisco”只能访问 10.1.1.2 服务器，拒绝其他所有访问。要验证 ACL，请参阅适用于用户/组的可下载 ACL 部分。

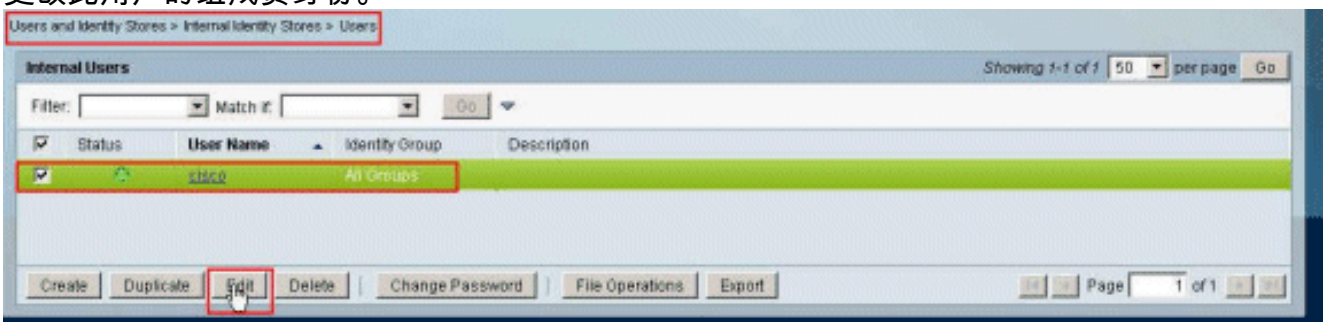
1. 在导航栏中，单击**用户和身份库 > 身份组**，然后单击**创建**以创建新组。



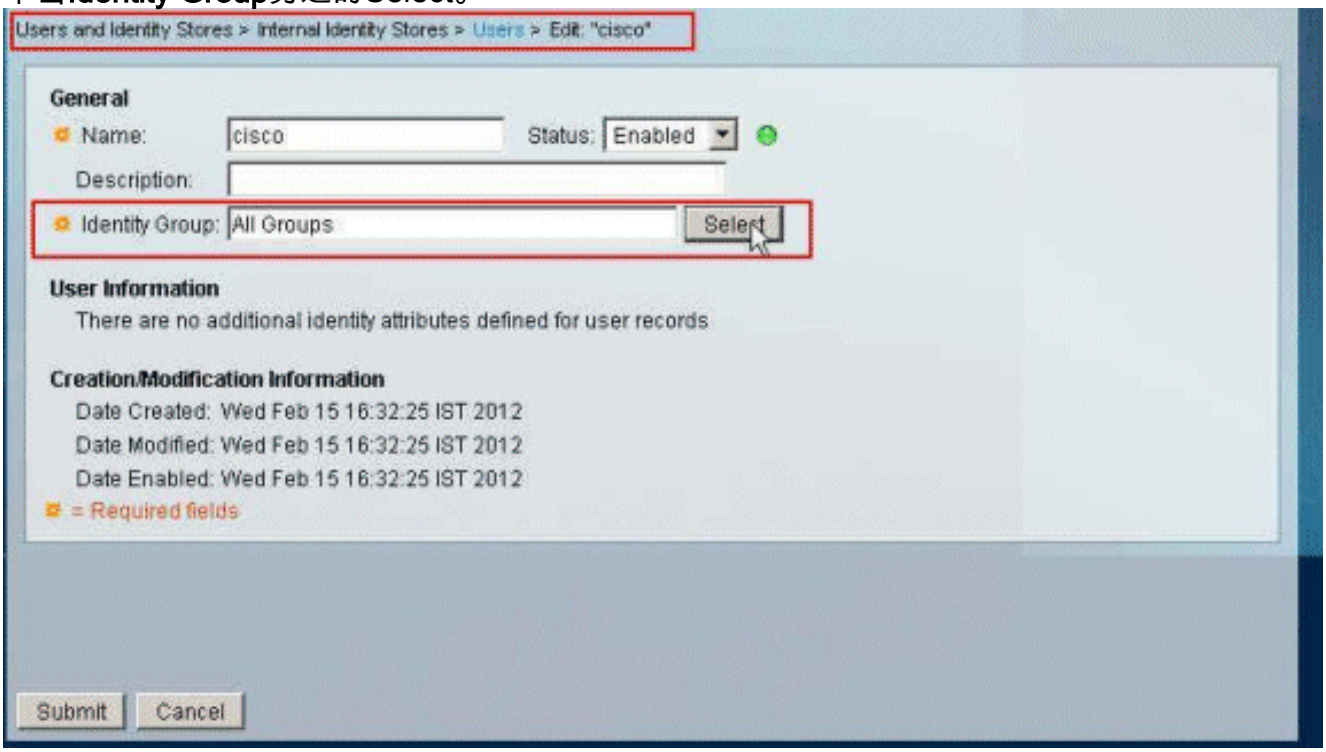
2. 提供组名(示**例组)**，然后单击**提交**。



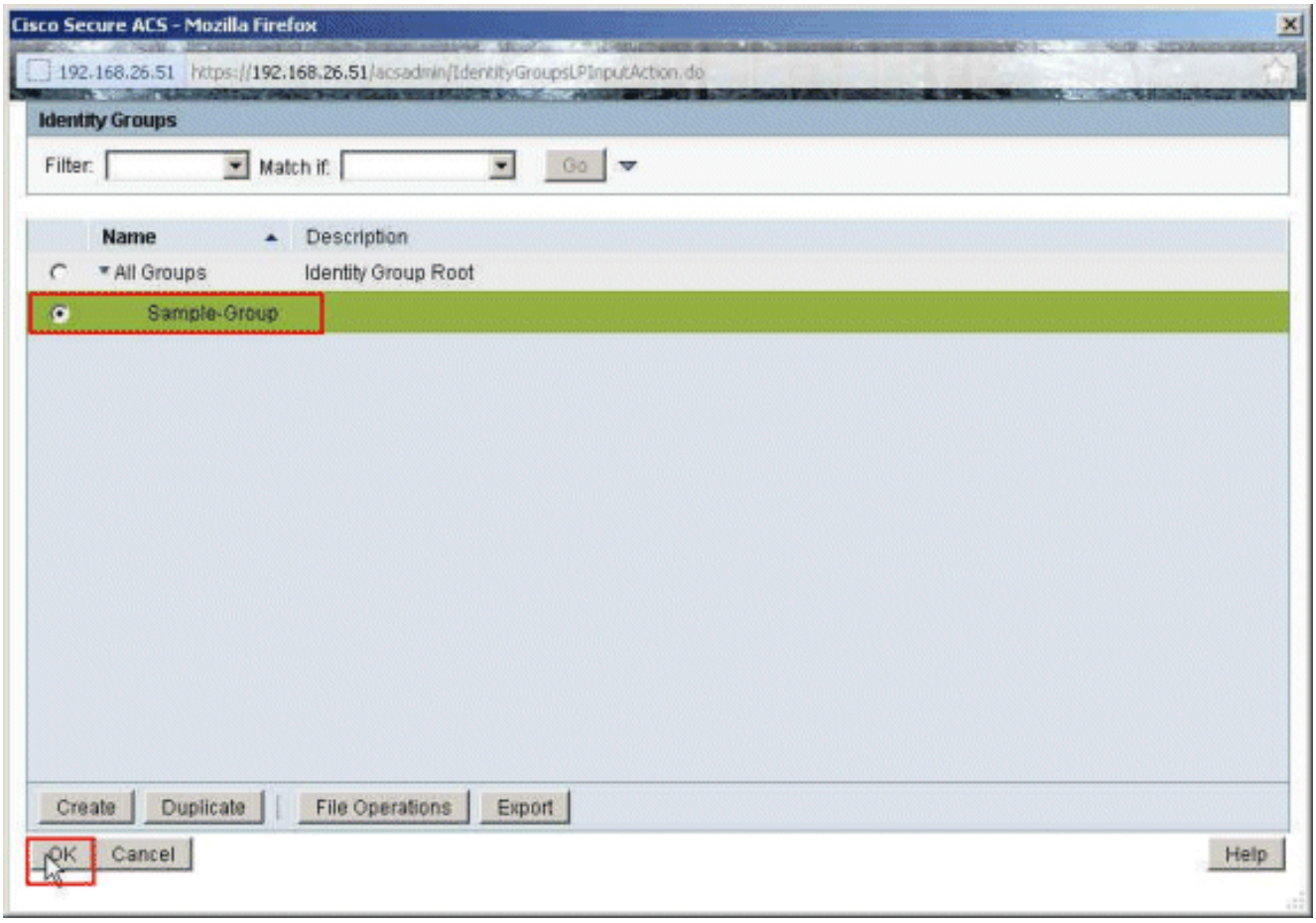
3. 选择**User Identity Stores > Internal Identity Stores > Users**，然后选择用户**cisco**。单击**Edit**以更改此用户的组成员身份。



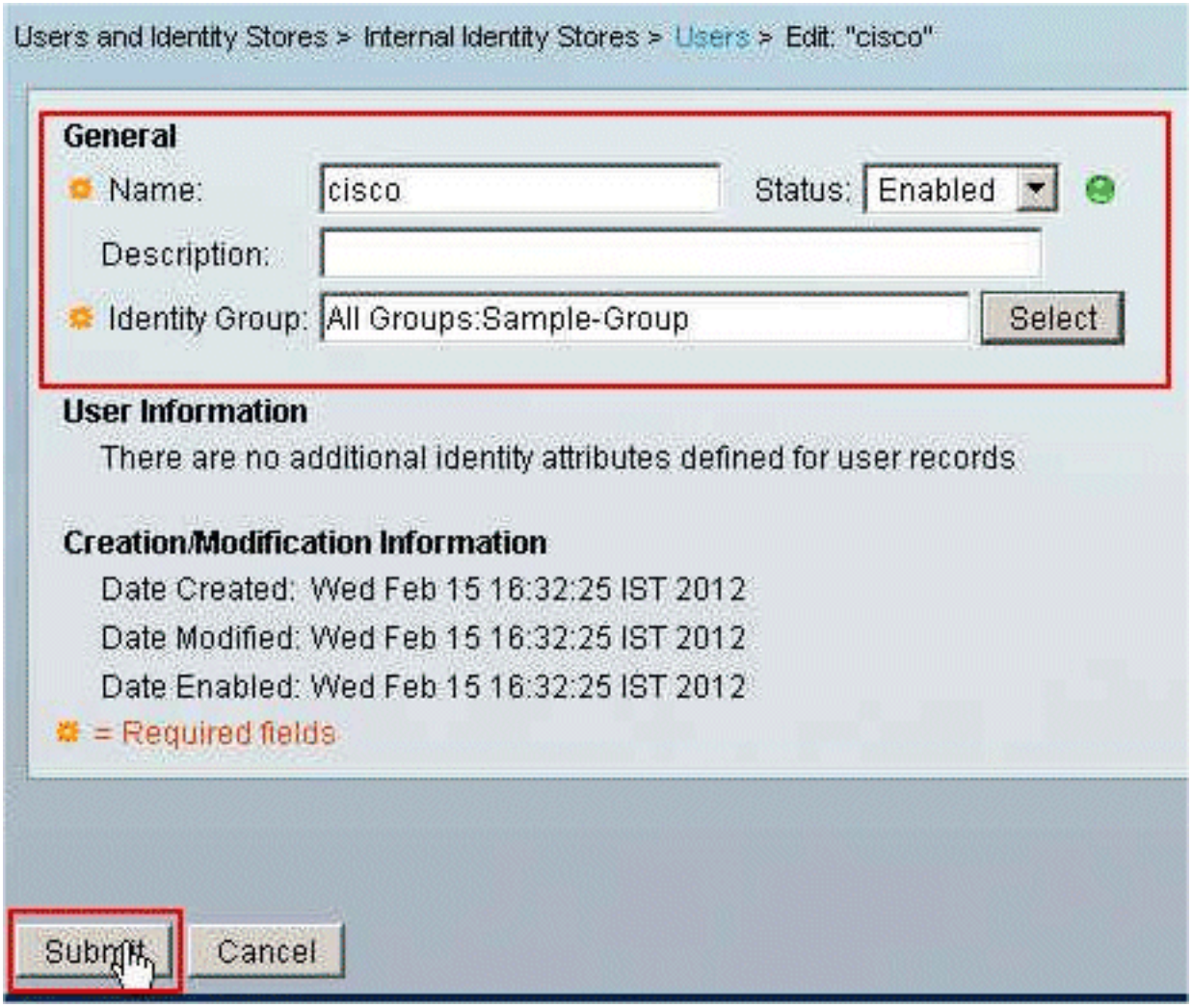
4. 单击**Identity Group**旁边的Select。



5. 选择新创建的组(即Sample-Group)，然后单击“确定”。

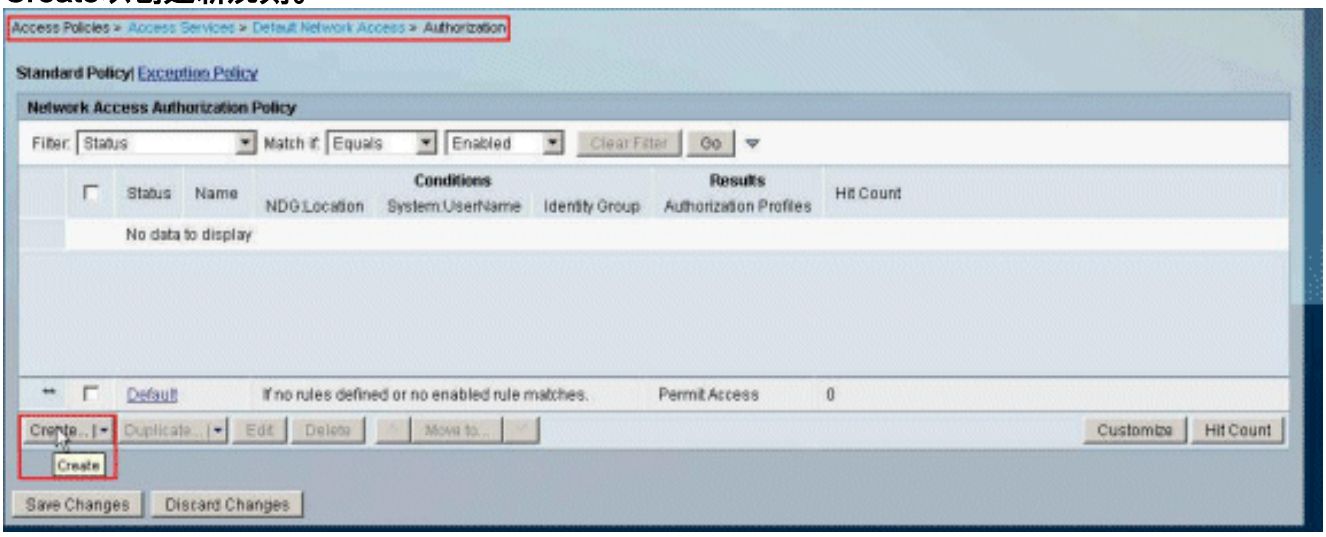


6. 单击“Submit”。

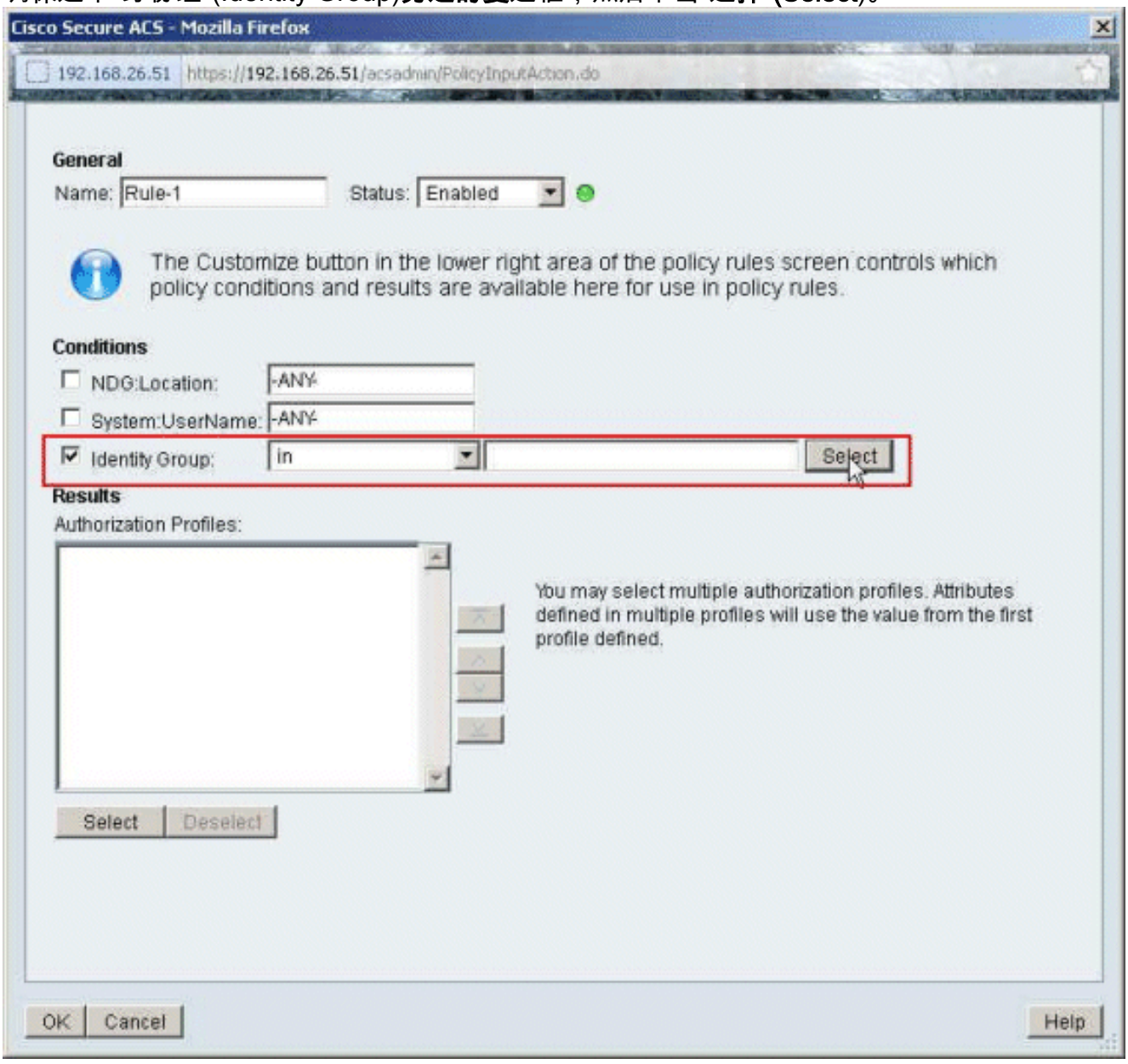


7. 选择Access Policies > Access Services > Default Network Access > Authorization，然后单击

