ASA 8.3 and Later: Radius Authorization (ACS 5.x) for VPN Access Using Downloadable ACL with CLI and ASDM Configuration Example

Contents

Introduction

This document describes how to configure the security appliance to authenticate users for network access. Since you can implicitly enable RADIUS authorizations, this document contains no information about the configuration of RADIUS authorization on the security appliance. It does provide information about how the security appliance handles access list information received from RADIUS servers.

You can configure a RADIUS server to download an access list to the security appliance or an

access list name at the time of authentication. The user is authorized to do only what is permitted in the user-specific access list.

Downloadable access lists are the most scalable means when you use Cisco Secure Access Control Server (ACS) to provide the appropriate access lists for each user. For more information on Downloadable Access List Features and the Cisco Secure ACS, refer to Configuring a RADIUS Server to Send Downloadable Access Control Lists and Downloadable IP ACLs.

Refer to ASA/PIX 8.x: Radius Authorization (ACS) for Network Access using Downloadable ACL with CLI and ASDM Configuration Example for the identical configuration on Cisco ASA with versions 8.2 and earlier.

Prerequisites

Requirements

This document assumes that the Adaptive Security Appliance (ASA) is fully operational and configured to allow the Cisco Adaptive Security Device Manager (ASDM) or CLI to make configuration changes.

Note: Refer to Allowing HTTPS Access for ASDM in order to allow the device to be remotely configured by the ASDM or Secure Shell (SSH).

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA Software version 8.3 and later
- Cisco ASDM version 6.3 and later
- Cisco VPN Client version 5.x and later
- Cisco Secure ACS 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

You can use downloadable IP ACLs in order to create sets of ACL definitions that you can apply to many users or user groups. These sets of ACL definitions are called ACL contents.

Downloadable IP ACLs operate this way:

1. When ACS grants a user access to the network, ACS determines whether a downloadable IP ACL is assigned to the Authorization Profile in the result section.
2. If ACS locates a downloadable IP ACL that is assigned to the Authorization Profile, ACS

sends an attribute (as part of the user session, in the RADIUS access-accept packet) that specifies the named ACL, and the version of the named ACL.
3. If the AAA client responds that it does not have the current version of the ACL in its cache (that is, the ACL is new or has changed), ACS sends the ACL (new or updated) to the device.

Downloadable IP ACLs are an alternative to the configuration of ACLs in the RADIUS Cisco cisco-av-pair attribute [26/9/1] of each user or user group. You can create a downloadable IP ACL once, give it a name, and then assign the downloadable IP ACL to any Authorization Profile if you reference its name. This method is more efficient than if you configure the RADIUS Cisco cisco-av-pair attribute for Authorization Profile.

When you enter the ACL definitions in the ACS web interface, do not use keyword or name entries; in all other respects, use standard ACL command syntax and semantics for the AAA client on which you intend to apply the downloadable IP ACL. The ACL definitions that you enter into ACS comprise one or more ACL commands. Each ACL command must be on a separate line.

In ACS, you can define multiple Downloadable IP ACLs and use them in different Authorization Profiles. Based on the conditions in the Access Service Authorization rules, you can send different Authorization Profiles containing downloadable IP ACLs to different AAA clients.

Further, you can change the order of the ACL contents in a downloadable IP ACL. ACS examines ACL contents, starting from the top of the table, and downloads the first ACL content that it finds. When you set the order, you can ensure system efficiency if you position the most widely applicable ACL contents higher on the list.

In order to use a downloadable IP ACL on a particular AAA client, the AAA client must adhere to these rules:

- Use RADIUS for authentication
- Support downloadable IP ACLs

These are examples of Cisco devices that support downloadable IP ACLs:

- ASA
- Cisco devices that run IOS version 12.3(8)T and later

This is an example of the format that you must use in order to enter ASA ACLs in the ACL Definitions box:

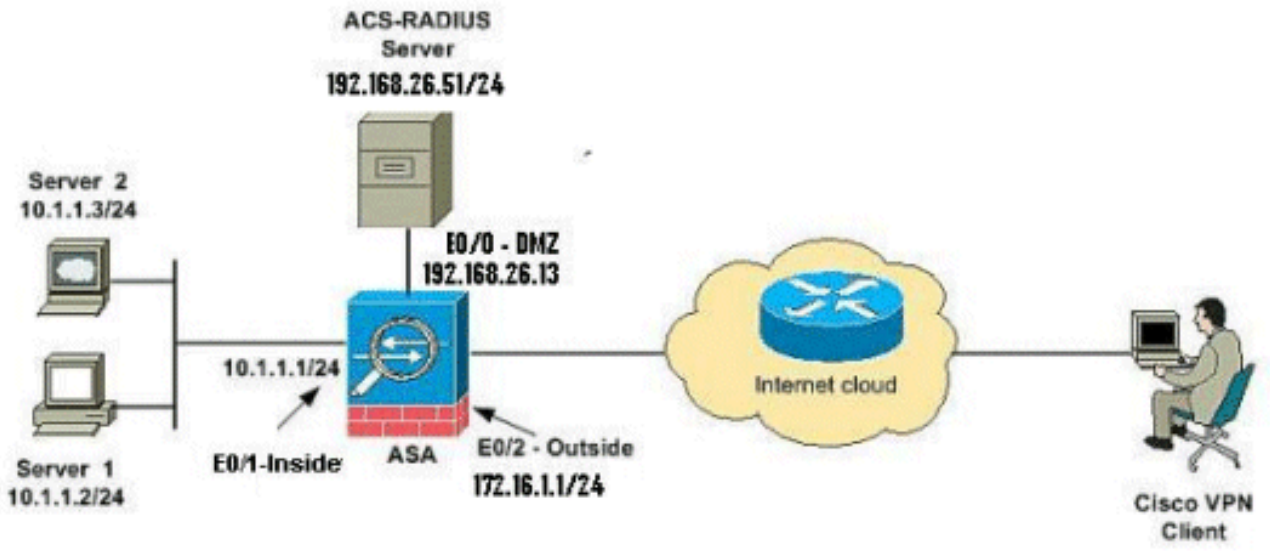
```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3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

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses this network setup:



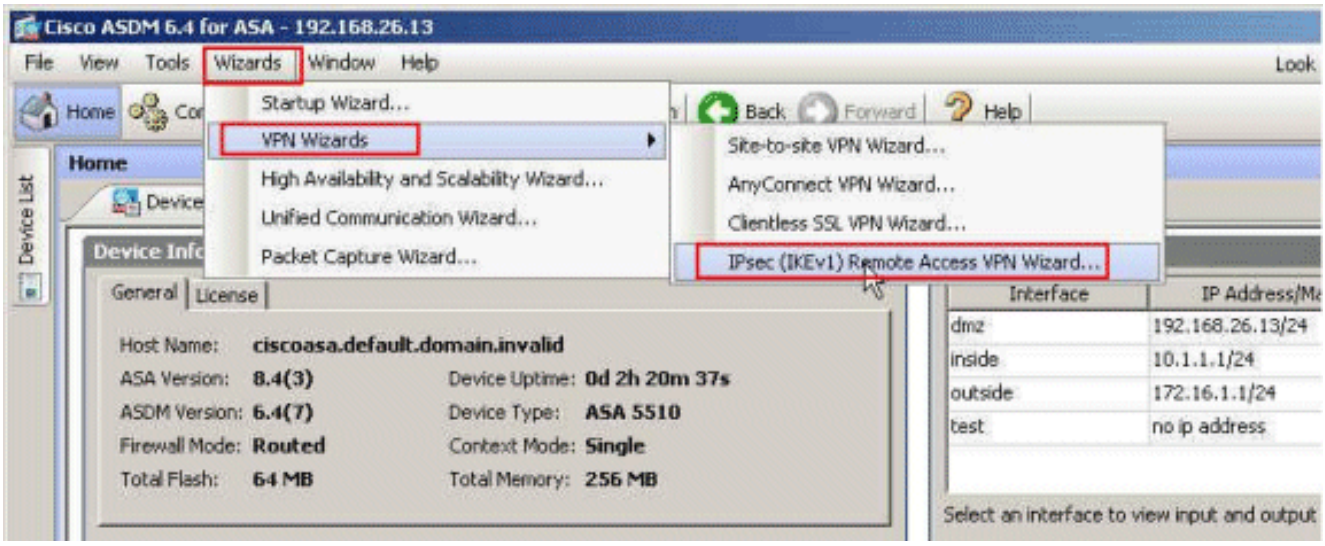
Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which were used in a lab environment.

Configure Remote Access VPN (IPsec)

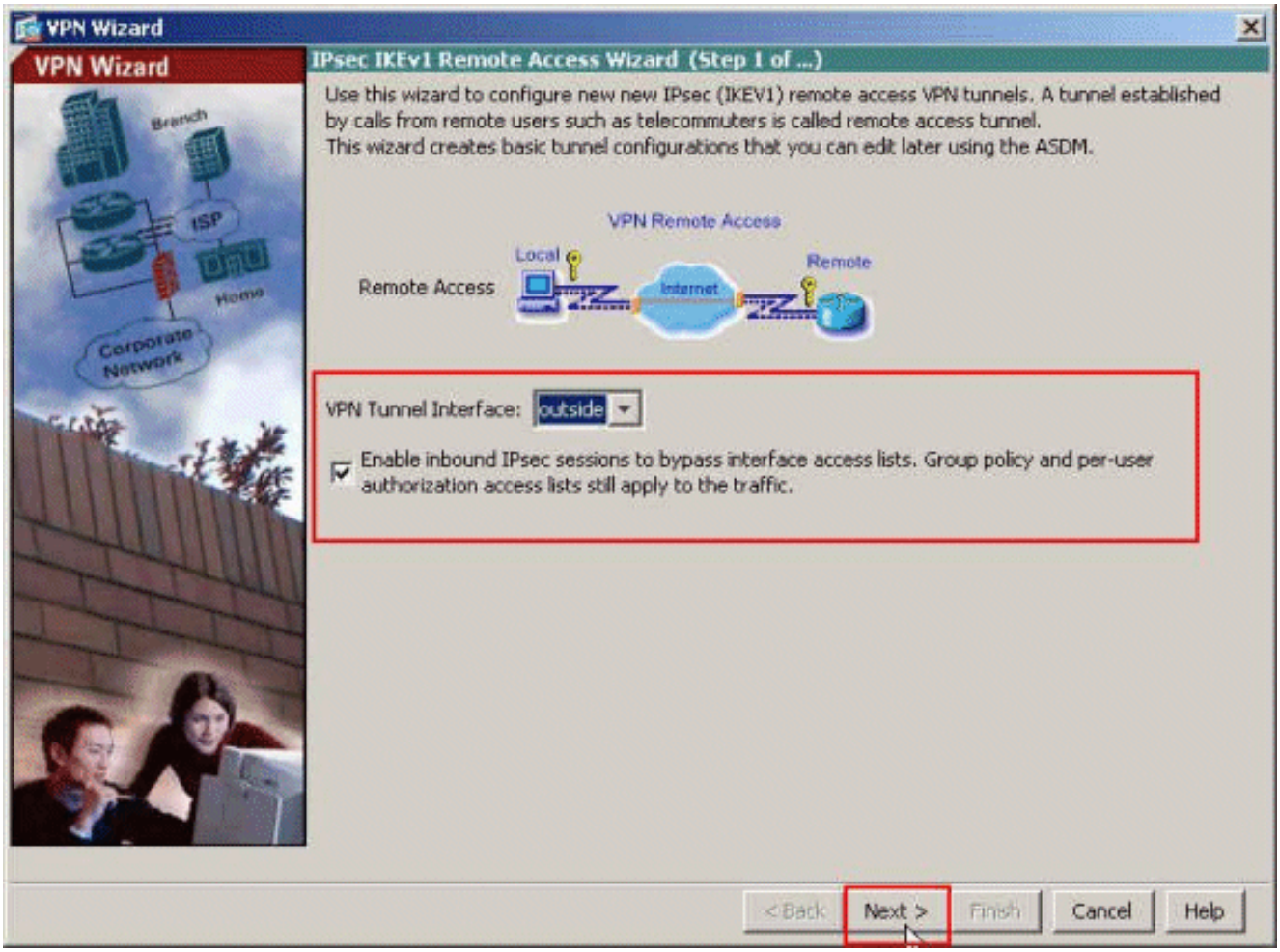
ASDM Procedure

Complete these steps in order to configure the remote access VPN:

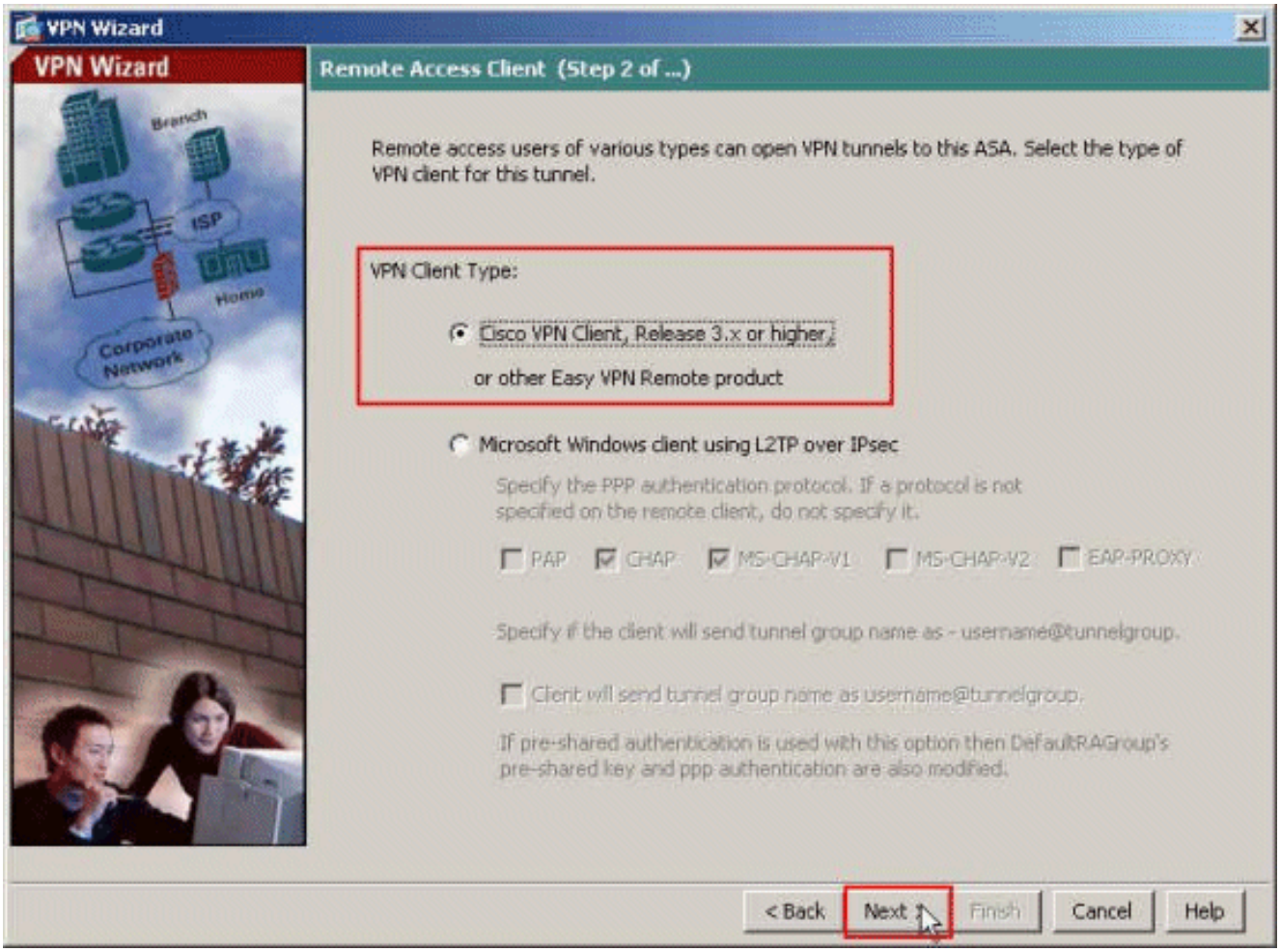
1. Select **Wizards** > **VPN Wizards** > **IPsec(IKEv1) Remote Access VPN Wizard** from the Home
window.



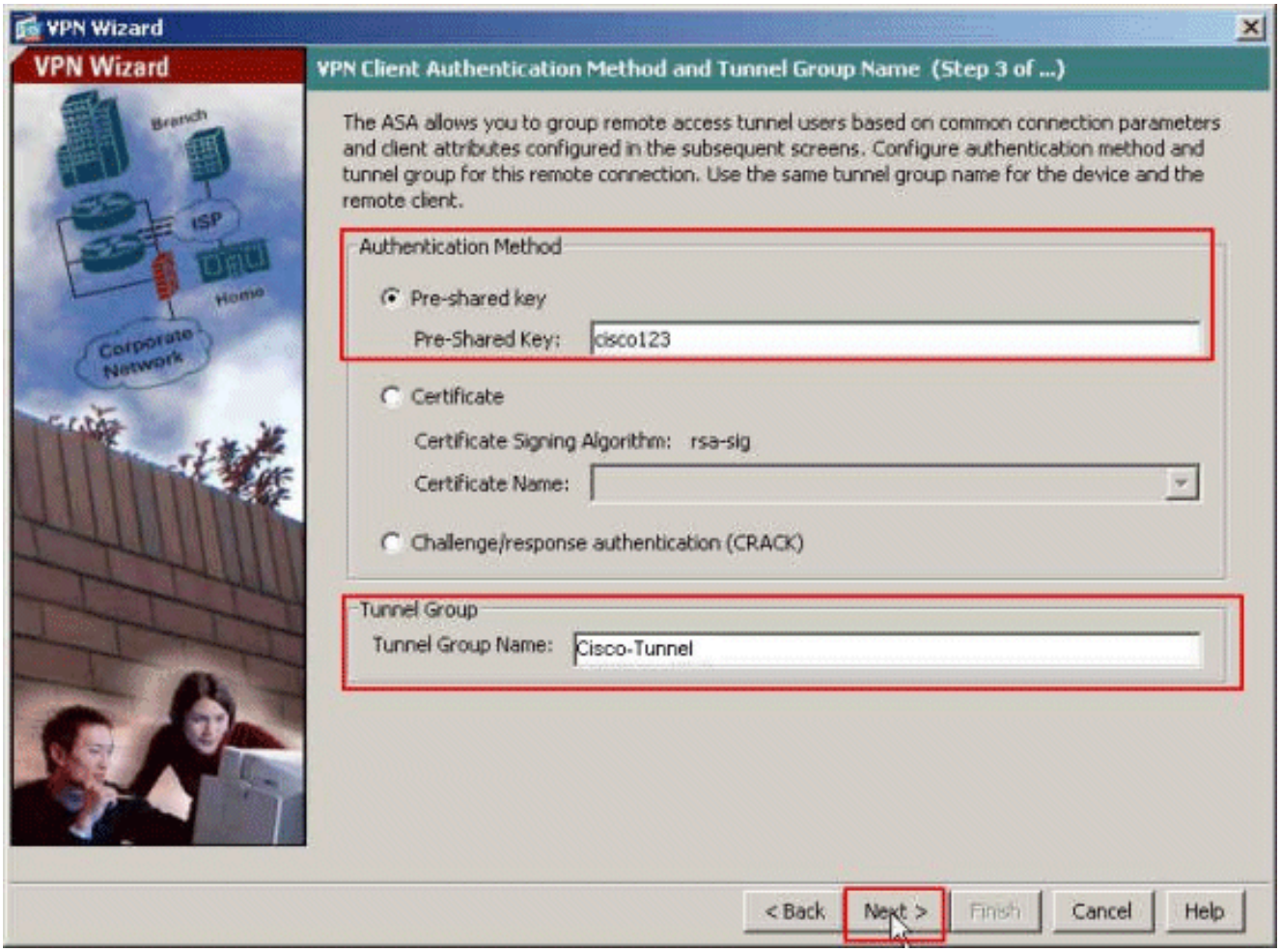
2. Select the **VPN Tunnel Interface** as required (**Outside**, in this example), and also make sure that the checkbox next to **Enable inbound IPsec sessions to bypass interface access lists** is
checked.



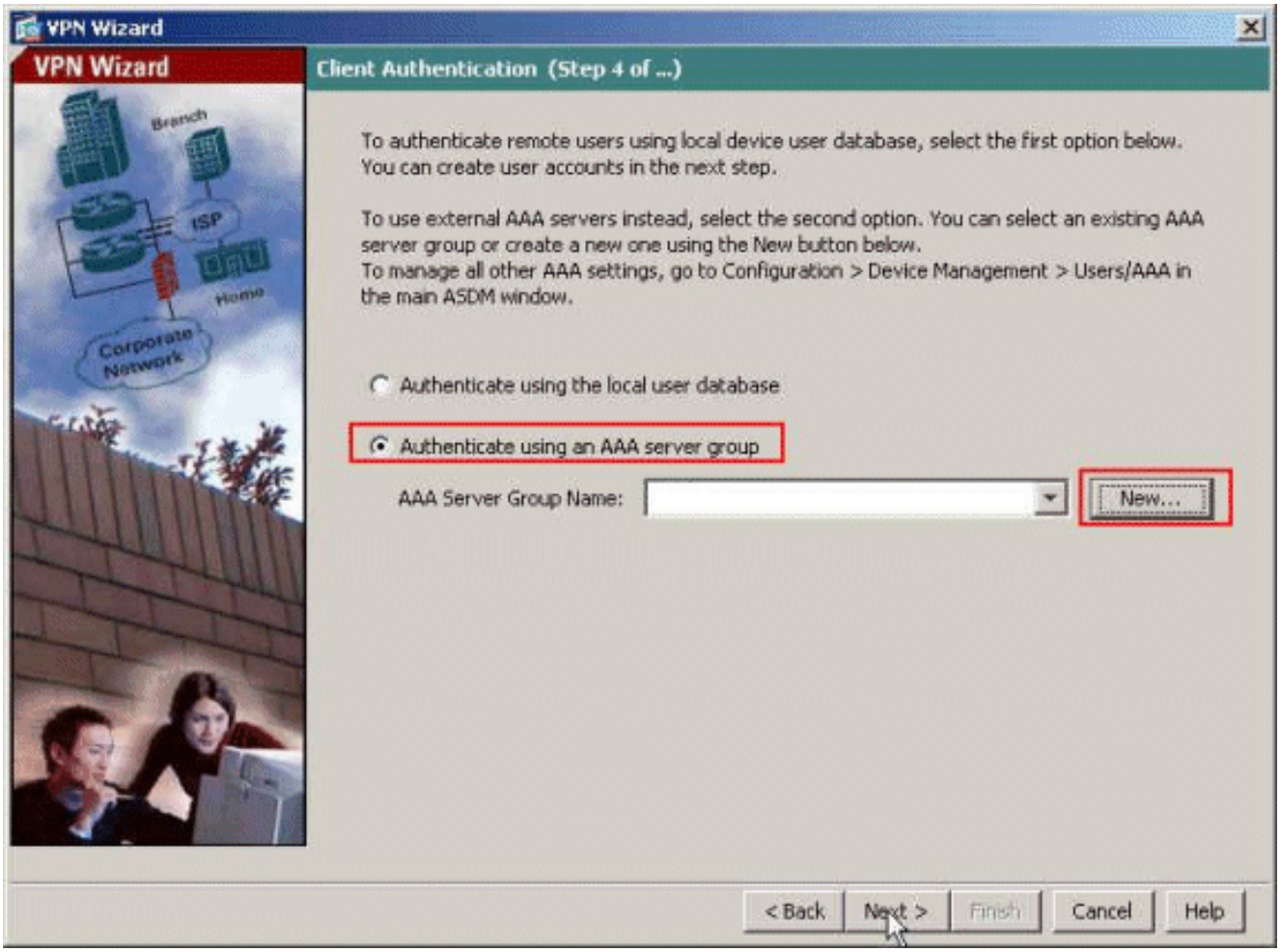
3. Choose the VPN Client Type as **Cisco VPN Client, Release 3.x or higher**. Click **Next**.



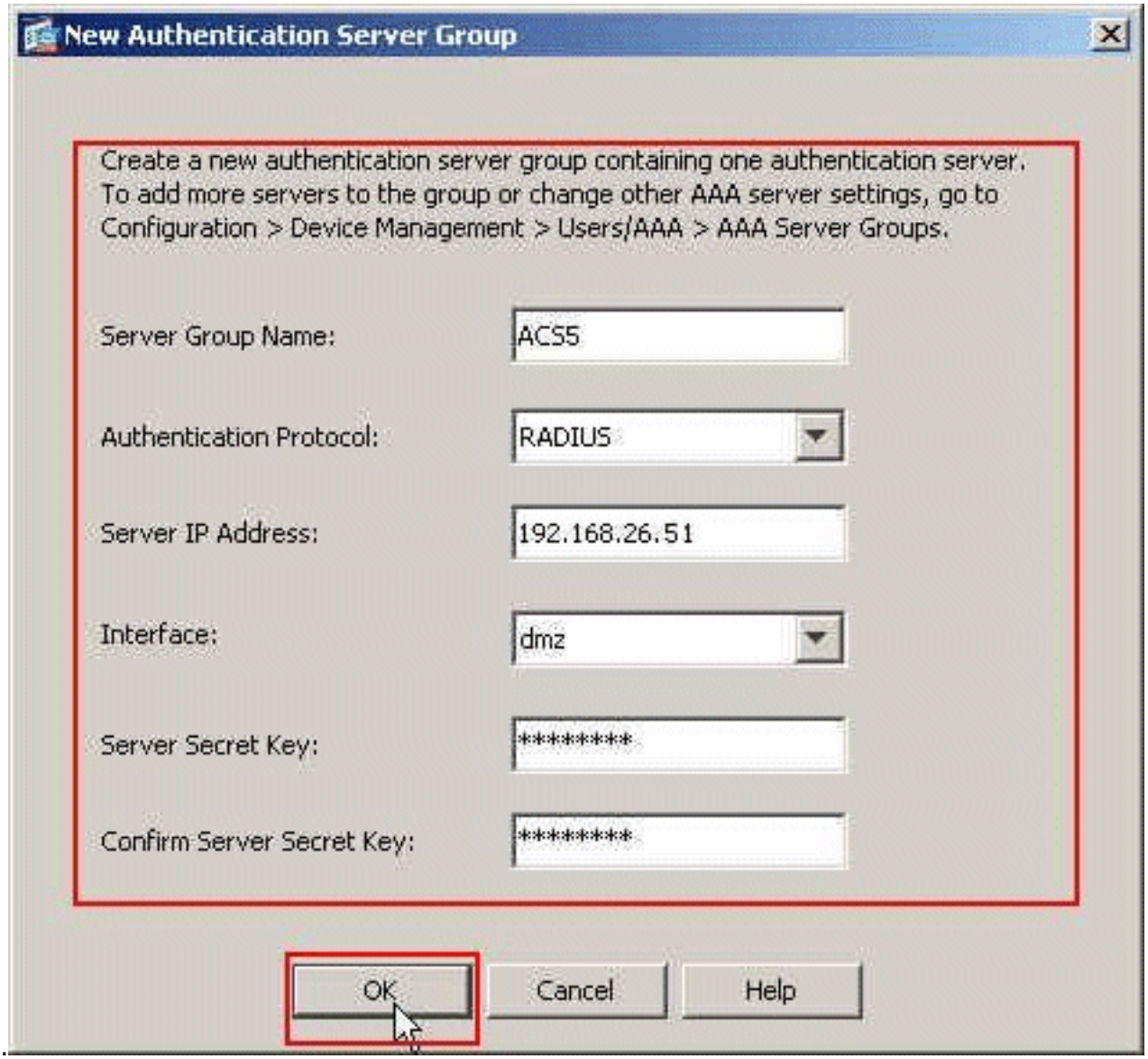
4. Choose the **Authentication Method** and provide the Authentication information. The Authentication method used here is **Pre-Shared Key**. Also, provide a **Tunnel Group** name in the space provided. The **Pre-shared Key** used here is **cisco123** and the **Tunnel Group Name** used here is **Cisco-Tunnel**. Click
Next.



5. Choose whether you want remote users to be authenticated to the local user database or to an external AAA server group. Here, we choose **Authenticate using an AAA server group**. Click **New** next to the AAA Server Group Name field in order to create a new AAA Server Group
Name.

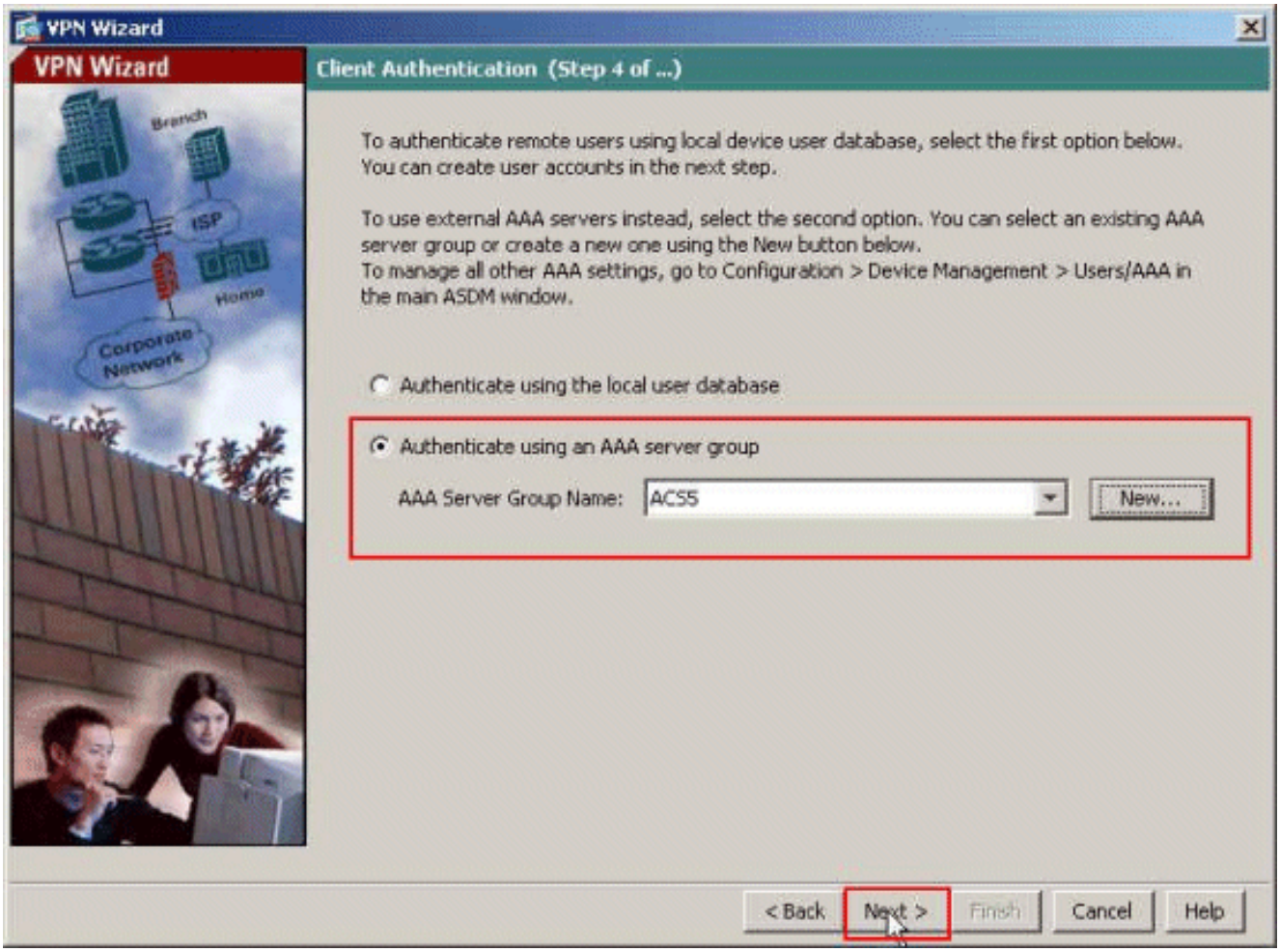


6. Provide the Server Group Name, Authentication Protocol, Server IP Address, Interface name, and the Server Secret Key in the respective spaces provided, and click

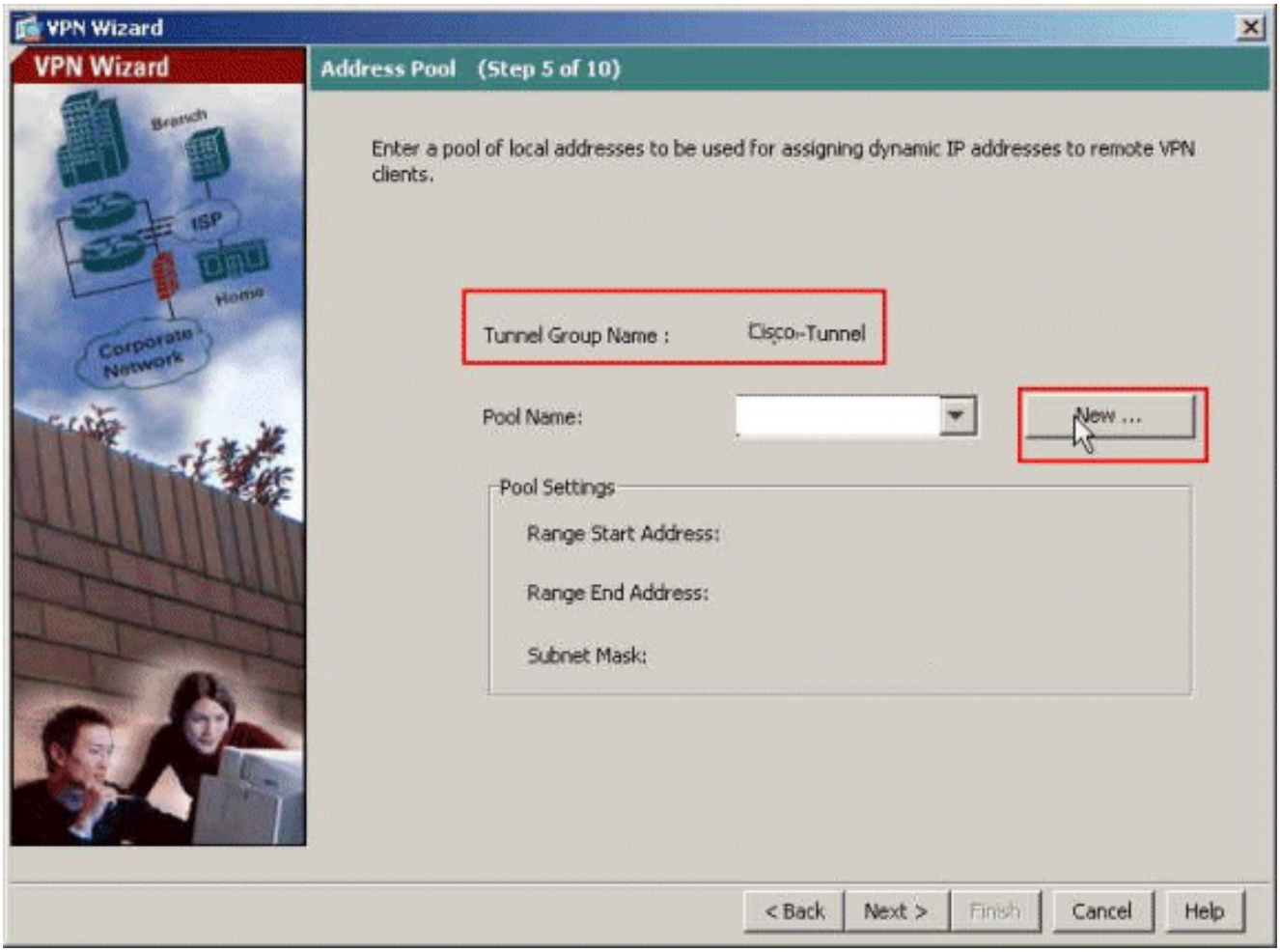


OK.

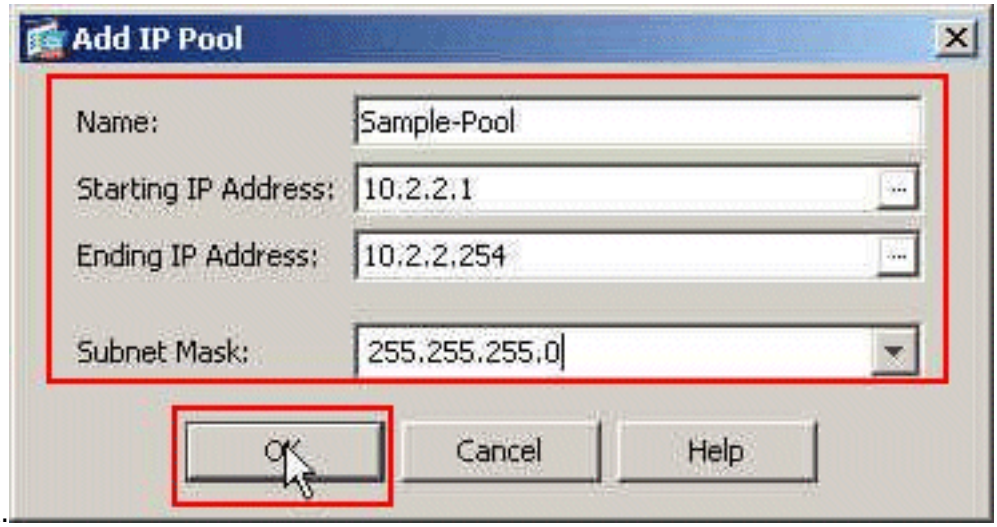
7. Click **Next**.



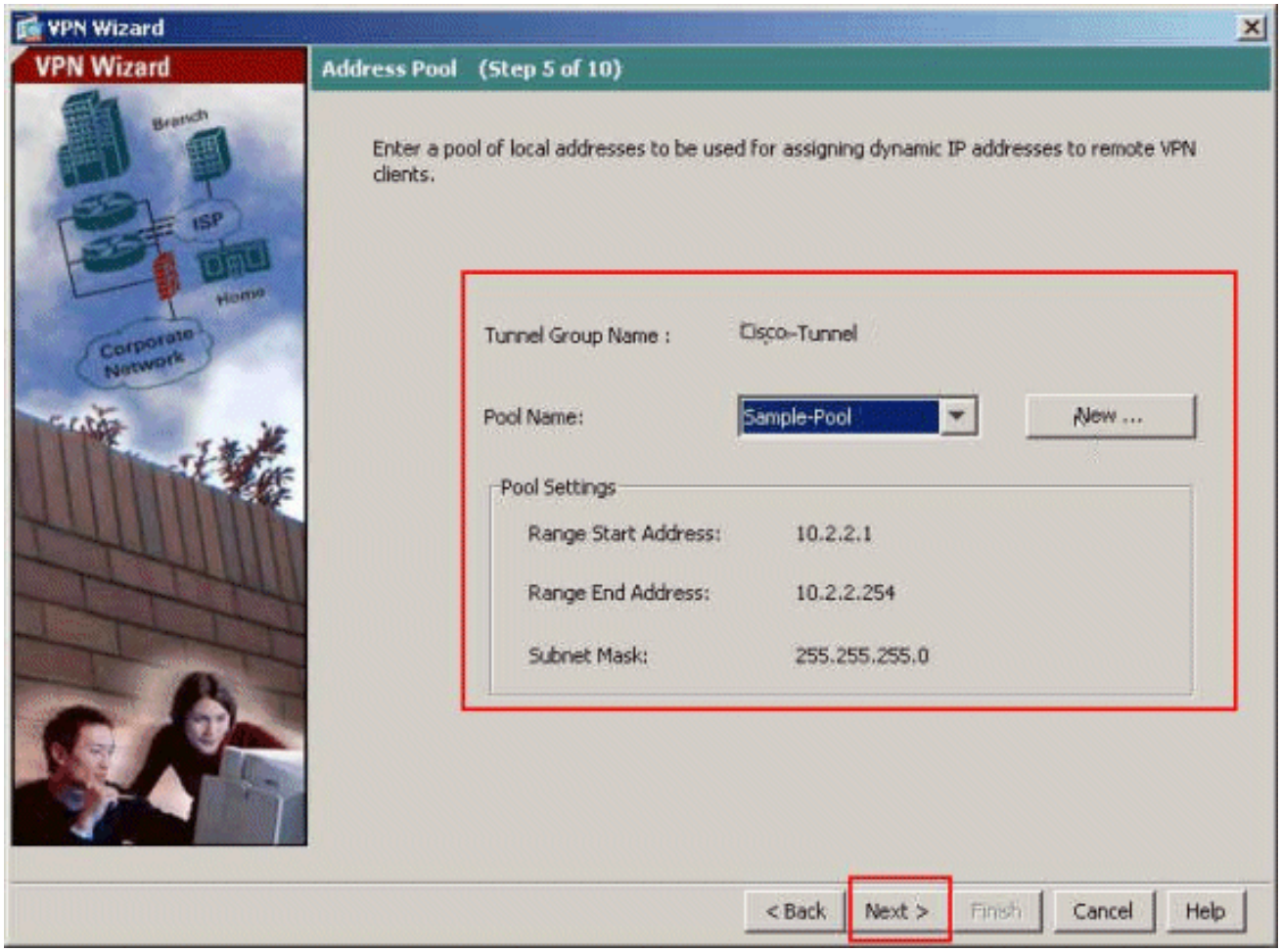
8. Define a pool of local addresses to be dynamically assigned to remote VPN Clients when they connect. Click **New** in order to create a new Pool of local address.



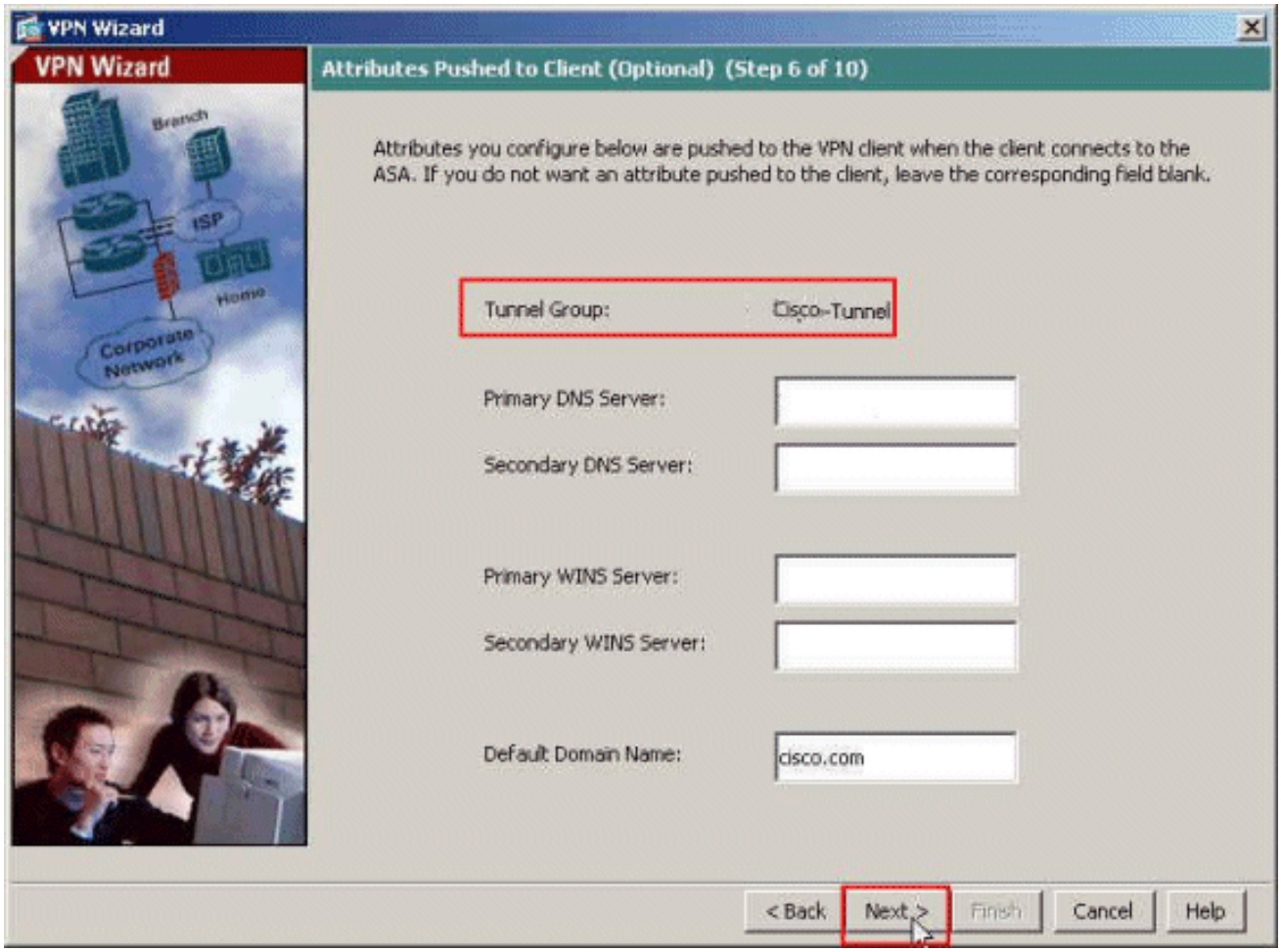
9. In the Add IP Pool window, provide the pool Name, Starting IP Address, Ending IP Address, and the Subnet Mask. Click **OK**.



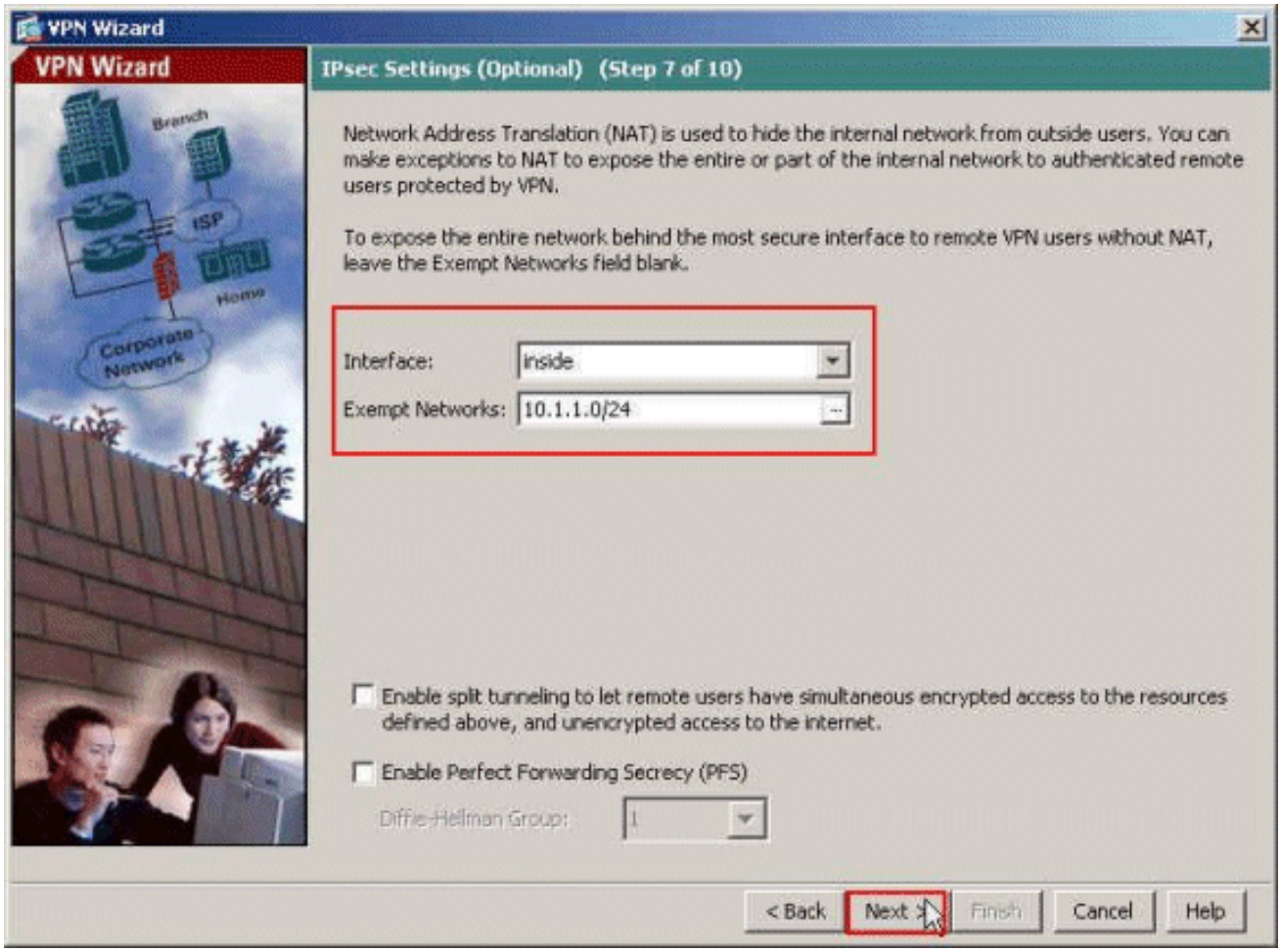
10. Select the Pool Name from the drop-down list, and click **Next**. The Pool Name for this example is **Sample-Pool** which was created in Step 9.



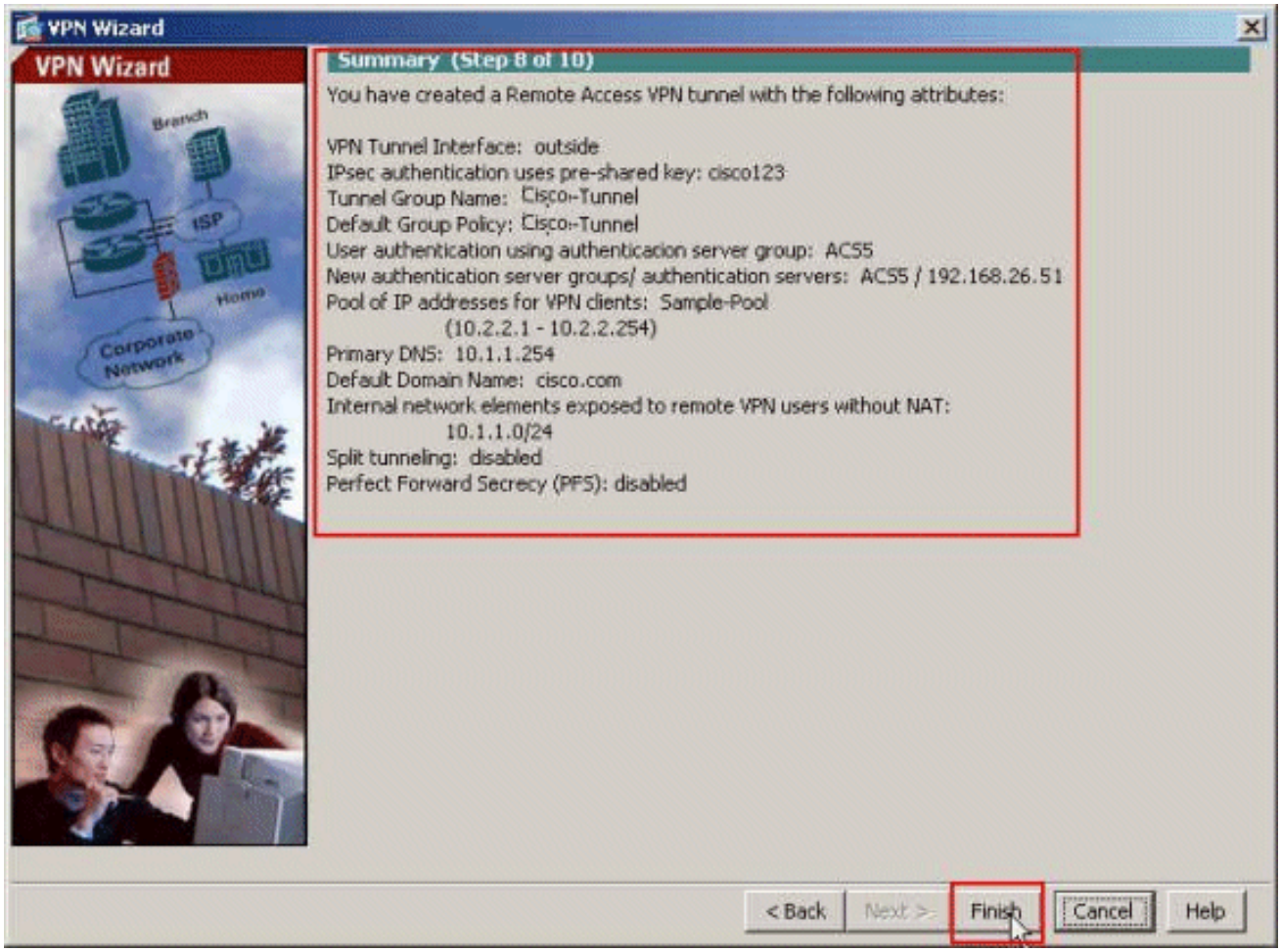
11. *Optional:* Specify the DNS and WINS server information and a Default Domain Name to be pushed to remote VPN
    Clients.



12. Specify which, if any, internal hosts or networks should be exposed to remote VPN users. Click **Next** after providing the Interface name and the networks to be exempted in the Exempt Networks field.If you leave this list empty, it allows remote VPN users to access the entire inside network of the ASA.You can also enable split tunneling on this window. Split tunneling encrypts traffic to the resources defined earlier in this procedure and provides unencrypted access to the Internet at large by not tunneling that traffic. If split tunneling is *not* enabled, all traffic from remote VPN users is tunneled to the ASA. This can become very bandwidth and processor intensive, based on your configuration.



13. This window shows a summary of the actions that you have taken. Click **Finish** if you are satisfied with your
configuration.



Configure the ASA with CLI

This is the CLI configuration:

Running Configuration on the ASA Device

```
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#
```

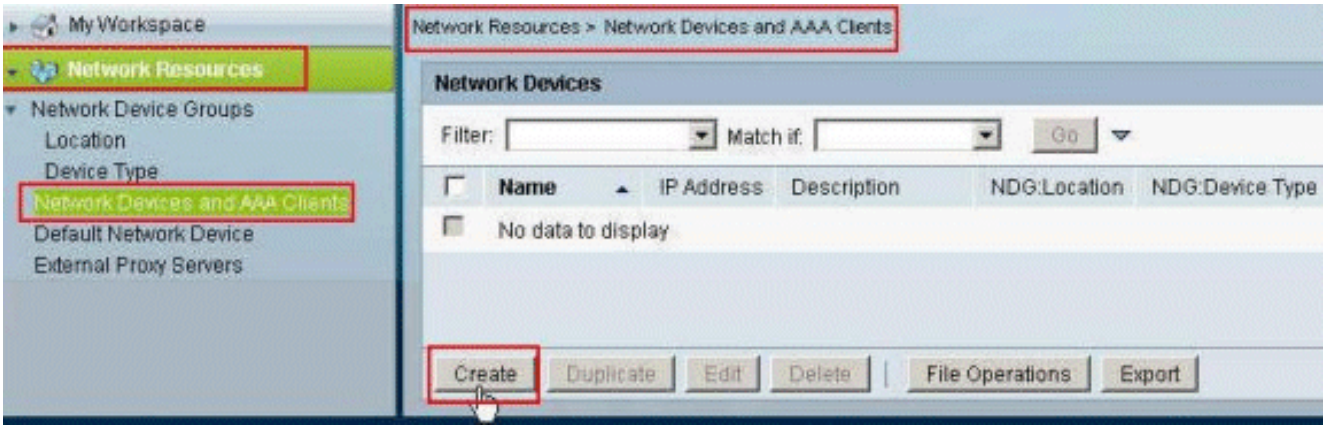
Configure ACS for Downloadable ACL for Individual User

You can configure downloadable access lists on Cisco Secure ACS 5.x as a Named Permissions Object and then assign it to an Authorization Profile which will be chosen in the result section of the Rule in the Access-Service.

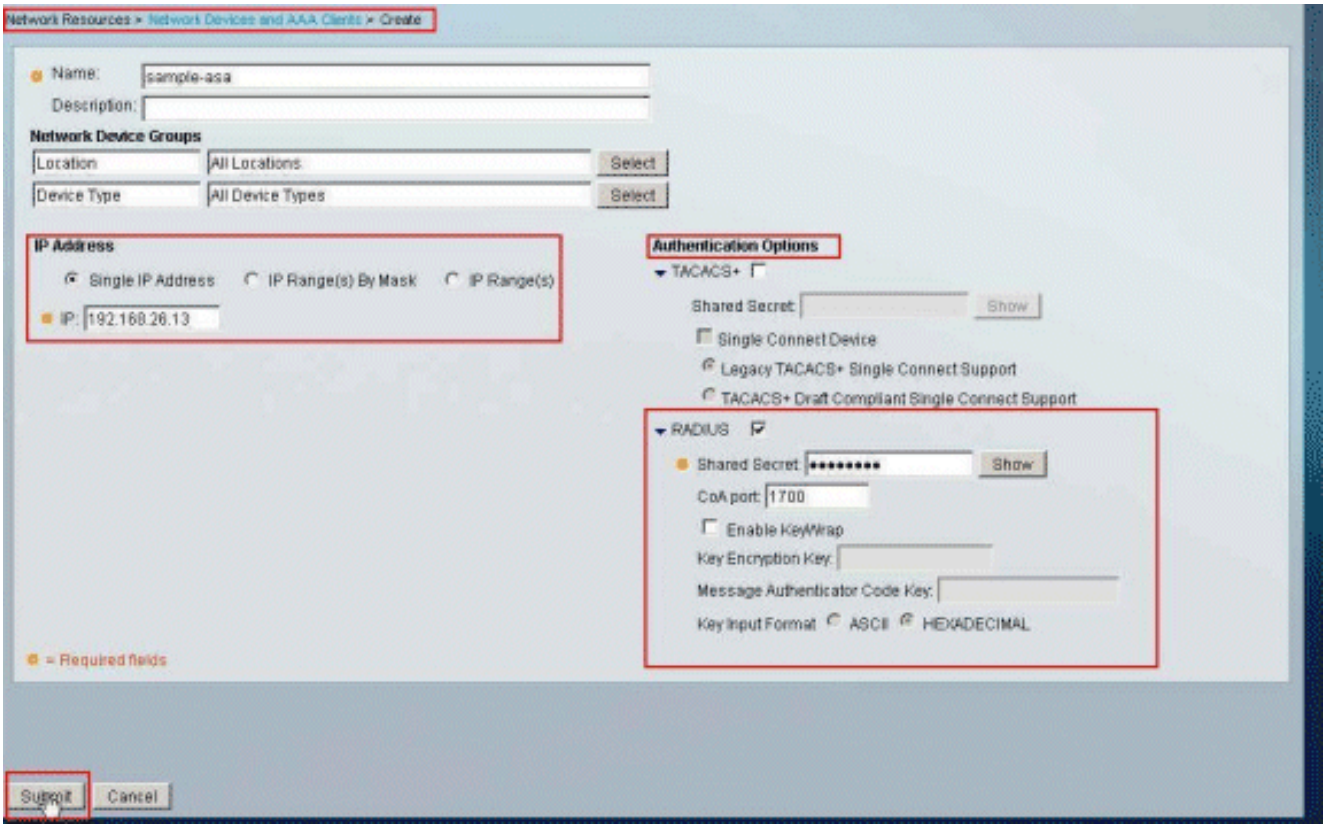
In this example, the IPsec VPN user **cisco** authenticates successfully, and the RADIUS server sends a downloadable access list to the security appliance. The user "cisco" can access only the 10.1.1.2 server and denies all other access. In order to verify the ACL, see the Downloadable ACL for User/Group section.

Complete these steps in order to configure RADIUS client in a Cisco Secure ACS 5.x:

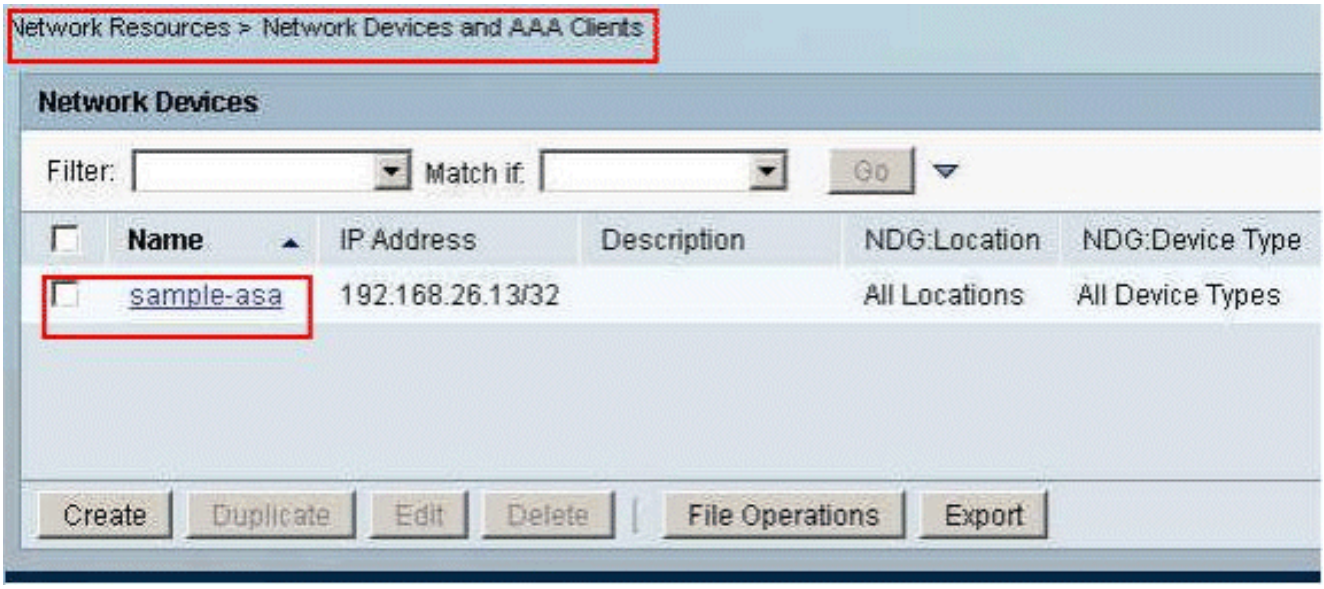
1. Choose **Network Resources** > **Network Devices and AAA Clients**, and click **Create** in order to add an entry for the ASA in the RADIUS server database.



2. Enter a locally significant Name for the ASA (**sample-asa**, in this example), then enter **192.168.26.13** in the IP address field. Choose **RADIUS** in the Authentication Options section by checking the **RADIUS** checkbox and enter **cisco123** for the Shared Secret field. Click **Submit**.

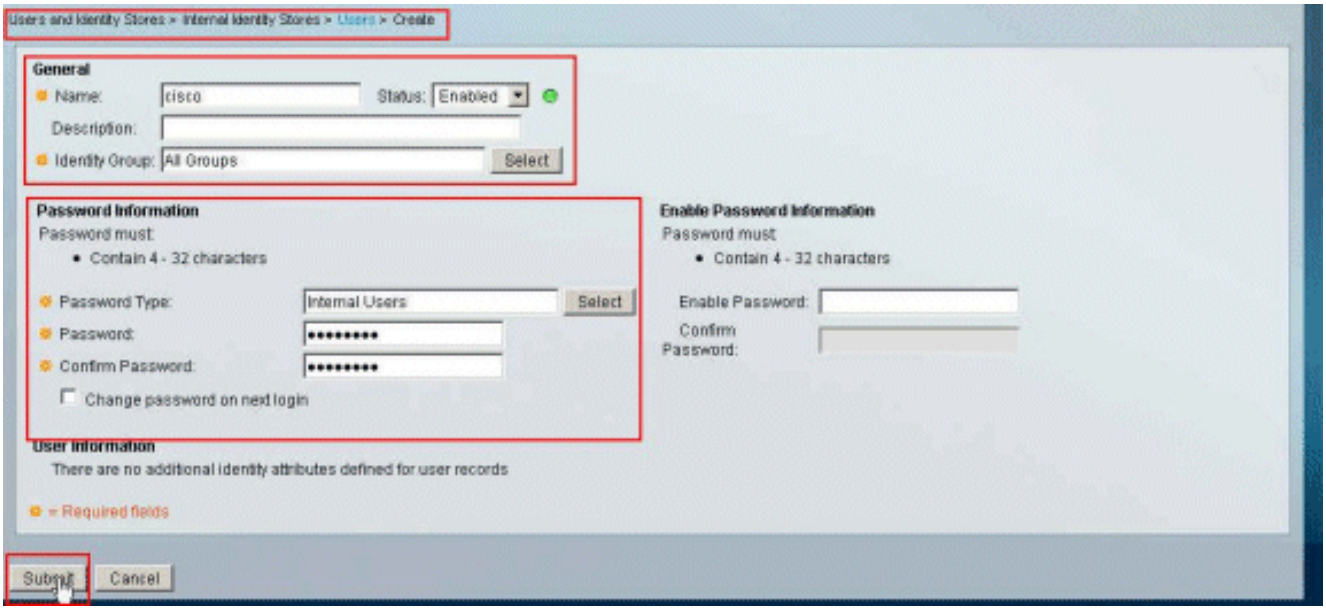


3. The ASA is added successfully to the RADIUS server (ACS) database.

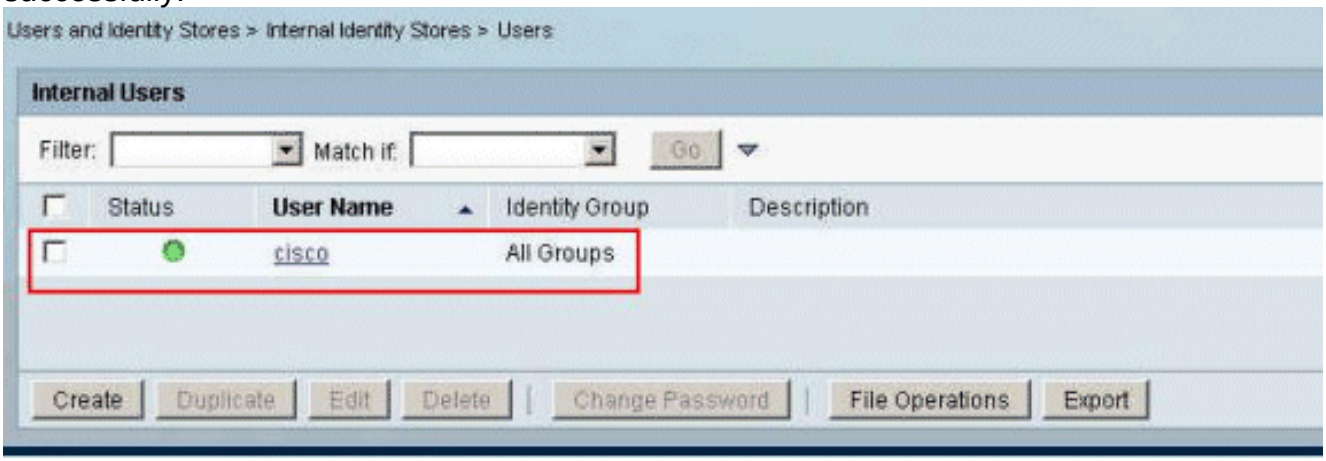


4. Choose **Users and Identity Stores** > **Internal Identity Stores** > **Users**, and click **Create** in order to create a user in the local database of the ACS for VPN authentication.

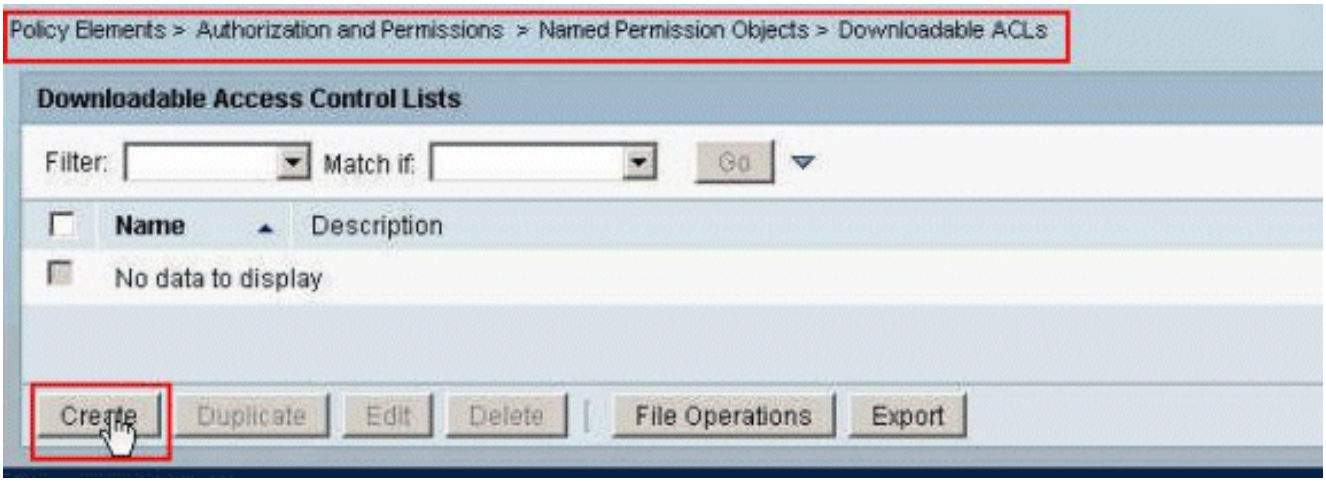
5. Enter the username **cisco**. Select the password type as **Internal Users**, and enter the password (**cisco123**, in this example). Confirm the password, and click **Submit**.



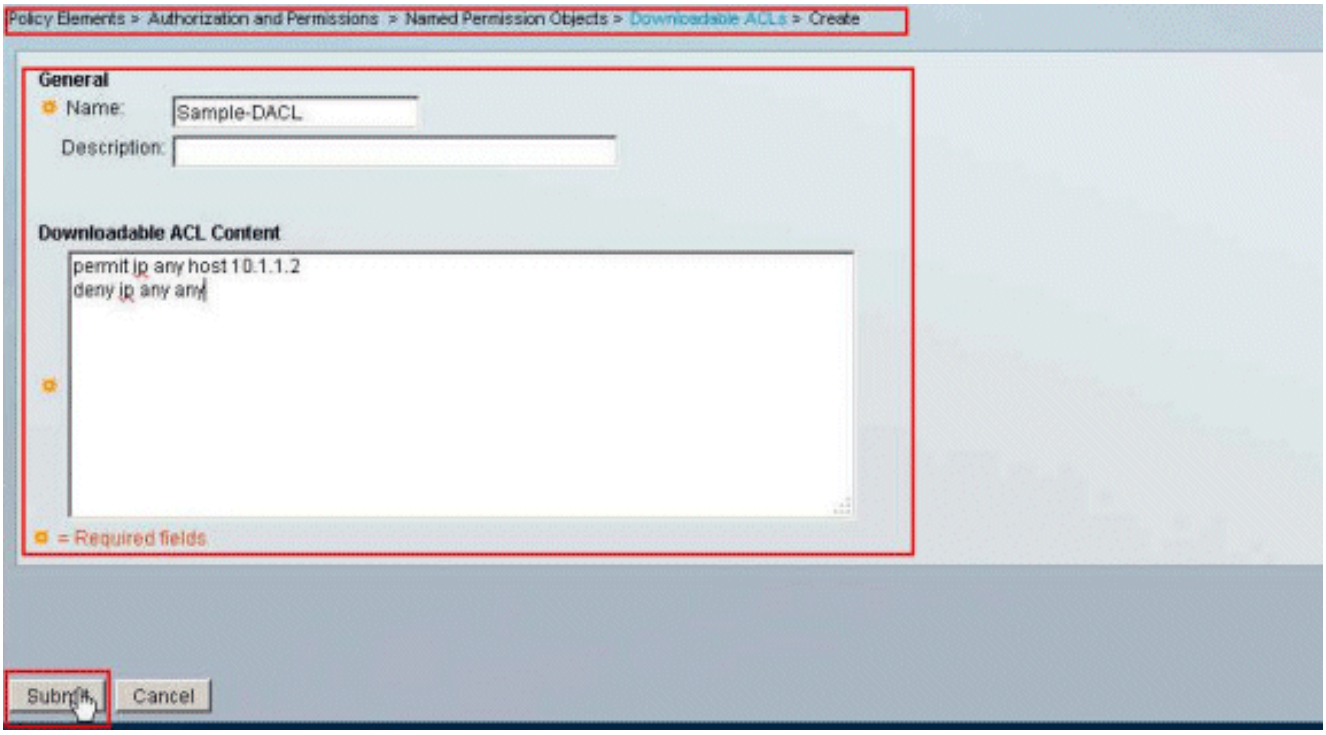