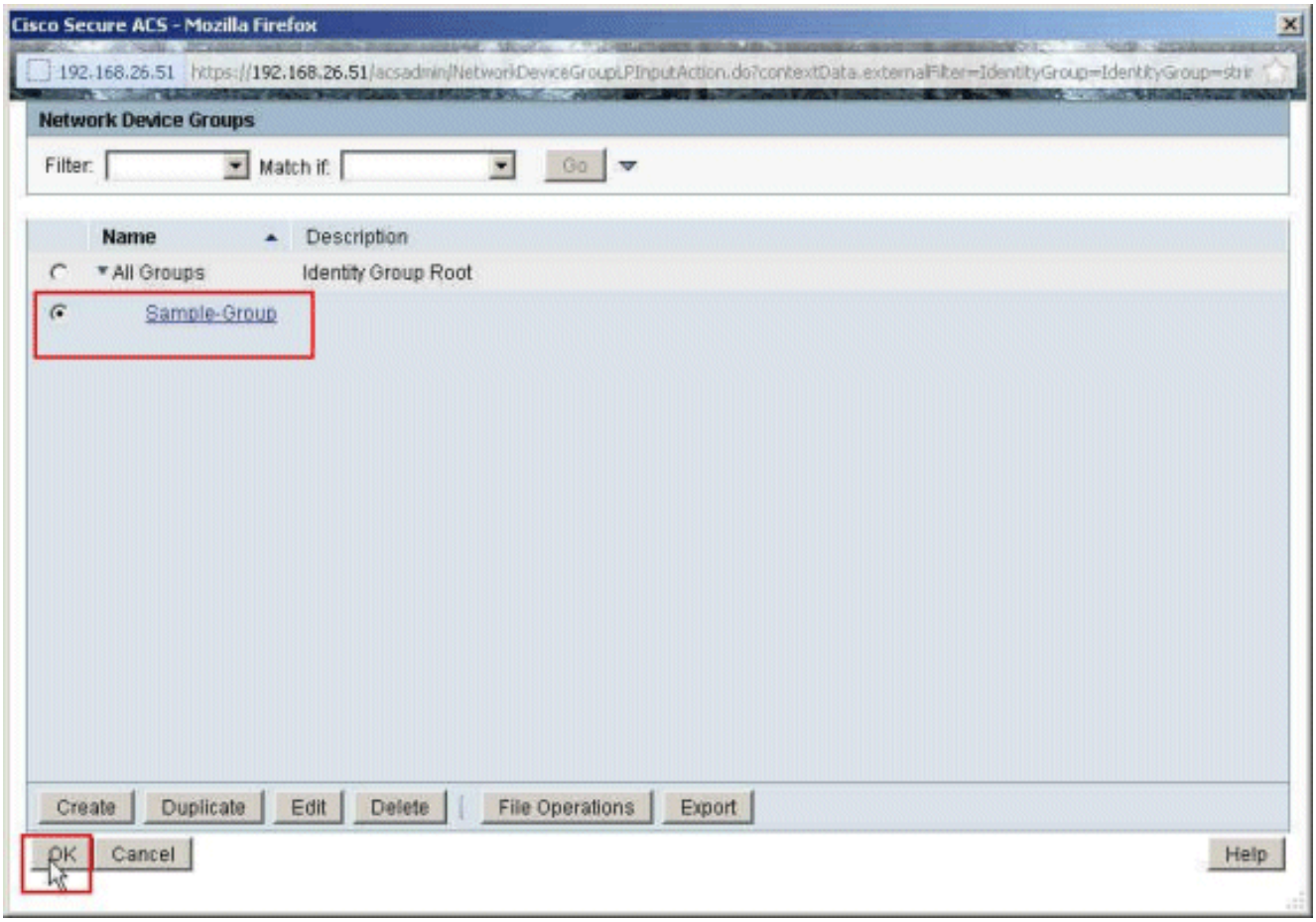
Create以创建新规则。



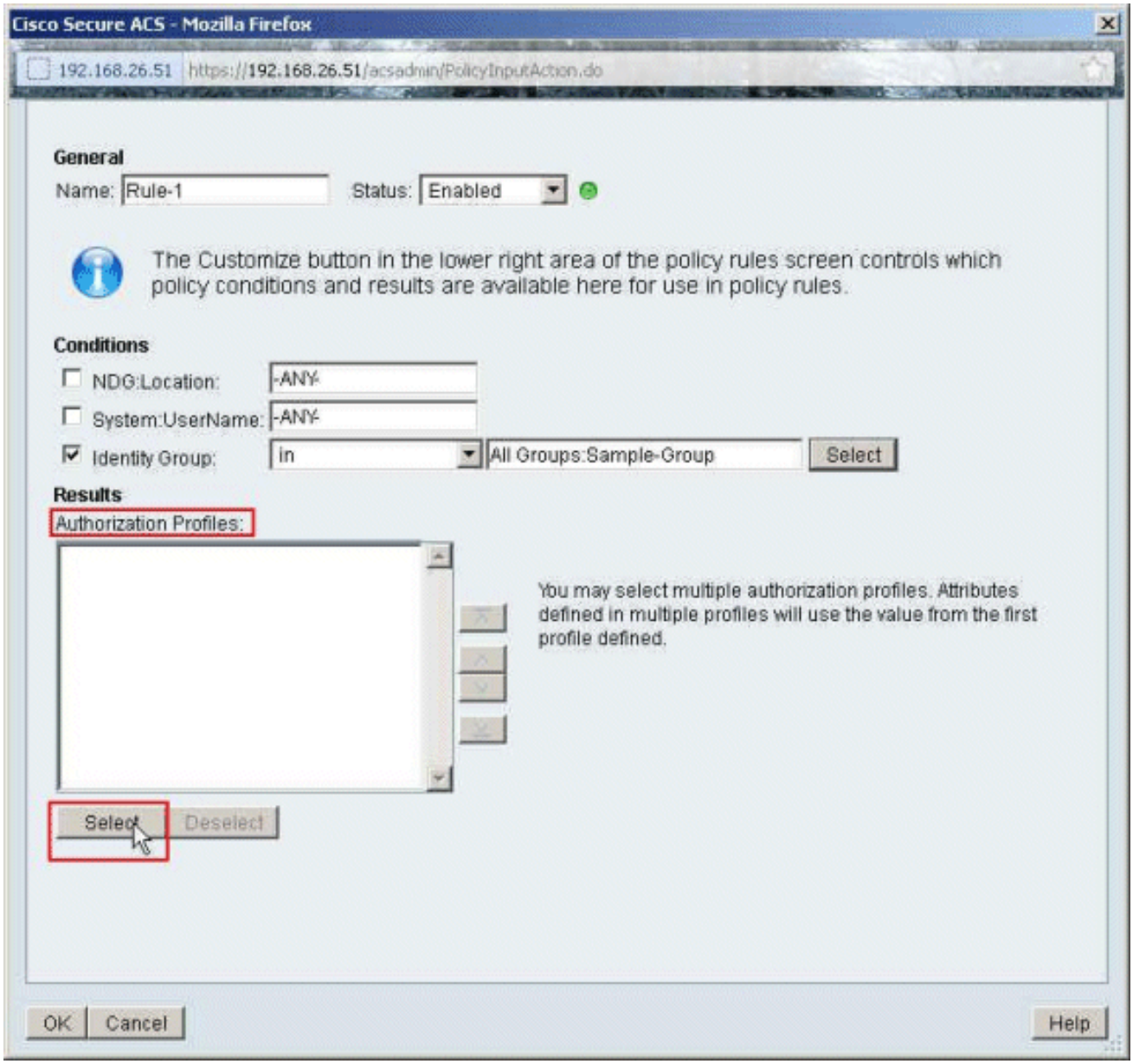
8. 确保选中“身份组”(Identity Group)旁边的复选框，然后单击“选择”(Select)。



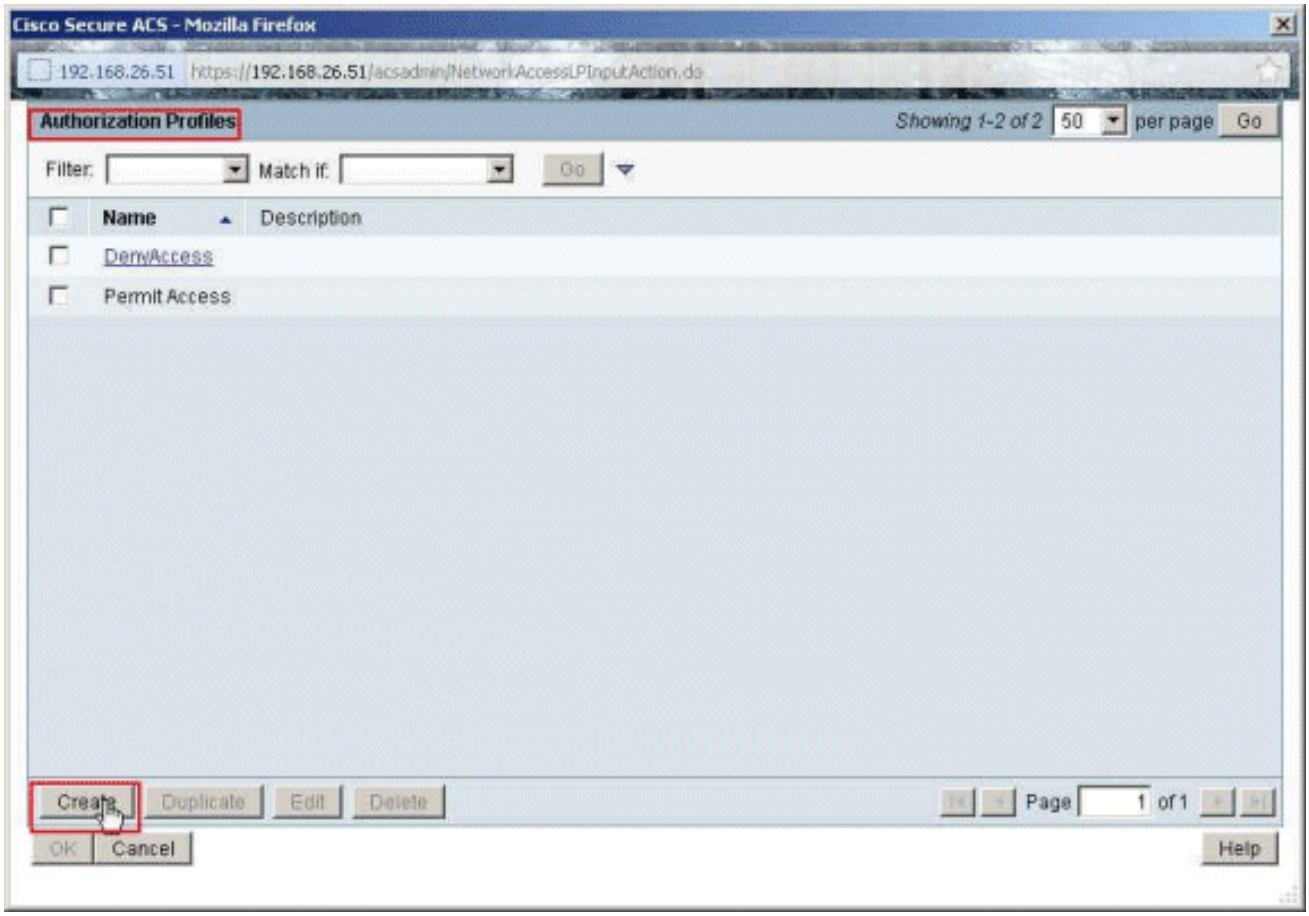
9. 选择Sample-Group,然后单击OK。



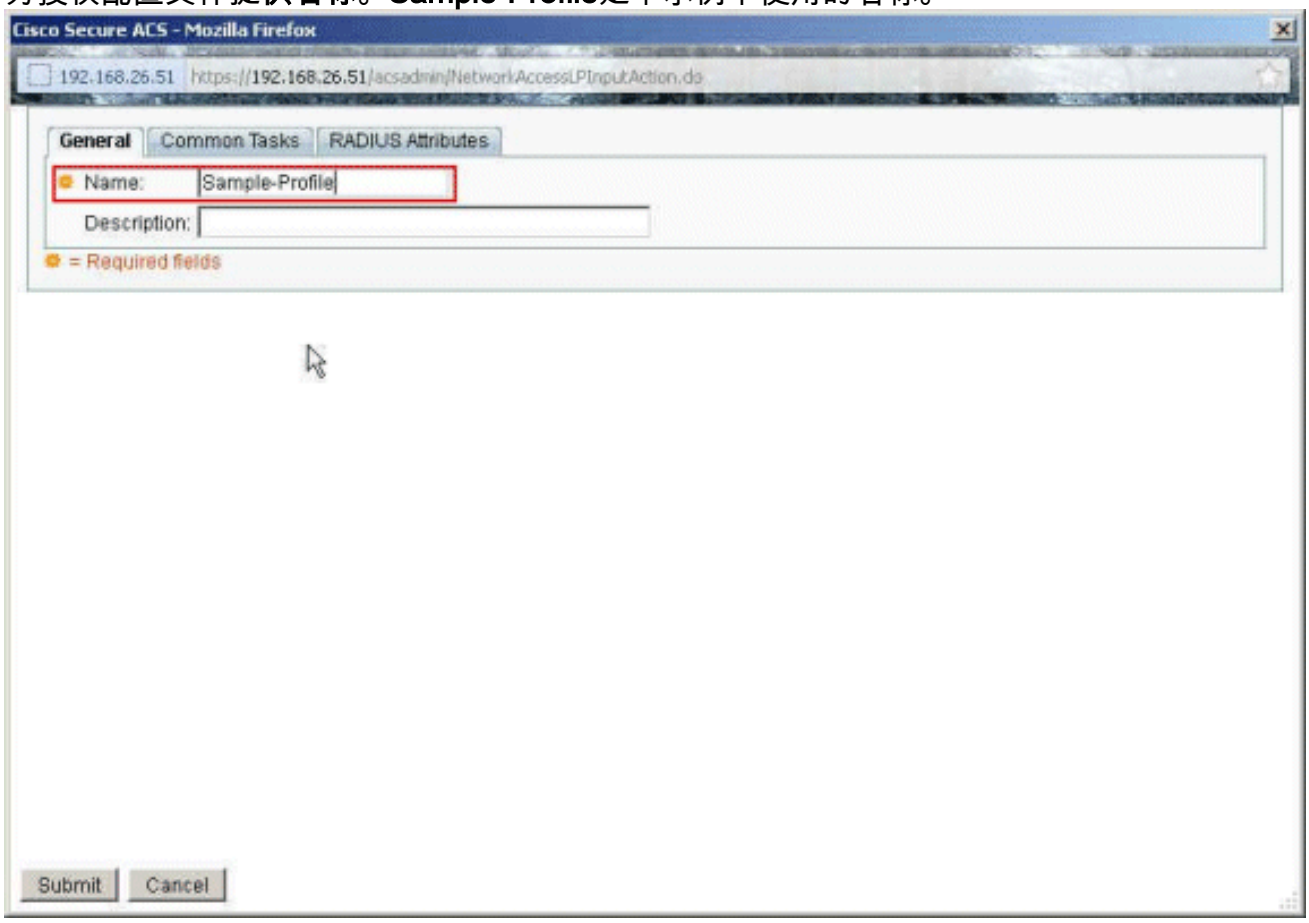
10. 在“授权配置文件”(Authorization Profiles)部分，单击**选择**。



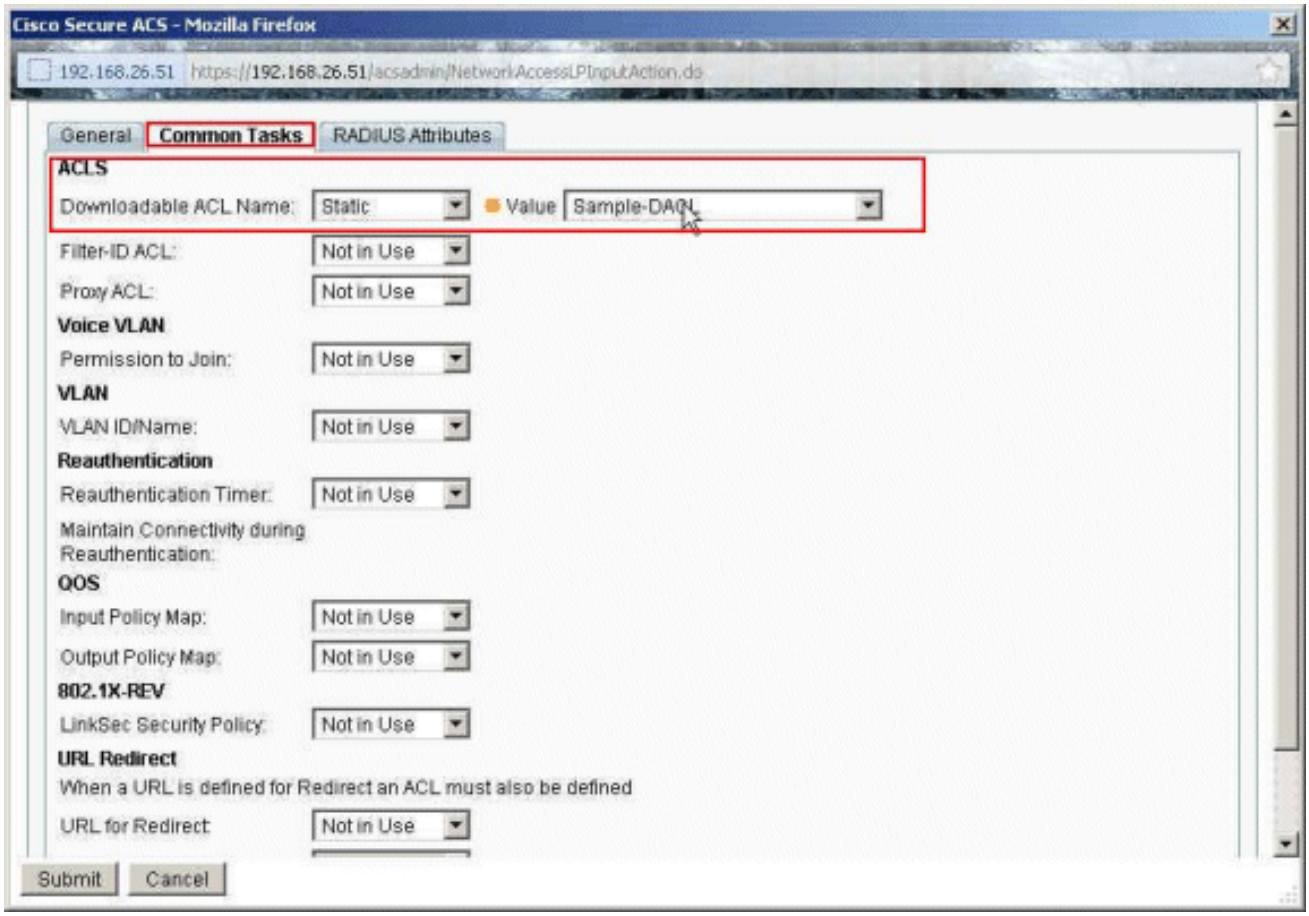
11. 单击**Create**以创建新的授权配置文件。



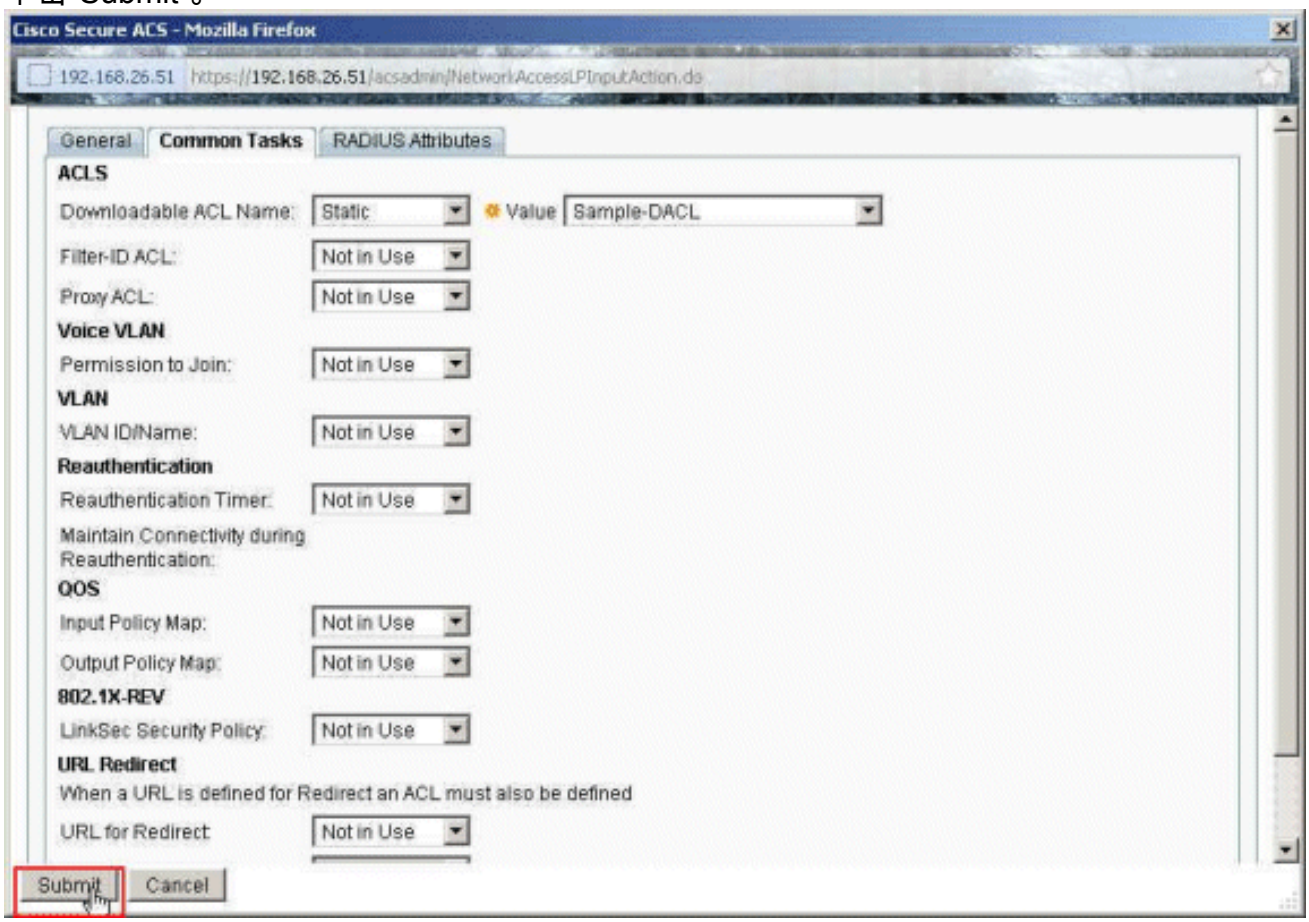
12. 为授权配置文件提**供名称。Sample-Profile**是本示例中使用的名称。