6. The user **cisco** is created successfully.



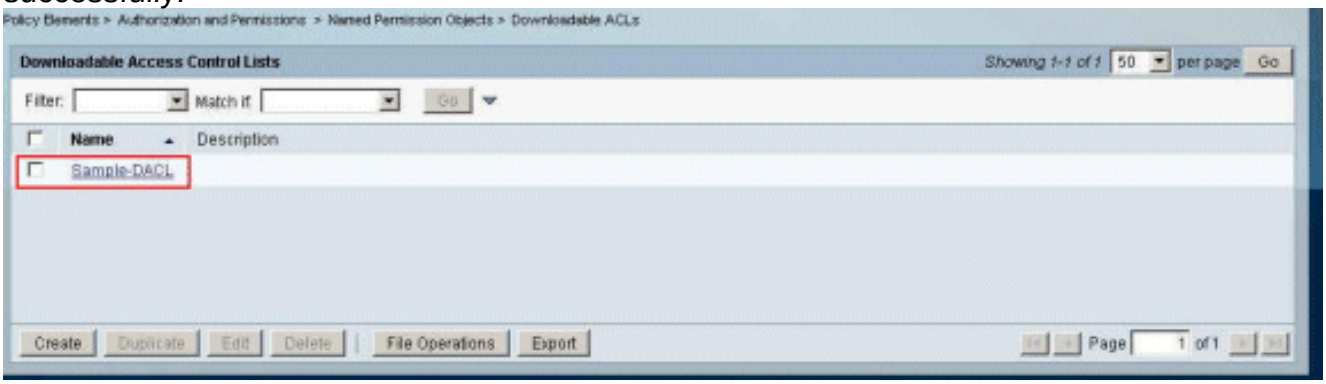
7. In order to create a Downloadable ACL, choose **Policy Elements** > **Authorization and Permissions** > **Named Permission Objects** > **Downloadable ACLs**, and click **Create**.



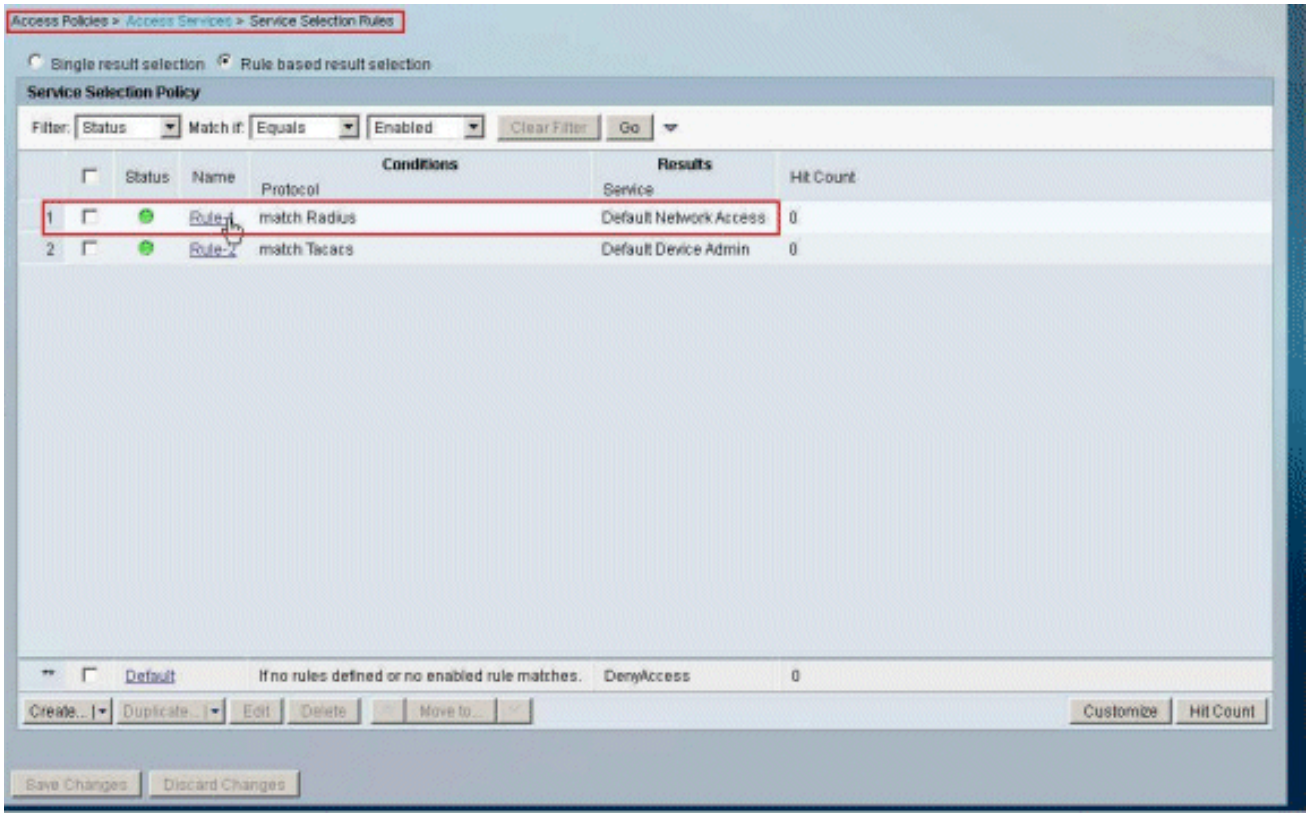
8. Provide the **Name** for the Downloadable ACL, as well as the **ACL Content**. Click **Submit**.



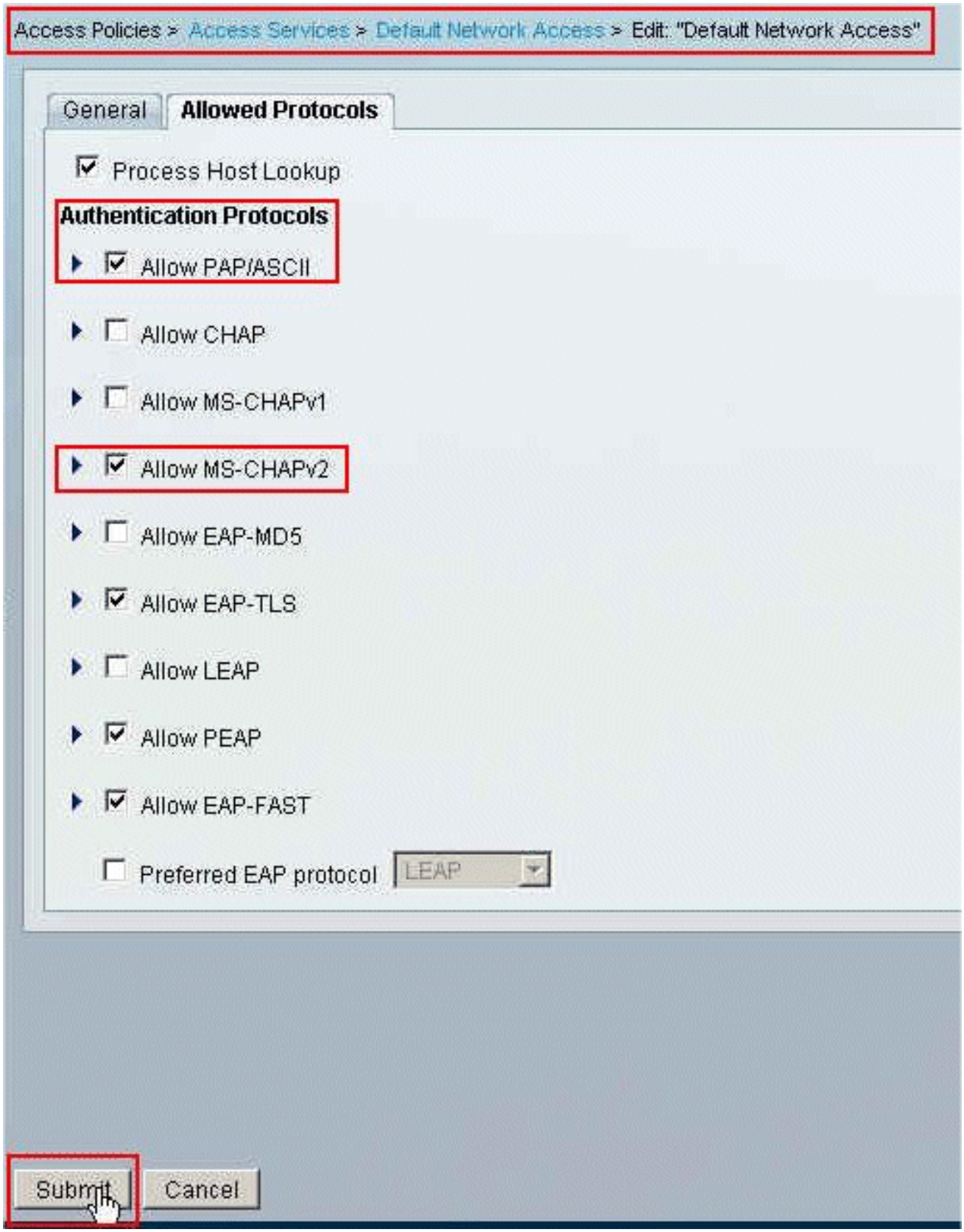
9. The Downloadable ACL **Sample-DACL** is created successfully.



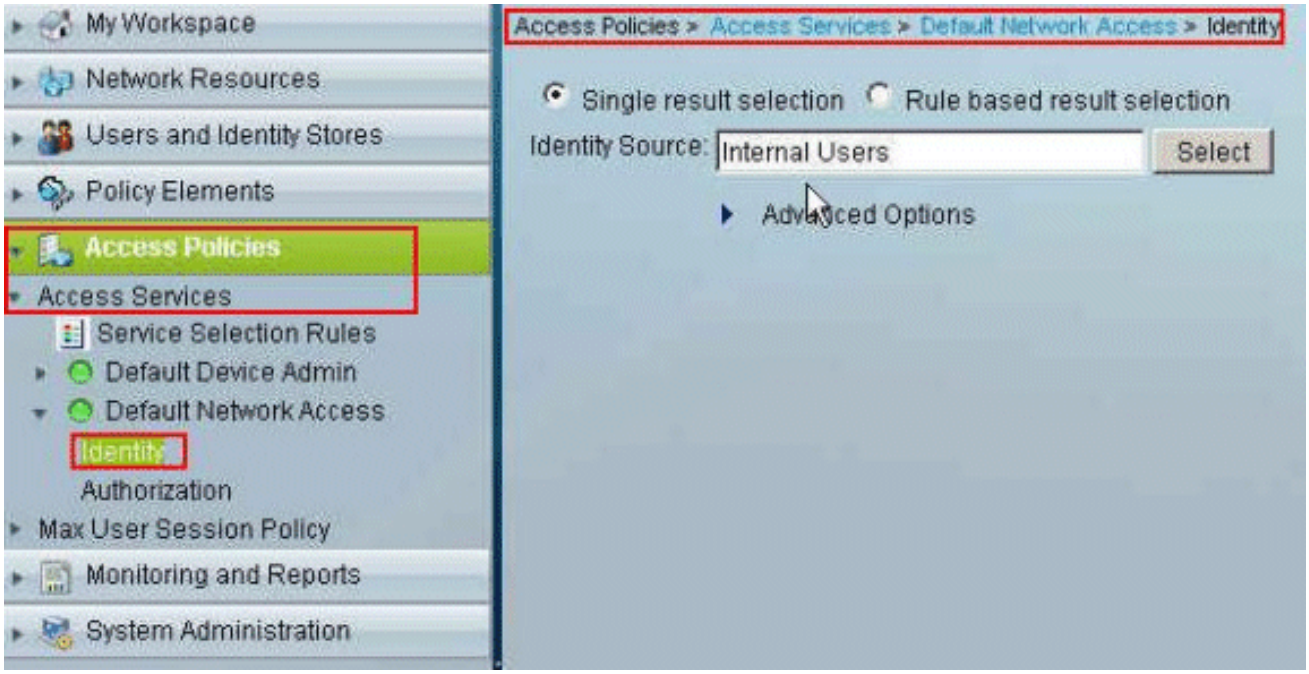
10. In order to configure the Access-Policies for VPN Authentication, choose **Access Policies** > **Access Services** > **Service Selection Rules**, and determine which service is catering to the RADIUS protocol. In this example, **Rule 1** matches **RADIUS**, and Default Network Access will cater to the RADIUS request.



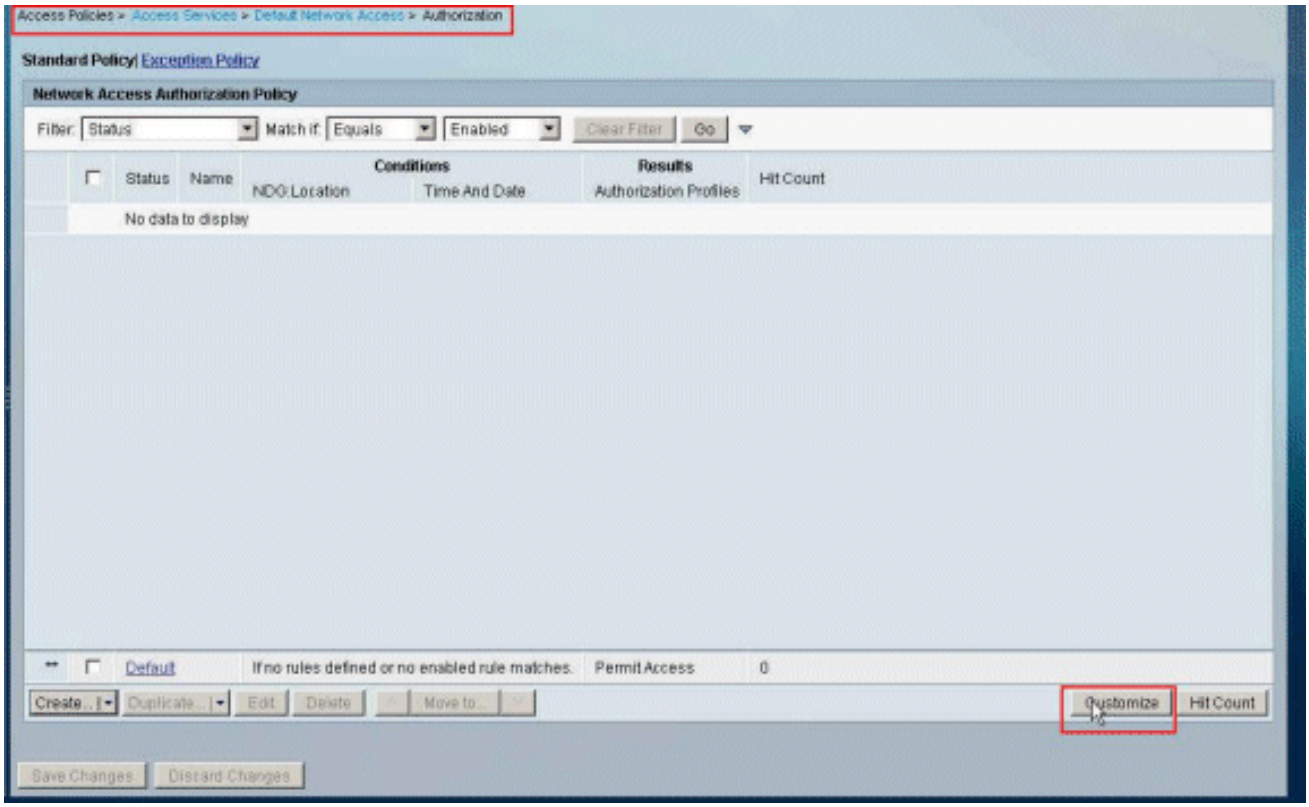
11. Choose the **Access Service** determined from Step 10. In this example, **Default Network Access** is used. Choose the **Allowed Protocols** tab, and make sure that **Allow PAP/ASCII** and **Allow MS-CHAPv2** are selected .Click
Submit.



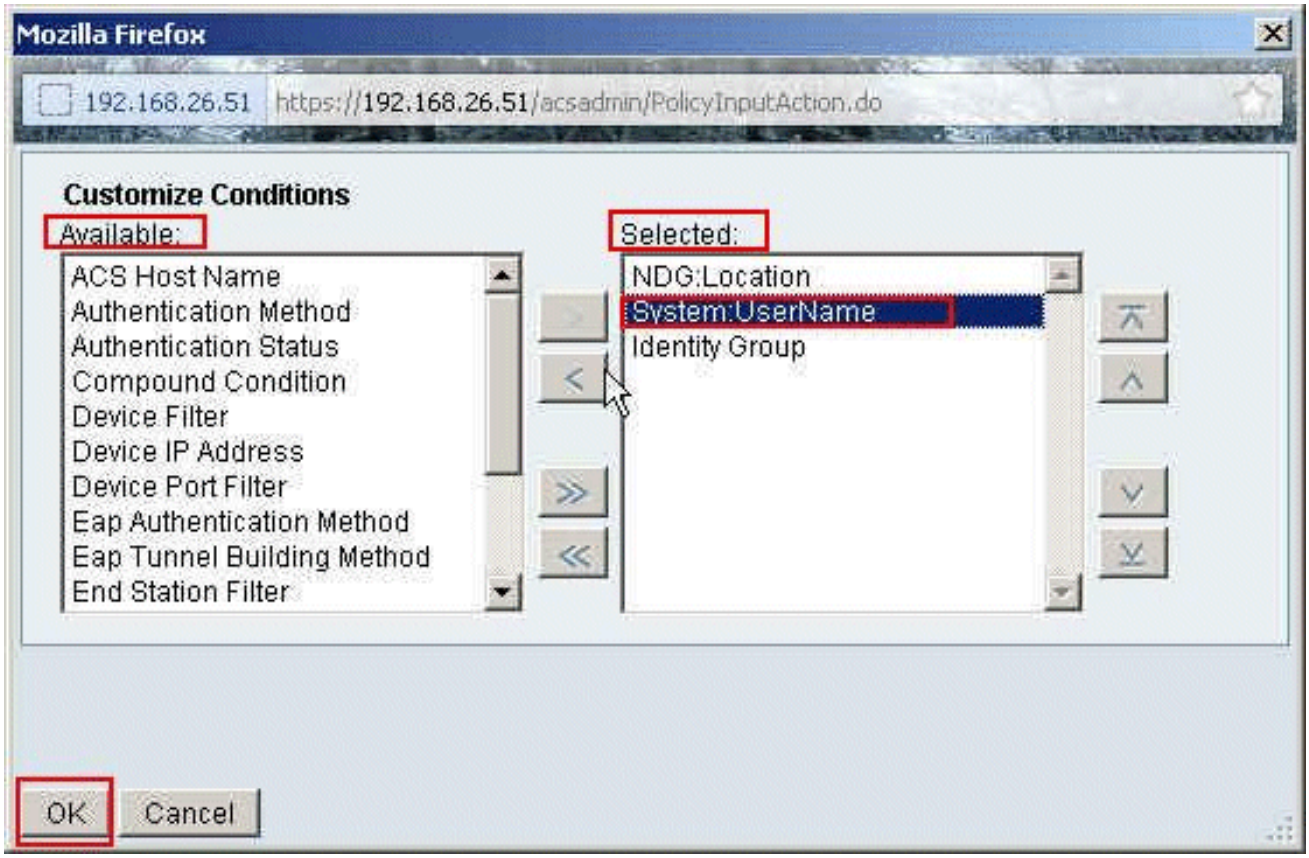
12. Click on the **Identity Section** of the **Access Services**, and make sure that **Internal Users** is selected as the Identity Source. In this example, we have taken default network access.



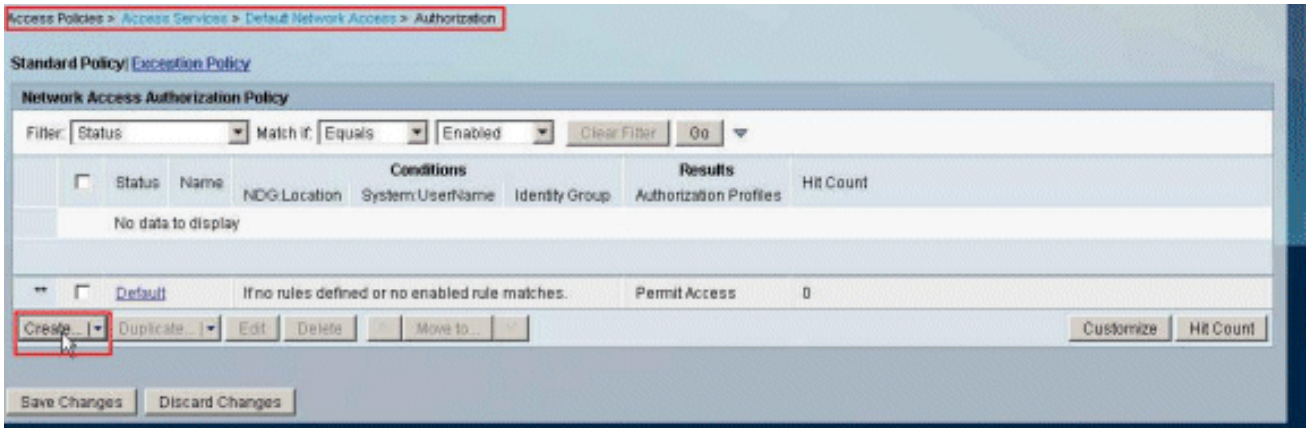
13. Choose **Access Policies** > **Access Services** > **Default Network Access** > **Authorization**, and click **Customize**.



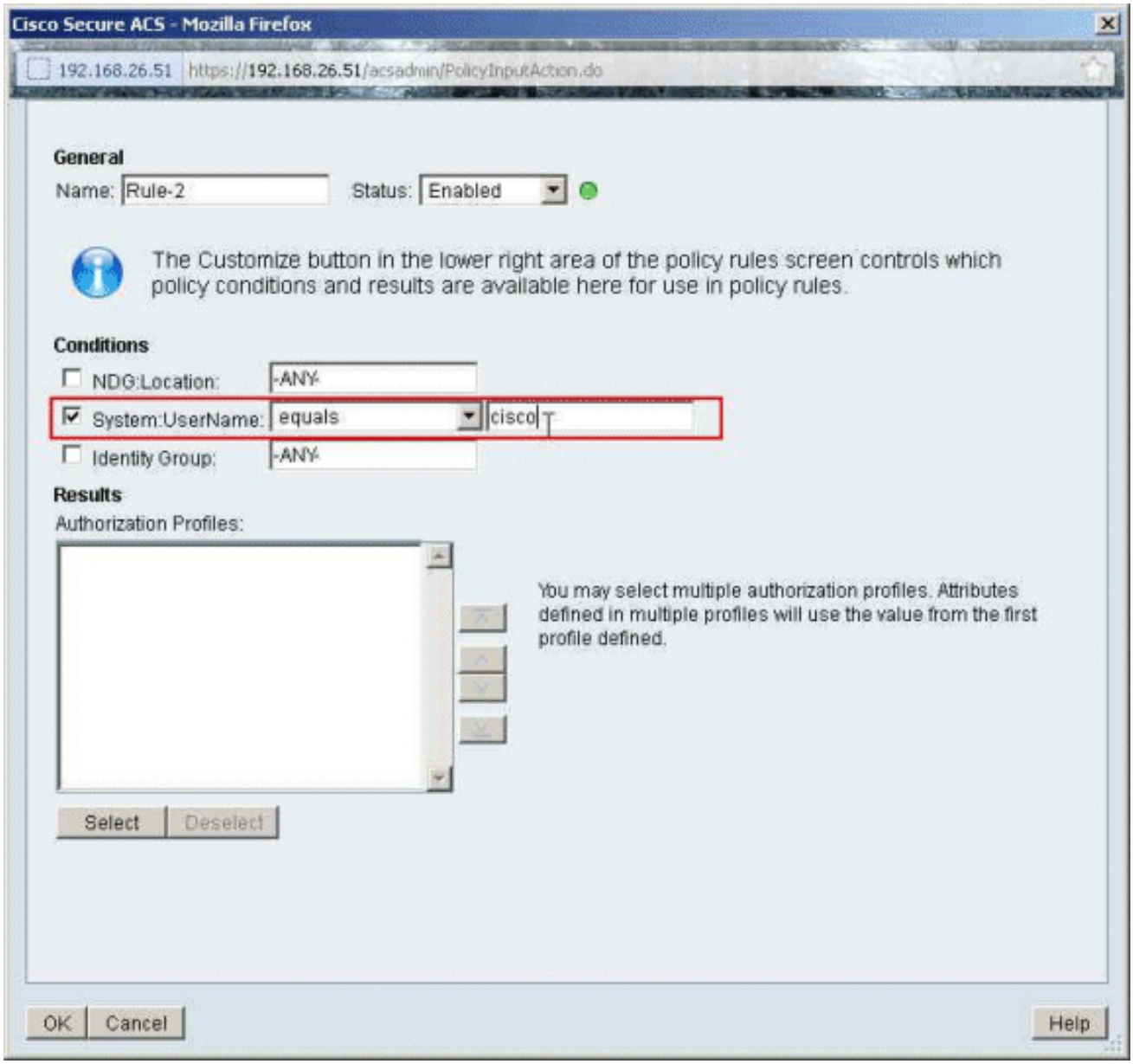
14. Move **System:UserName** from the **Available** column to the **Selected** column, and click **OK**.



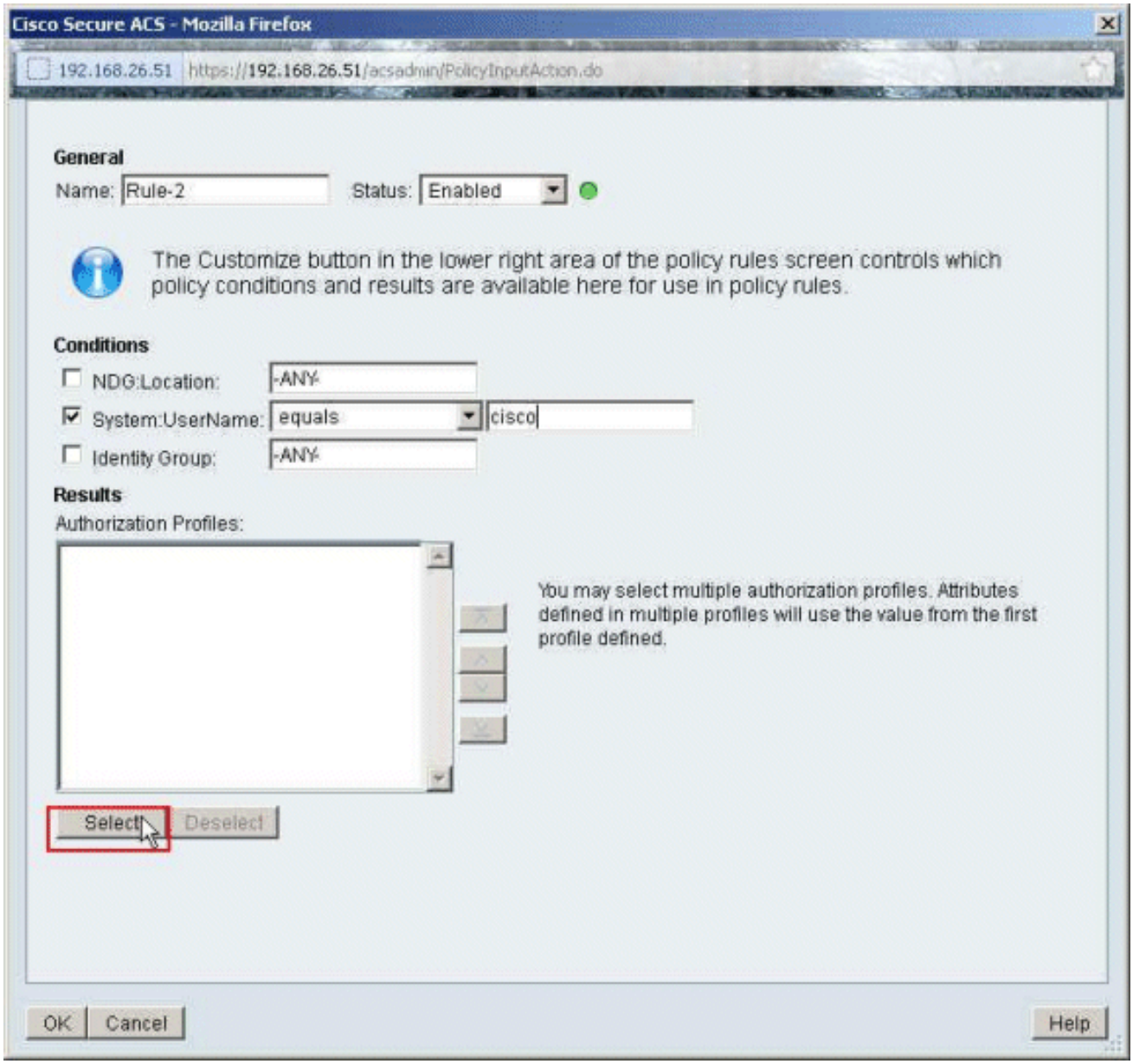
15. Click **Create** in order to create a new Rule.



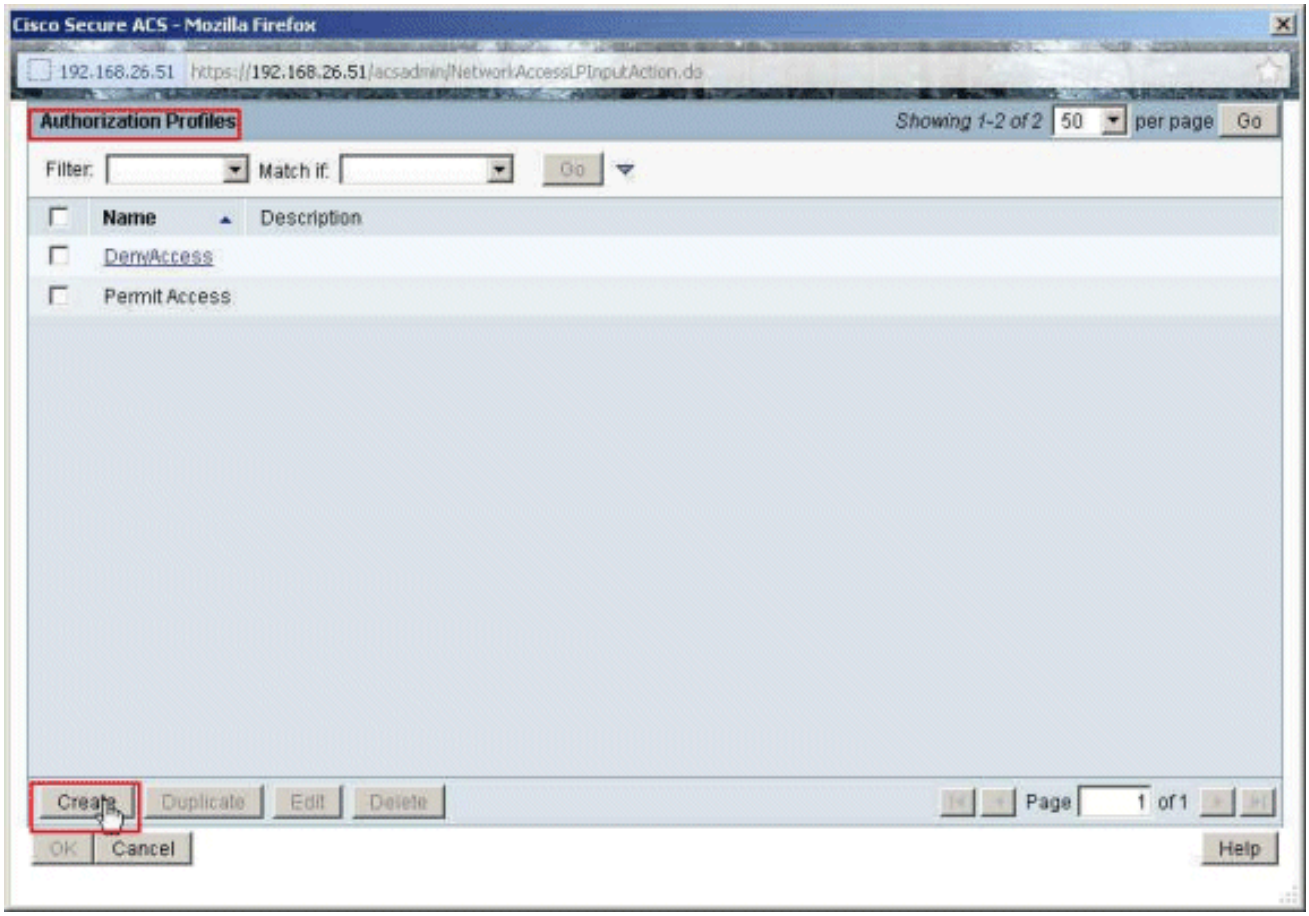