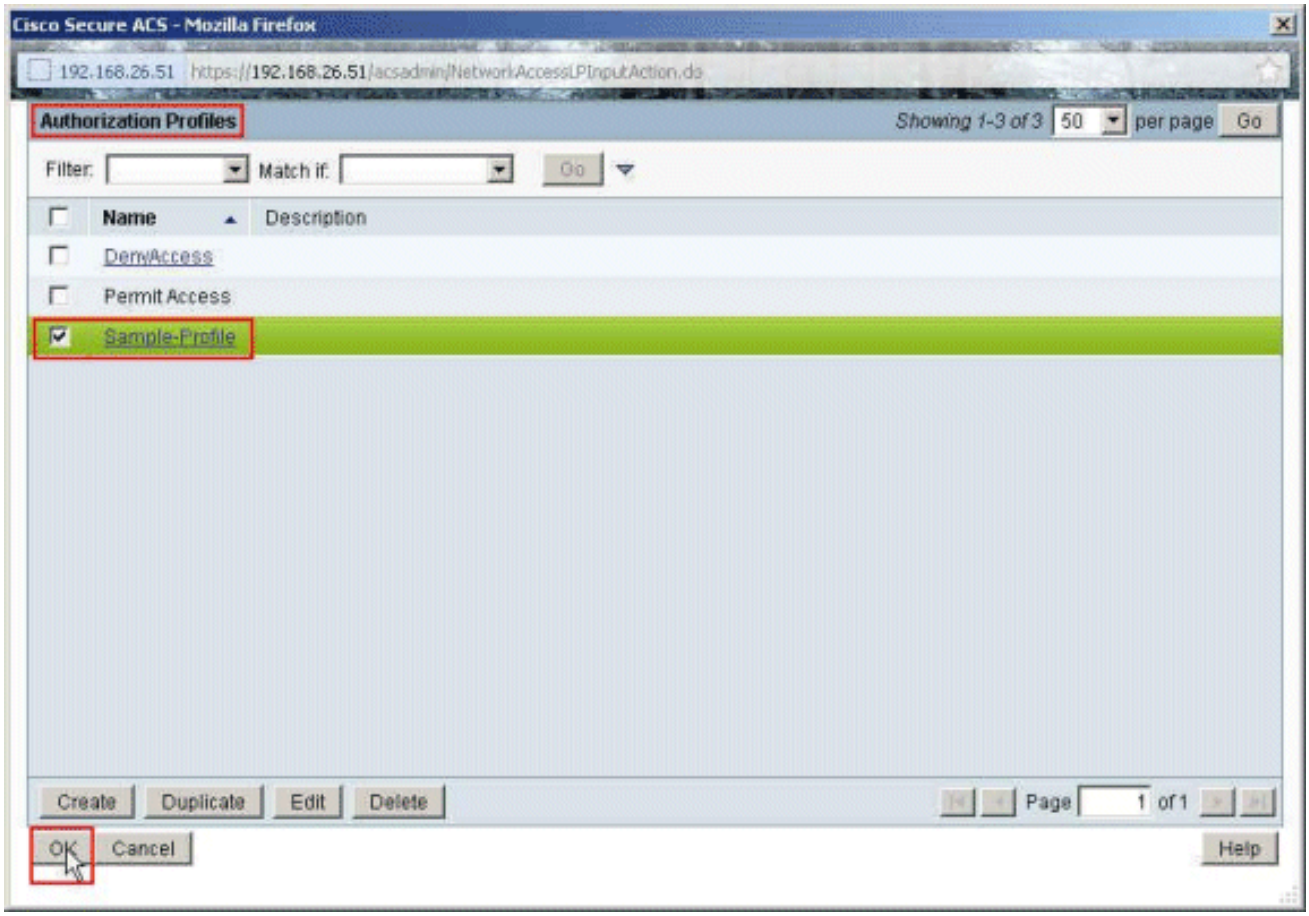
13. 选择**Common Tasks**选项卡，并从Downloadable ACL Name下拉列**表**中选择**Static**。从Value下拉列**表中选择新**创建的DACL（示例 — DACL）。



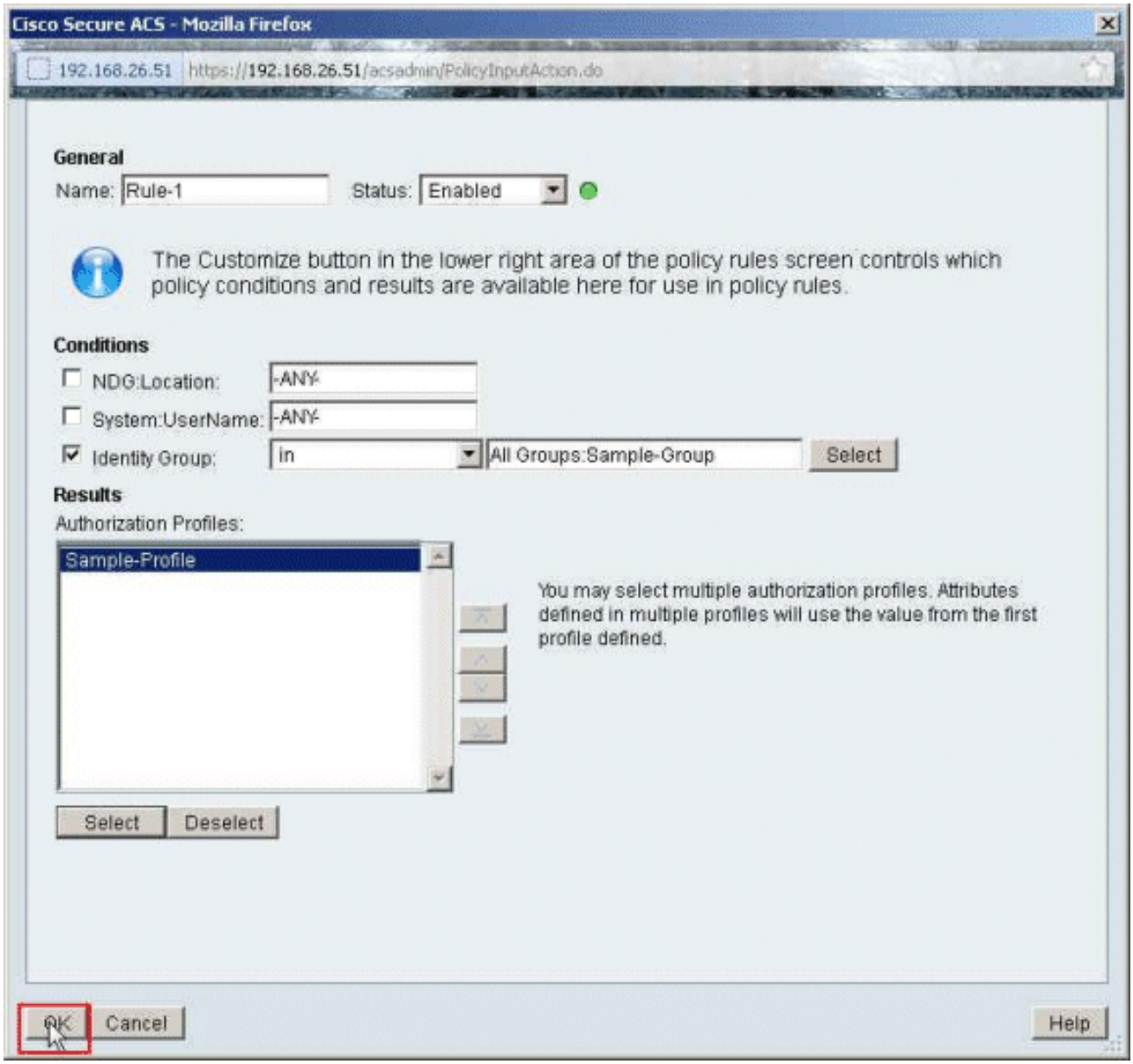
14. 单击“Submit”。



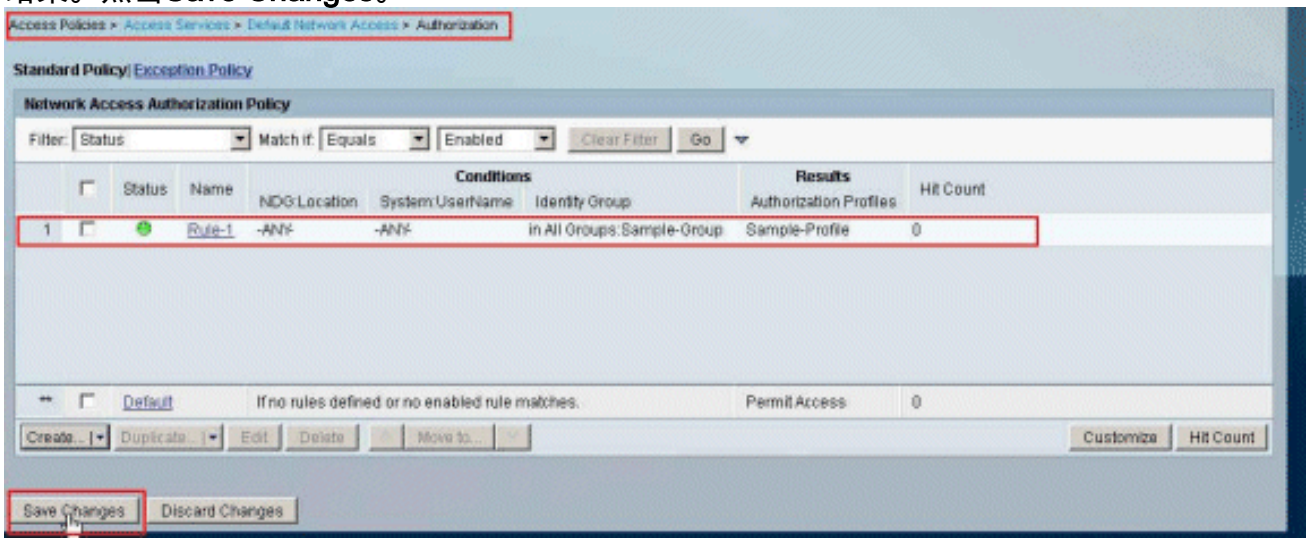
15. 选择之前创建的授**权配置文件**示例配置文件，然后单**击确定**。


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. Click **OK**.



17. 验证是**否已创**建Rule-1，并**将Identity Group Sample-Group**作为条件，**将Sample-Profile**作为结果。点击**Save Changes**。

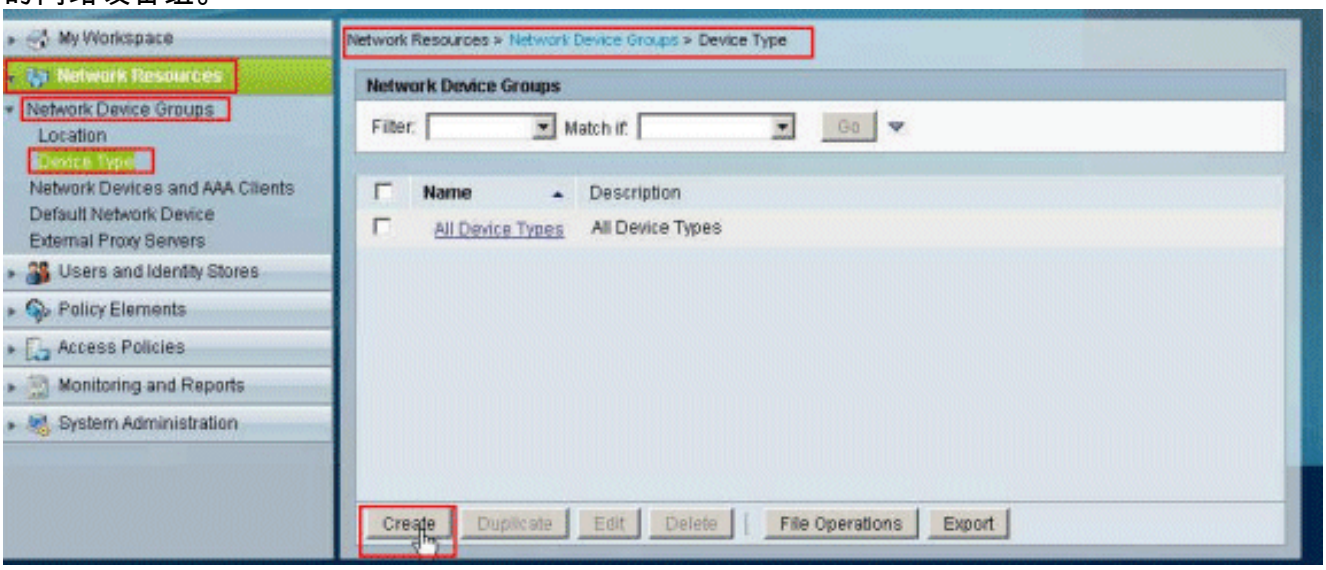


为网络设备组的可下载ACL配置ACS

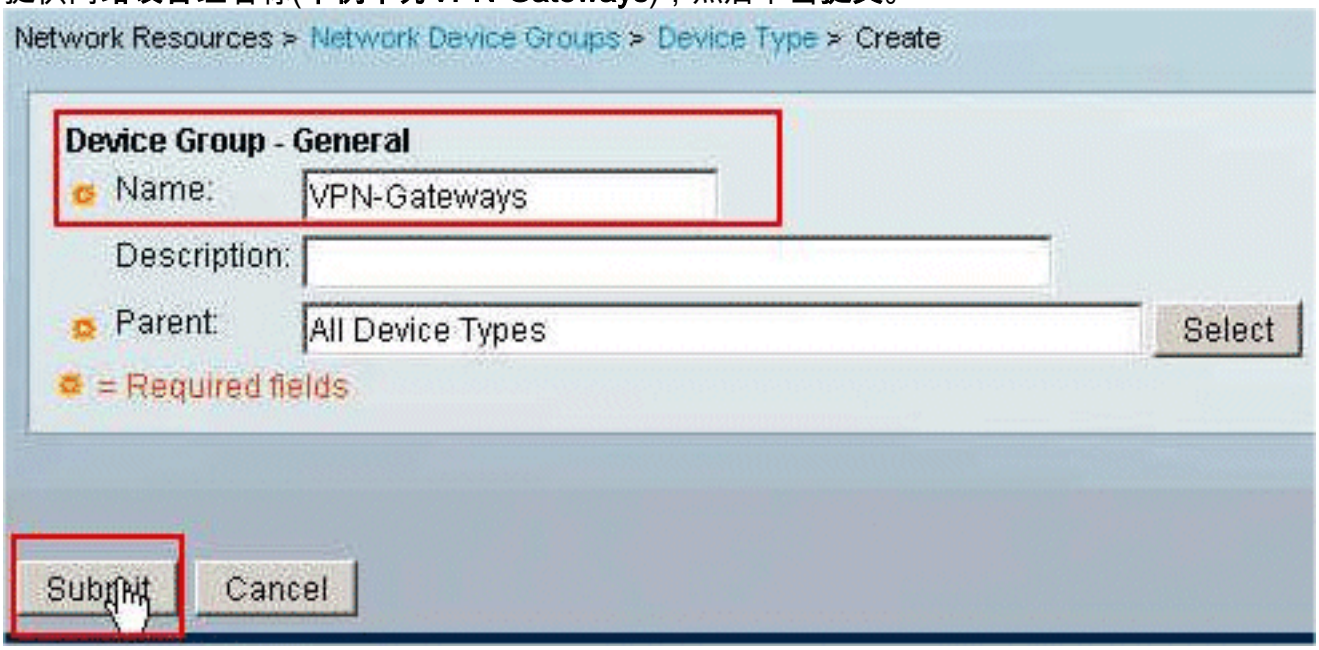
完成为单个用户的可下载ACL配置ACS的步骤1至步骤12，并执行这些步骤以在Cisco Secure ACS中为网络设备组配置可下载ACL。

在本示例中，RADIUS客户端(ASA)属于网络设备组**VPN-Gateways**。来自ASA的用户“cisco”的VPN身份验证请求成功进行身份验证，并且RADIUS服务器向安全设备发送可下载的访问列表。用户“cisco”只能访问 10.1.1.2 服务器，拒绝其他所有访问。要验证 ACL，请参阅适用于用户/组的可下载 ACL 部分。

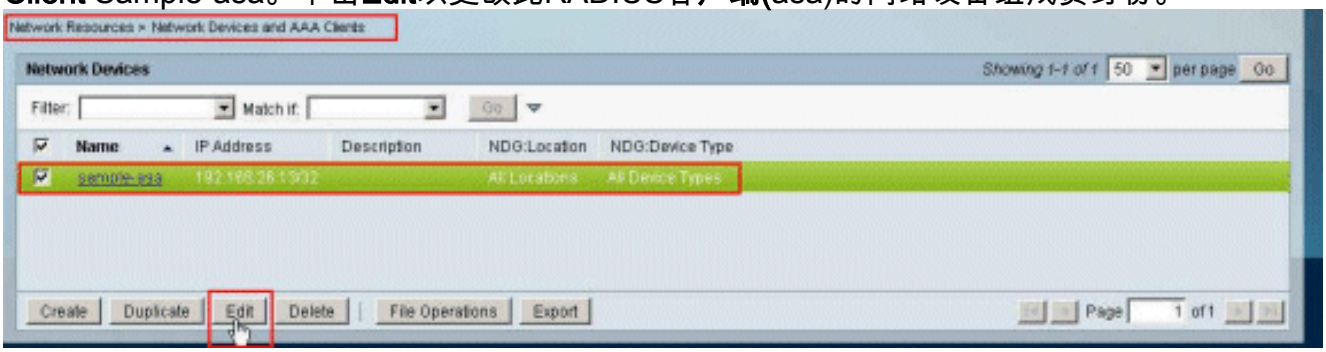
1. 选择**Network Resources > Network Device Groups > Device Type**，然后单击**Create**以创建新的网络设备组。



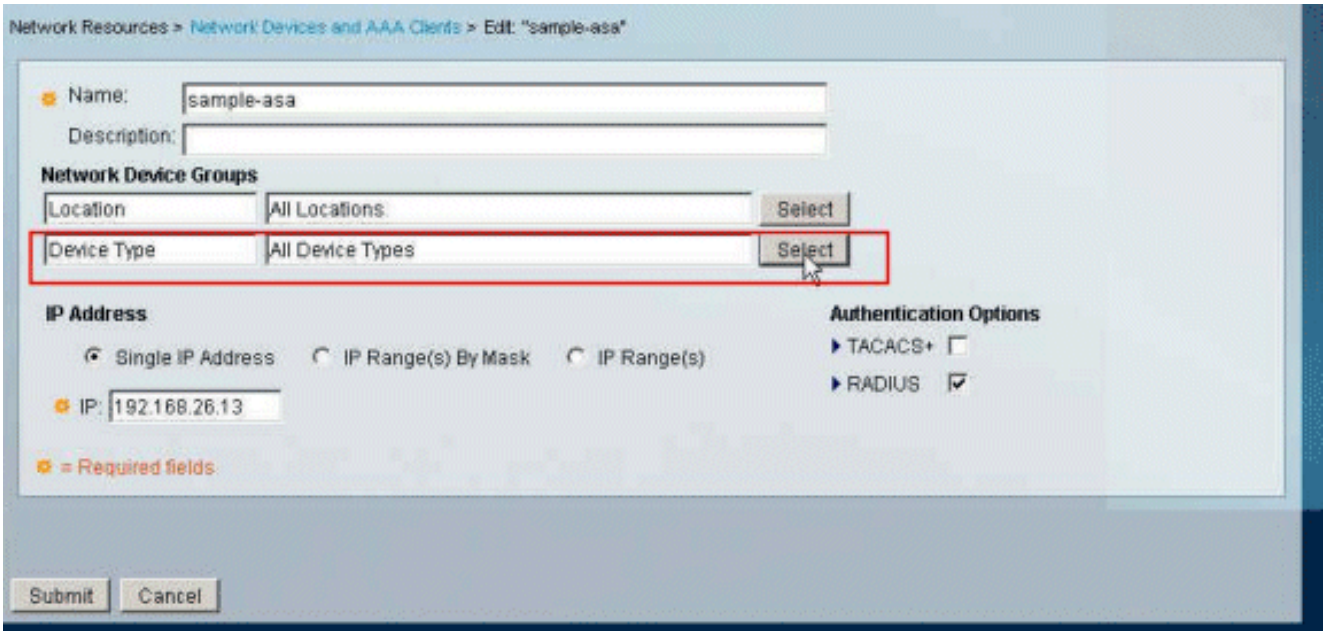
2. 提供网**络设备组**名称(**本例中为VPN-Gateways**)，然后单击**提交**。



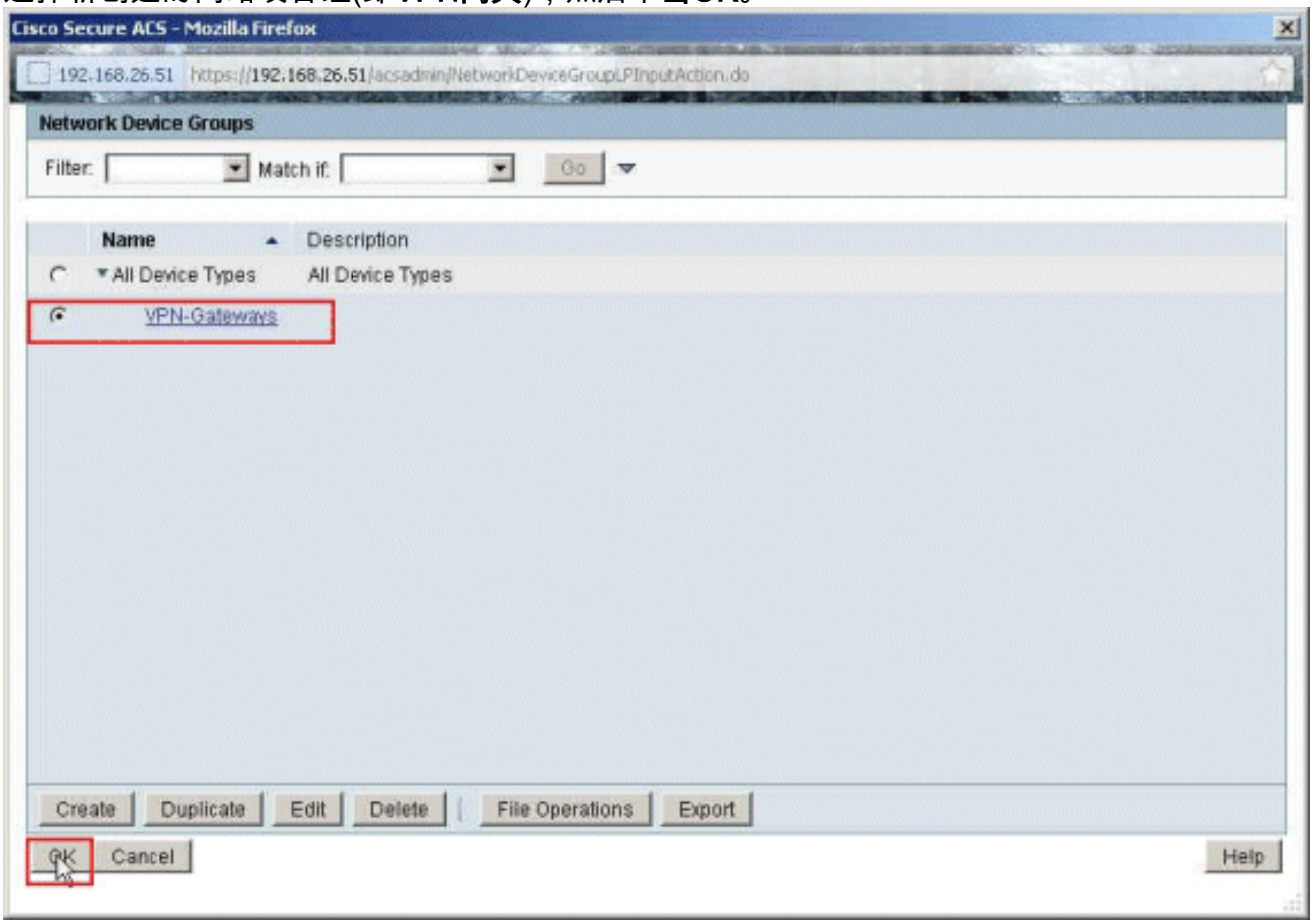
3. 选择**Network Resources > Network Devices and AAA Clients**，然后选择之前创建的**RADIUS Client** Sample-asa。单击**Edit**以更改此RADIUS客**户端(**asa)的网络设备组成员身份。



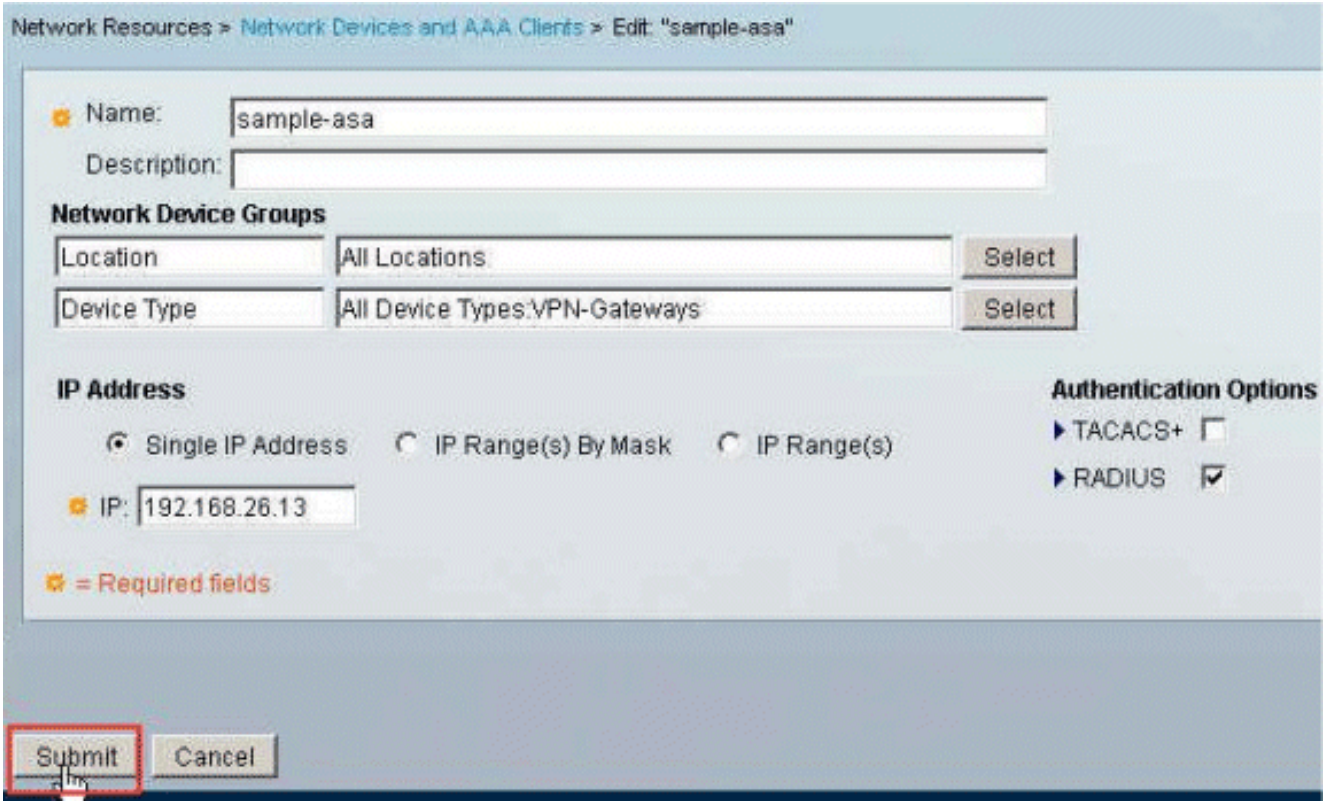
4. 单击“Device Type（设备类型）”旁边的“Select（选择）”。



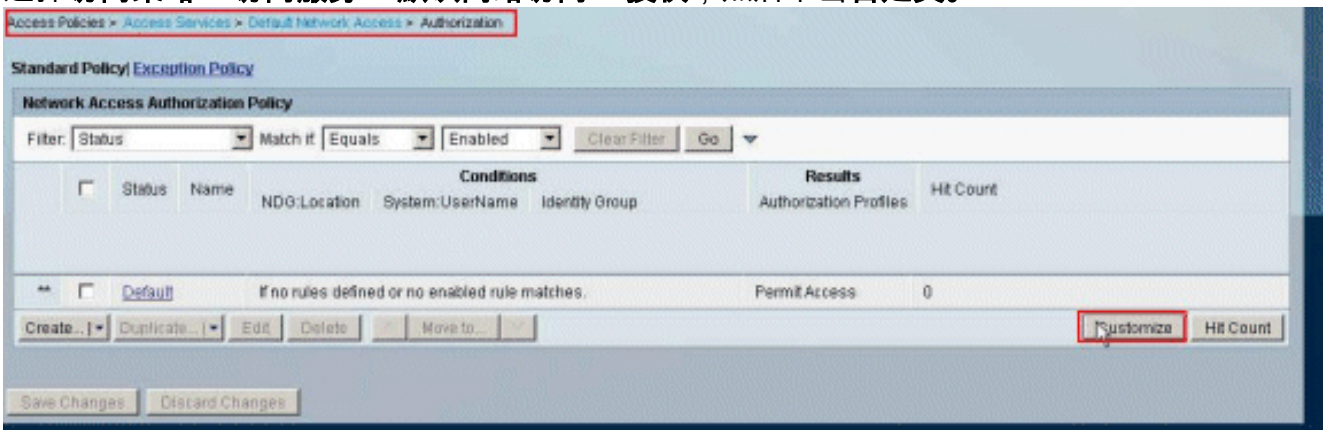
5. 选择新创建的网络设备组(即**VPN网关**)，然后单**击OK**。



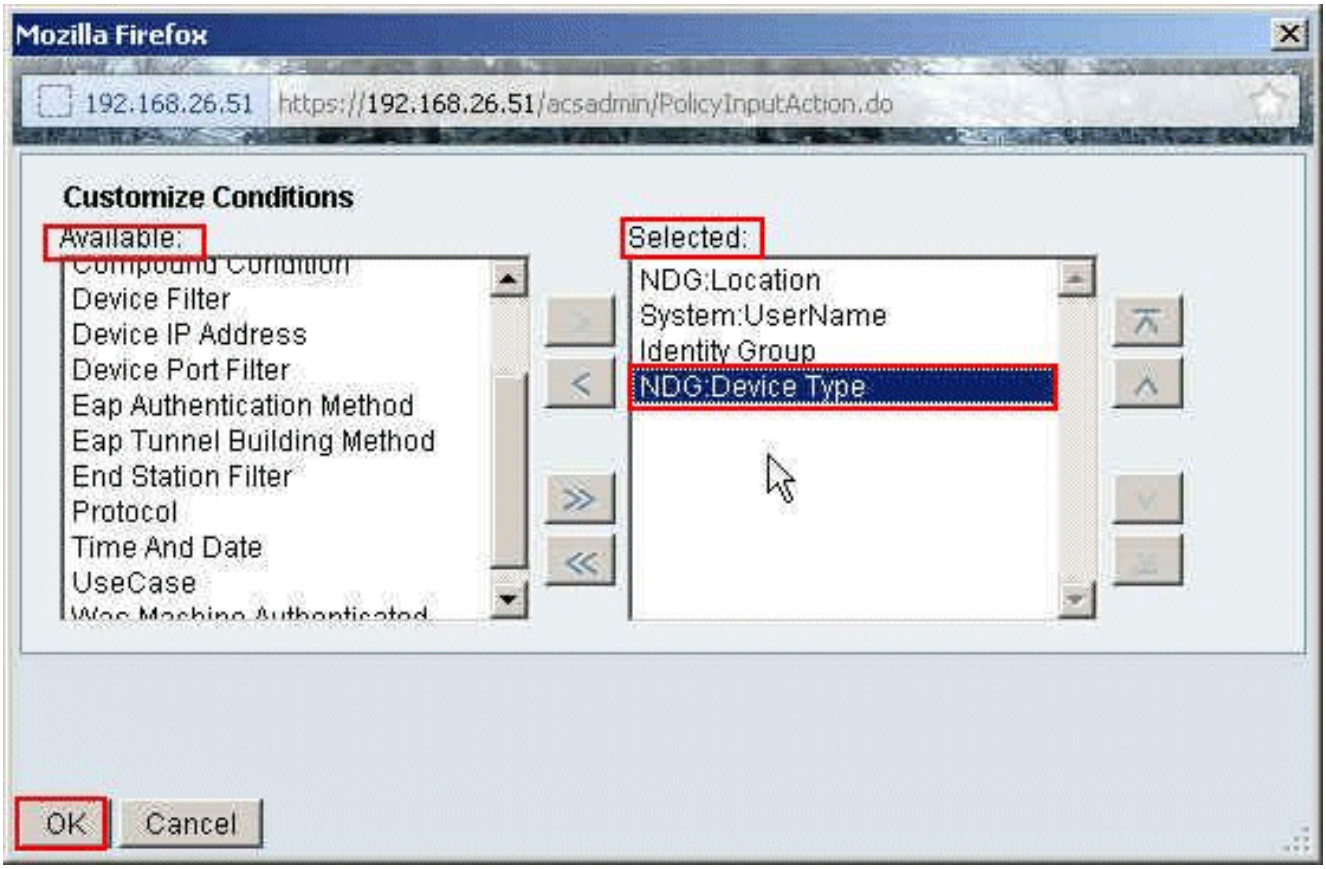
6. 单击“Submit”。



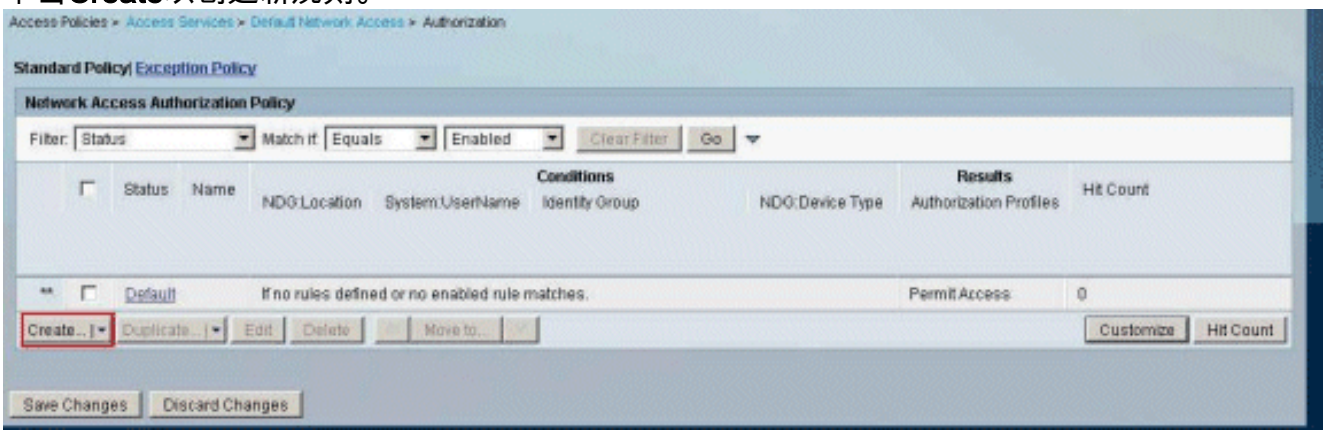
7. 选择**访问策略 > 访问服务 > 默认网络访问 > 授权**，然后单击**自定义。**



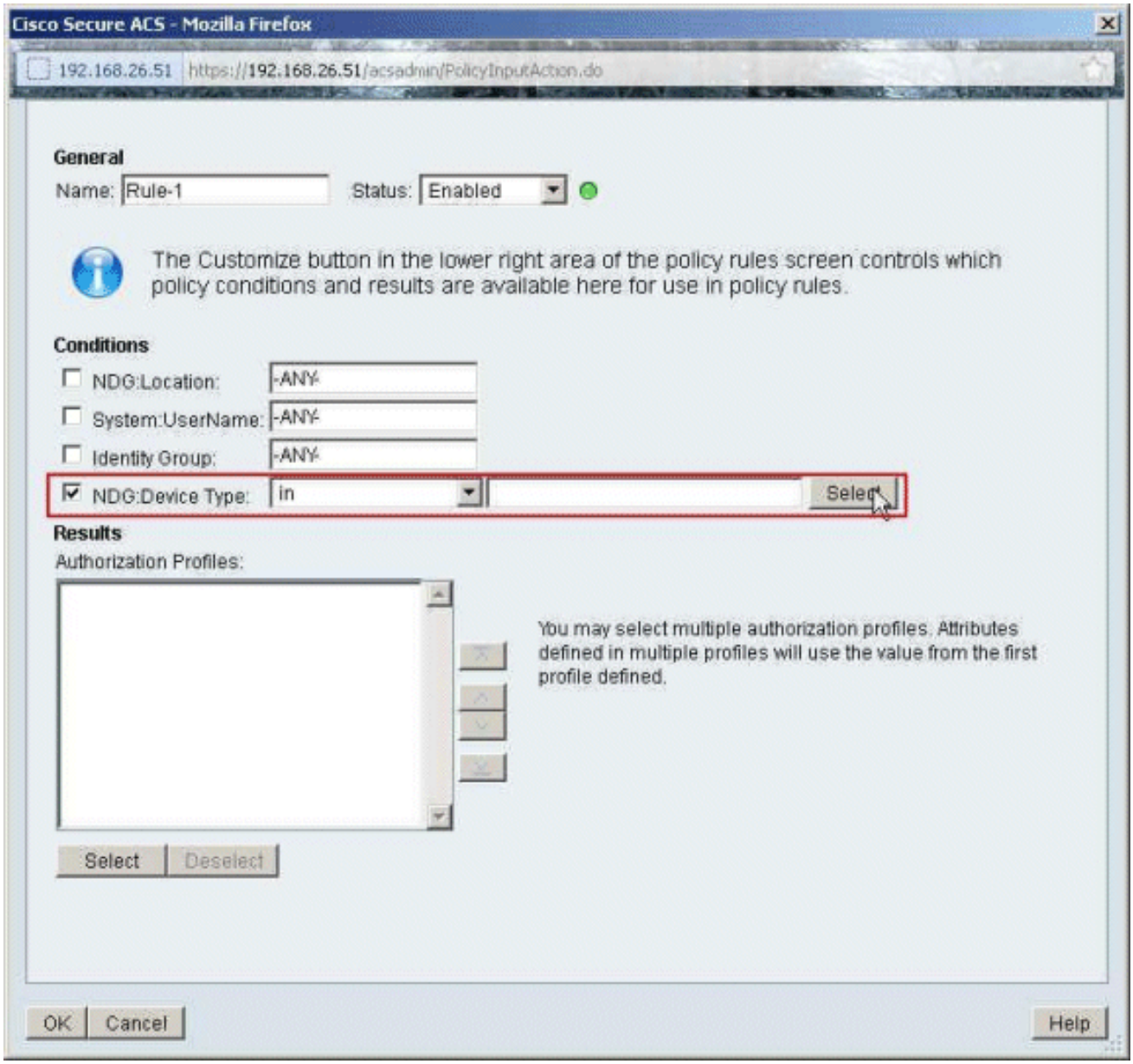
8. 将**NDG：设备类**型从“**可用**”部分移**到“选**定”部分，然后单**击“确定”。**