16. Make sure that the checkbox next to **System:UserName** is selected, choose **equals** from the drop-down list, and enter the username **cisco**.



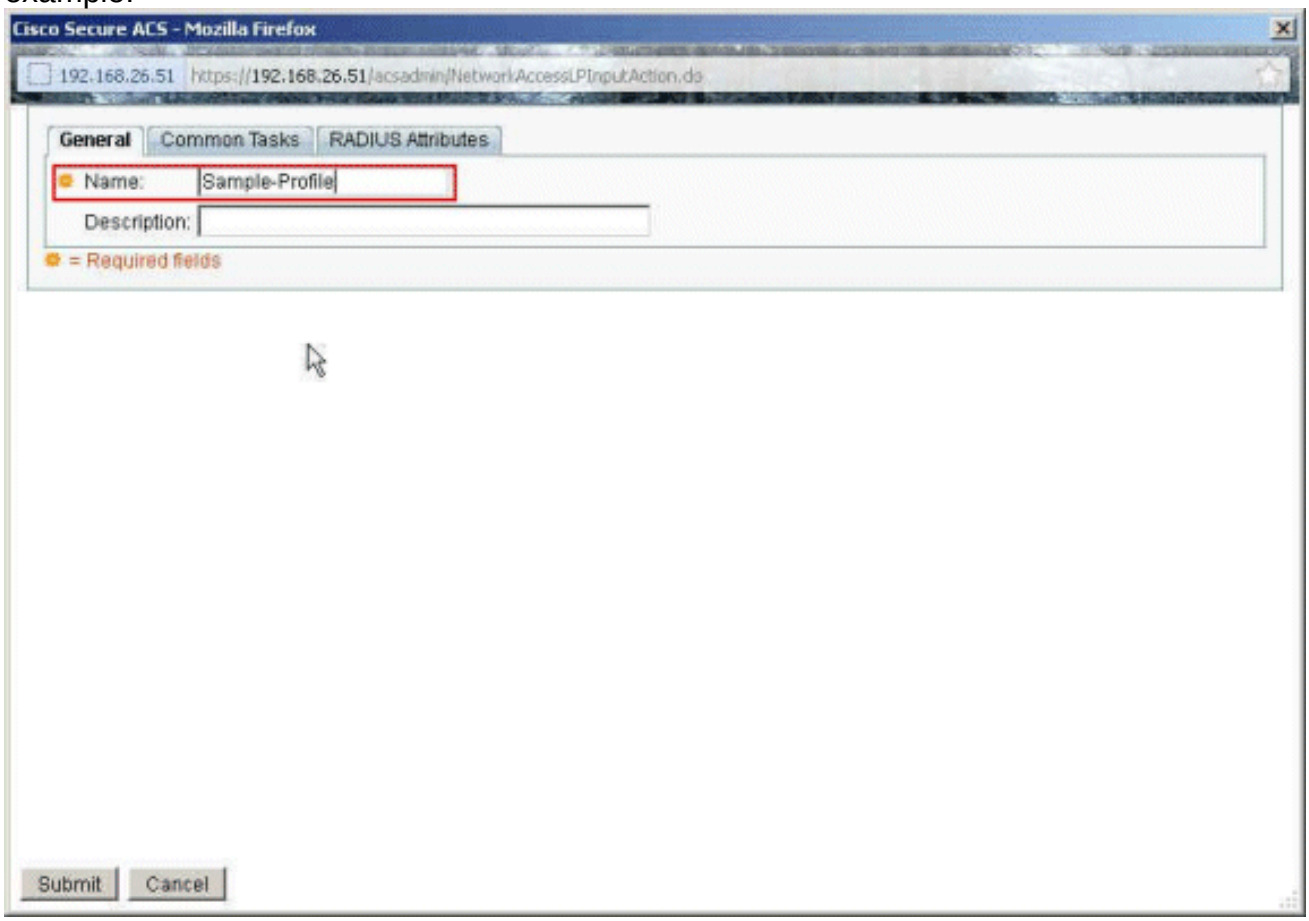
17. Click **Select**.



18. Click **Create** in order to create a new Authorization Profile.

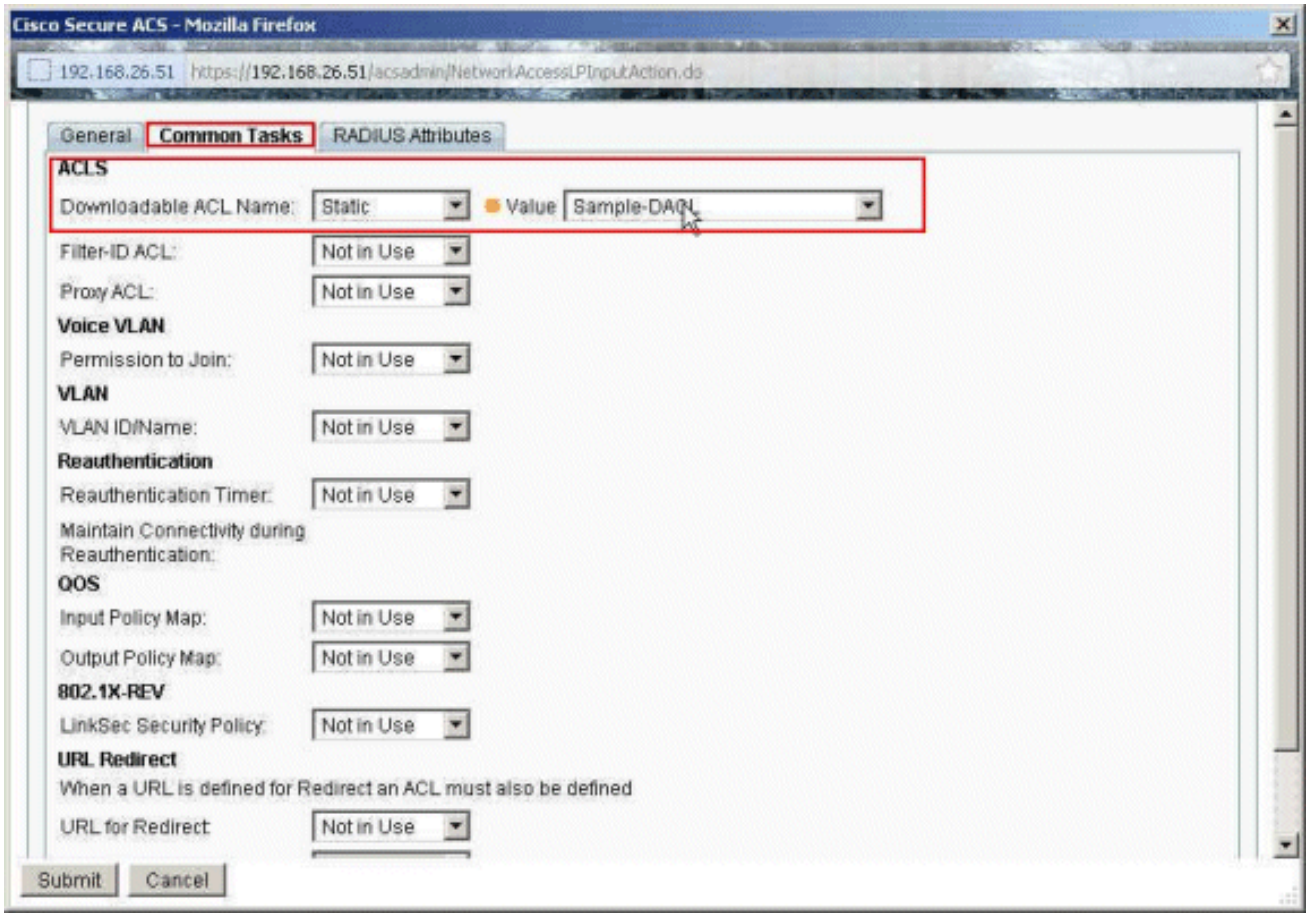


19. Provide a name for the **Authorization Profile**. **Sample-Profile** is used in this example.

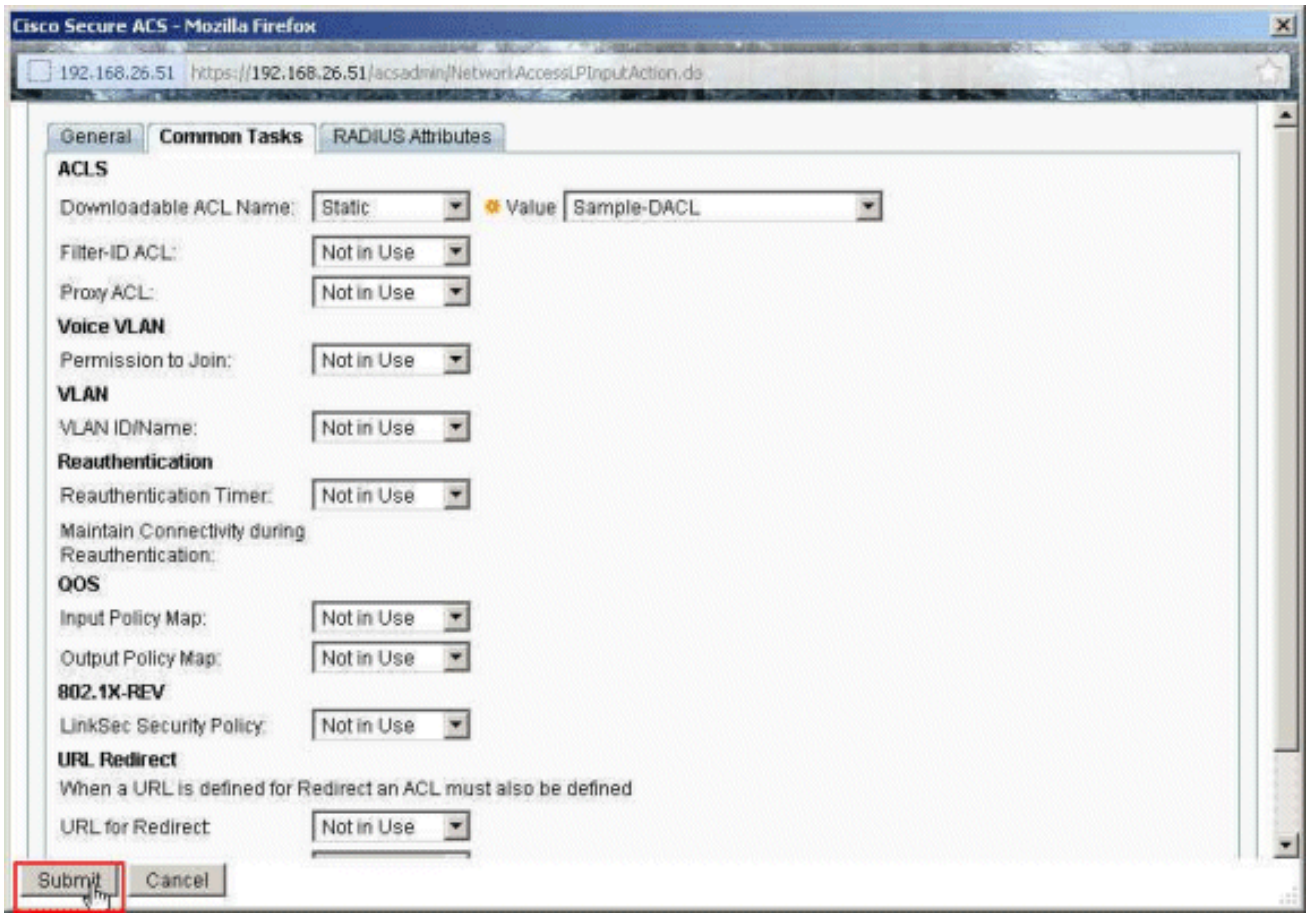


20. Choose the **Common Tasks** tab, and select **Static** from the drop-down list for the **Downloadable ACL Name**. Choose the newly created **DACL (Sample -DACL)** from the value drop-down

list.

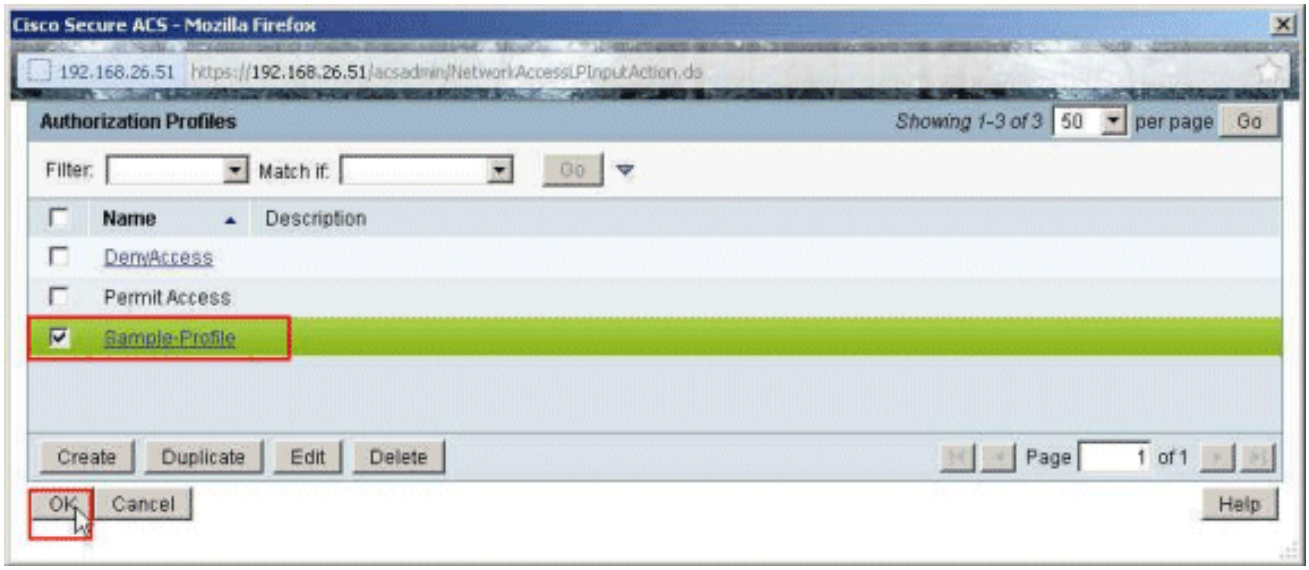


21. Click **Submit**.

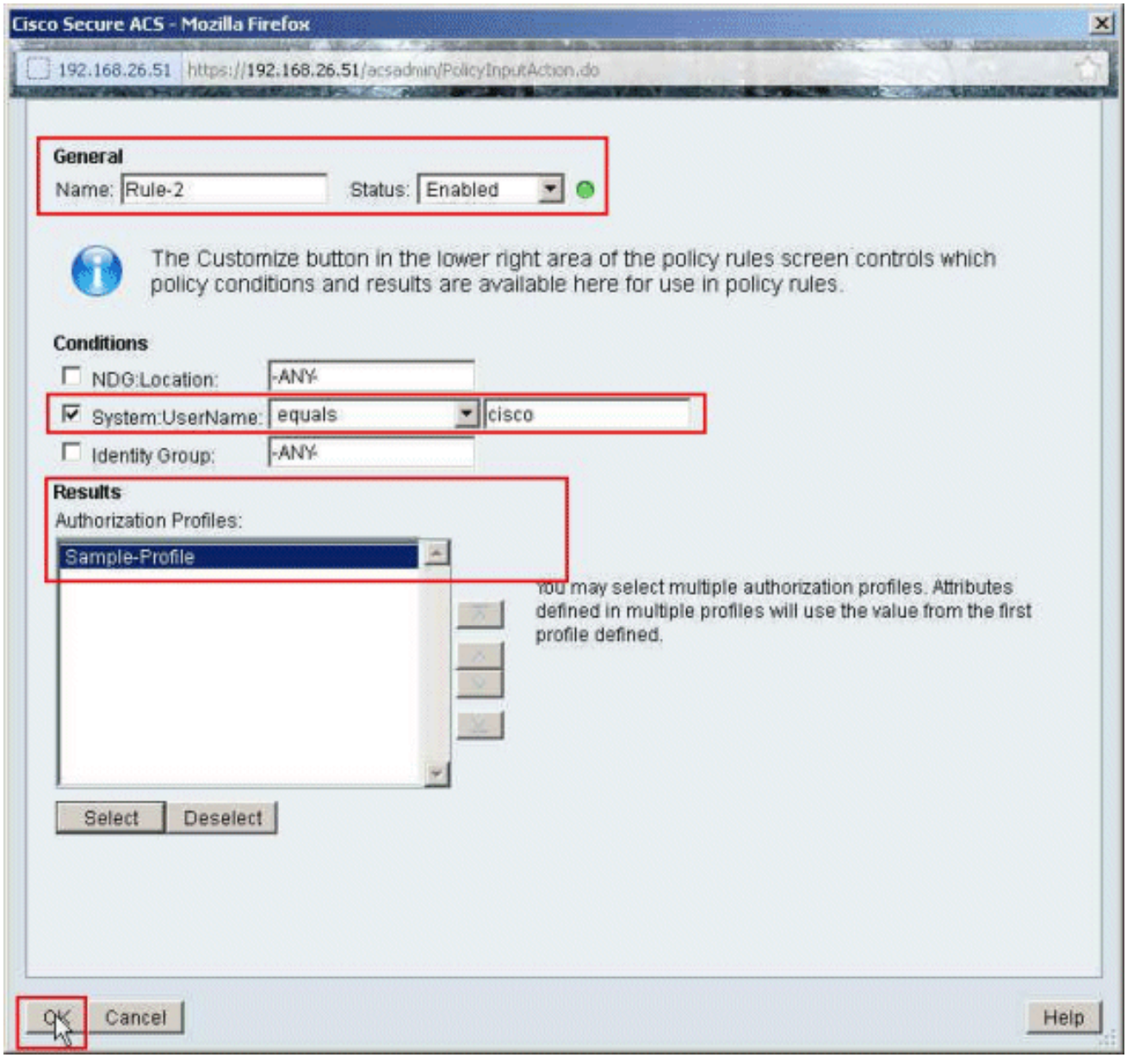


22. Make sure that the checkbox next to **Sample-Profile** (the newly created Authorization Profile) is checked, and click

OK.

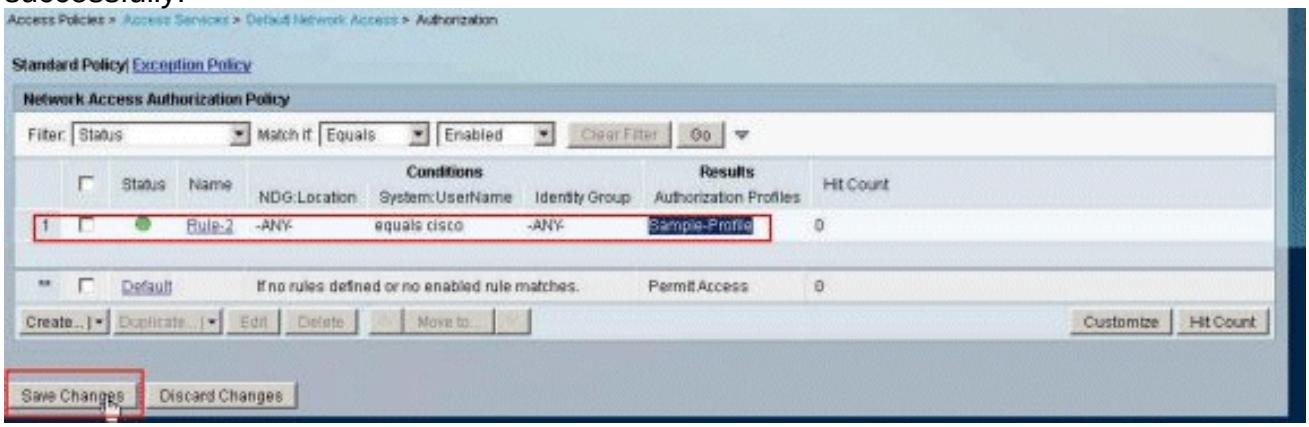


23. Once you have verified that the newly created **Sample-Profile** is selected in the **Authorization Profiles** field, click
OK.



24. Verify that the new rule (**Rule-2**) is created with System:UserName **equals cisco** conditions and **Sample-Profile** as the Result. Click **Save Changes**. Rule 2 is created

successfully.



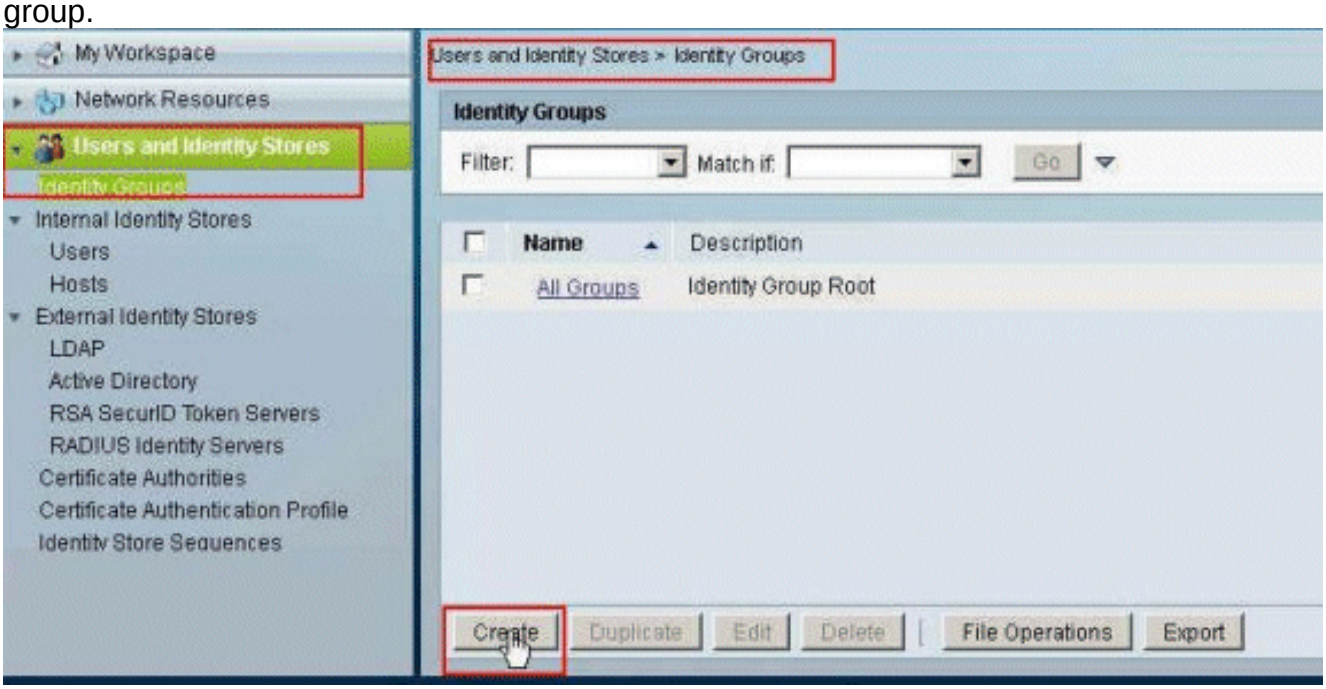
Configure ACS for Downloadable ACL for Group

Complete Steps 1 through 12 of the Configure ACS for Downloadable ACL for Individual User and perform these steps in order to configure Downloadable ACL for Group in a Cisco Secure ACS.

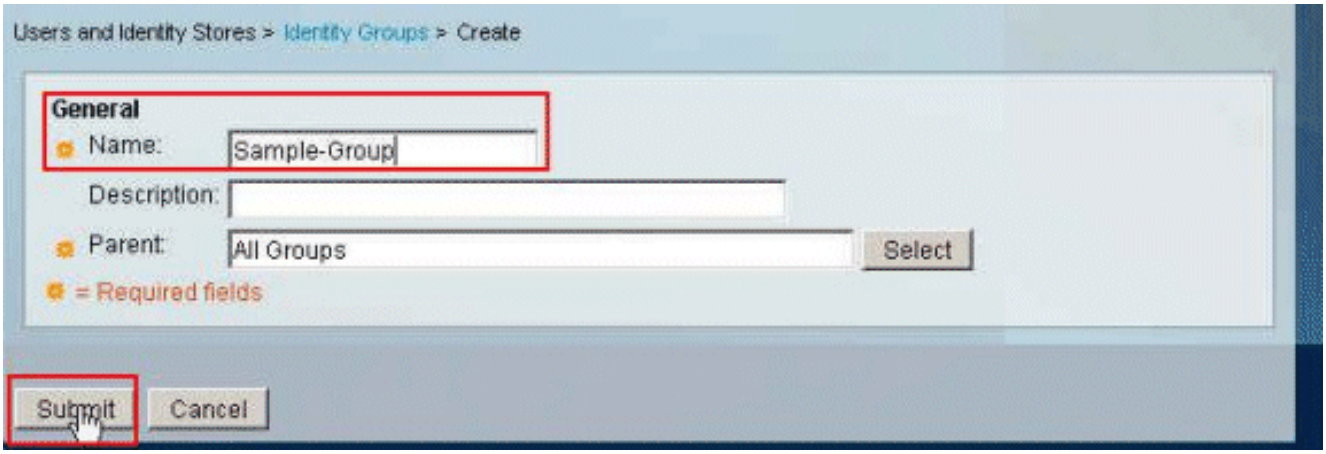
In this example, the IPsec VPN user "cisco" belongs to the **Sample-Group**.

The **Sample-Group** user **cisco** authenticates successfully, and the RADIUS server sends a downloadable access list to the security appliance. The user "cisco" can access only the 10.1.1.2 server and denies all other access. In order to verify the ACL, refer to the Downloadable ACL for User/Group section.