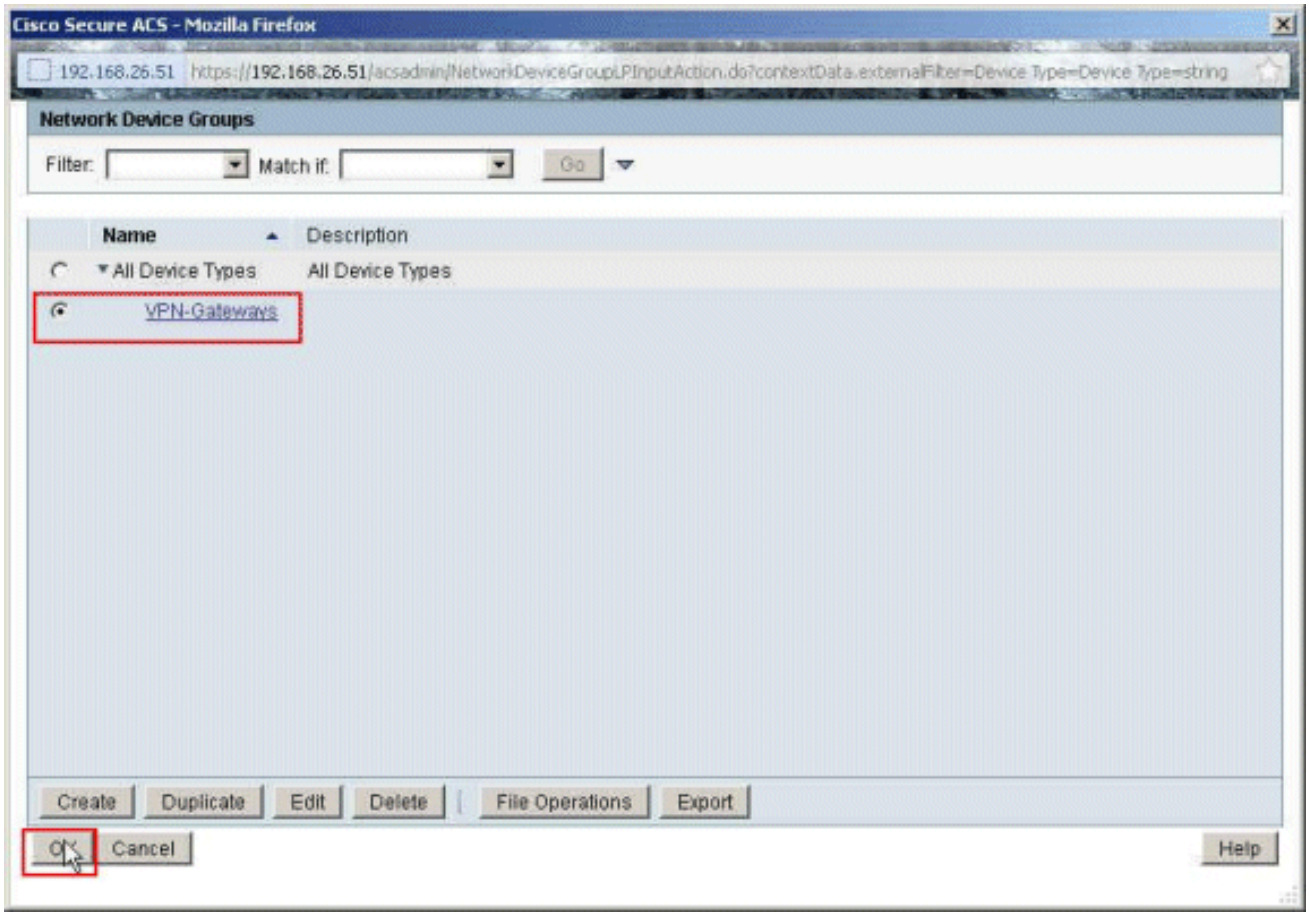
9. 单击**Create**以创建新规则。



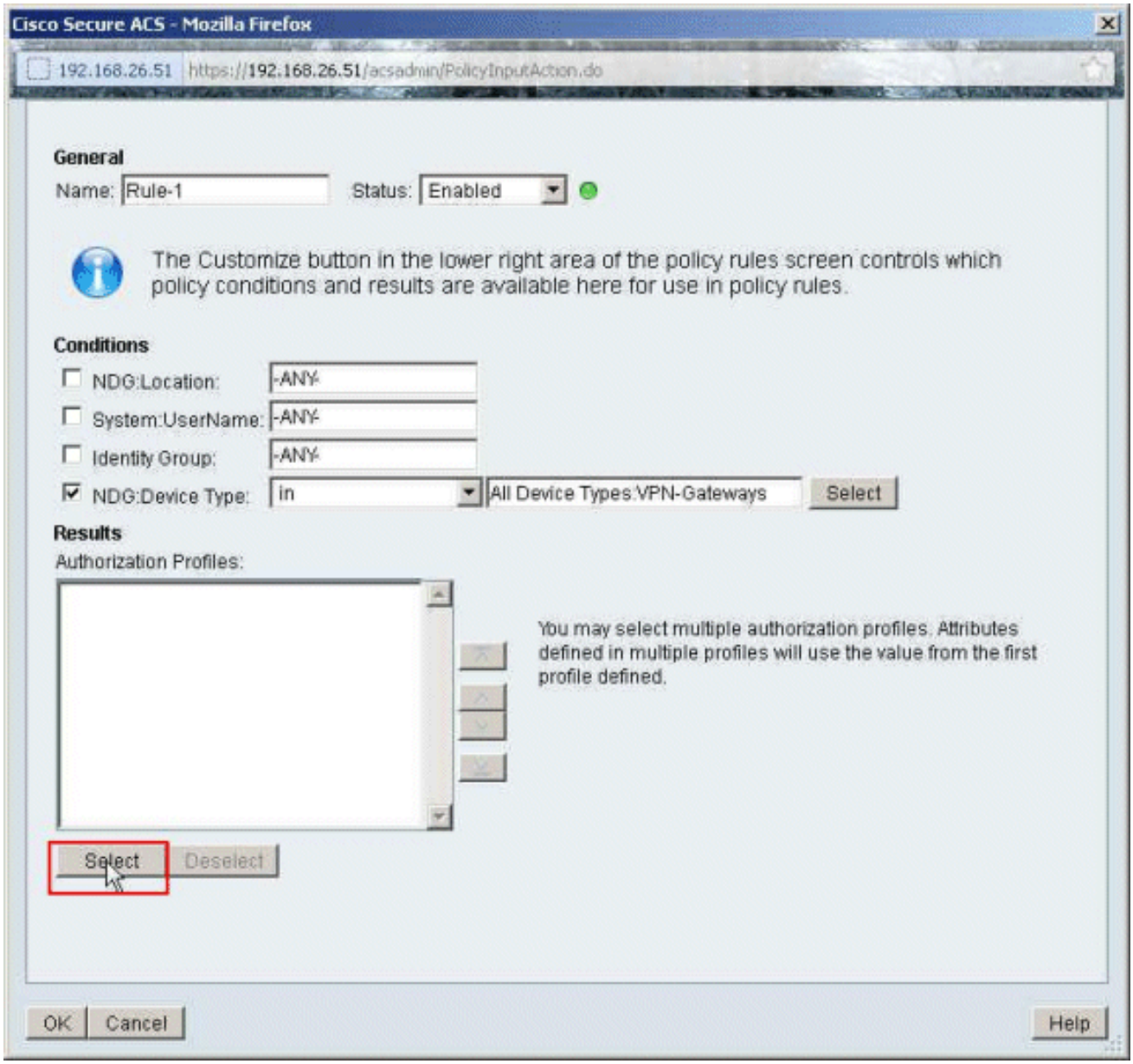
10. 确保选中NDG:Device Type**旁的复选**框，并从下**拉列**表中选择“in”。单击**选择**。



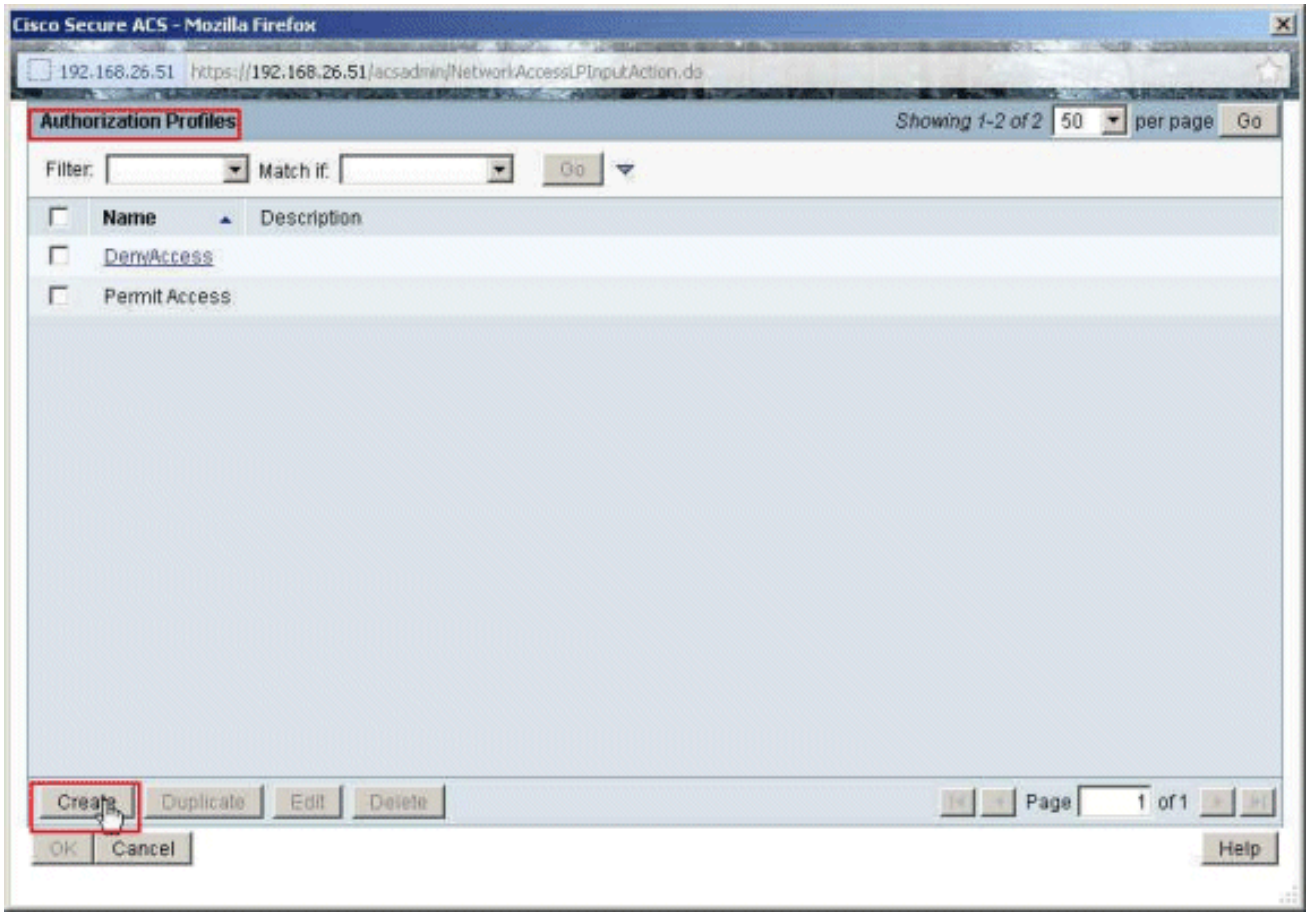
11. 选择之前创建的**网络设备组**VPN网关，然后单**击OK**。


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

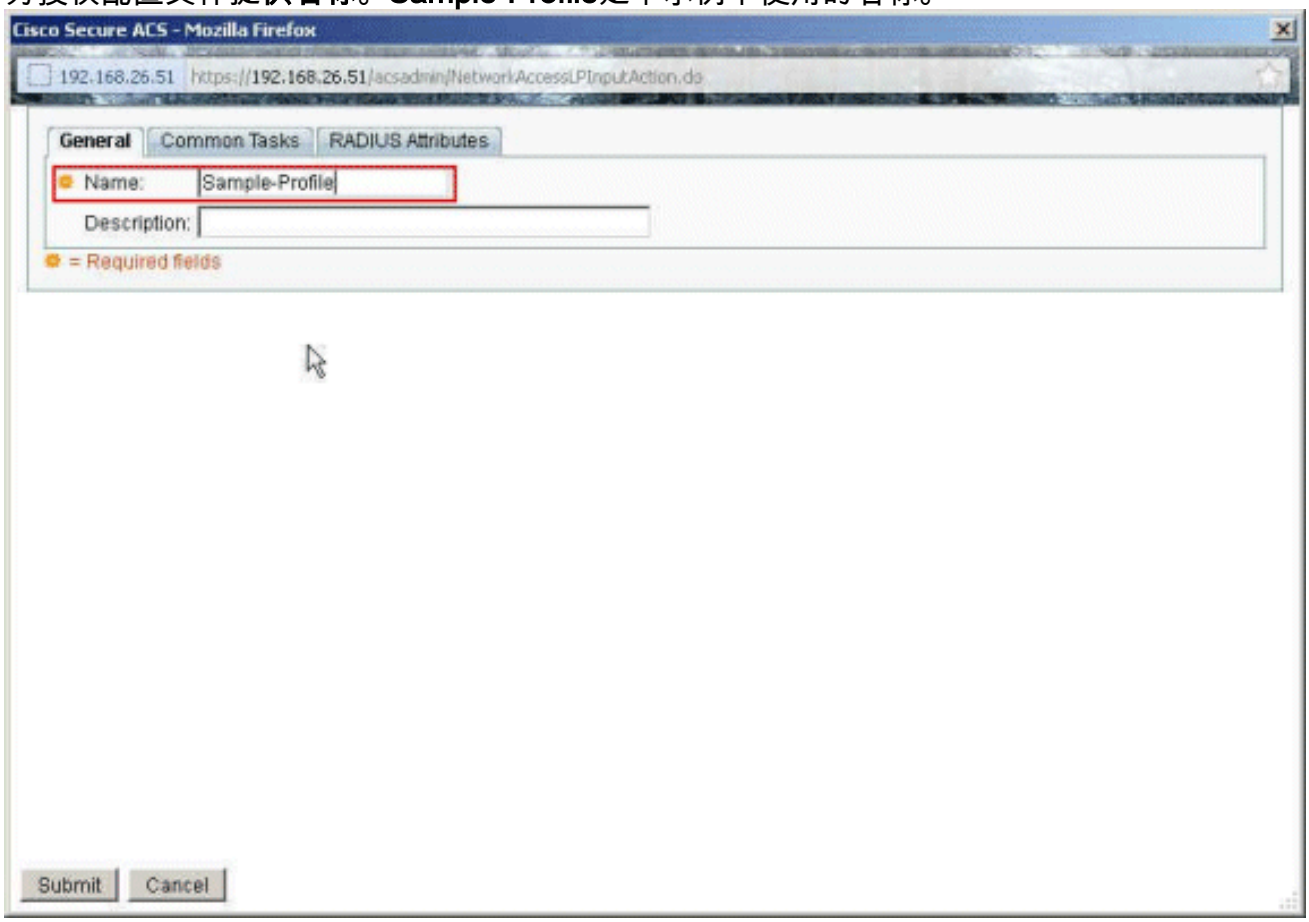
12. 单击**选择**。



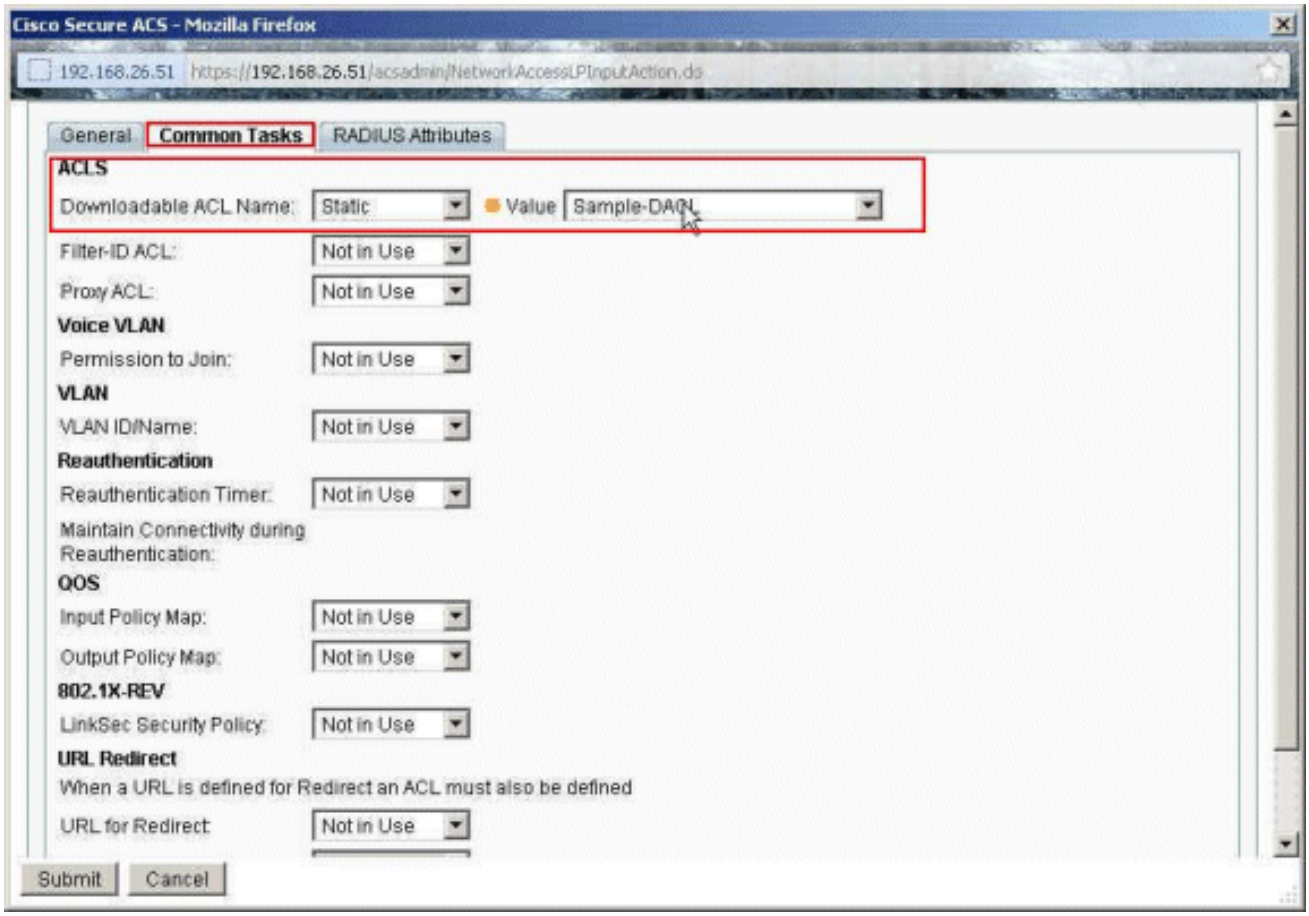
13. 单击**Create**以创建新的授权配置文件。



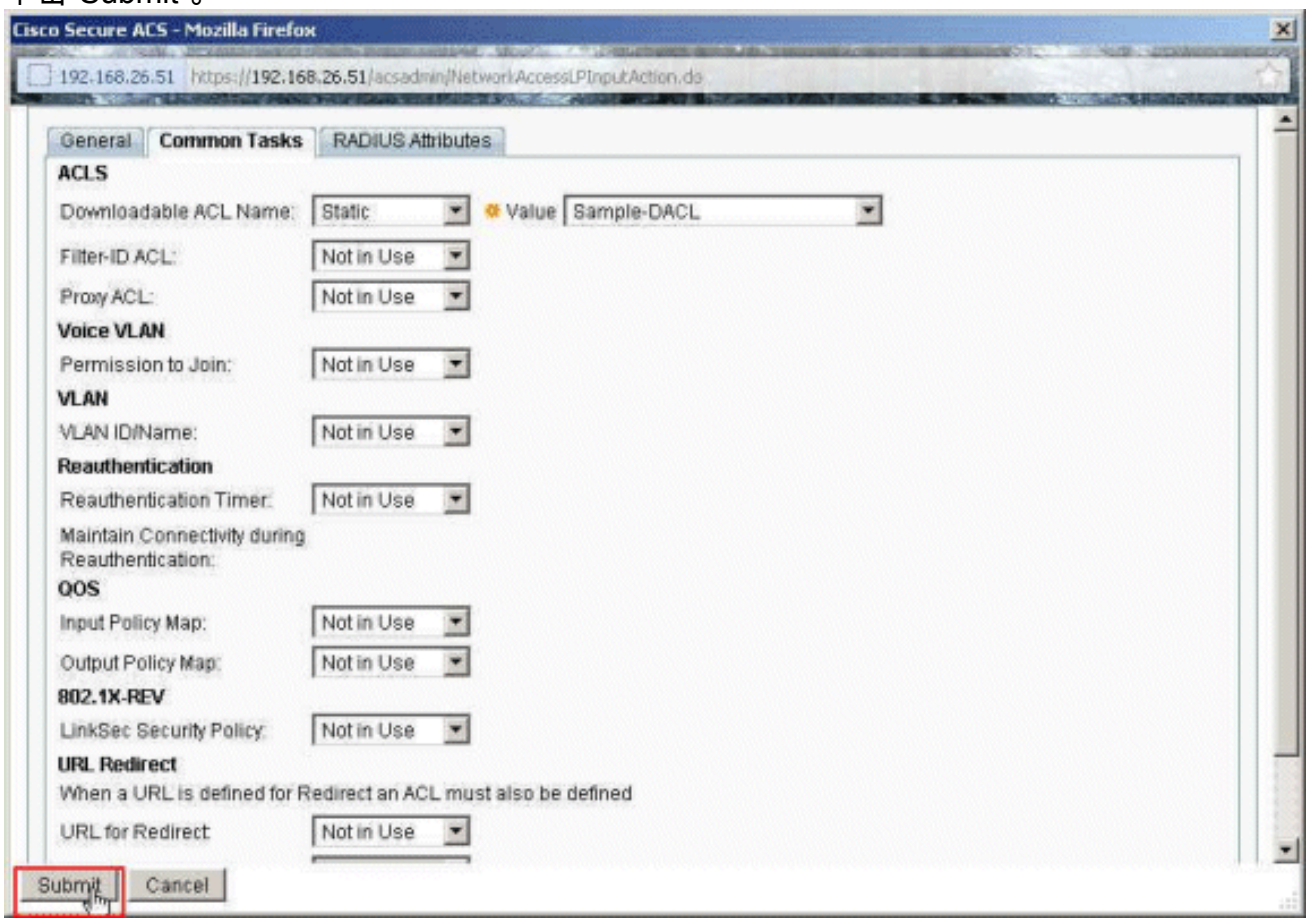
14. 为授权配置文件提**供名称。Sample-Profile**是本示例中使用的名称。