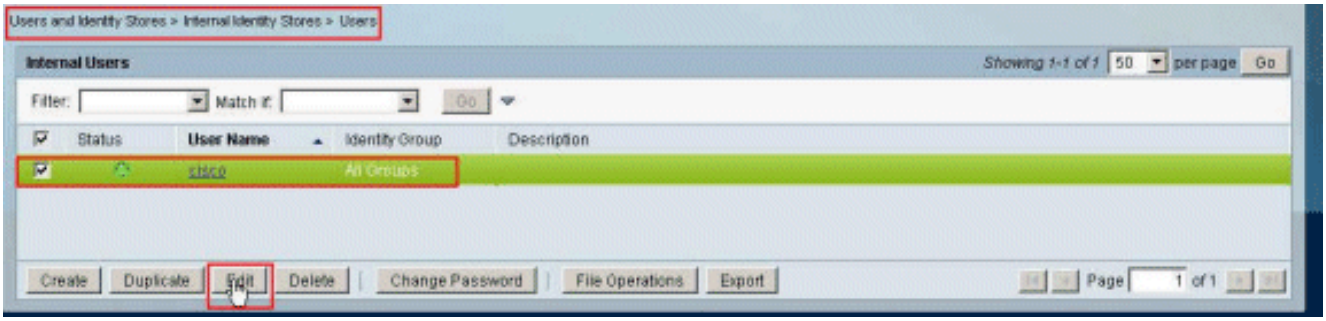
1. In the navigation bar, click **Users and Identity Stores** > **Identity Groups**, and click **Create** in order to create a new group.



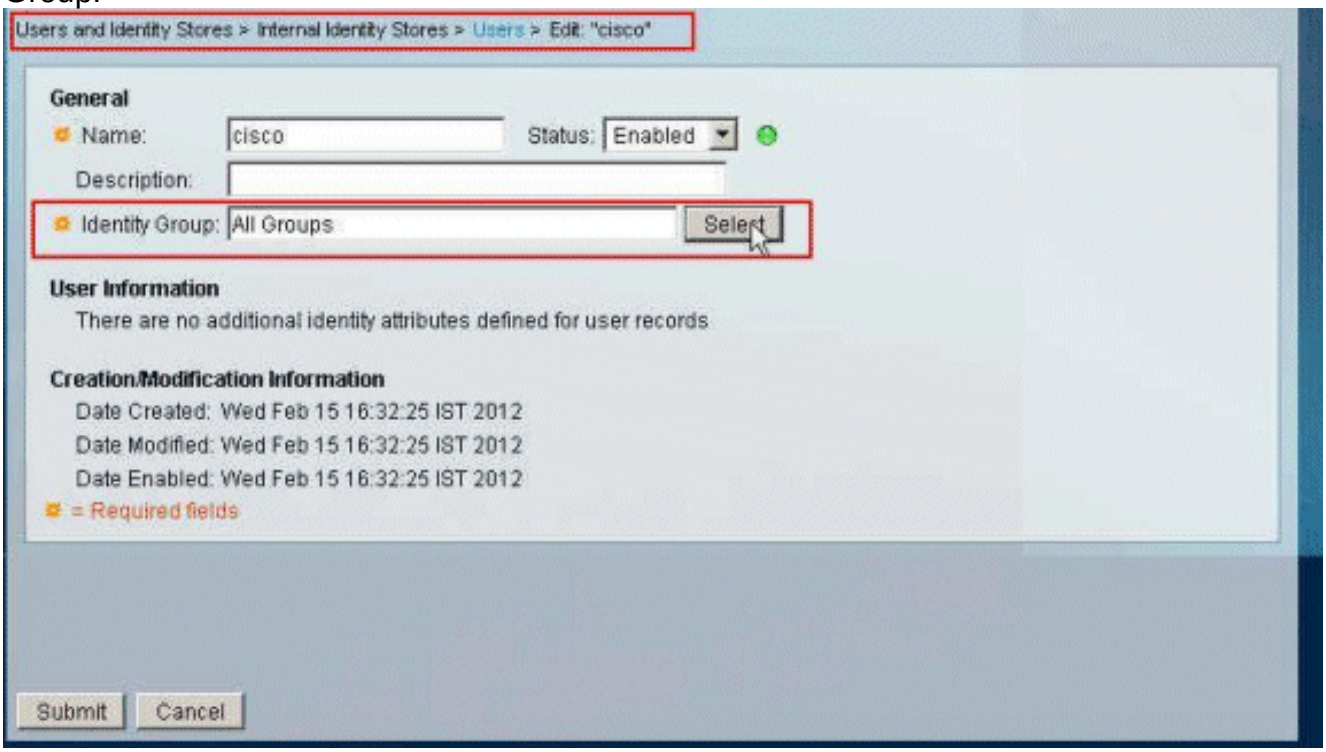
2. Provide a group name (**Sample-Group**), and click **Submit**.



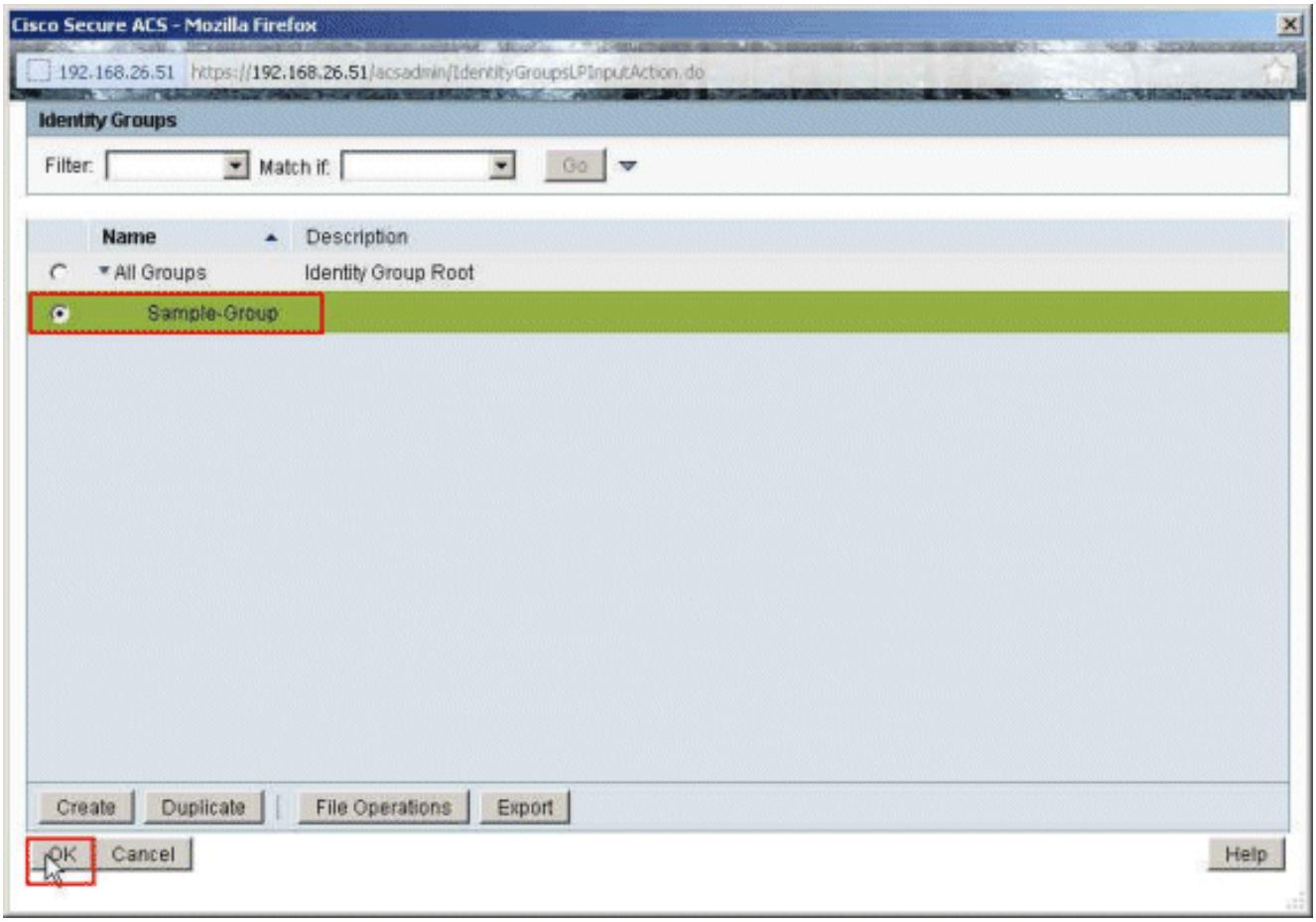
3. Choose **User Identity Stores** > **Internal Identity Stores** > **Users**, and select the user **cisco**. Click **Edit** in order to change the group membership of this user.



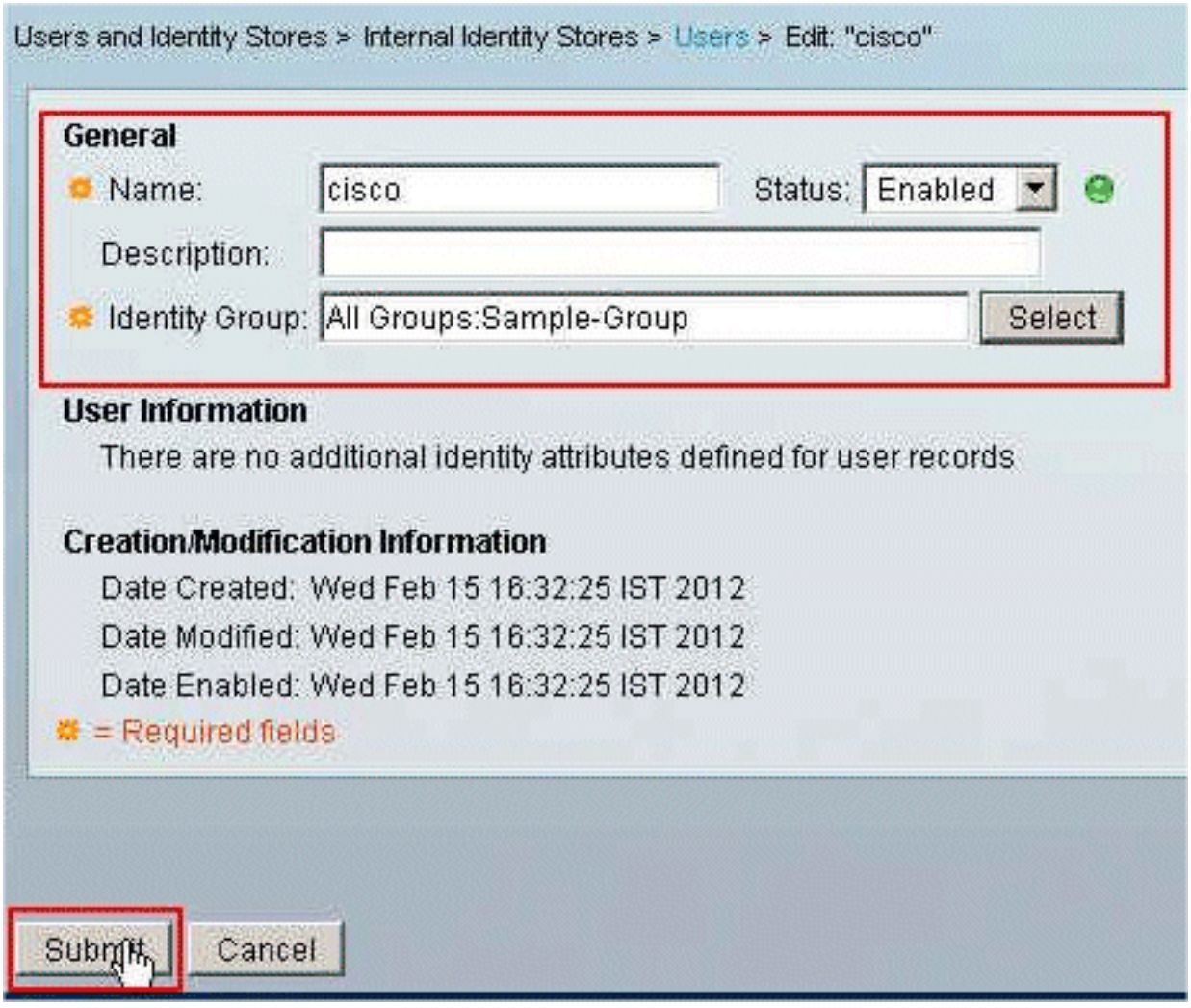
4. Click **Select** next to the Identity Group.



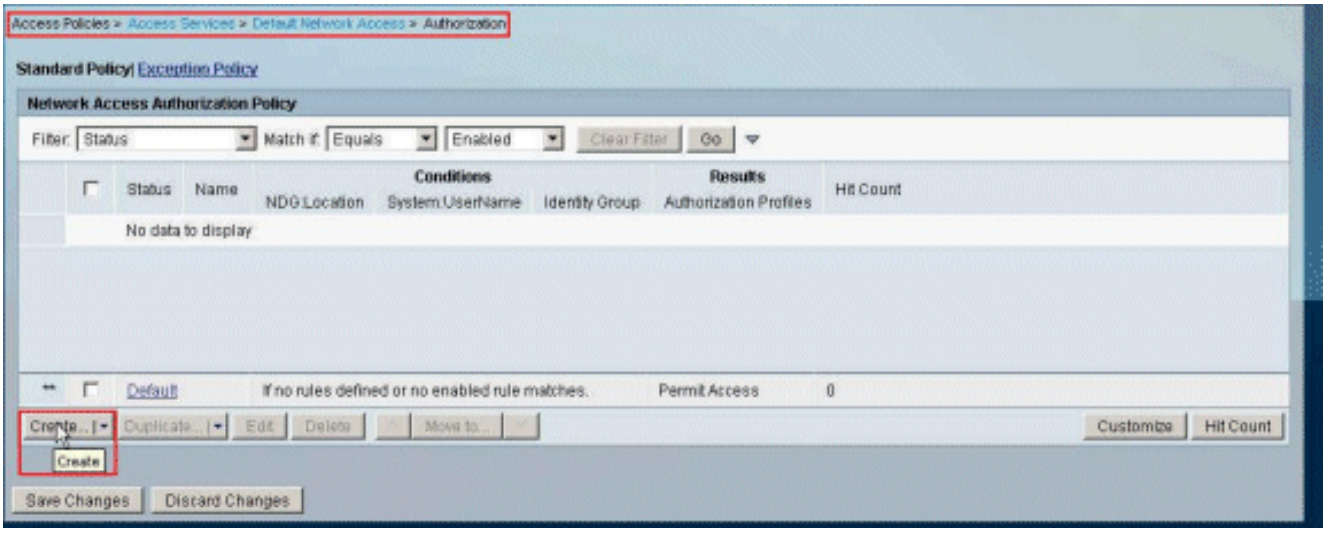
5. Select the newly created group (that is, **Sample-Group**), and click **OK**.



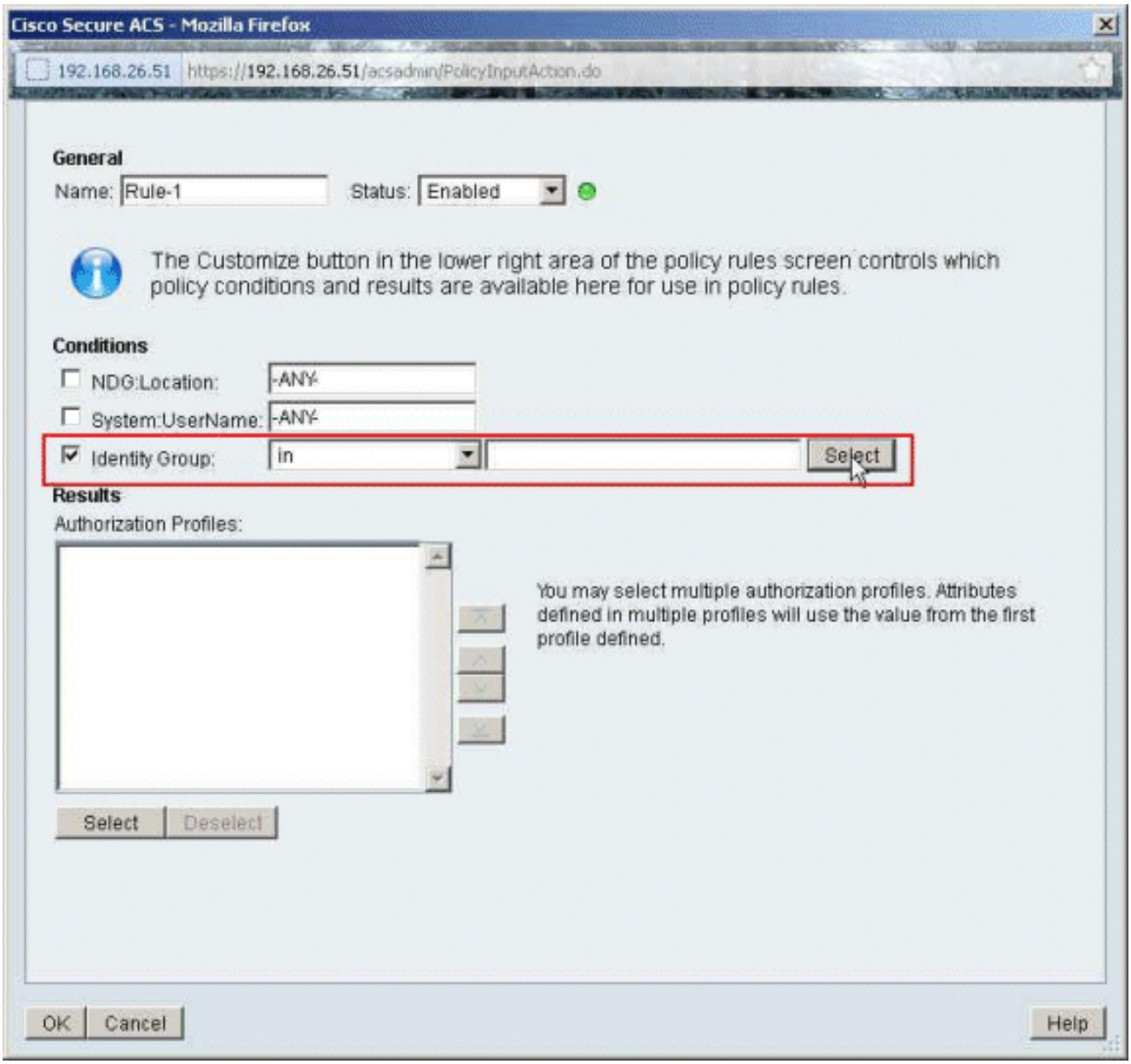
6. Click **Submit**.



7. Choose **Access Policies** > **Access Services** > **Default Network Access** > **Authorization**, and click **Create** in order to create a new Rule.

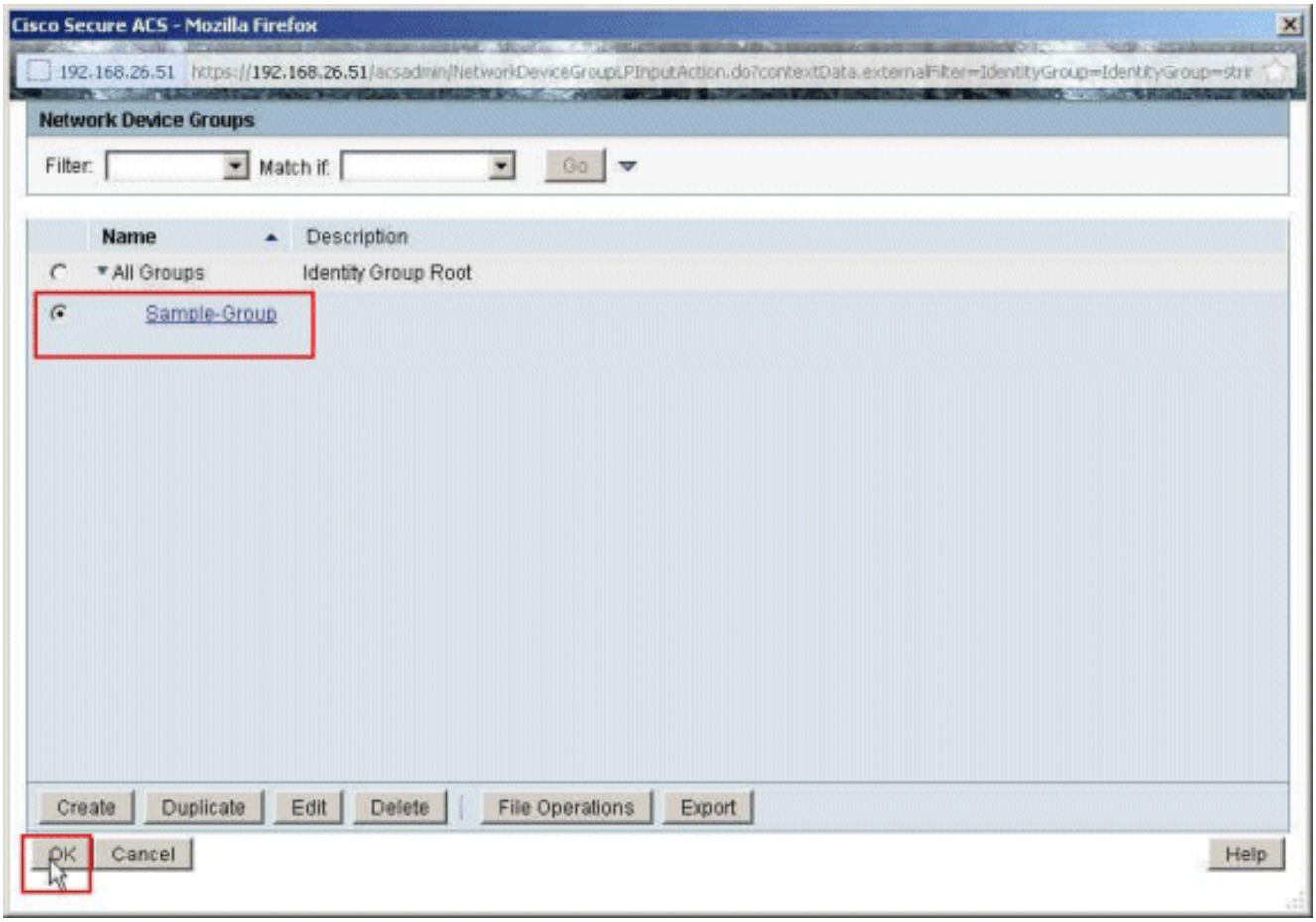


8. Make sure that the checkbox next to **Identity Group** is checked, and click **Select**.

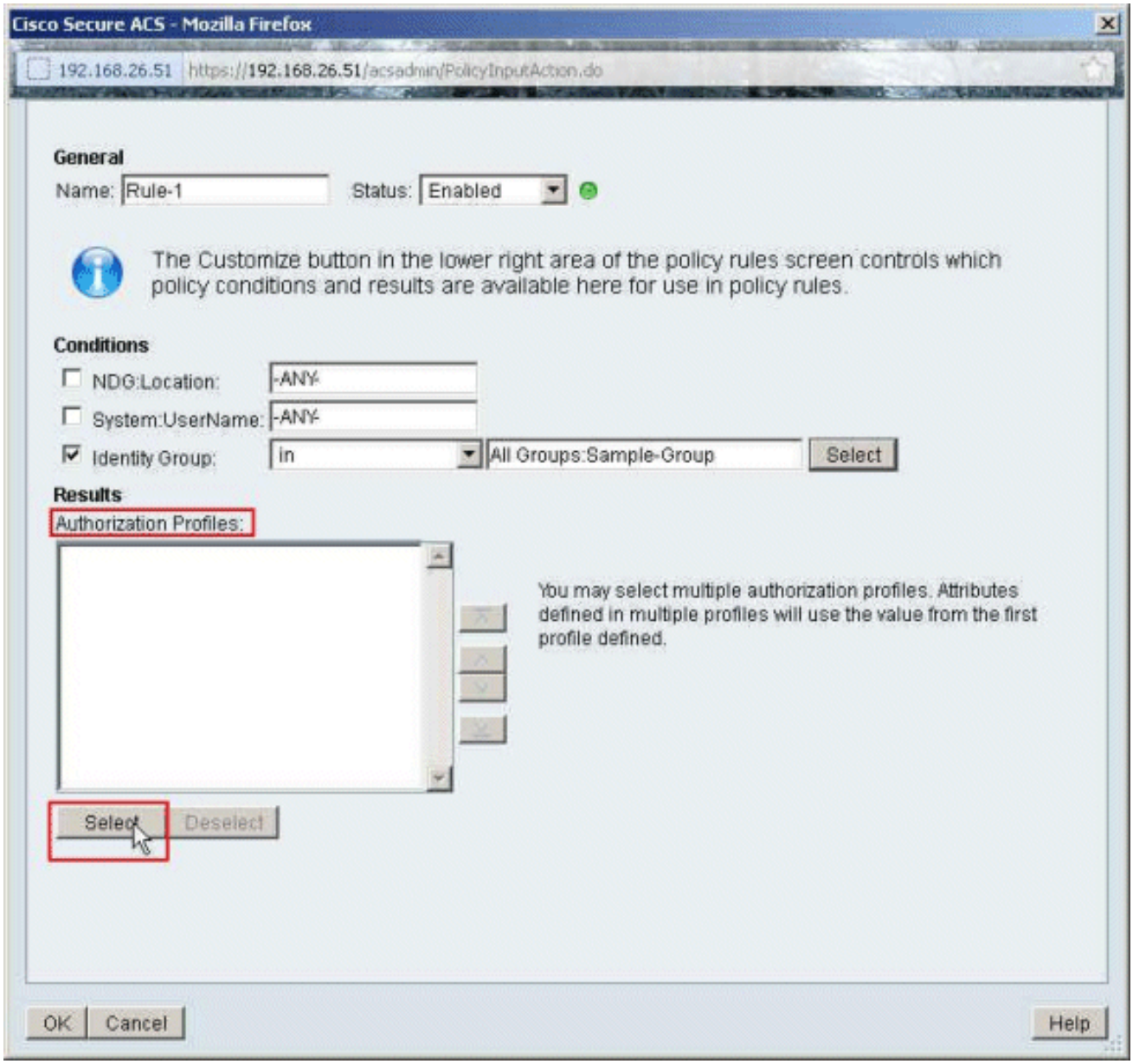


9. Choose **Sample-Group**, and click

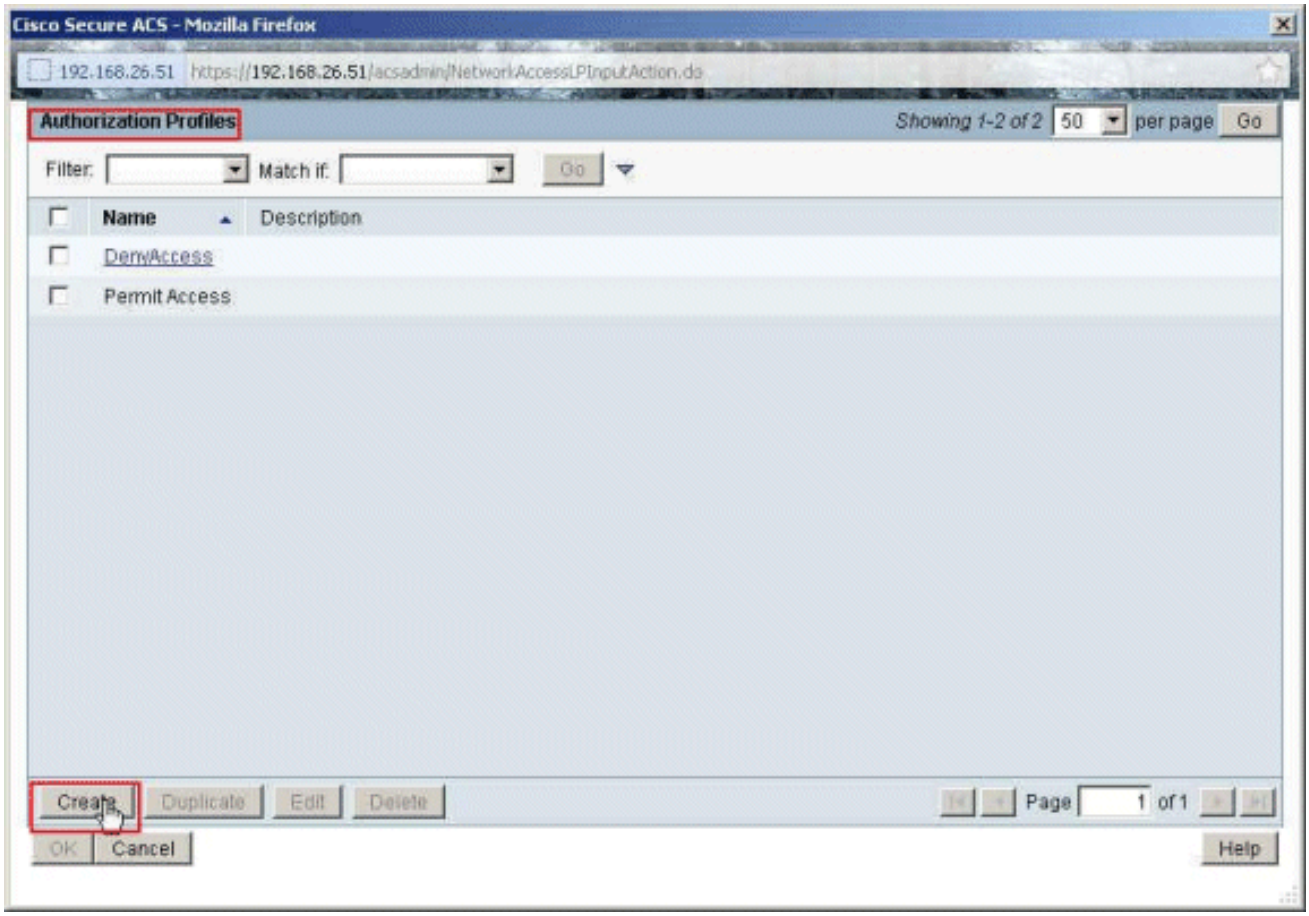
OK.



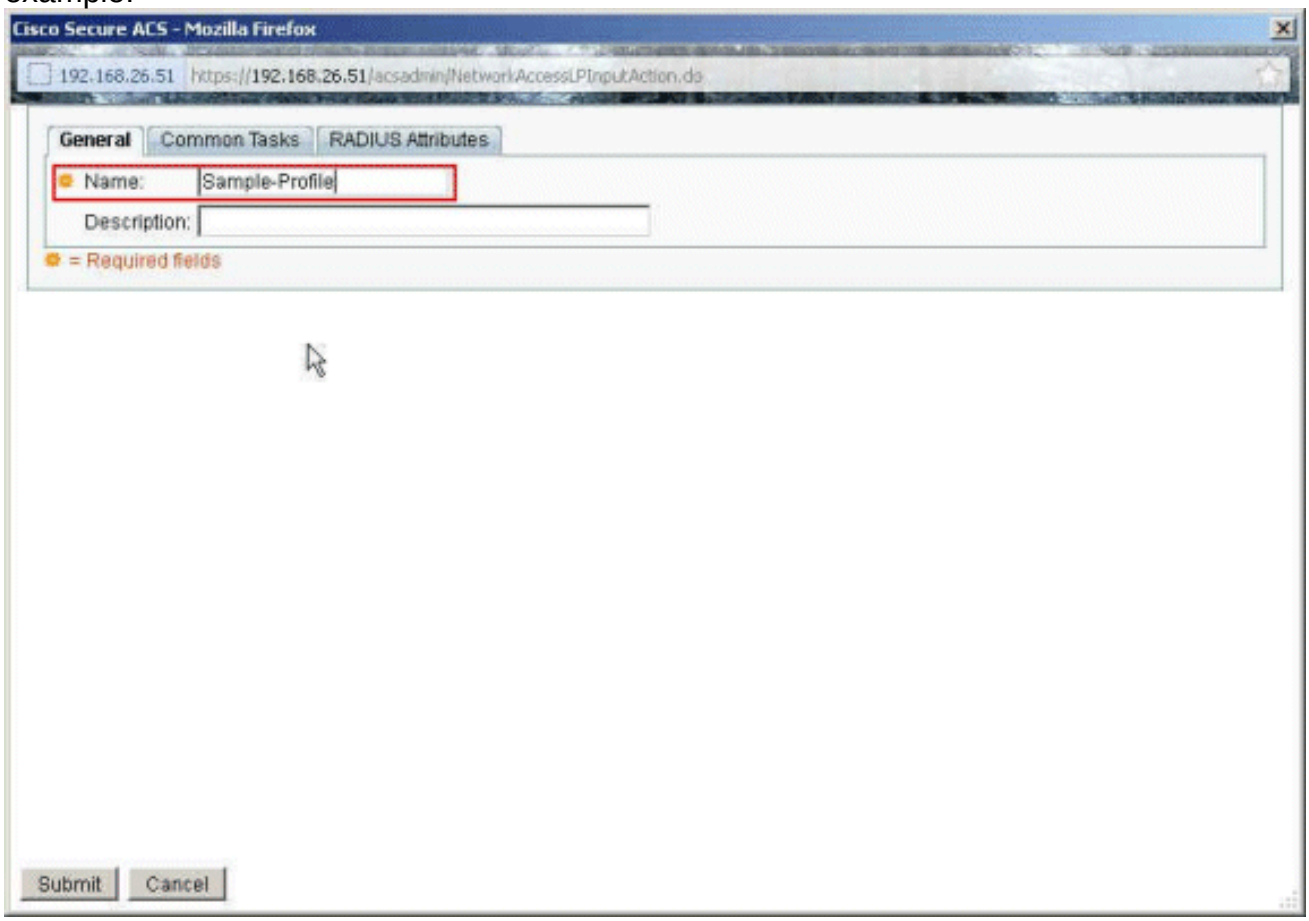
10. Click **Select**, in the Authorization Profiles section.



11. Click **Create** in order to create a new Authorization Profile.

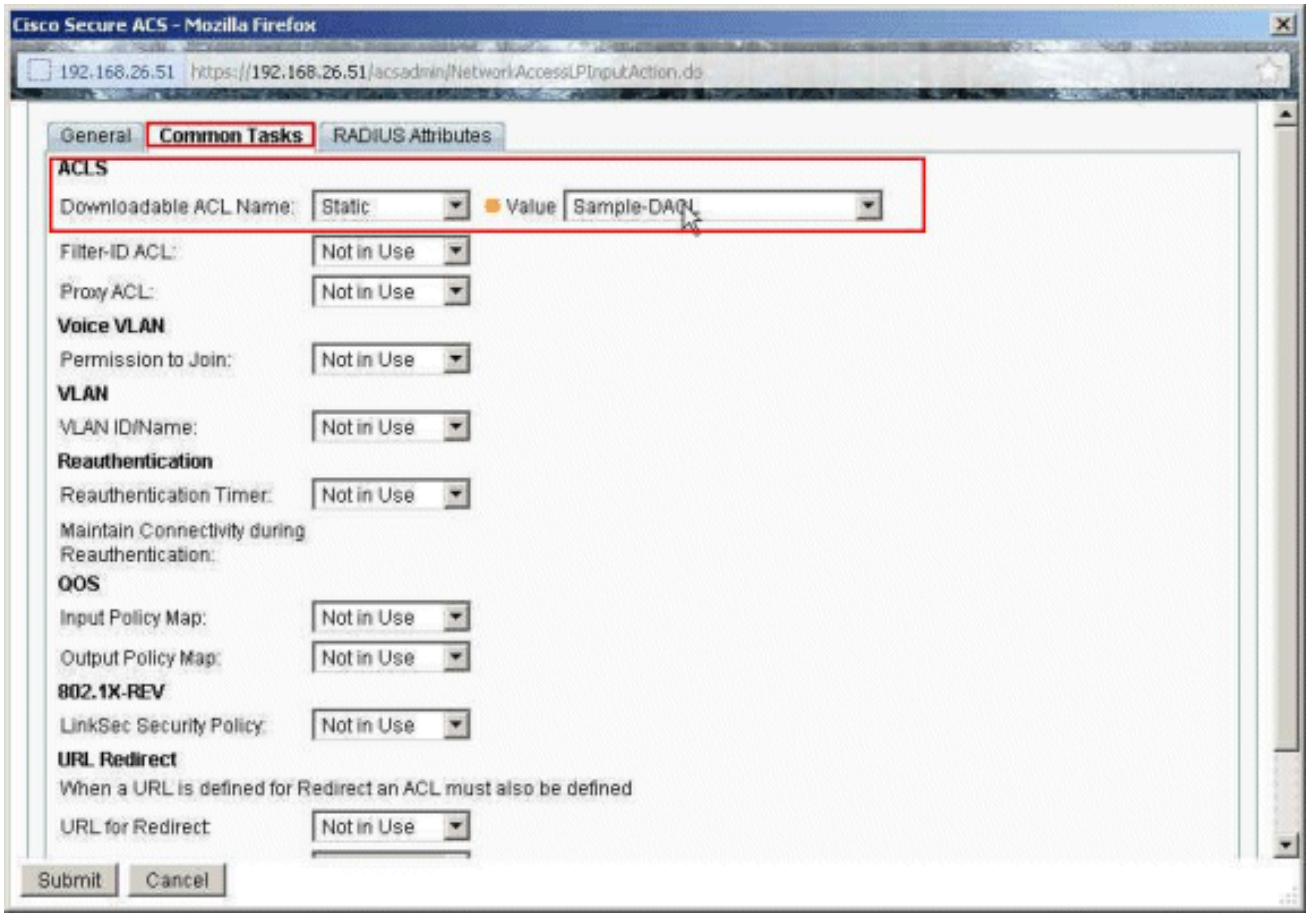


12. Provide a Name for the **Authorization Profile**. **Sample-Profile** is the name used in this example.

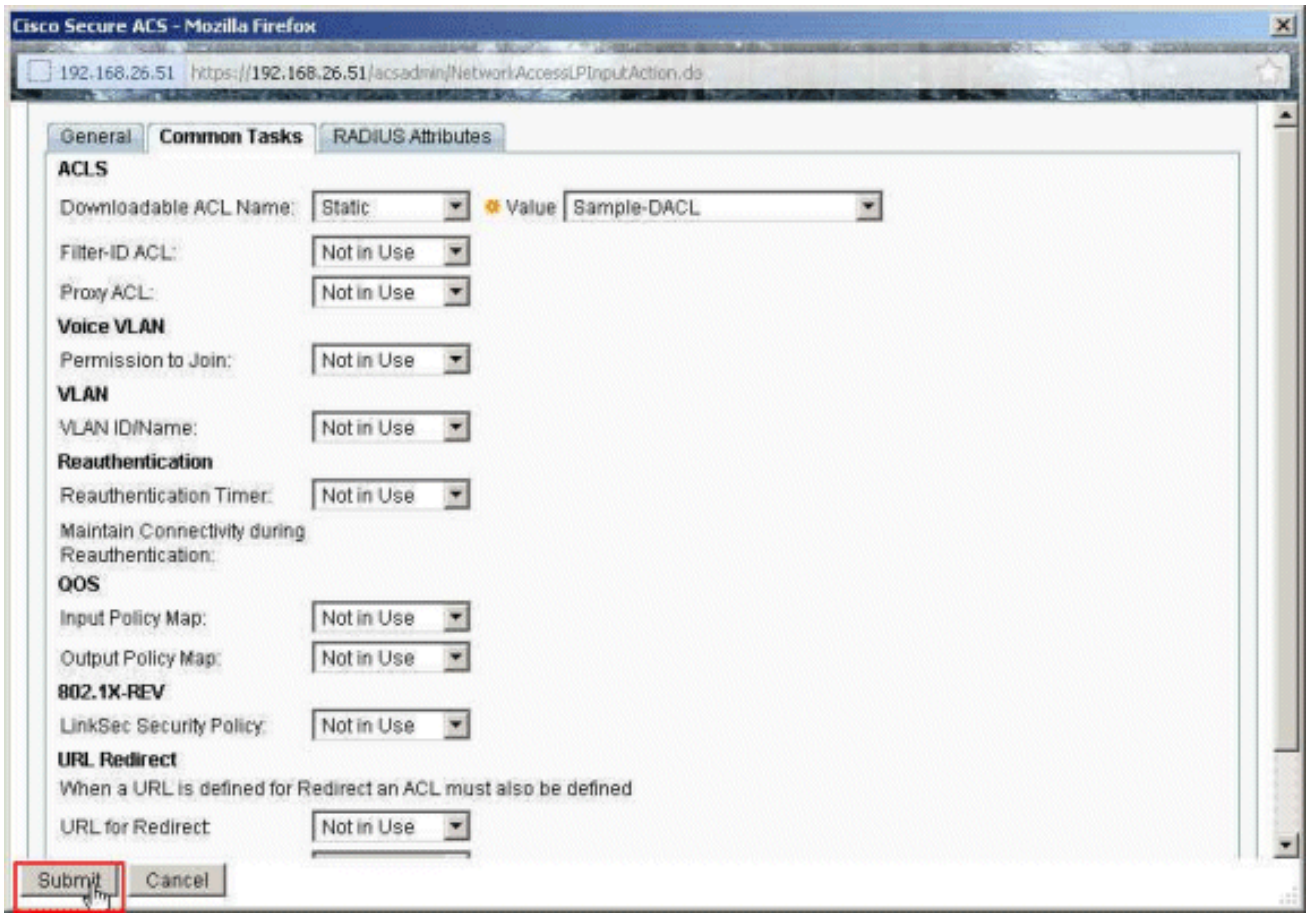


13. Choose the **Common Tasks** tab, and select **Static** from the drop-down list for the **Downloadable ACL Name**. Choose the newly created **DACL (Sample -DACL)** from the Value drop-down

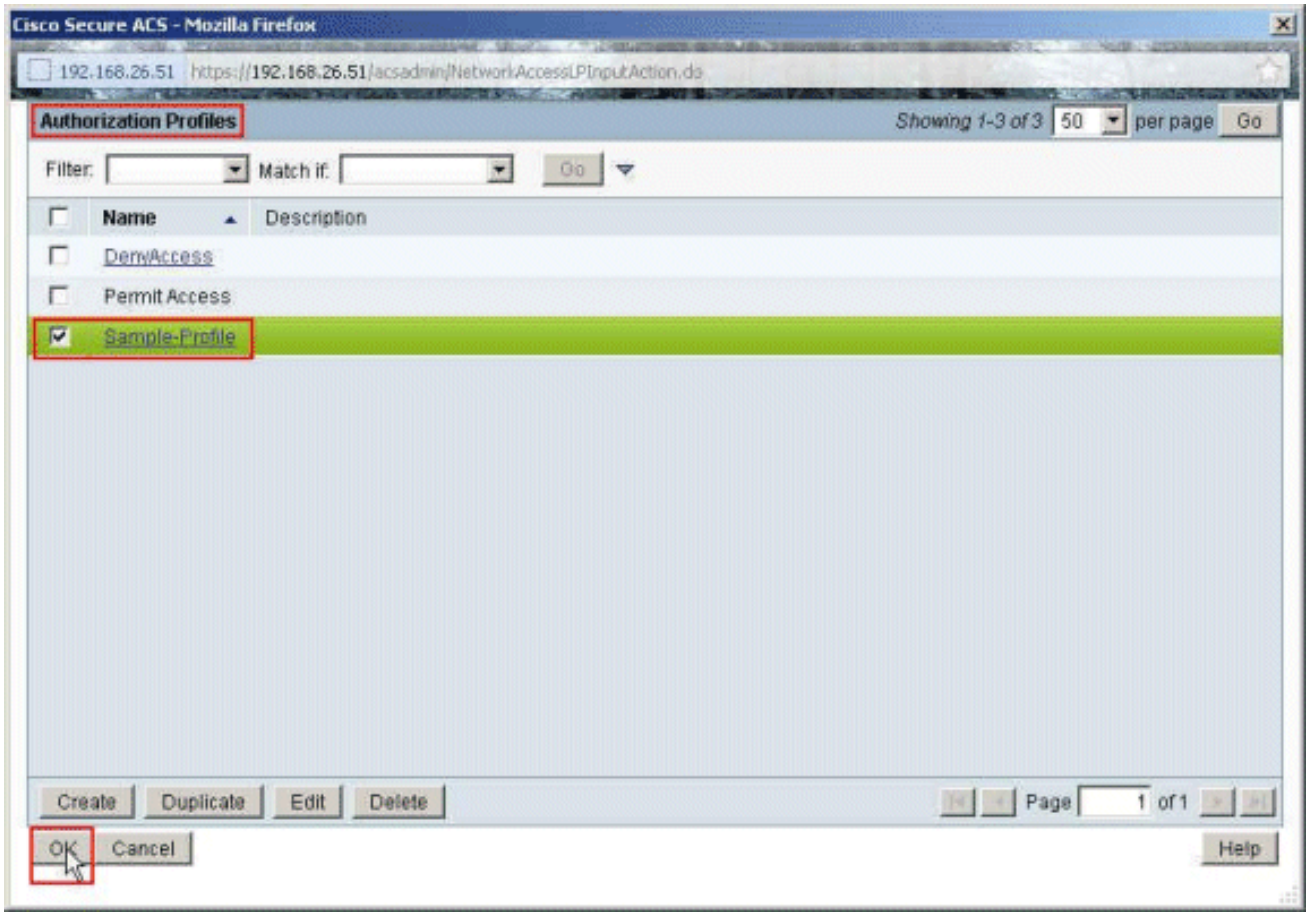
list.



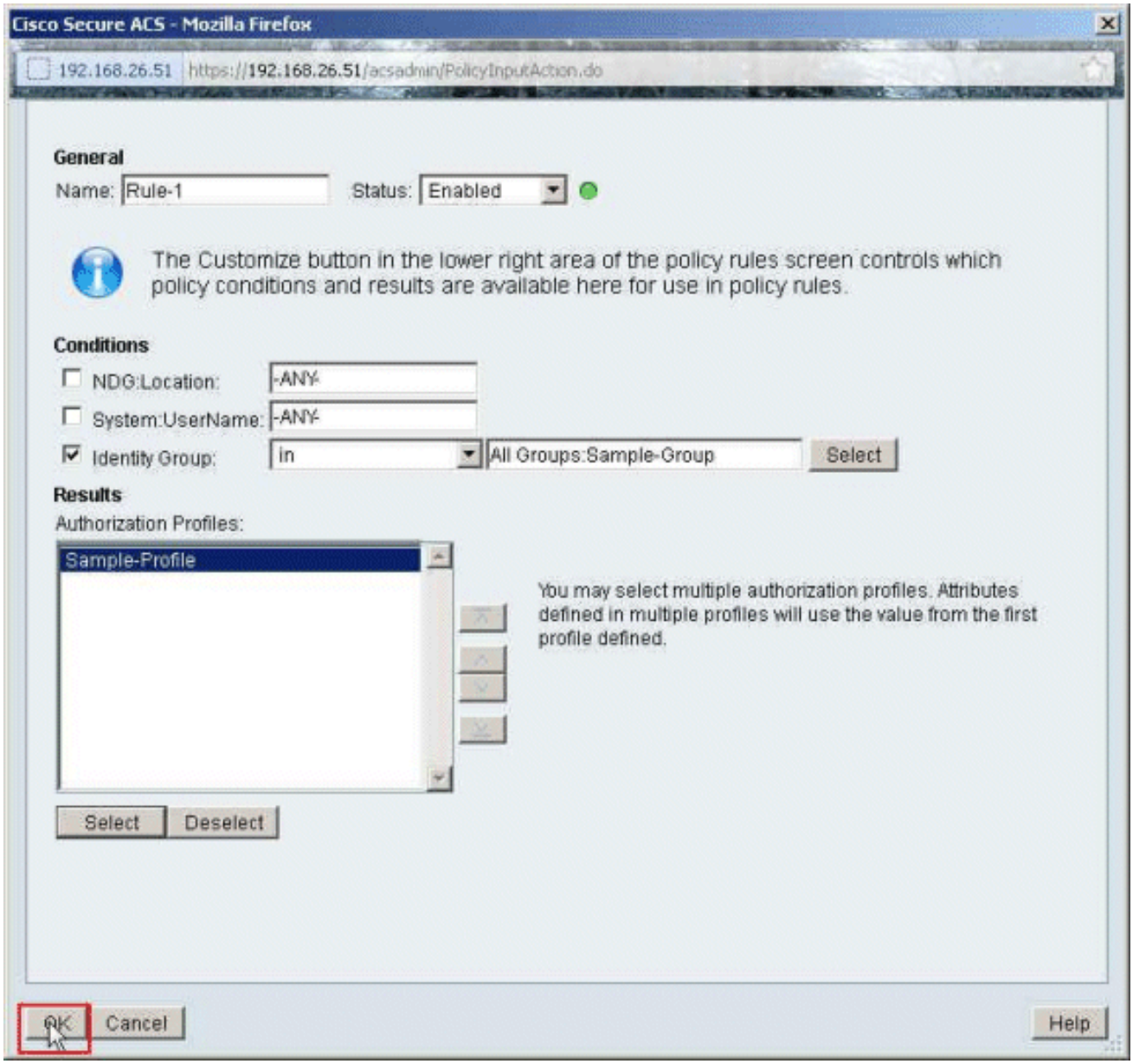
14. Click **Submit**.



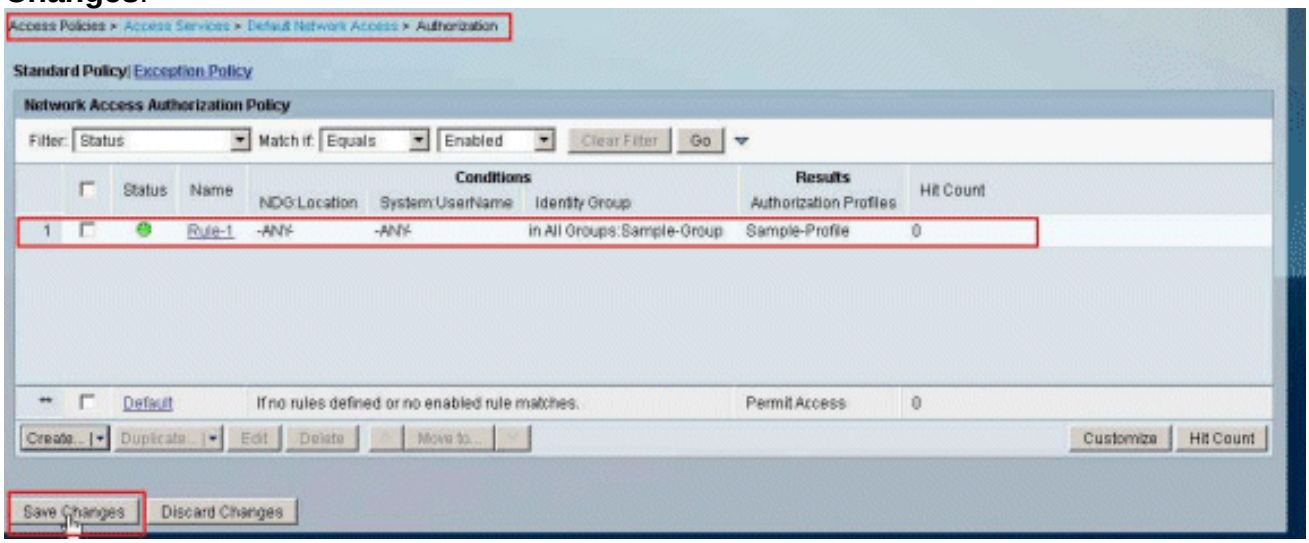