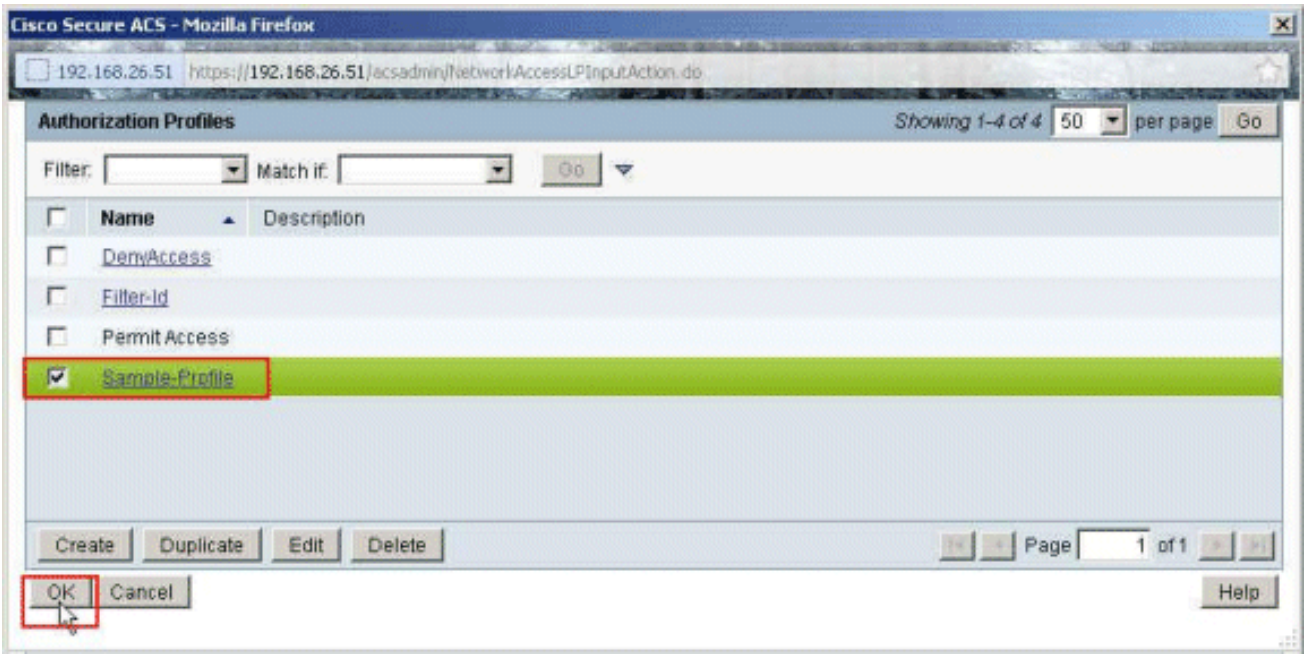
15. 选择**Common Tasks**选项卡，并从Downloadable ACL Name的下拉列**表**中选择Static。从value下拉列**表中选择新**创建的DACL(Sample-DACL)。



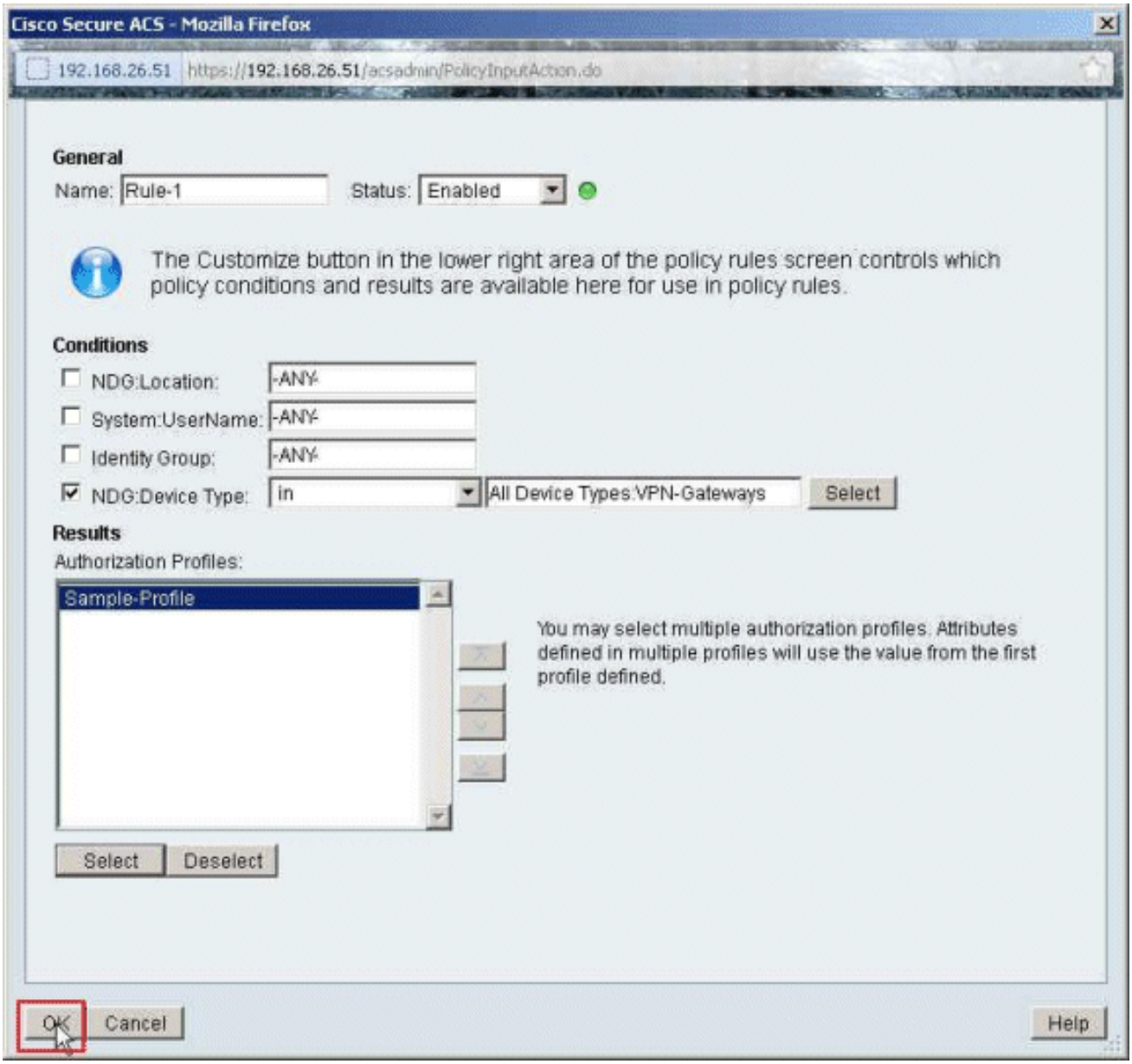
16. 单击“Submit”。



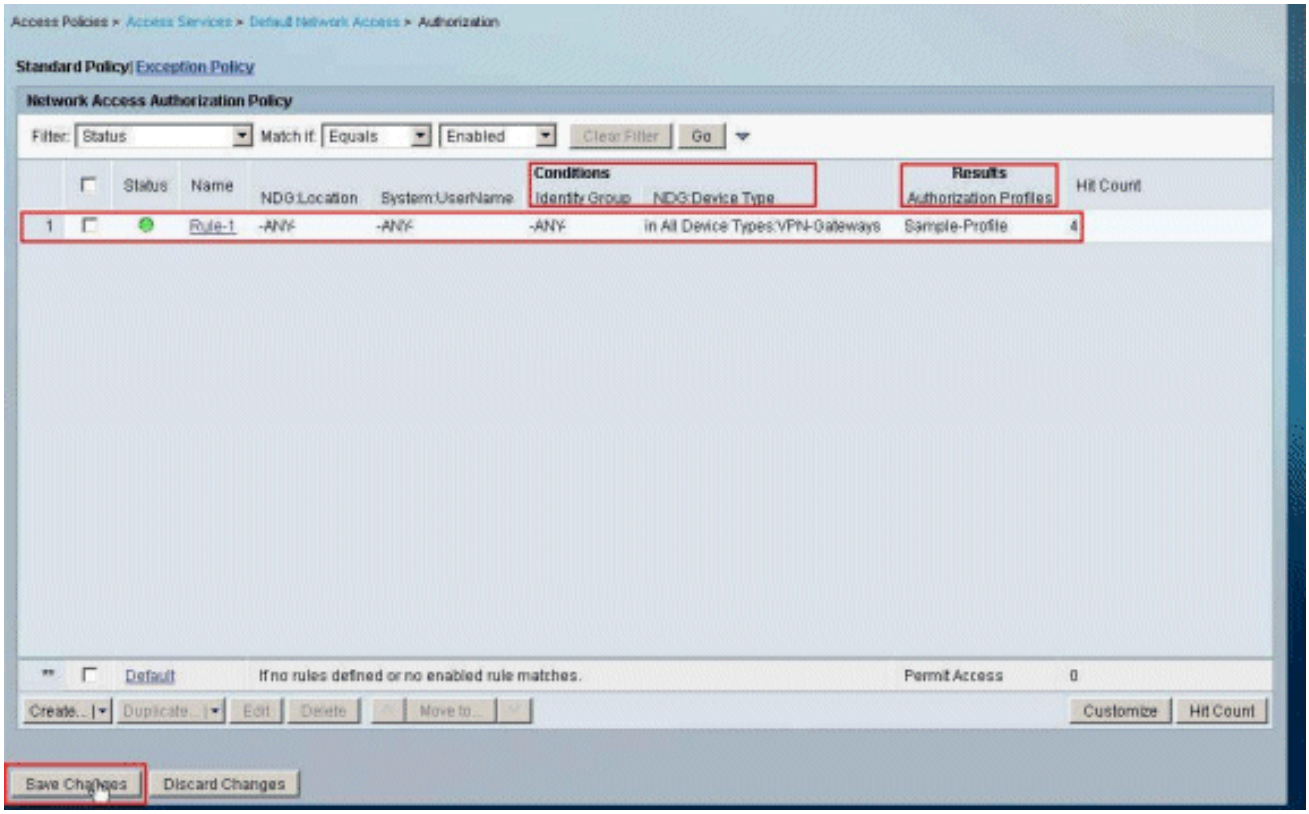
17. 选择**先前创建的**示例配置文件，然后单**击确定**。



18. Click
    OK.



19. 验证**Rule-1**是以**VPN-Gateways** 作为NDG:Device Type作为条件，**Sample-Profile作为**结果创建的。点击**Save Changes**。



为用户组配置 IETF RADIUS 设置

要在用户进行身份验证时从RADIUS服务器下载您已在安全设备上创建的访问列表的名称，请配置IETF RADIUS过滤器ID属性（属性编号11）：

```
filter-id=acl_name
```

示例组用户**cisco**成功进行身份验证，RADIUS服务器会为您已在安全设备上创建的访问列表下载ACL名称（新）。用户“cisco”可以访问ASA网络内除10.1.1.2服务器外的所**有**设备。要检验ACL，请参阅Filter-Id ACL部分。

根据示例，命名为new的ACL**已配**置为在ASA中进行过滤：

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

这些参数只有在以下条件成立时才会显。您已进行以下配置:

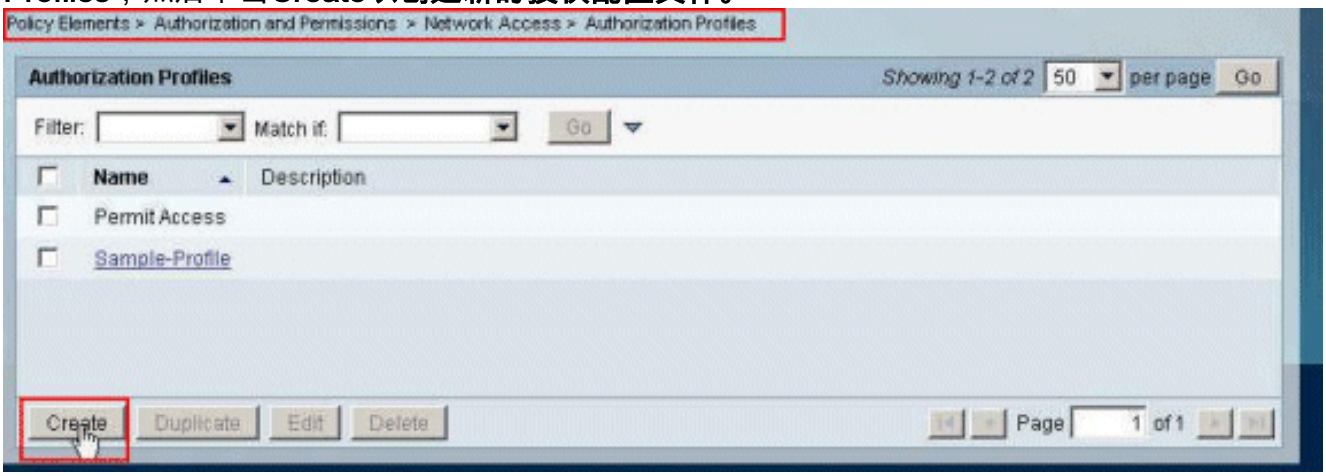
- 在 Network Configuration 中将 AAA 客户端配置为使用其中一个 RADIUS 协议
- 在Access-Service中规则的结果部分下选择具有RADIUS(IETF)Filter-Id的授权配置文件。

RADIUS 属性会作为每个用户的配置文件从 ACS 发送到请求的 AAA 客户端。

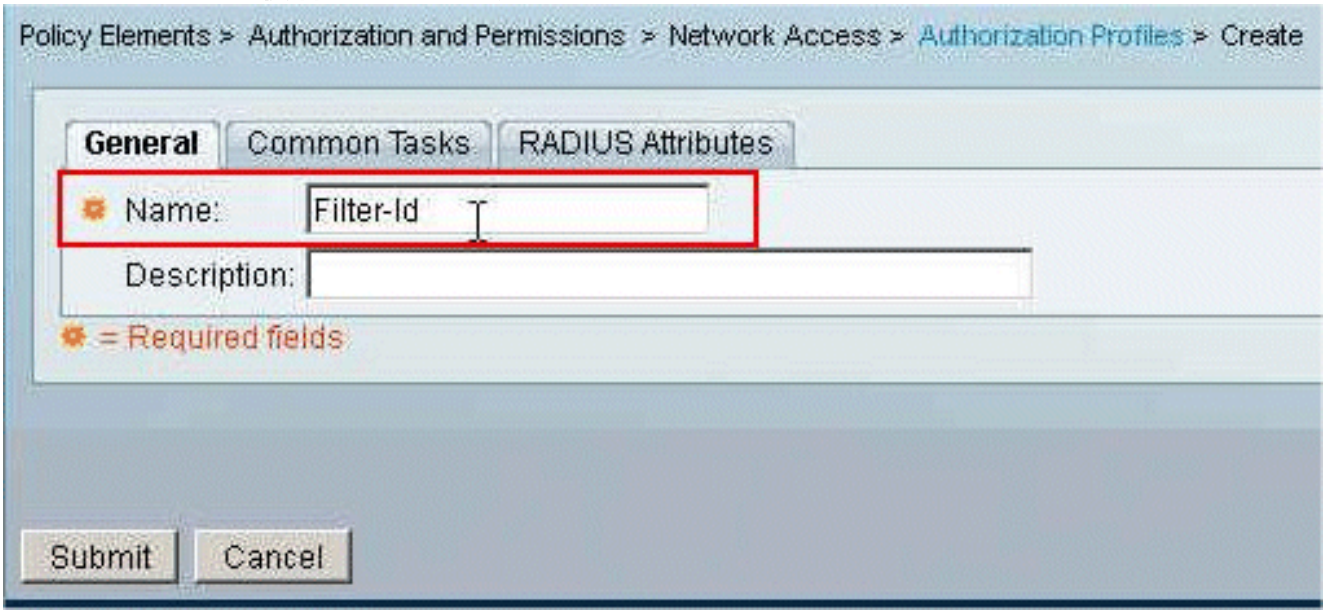
完成为单个用户的可下载ACL配置ACS的步骤1至6和10至12，然后完成为组的可下载ACL配置ACS的步骤1至6，并在本节中执行这些步骤以在Cisco Secure ACS中配置Filter-Id。

要将IETF RADIUS属**性设置**配置为应用与授权配置文件中一样，请执行以下步骤：

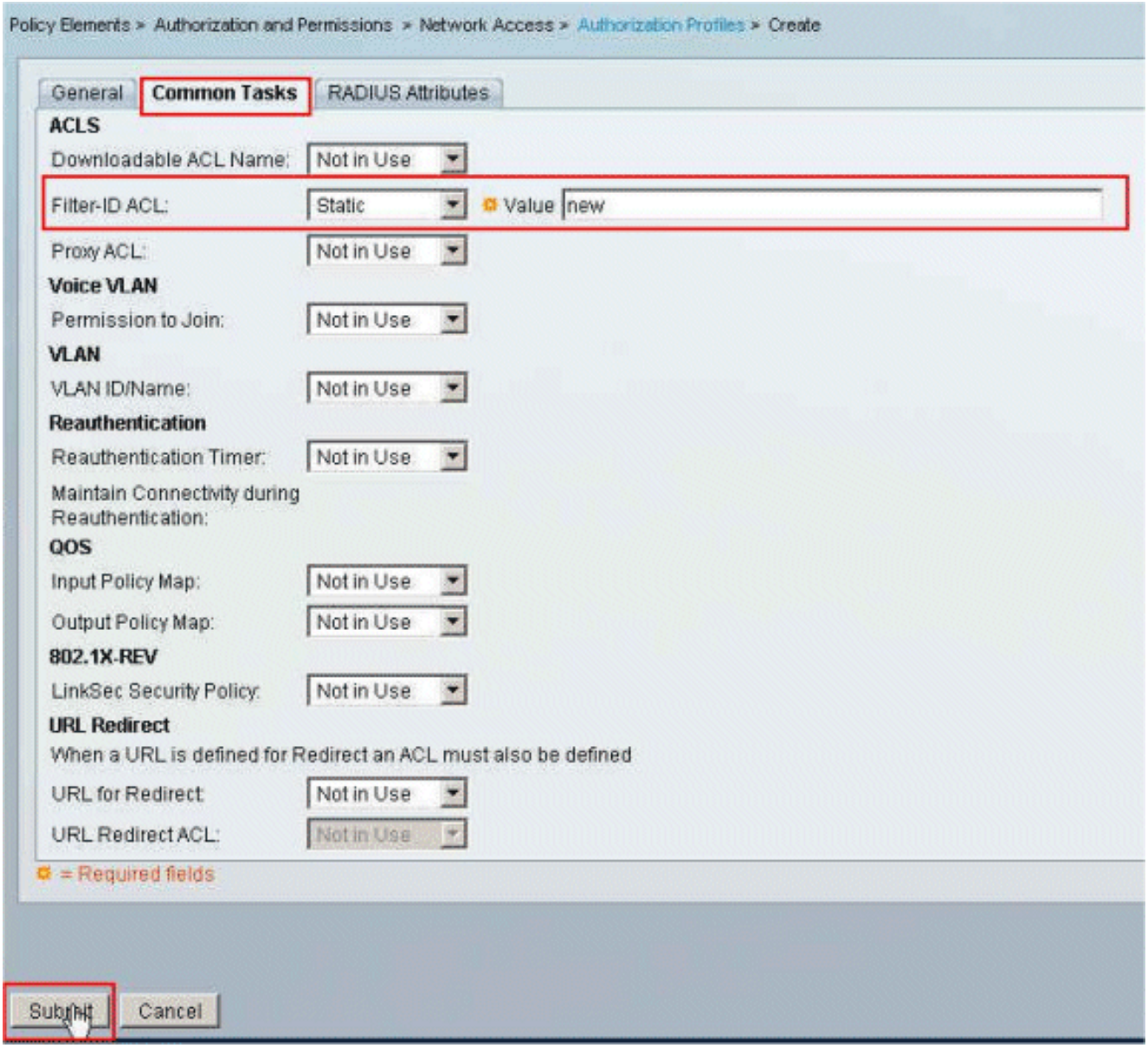
1. 选择Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles，然后单击Create以创建新的授权配置文件。