15. Choose the Authorization Profile **Sample-Profile** created earlier, and click **OK**.


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. Verify that **Rule-1** is created with the Identity Group **Sample-Group** as the condition and **Sample-Profile** as the Result. Click **Save Changes**.



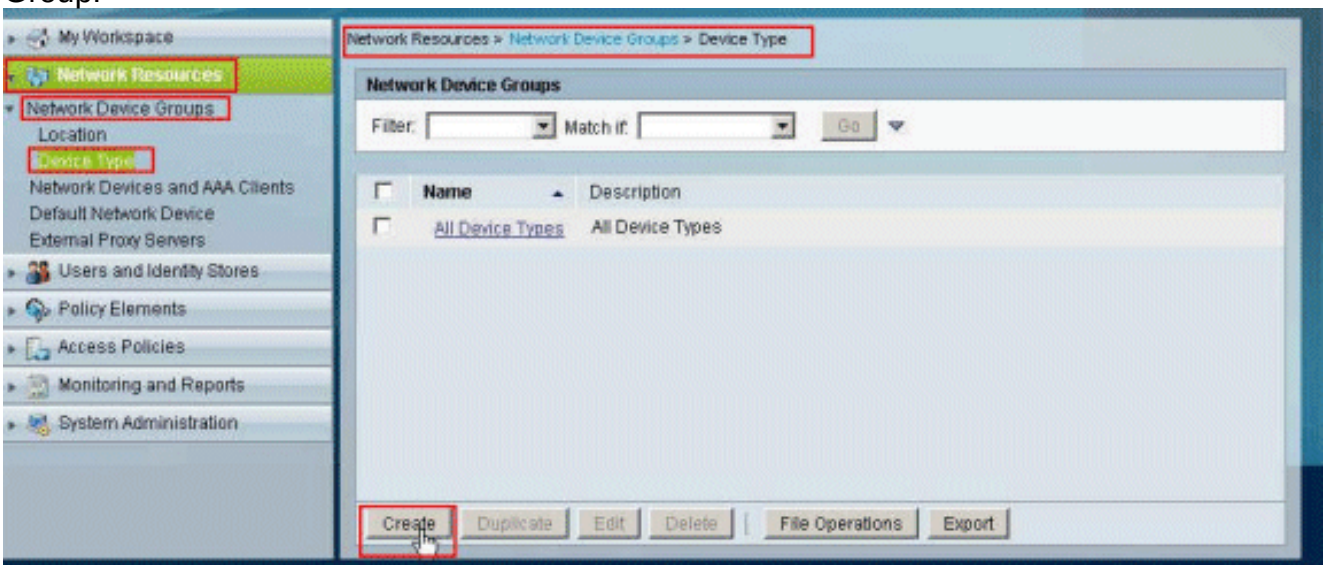
Configure ACS for Downloadable ACL for a Network Device Group

Complete Steps 1 through 12 of the Configure ACS for Downloadable ACL for Individual User and

perform these steps in order to configure Downloadable ACL for a Network Device Group in a Cisco Secure ACS.

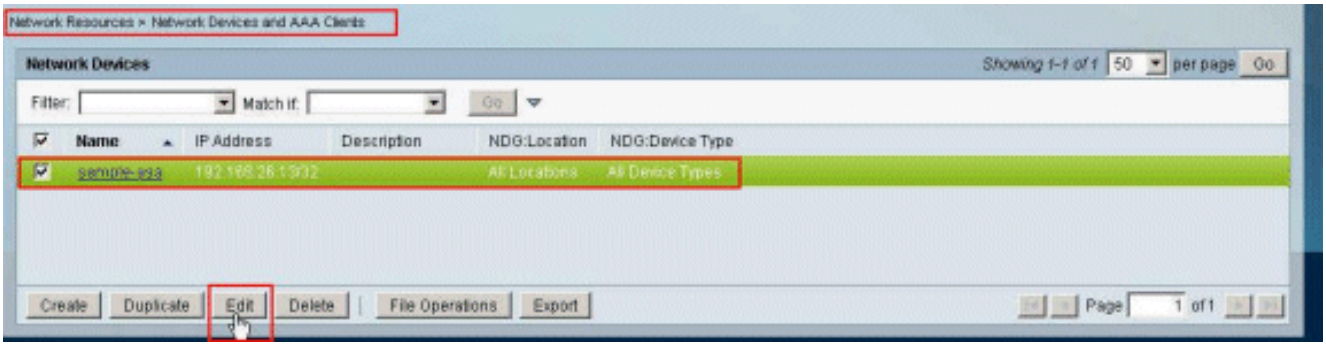
In this example, the RADIUS Client (ASA) belongs to the Network Device Group **VPN-Gateways**.The VPN authentication request coming from ASA for user "cisco" authenticates successfully, and the RADIUS server sends a downloadable access list to the security appliance. The user "cisco" can access only the 10.1.1.2 server and denies all other access. In order to verify the ACL, refer to the Downloadable ACL for User/Group section.

1. Choose **Network Resources** > **Network Device Groups** > **Device Type**, and click **Create** in order to create a new Network Device Group.

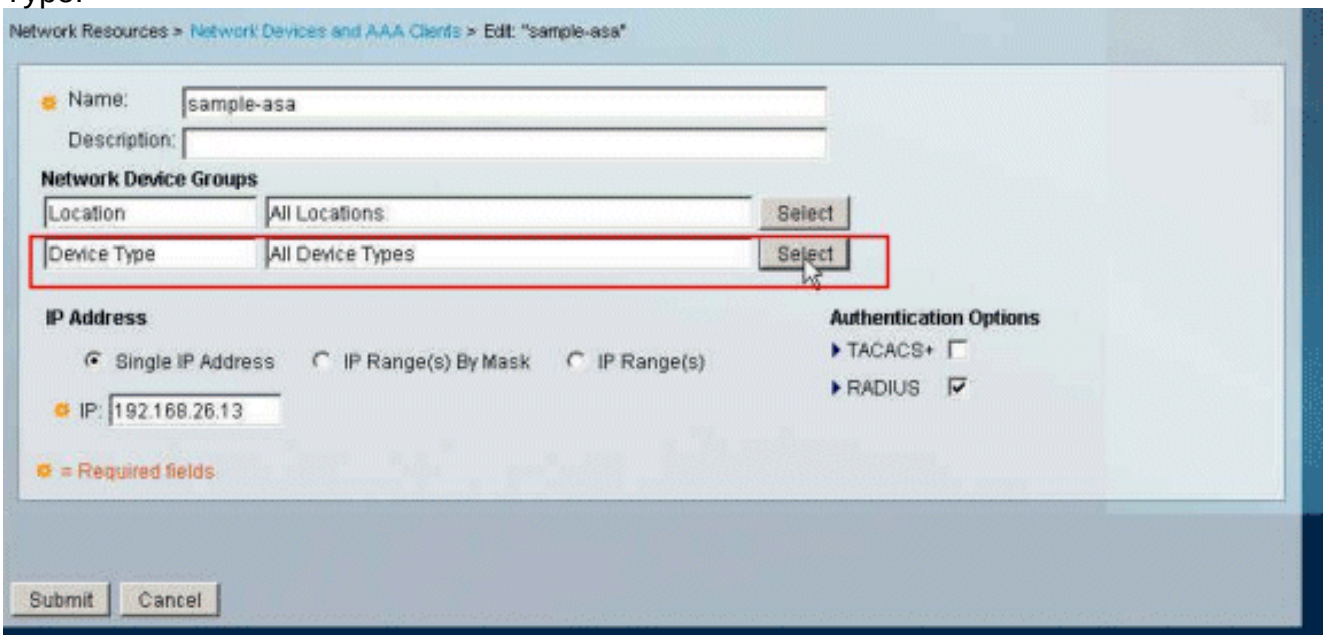


2. Provide a **Network Device Group** name (**VPN-Gateways** in this example), and click **Submit**.

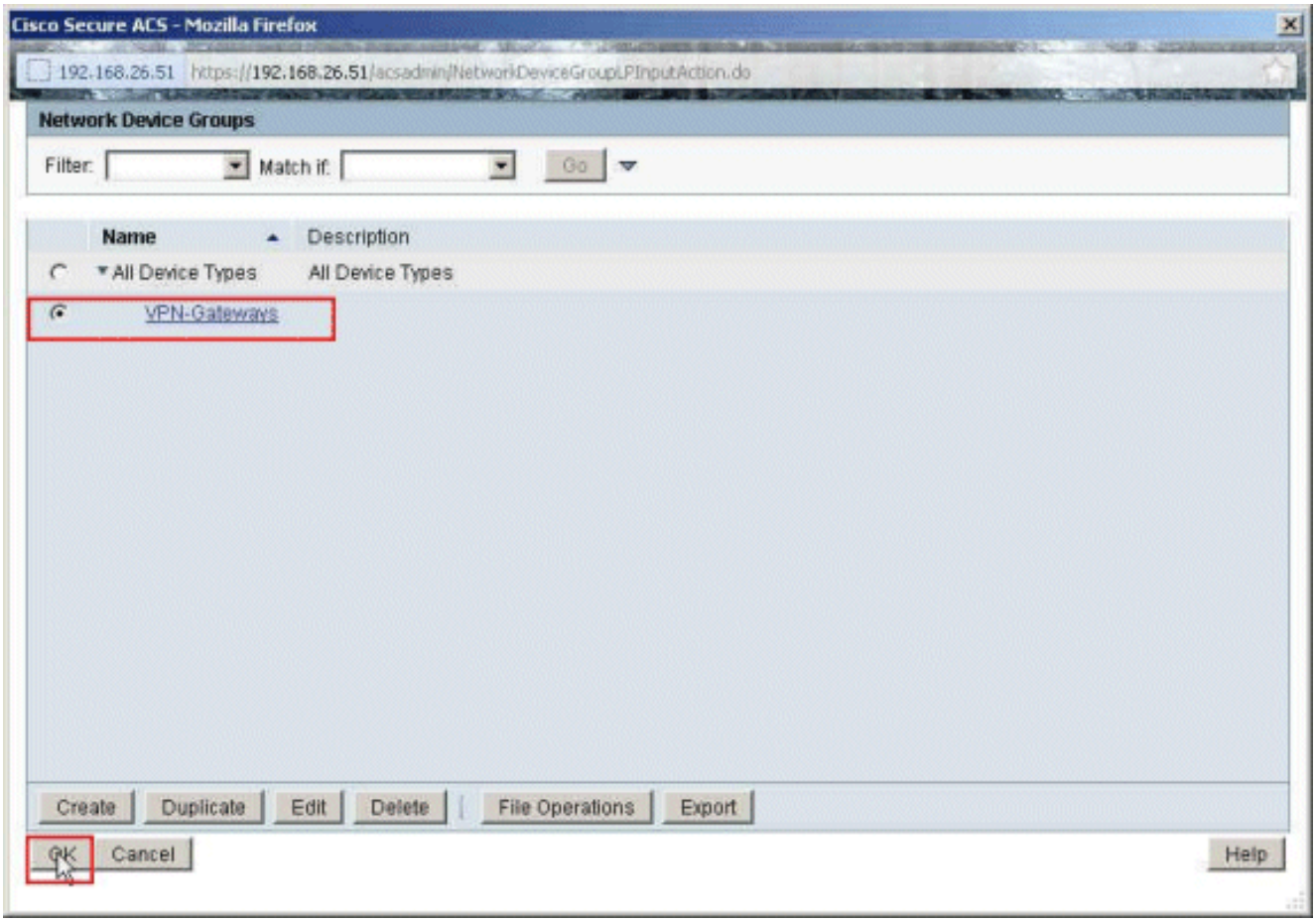
3. Choose **Network Resources** > **Network Devices and AAA Clients**, and select the **RADIUS** Client **sample-asa** created earlier. Click **Edit** in order to change the **Network Device Group** membership of this RADIUS Client (asa).



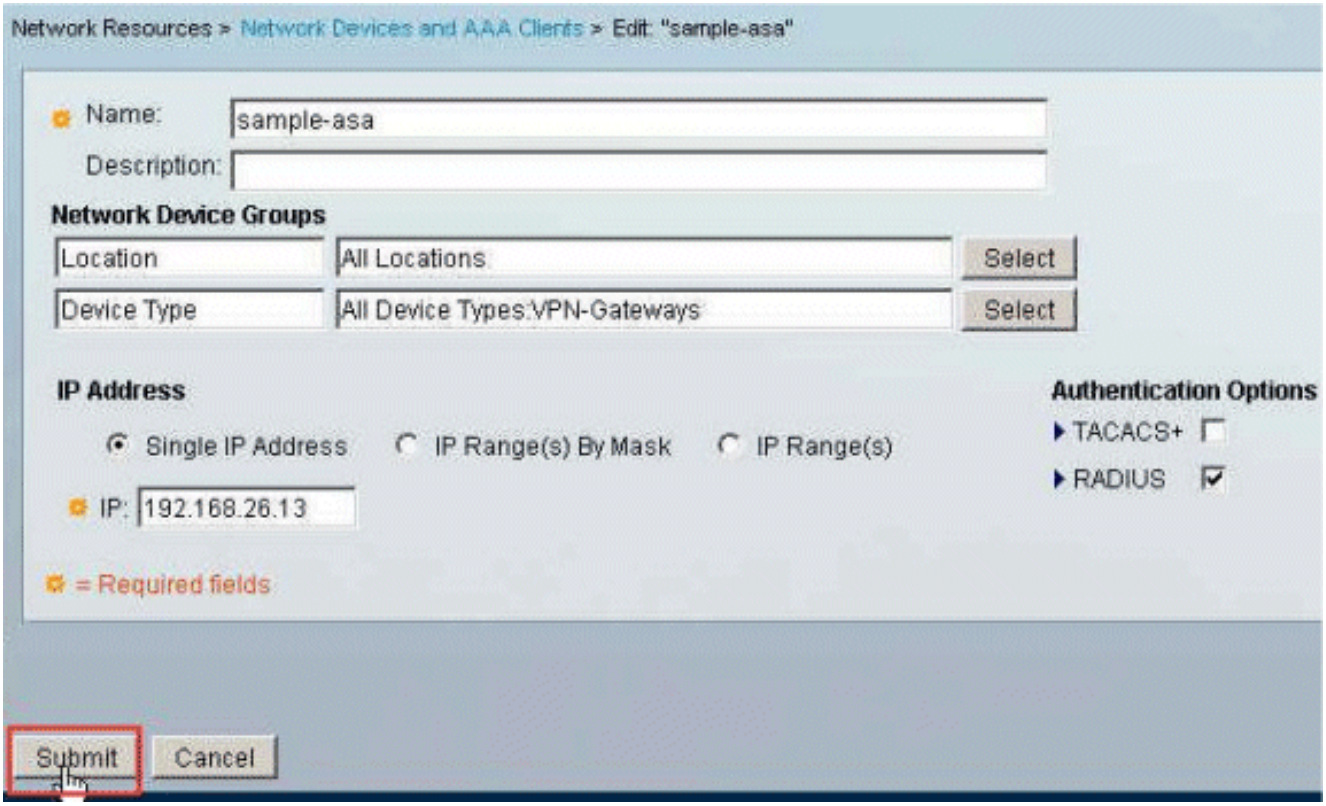
4. Click **Select** next to the Device Type.



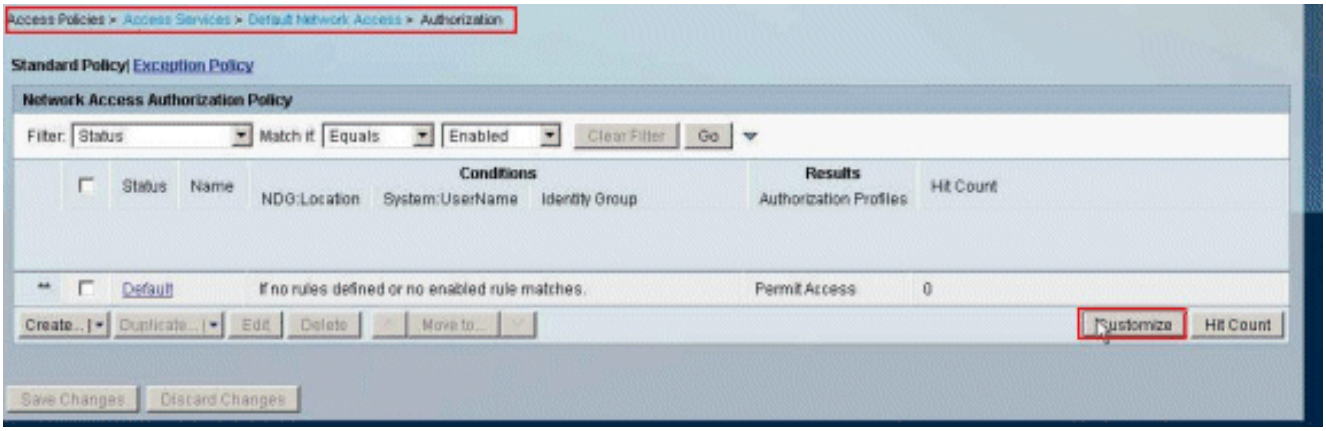
5. Select the newly created Network Device Group (which is **VPN-Gateways**), and click **OK**.



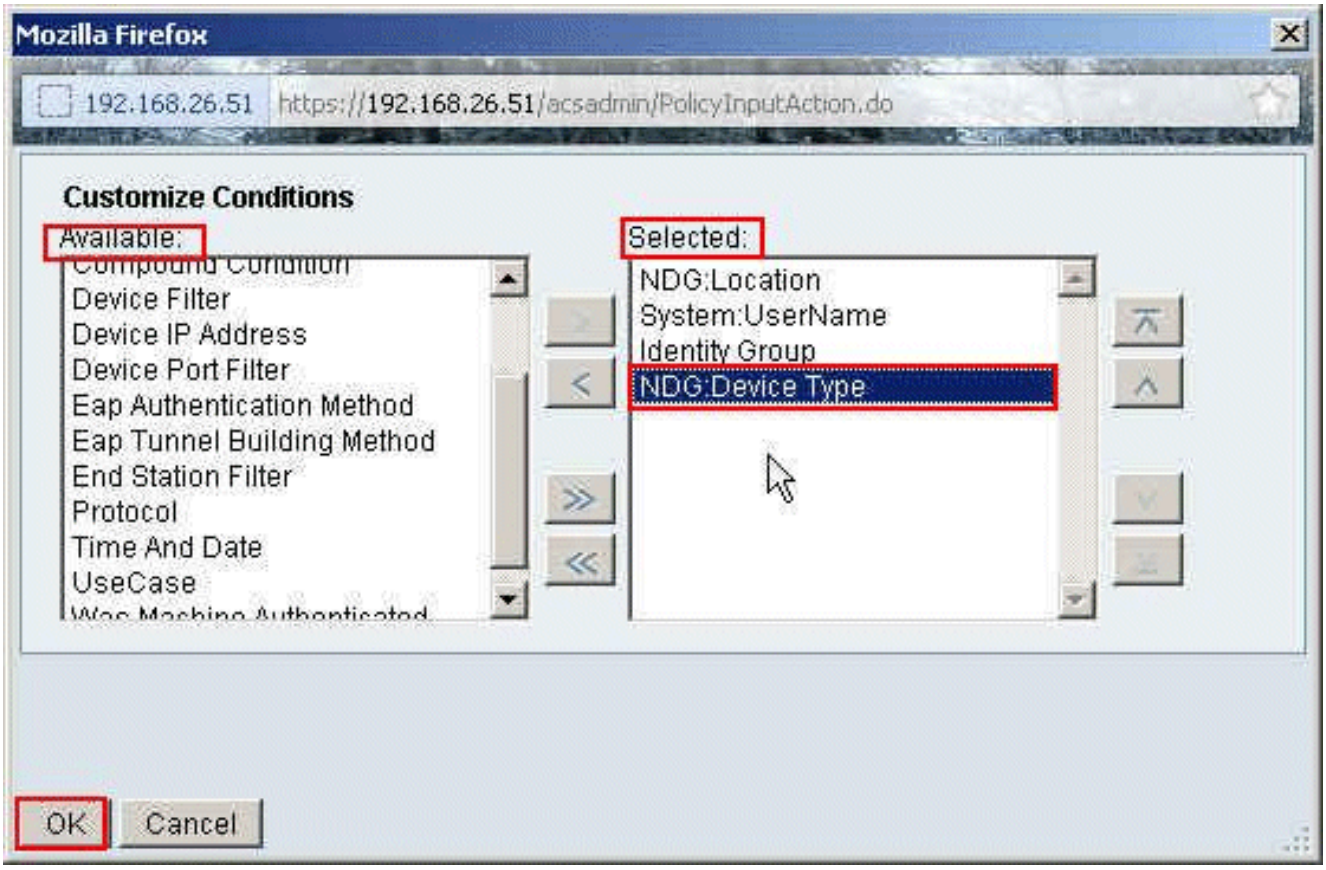
6. Click
Submit.



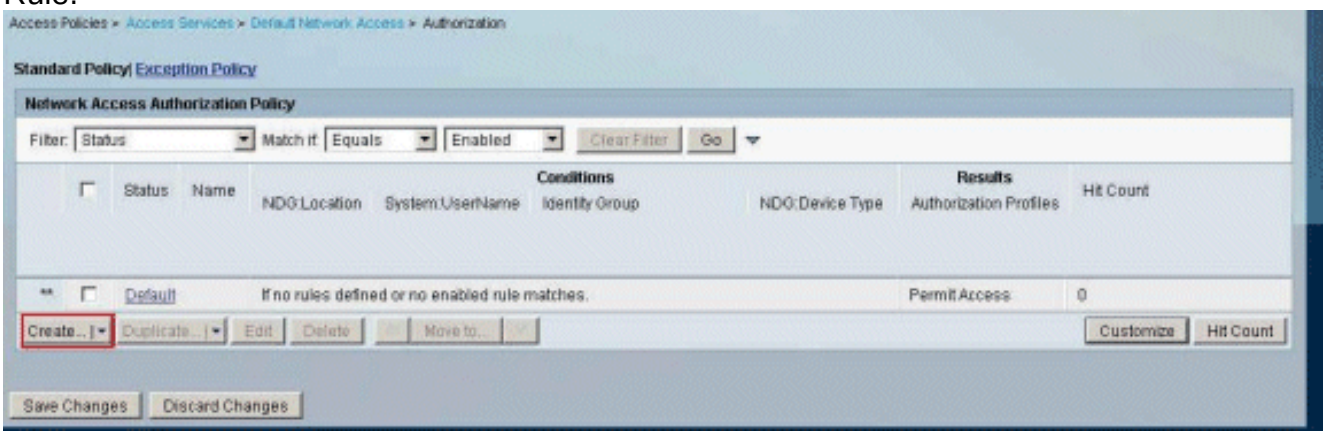
7. Choose **Access Policies** > **Access Services** > **Default Network Access** > **Authorization**, and click
Customize.



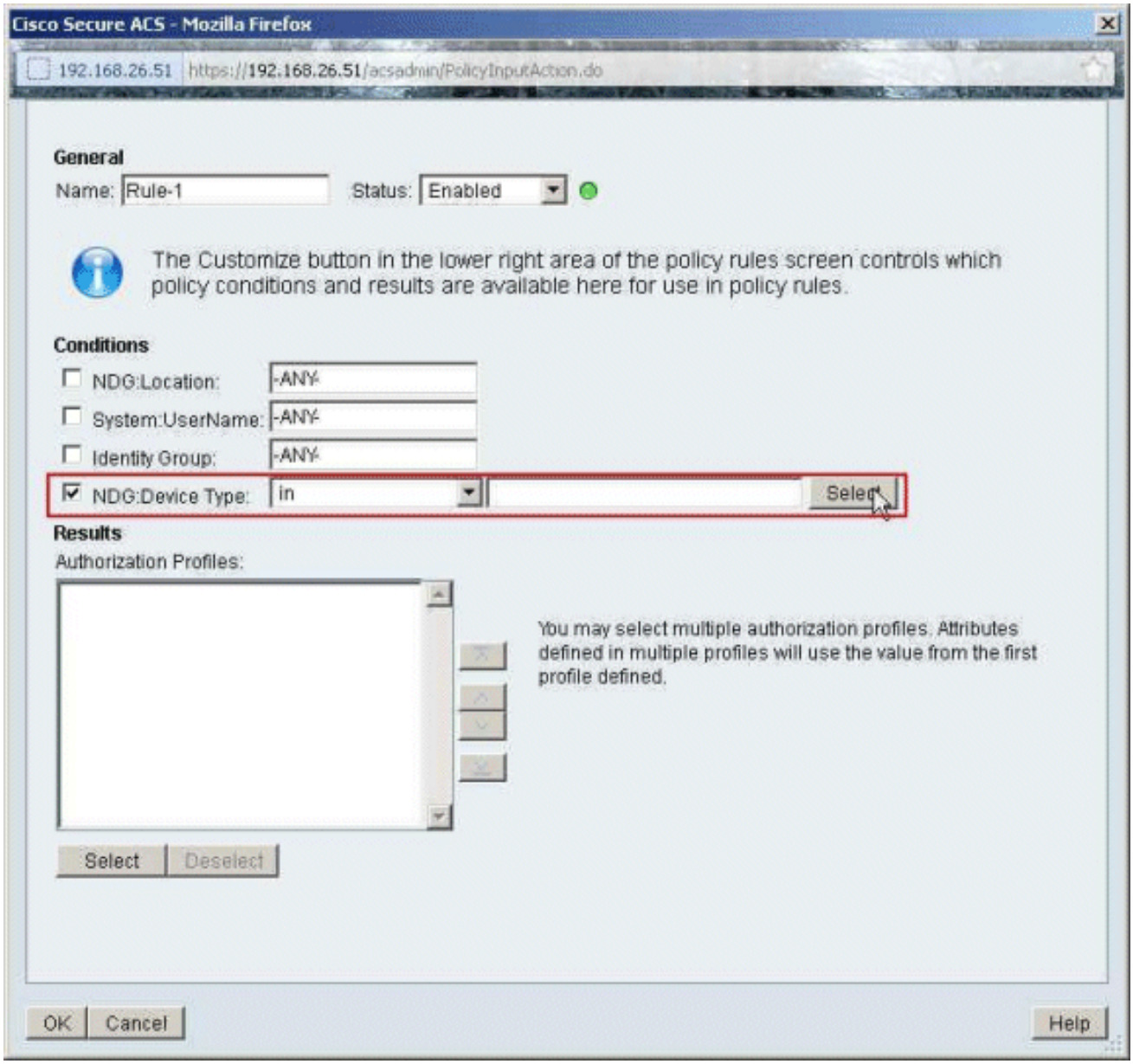
8. Move **NDG:Device Type** from the **Available** section to the **Selected** section, and click **OK**.



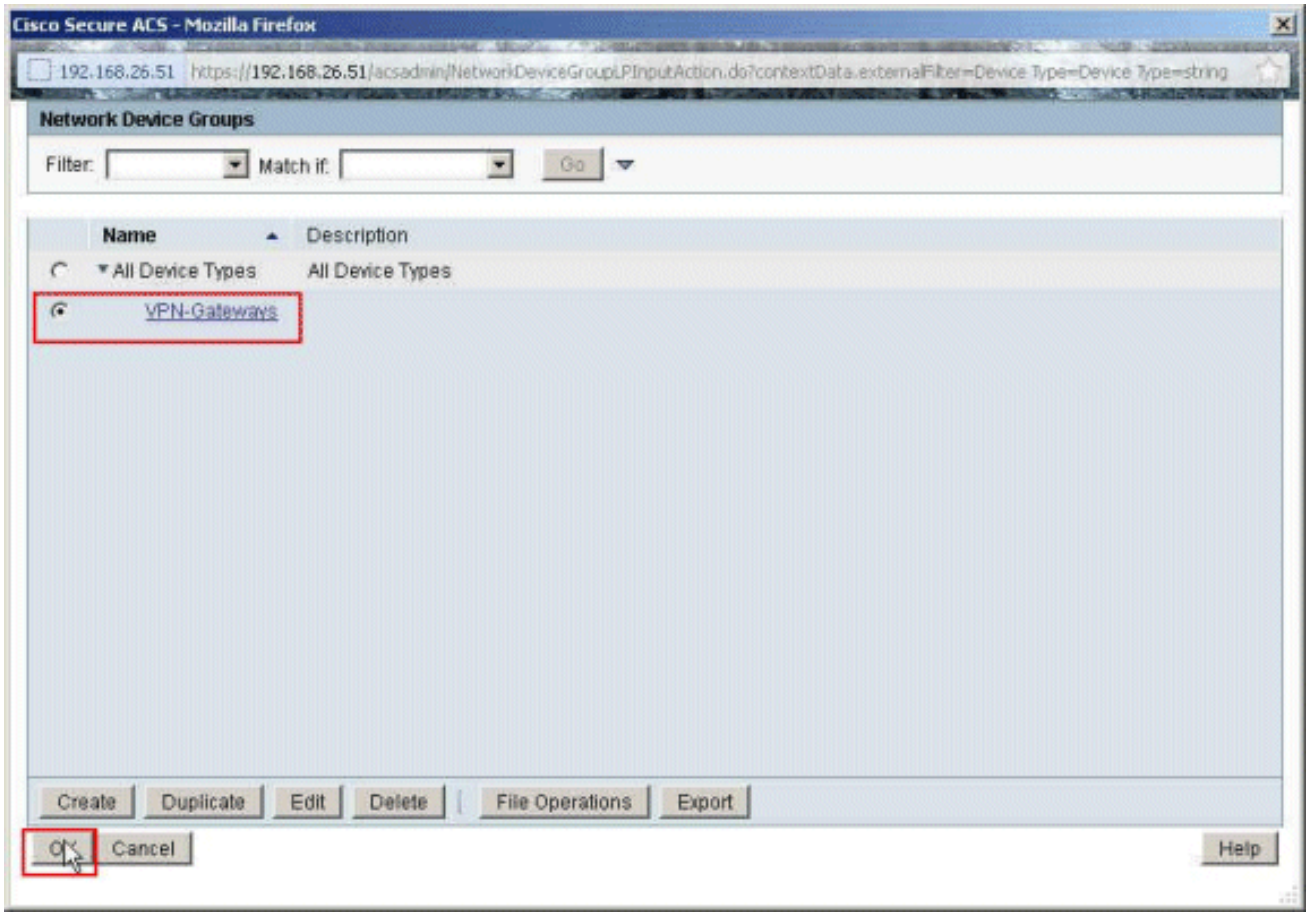
9. Click **Create** in order to create a new Rule.



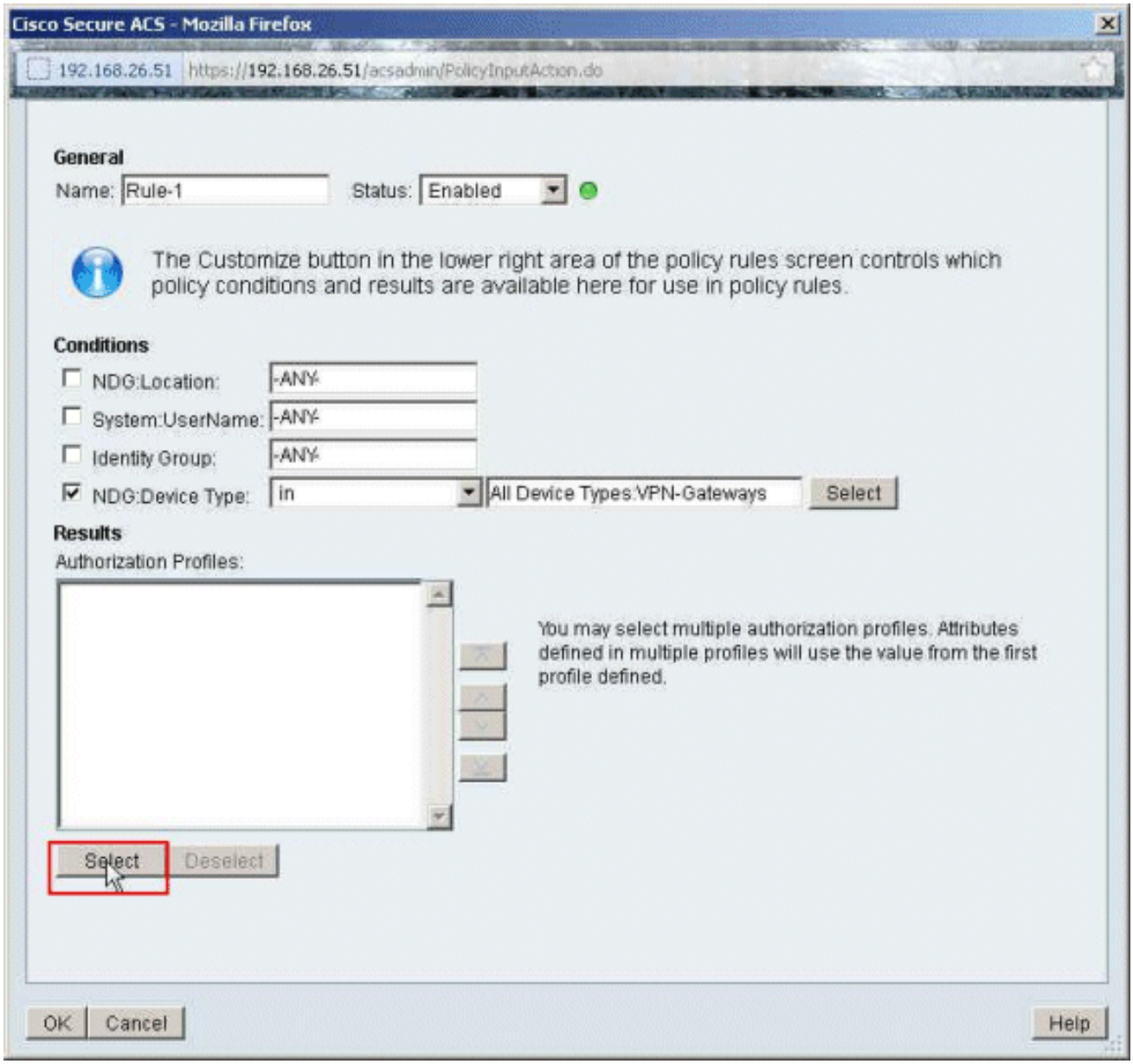
10. Make sure that the checkbox next to **NDG:Device Type** is selected and choose **in** from the drop-down list. Click **Select**.



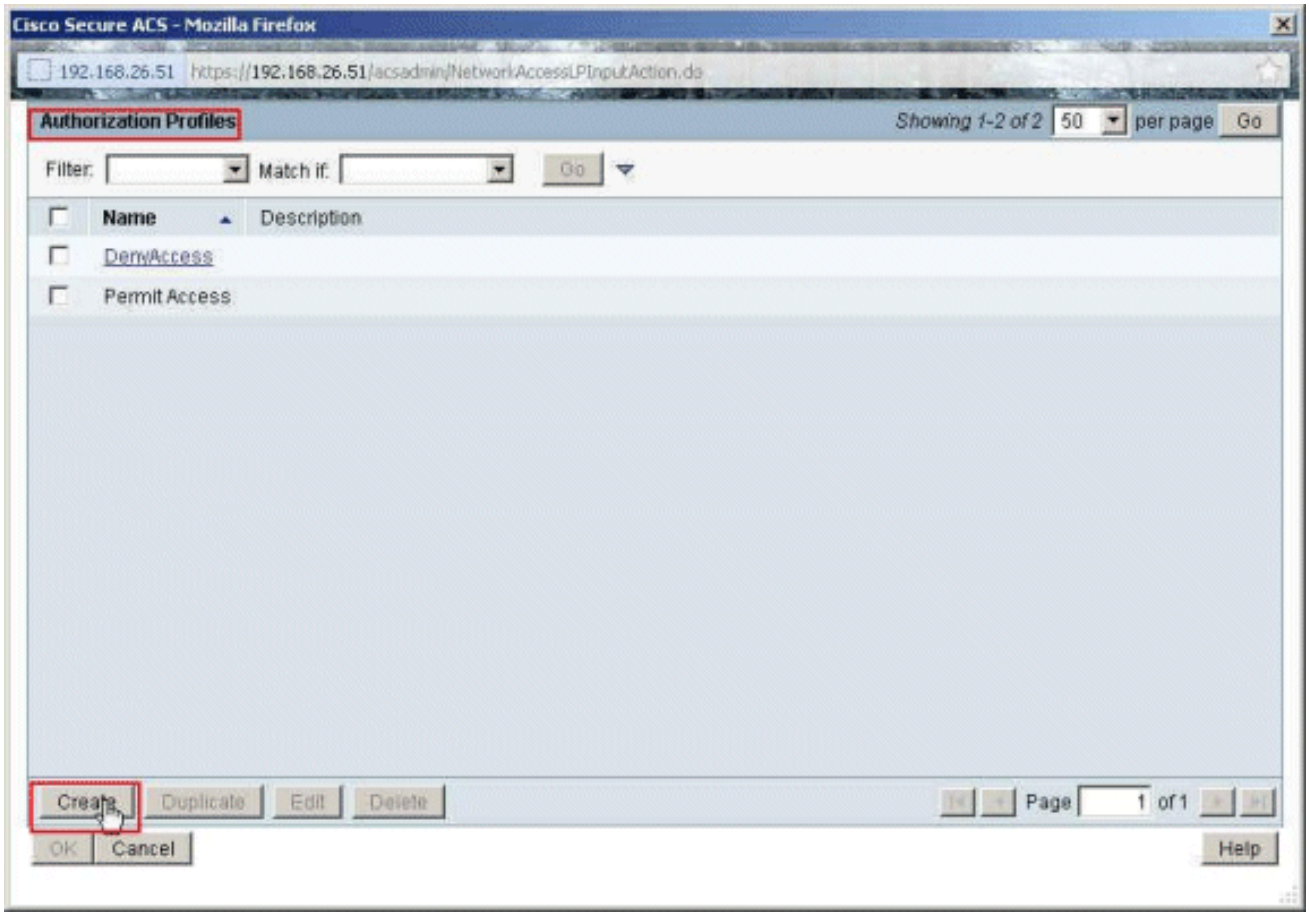
11. Choose the Network Device Group **VPN-Gateways** created earlier, and click **OK**.



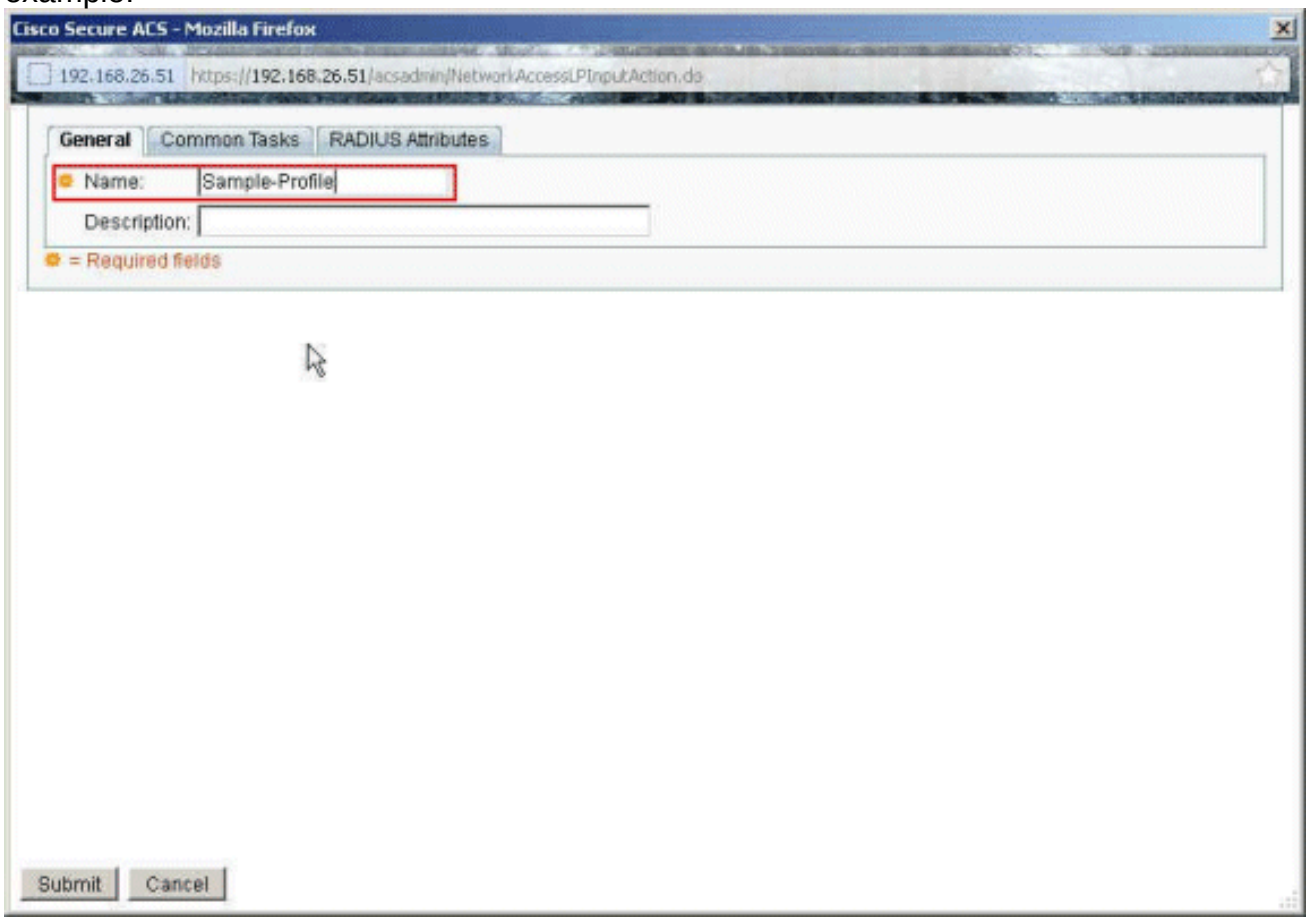
12. Click **Select**.



13. Click **Create** in order to create a new Authorization Profile.

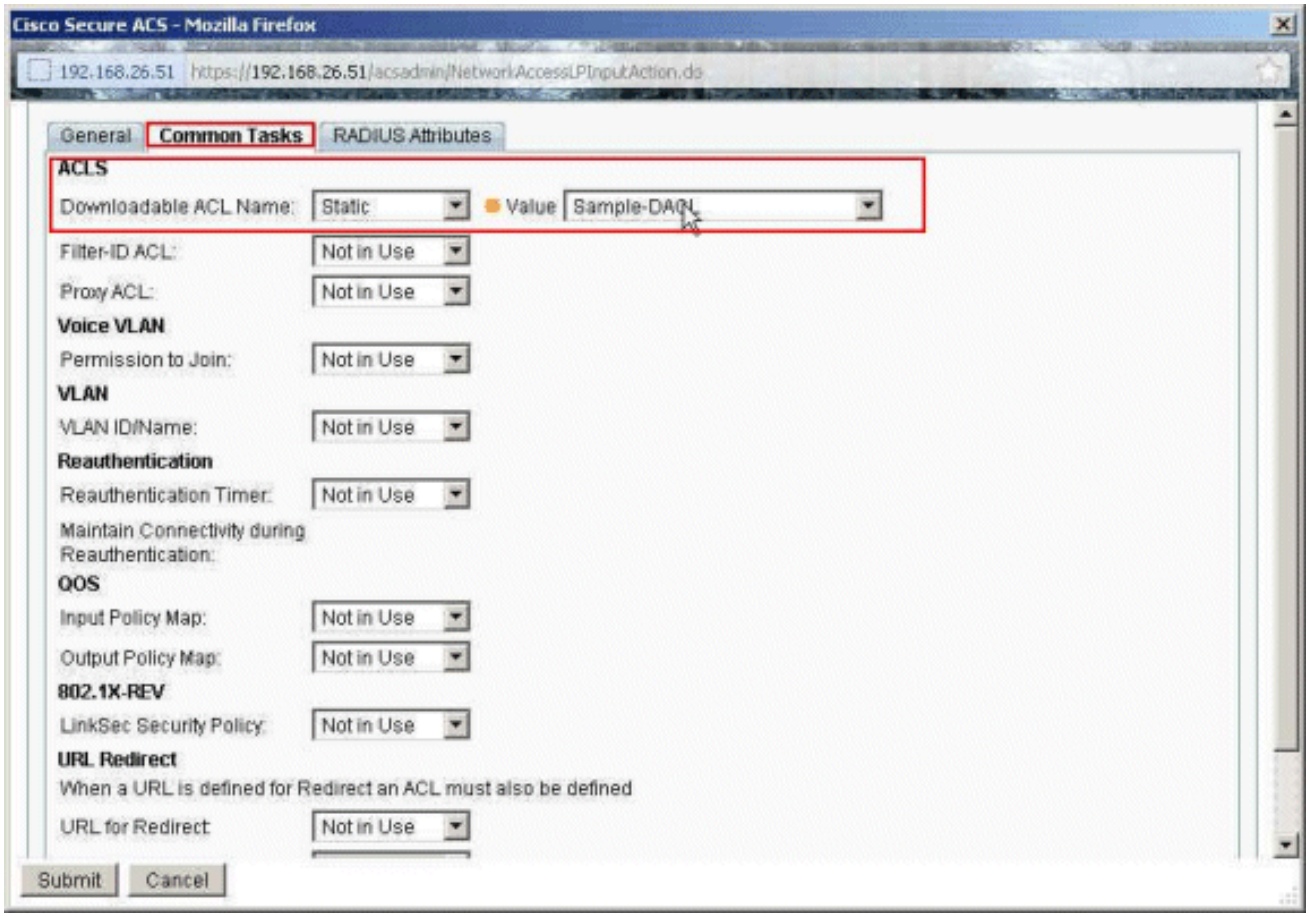


14. Provide a name for the **Authorization Profile**. **Sample-Profile** is the name used in this example.

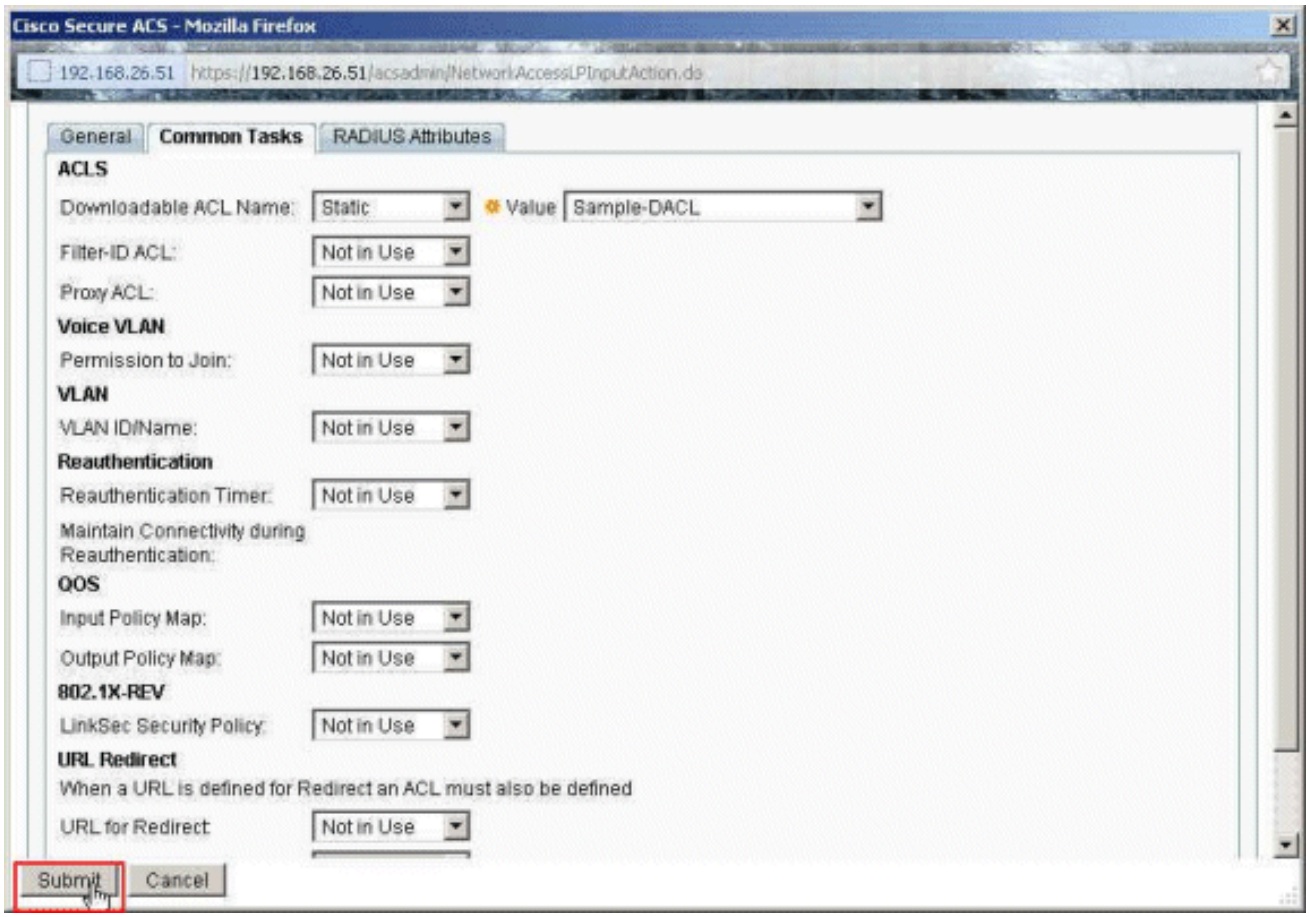


15. Choose the **Common Tasks** tab, and select **Static** from the drop-down list for the Downloadable ACL Name. Choose the newly created **DACL (Sample-DACL)** from the value drop-down

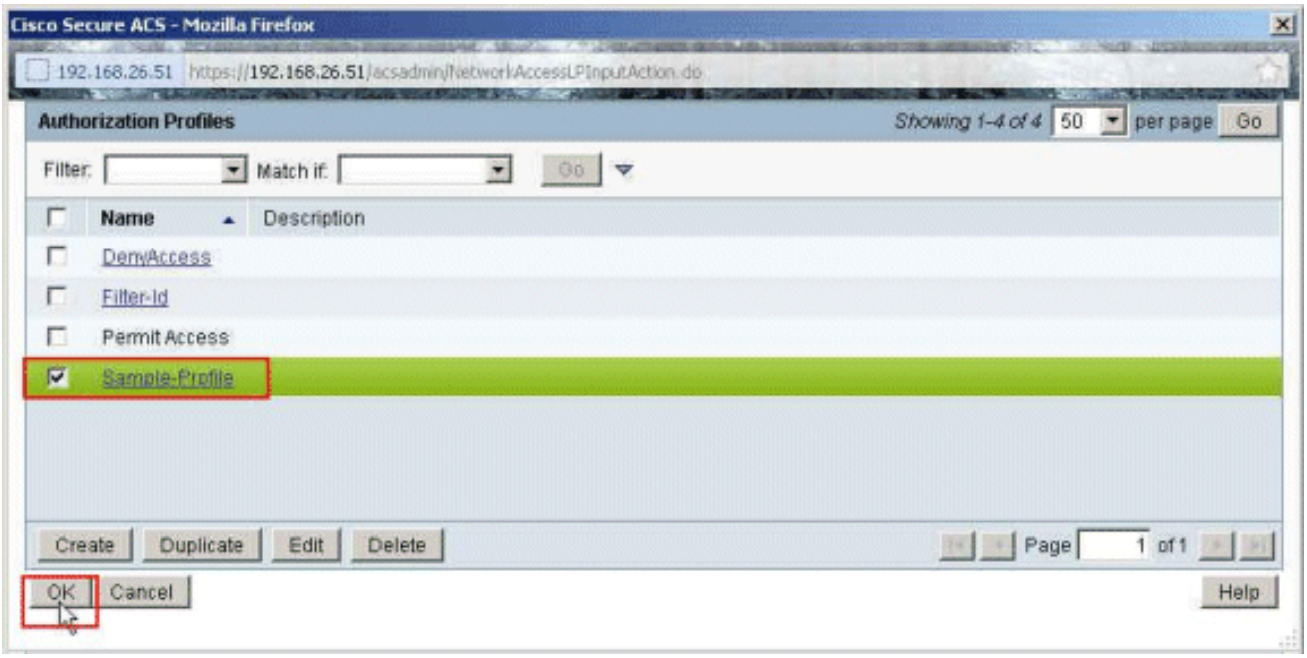
list.



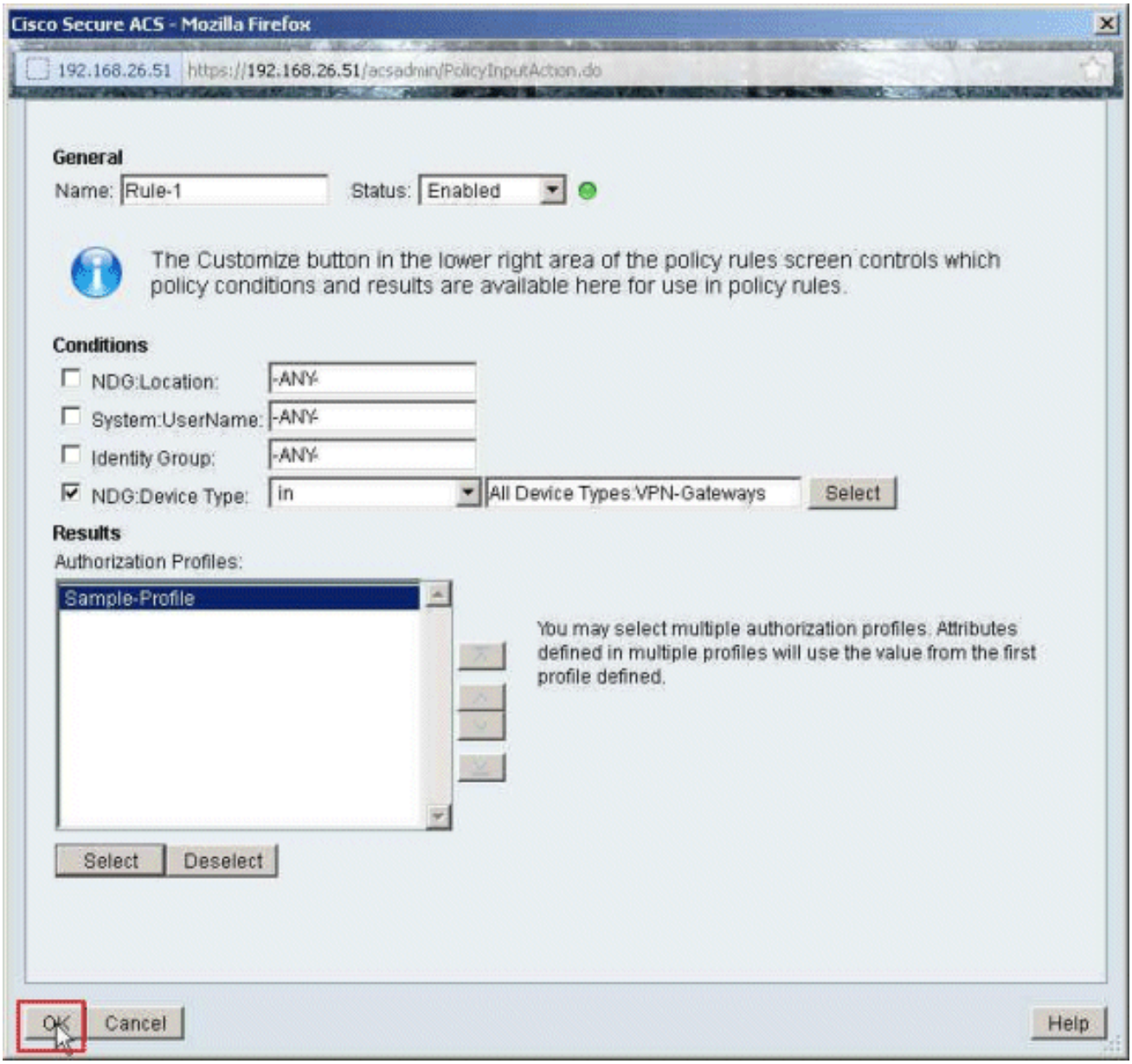
16. Click **Submit**.



17. Select **Sample-Profile** created earlier, and click **OK**.

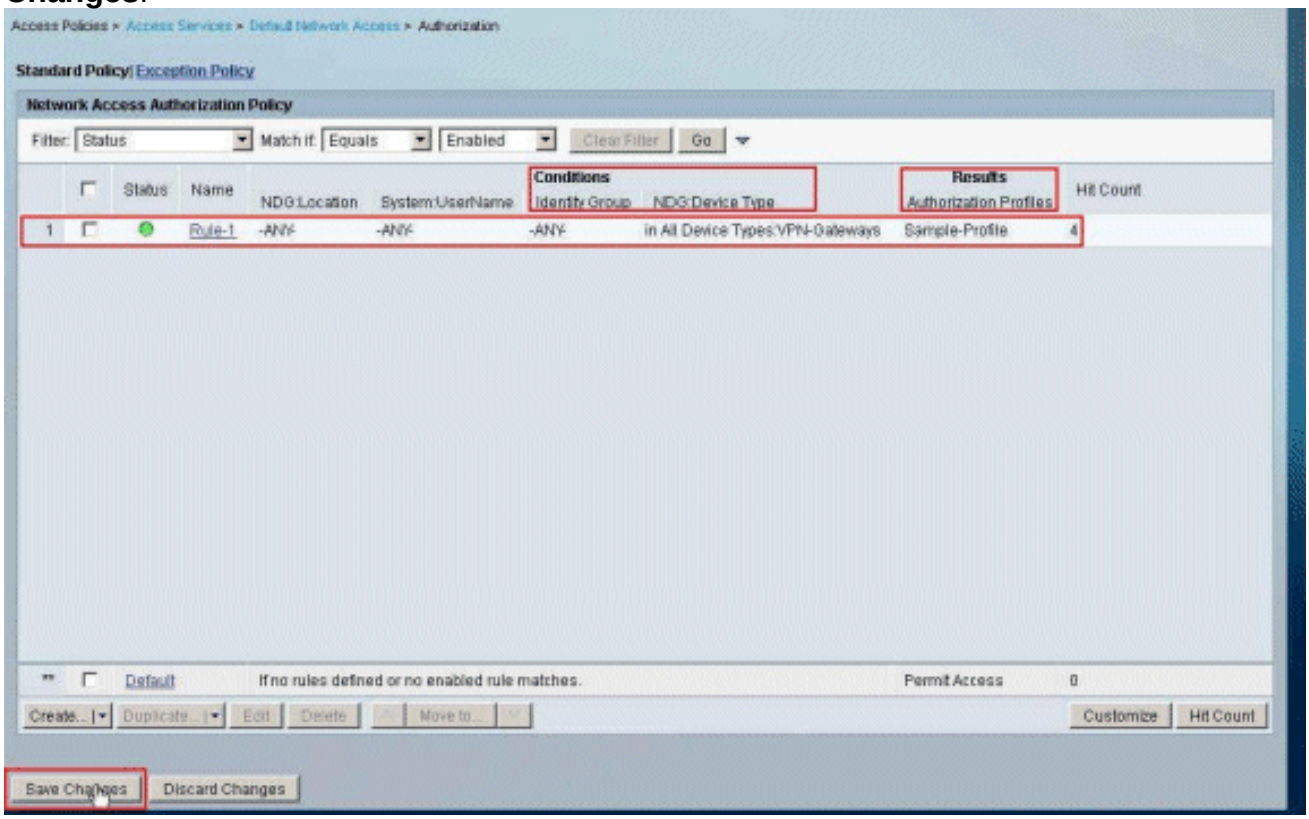


18. Click **OK**.



19. Verify that **Rule-1** is created with **VPN-Gateways** as NDG:Device Type as condition, and **Sample-Profile** as Result. Click **Save**

Changes.



Configure IETF RADIUS Settings for a User Group

In order to download a name for an access list that you have already created on the security appliance from the RADIUS server when a user authenticates, configure the IETF RADIUS filter-id attribute (attribute number 11):