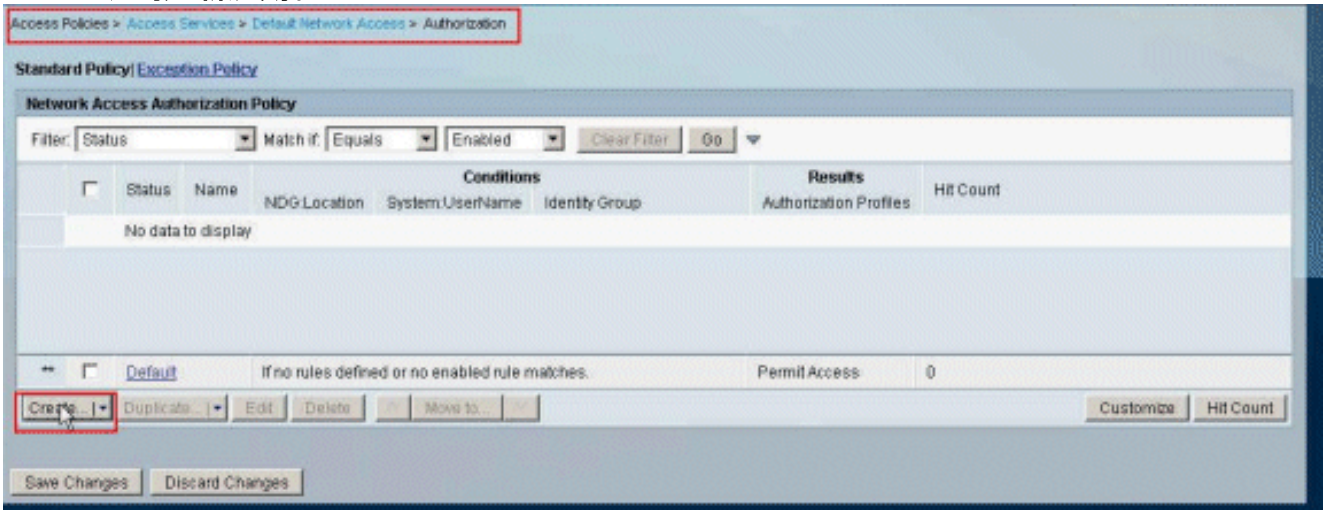
2. 为授权配置文件提供名称。Filter-Id是为简便起见在本示例中选择的授权配置文件名称。



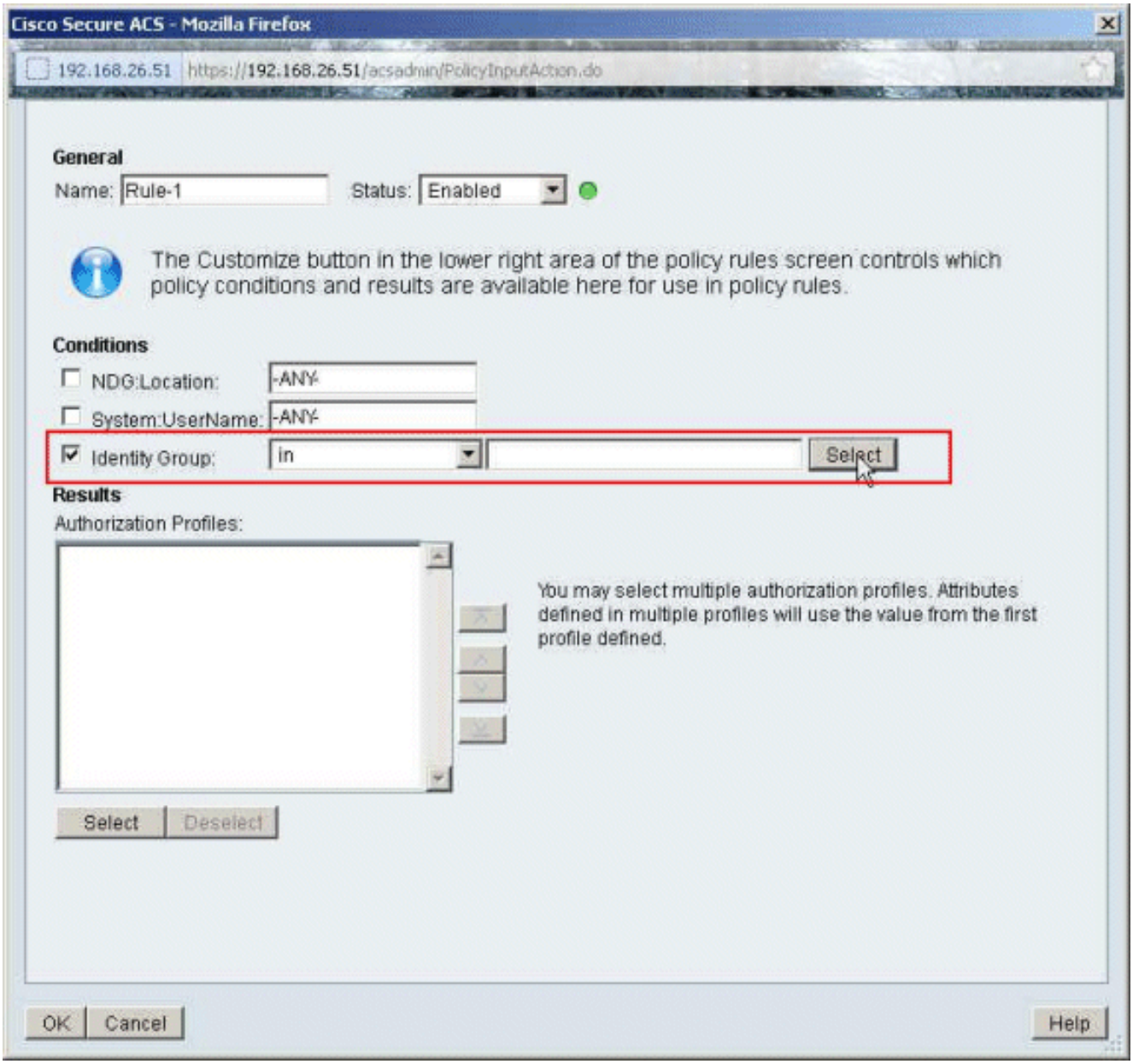
3. 单击Common Tasks选项卡，并从Filter-ID ACL的下拉列表中选择Static。在“值”字段中输入访问列表名称，然后单击“提交”。



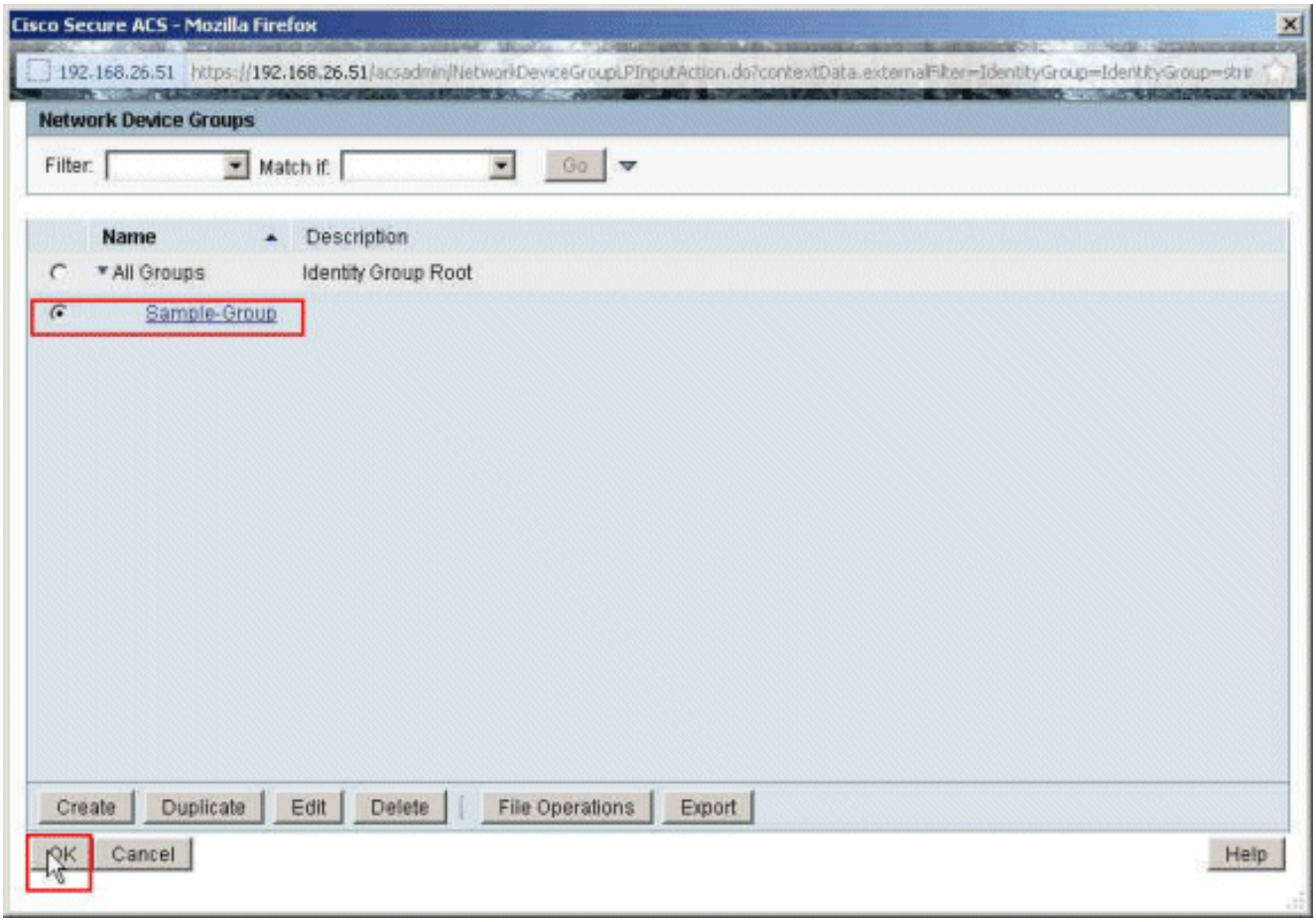
4. 选择**Access Policies > Access Services > Default Network Access > Authorization**，然后单击**Create以创建新规则。**



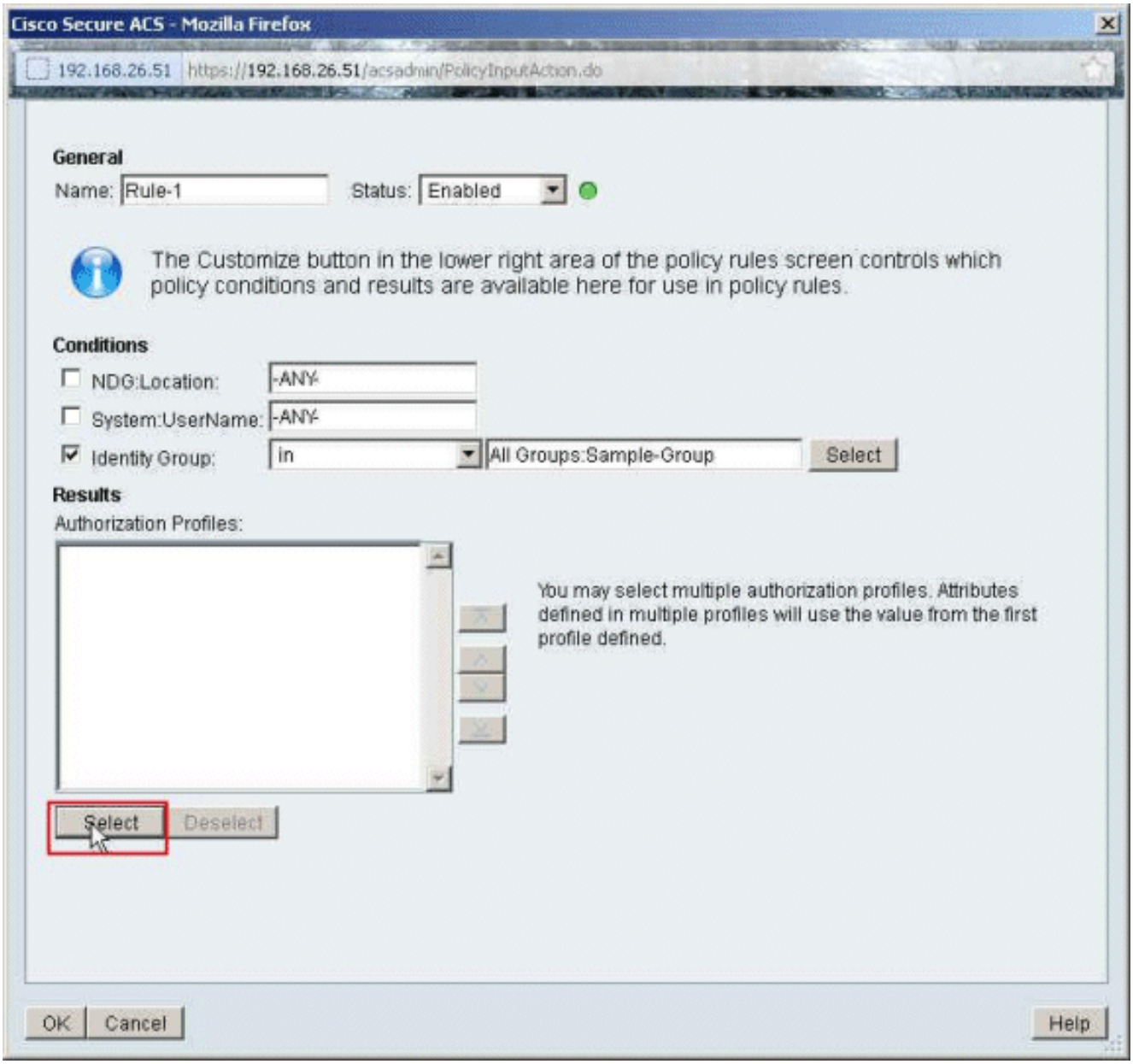
5. 确保选中“身份组”(Identity Group)**旁边的复**选框，然后单击“选**择”(Select**)。



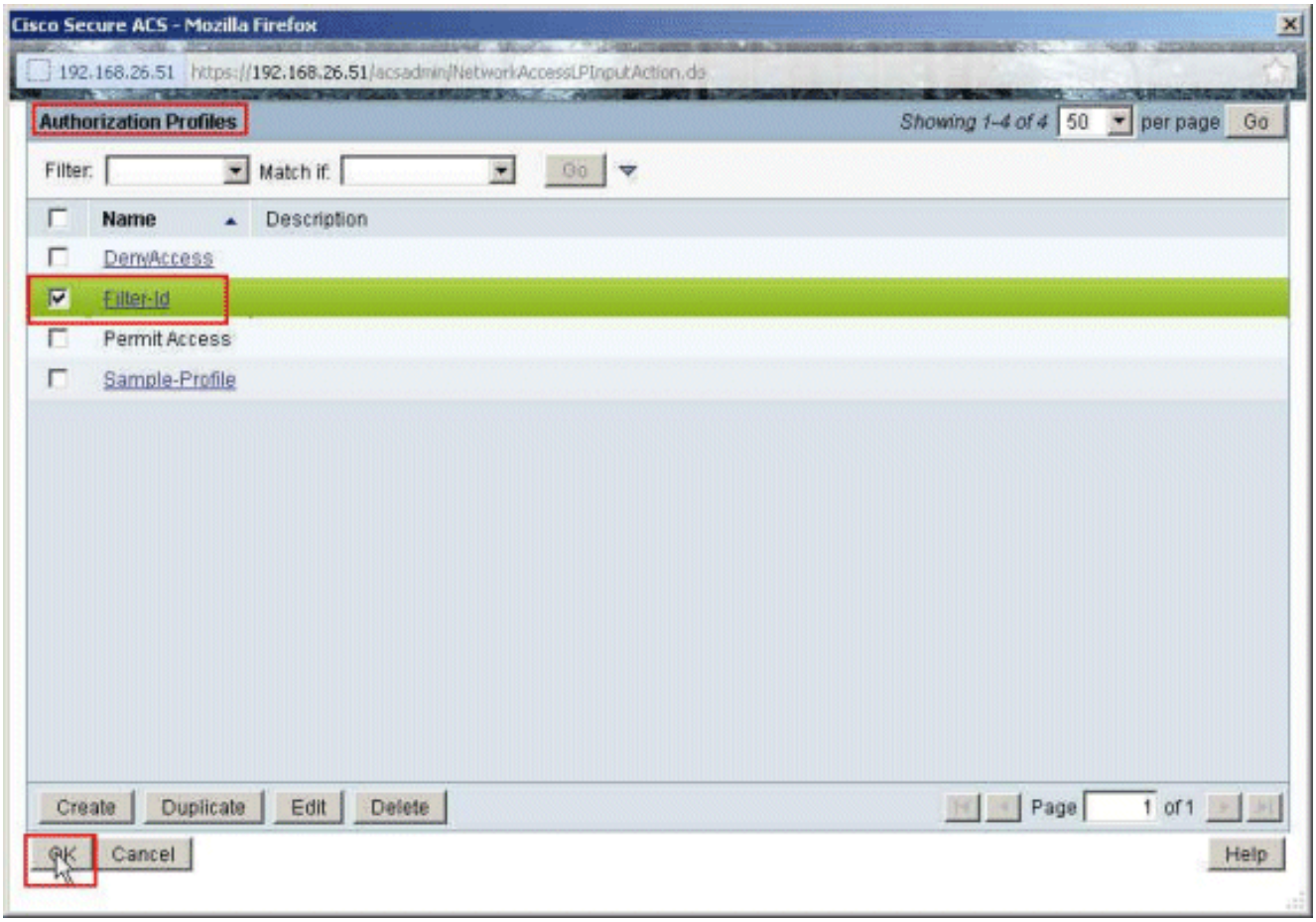
6. 选择Sample-Group,然后单击OK。



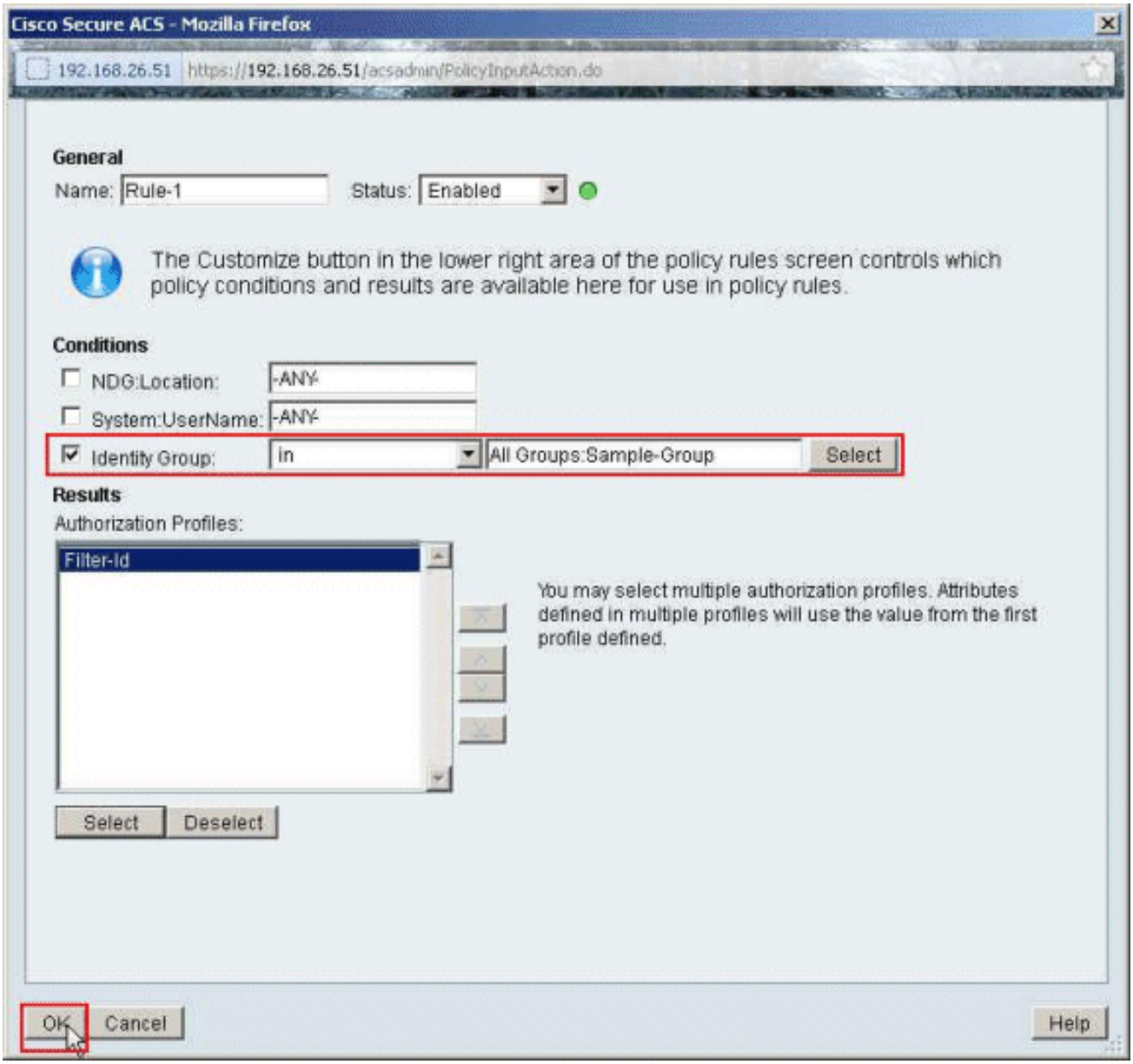
7. 在“授权配置文件”(Authorization Profiles)部分中单击**选择**。