```
filter-id=acl_name
```

The Sample-Group user**cisco** authenticates successfully, and the RADIUS server downloads an ACL name (new) for an access list that you have already created on the security appliance. The user "cisco" can access all devices that are inside the network of the ASA **except** the 10.1.1.2 server. In order to verify the ACL, see the Filter-Id ACL section.

As per the example, the ACL named **new** is configured for filtering in ASA:

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

These parameters appear only when these are true. You have configured:

- AAA client to use one of the RADIUS protocols in Network Configuration
- An authorization profile with RADIUS (IETF) Filter-Id is selected under the result section of the rule in the Access-Service.

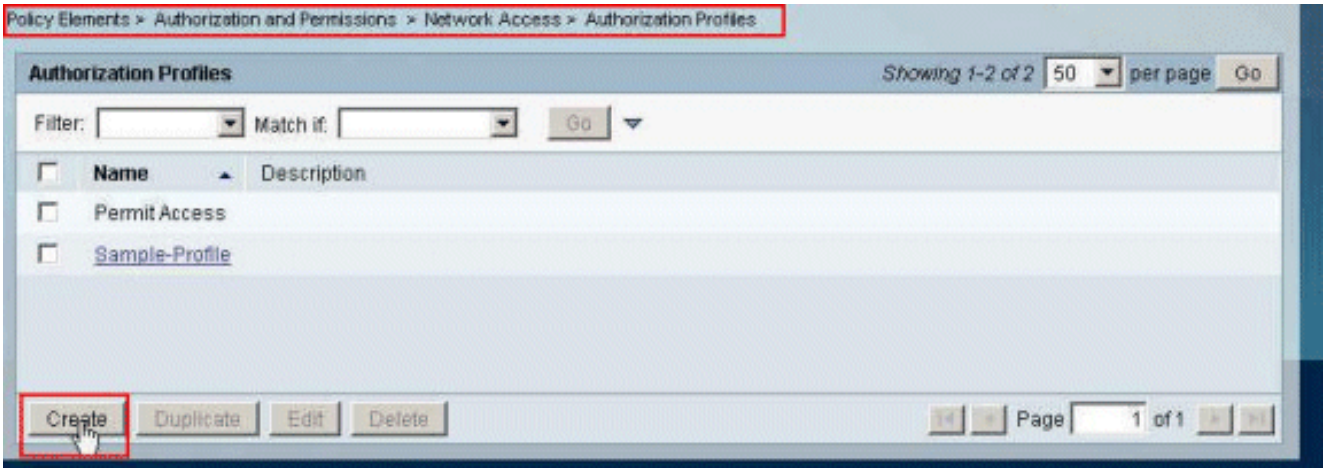
RADIUS attributes are sent as a profile for each user from ACS to the requesting AAA client.

Complete Steps 1 through 6 and 10 through 12 of the Configure ACS for Downloadable ACL for Individual User, followed by Steps 1 through 6 of the Configure ACS for Downloadable ACL for Group, and perform these steps in this section in order to configure Filter-Id in the Cisco Secure

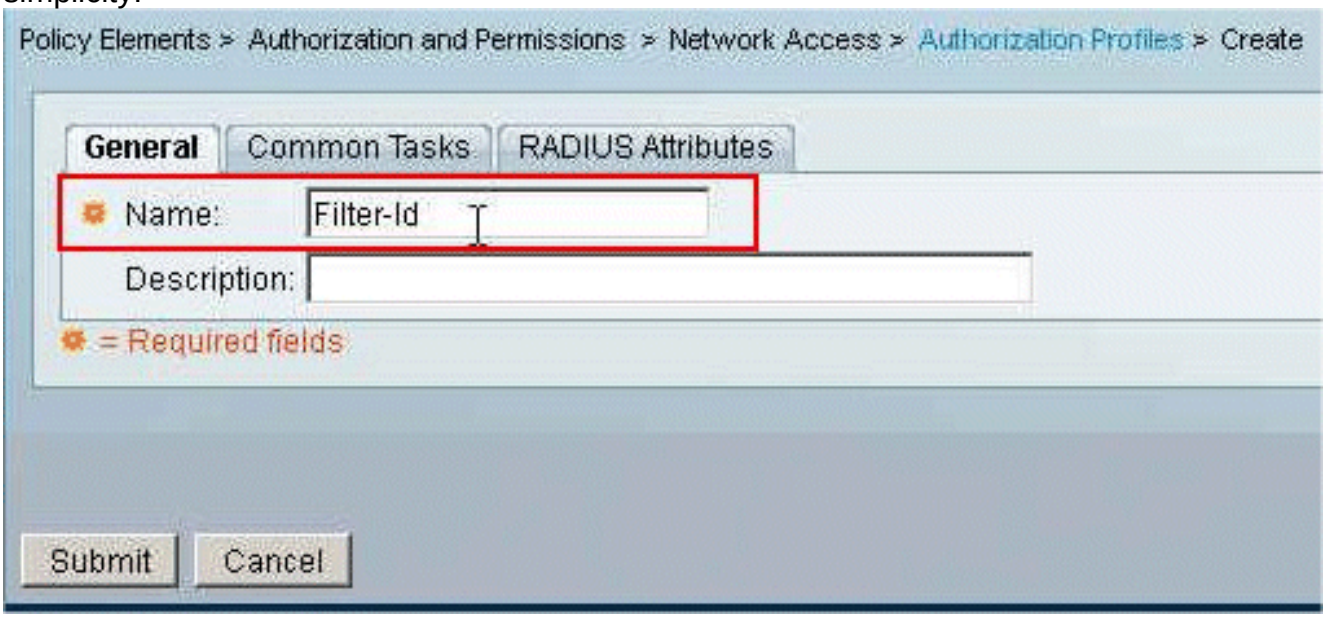
ACS.

In order to configure **IETF RADIUS** attribute settings to apply as in authorization profile, perform these steps:

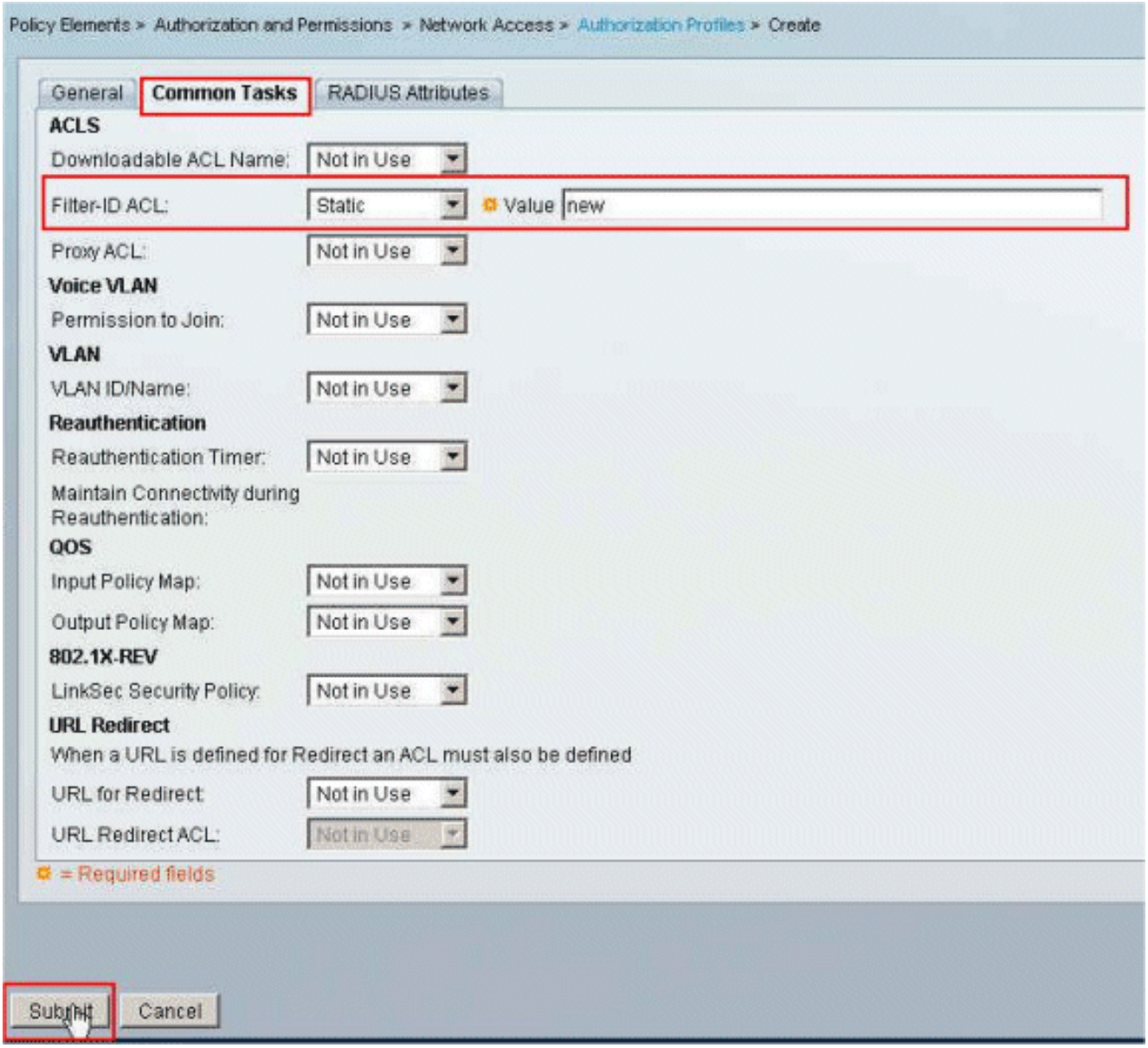
1. Choose **Policy Elements** > **Authorization and Permissions** > **Network Access** > **Authorization Profiles**, and click **Create** in order to create a new Authorization Profile.



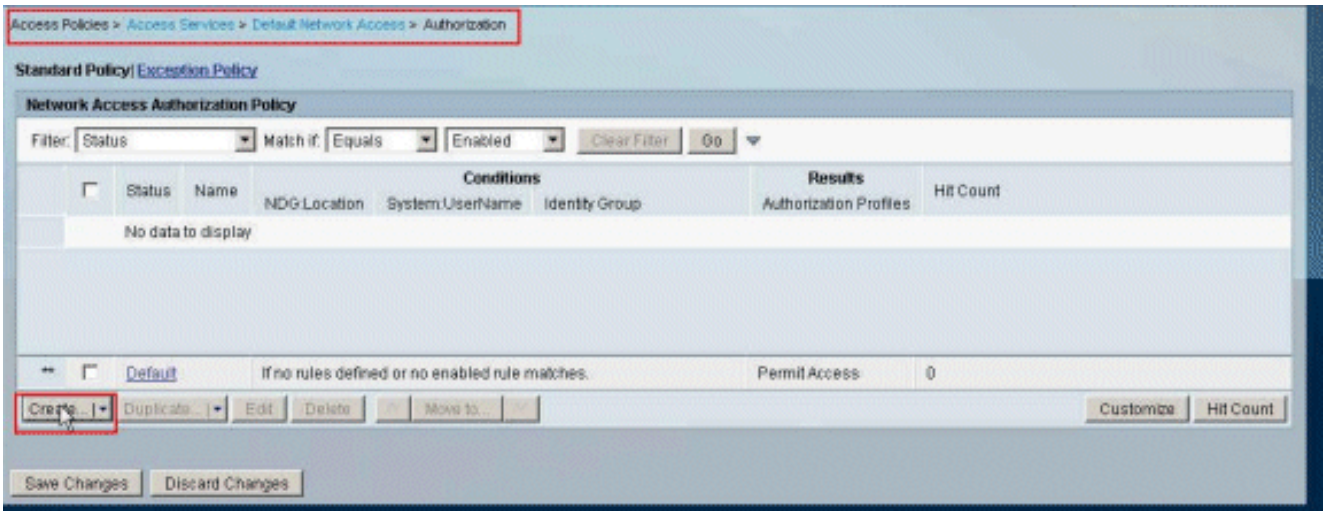
2. Provide a name for the **Authorization Profile**. **Filter-Id** is the Authorization Profile name chosen in this example for simplicity.