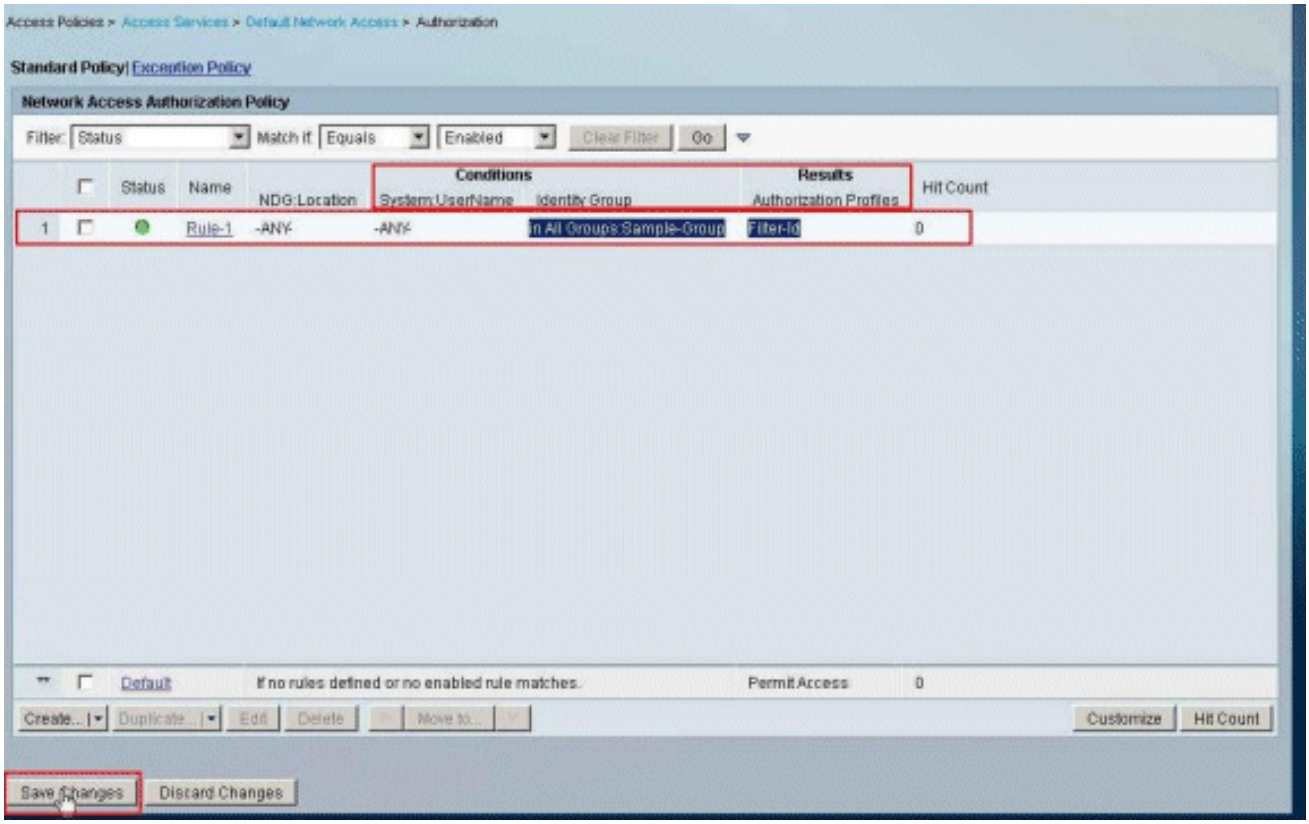
8. 选择之前创建的授**权配置文件**过滤器ID，然后单**击确定**。


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. Click **OK**.



10. 验证是**否已创**建Rule-1，并将身**份组样本**组作为条**件并将**Filter-Id作为结果。点击**Save Changes**。

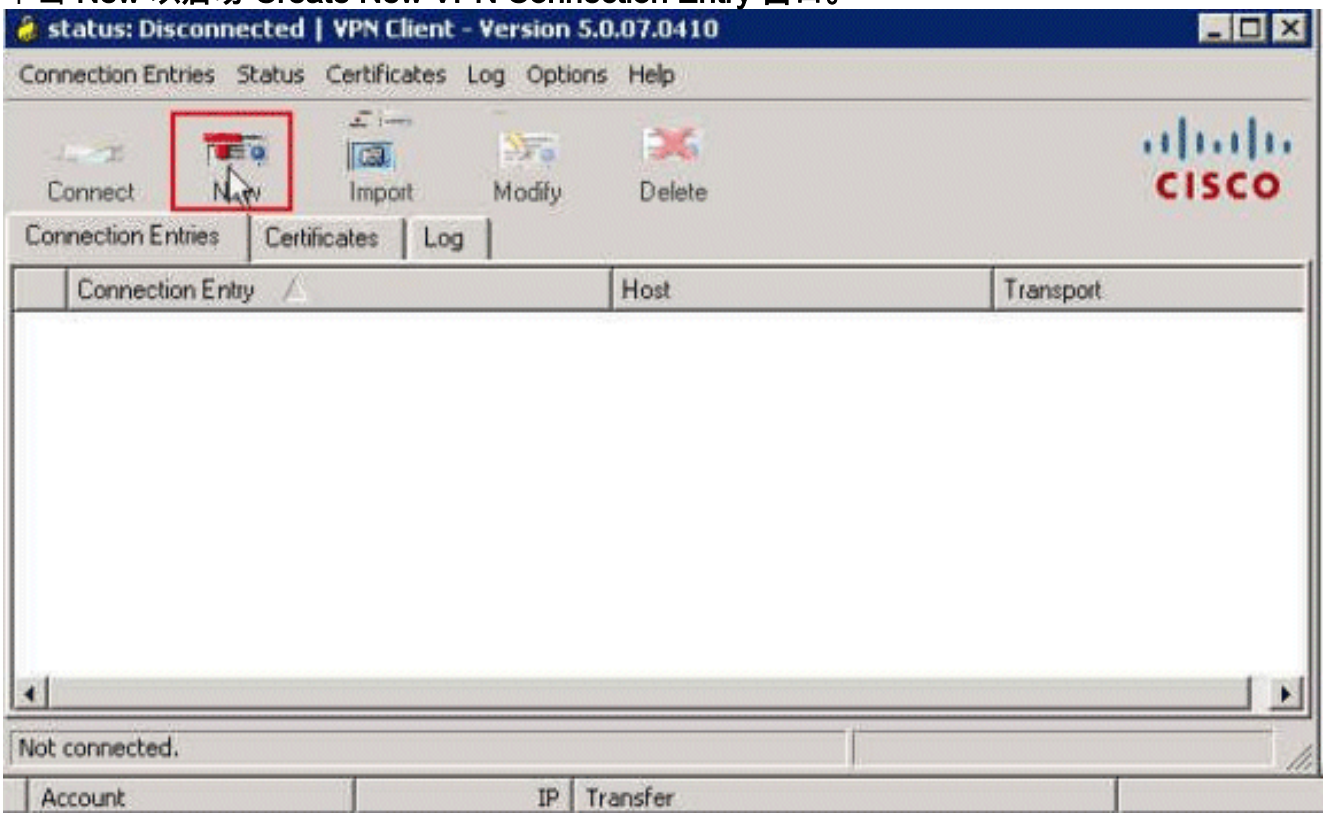


Cisco VPN 客户端配置

使用Cisco VPN客户端连接到Cisco ASA，以验证ASA是否已成功配置。

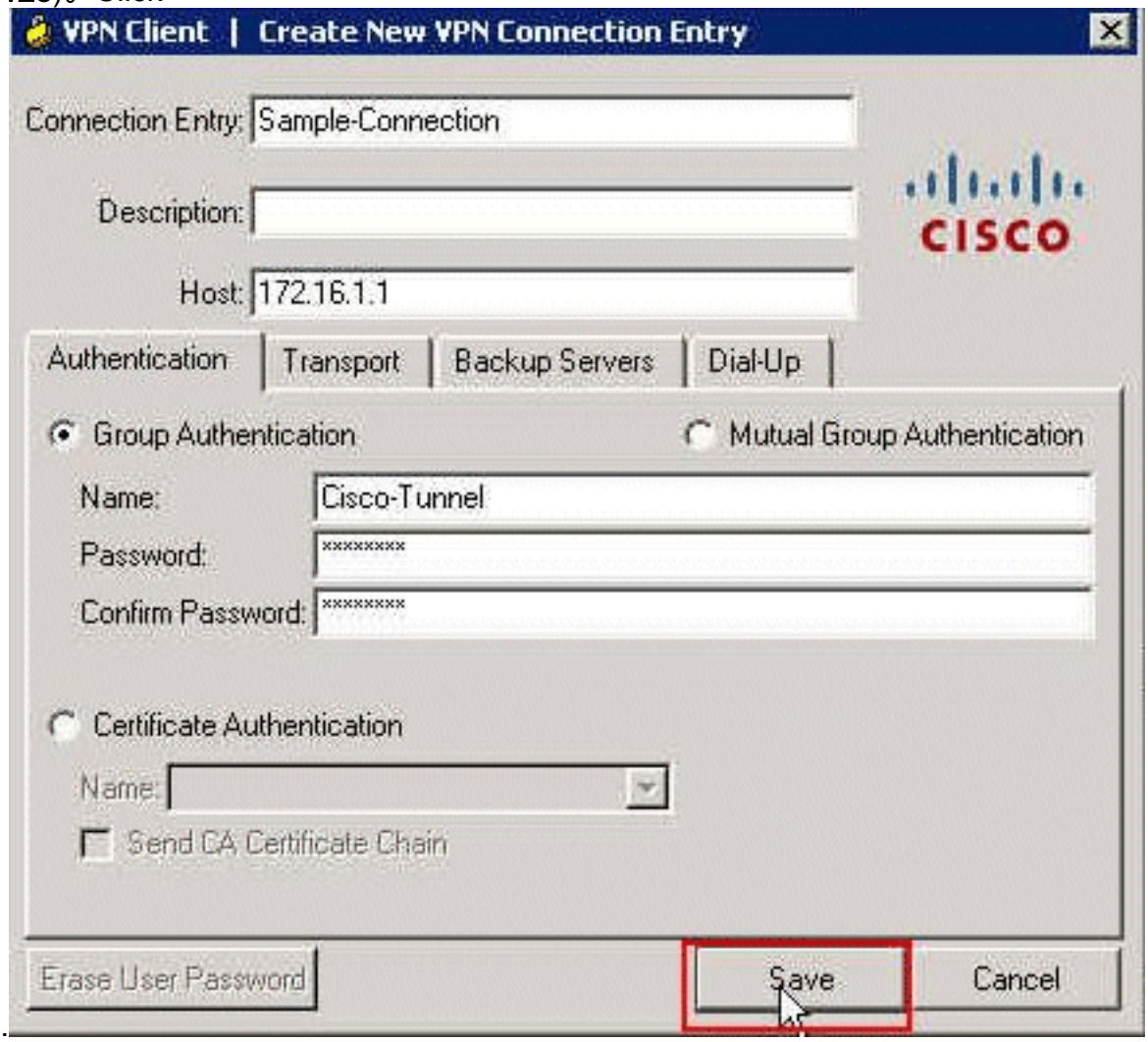
请完成以下步骤：

1. 选择**开始 > 程序 > Cisco Systems VPN 客户端 > VPN 客户端**。
2. 单击 **New 以启动 Create New VPN Connection Entry 窗口**。

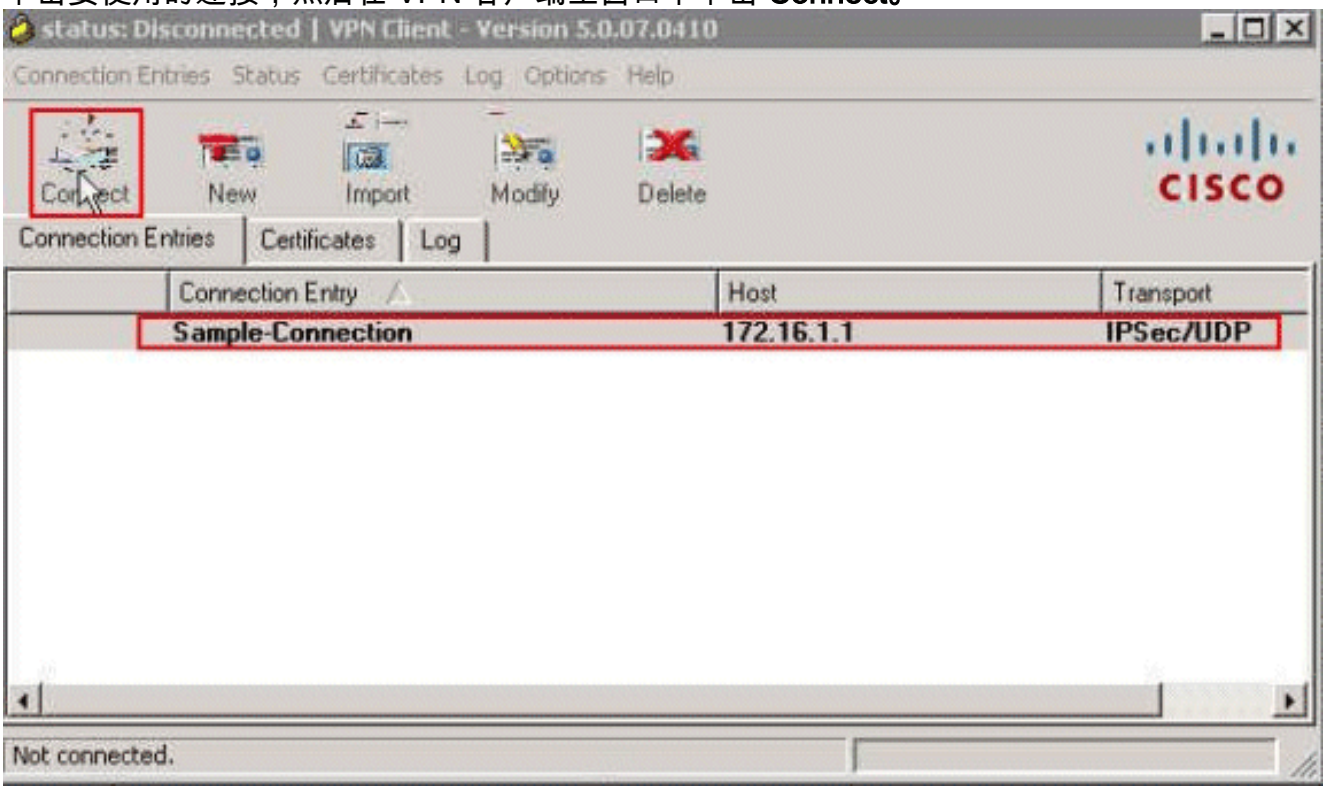


3. 填写新连接的详细信息：输入 Connection Entry 的名称与说明。在 Host 框中输入 **ASA 的外**

部 IP 地址。输入ASA中配置的VPN隧道组名**称(Cisco-Tunnel)**和密码(预共享密钥 — **cisco123**)。Click **Save**.

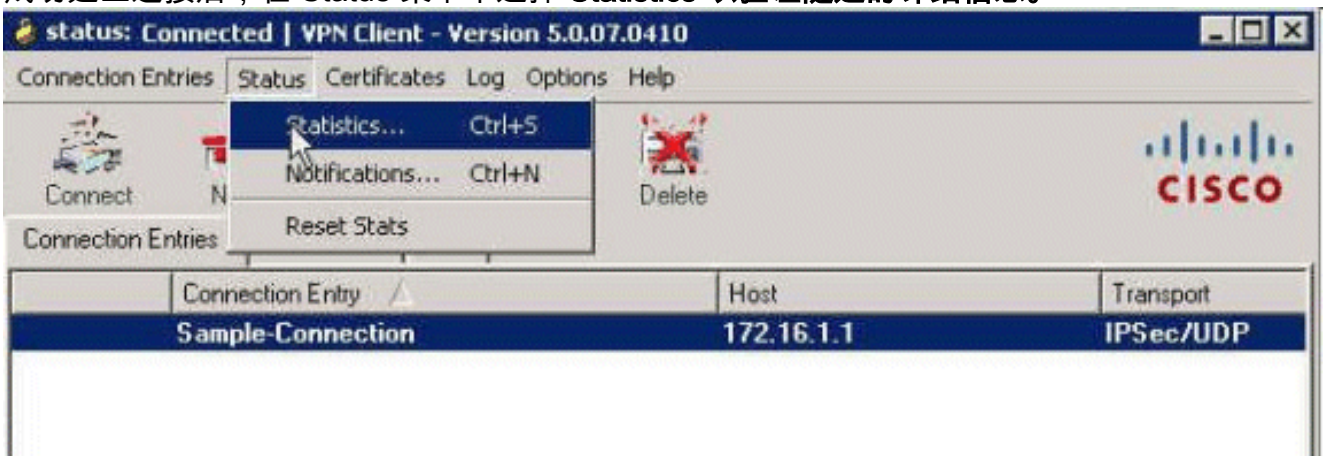


4. 单击要使用的连接，然后在 VPN 客户端主窗口中单击 **Connect。**



5. 出现提示时，输入用户名**cisco**和口令**cisco123**（如ASA中配置）进行身份验证，然后单击**OK**以连接到远程网络。

6. 成功建立连接后，在 Status 菜单中选择 **Statistics 以验证隧道的详细信息。**



验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

显示 Crypto 命令

- **show crypto isakmp sa - 显示对等体上的所有当前 IKE 安全关联 (SA)。**

```
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 - 显示当前 SA 使用的设置。**

```
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
```

适用于用户/组的可下载 ACL

验证用户 Cisco 的可下载 ACL。ACL从CSACS下载。

```
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
```

Filter-Id ACL

[011] Filter-Id已应用于Group - Sample-Group，并且组的用户会根据ASA中定义的ACL（新）进行过滤。

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。此外本部分还提供了 debug 输出示例。

注：有关远程访问IPsec VPN故障排除的详细信息，请参阅最常见的L2L和远程访问IPsec VPN故障排除解决方案。

清除安全关联

排除故障时，请确保在进行更改后清除现有的SA。在 PIX 的特权模式下，使用以下命令：

- **clear [crypto] ipsec sa** — 删除活动IPsec SA。关键字 crypto 是可选的。
- **clear [crypto] isakmp sa** — 删除活动IKE SA。关键字 crypto 是可选的。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关**debug命**令的重要信息。

- **debug crypto ipsec 7** — 显示第2阶段的IPsec协商。
- **debug crypto isakmp 7** — 显示第1阶段的ISAKMP协商。

相关信息

- Cisco ASA 5500 系列自适应安全设备支持页
- Cisco ASA 5500 系列自适应安全设备命令参考
- Cisco 自适应安全设备管理器
- IPsec 协商/IKE 协议支持页
- Cisco VPN 客户端支持页
- 思科安全访问控制系统
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems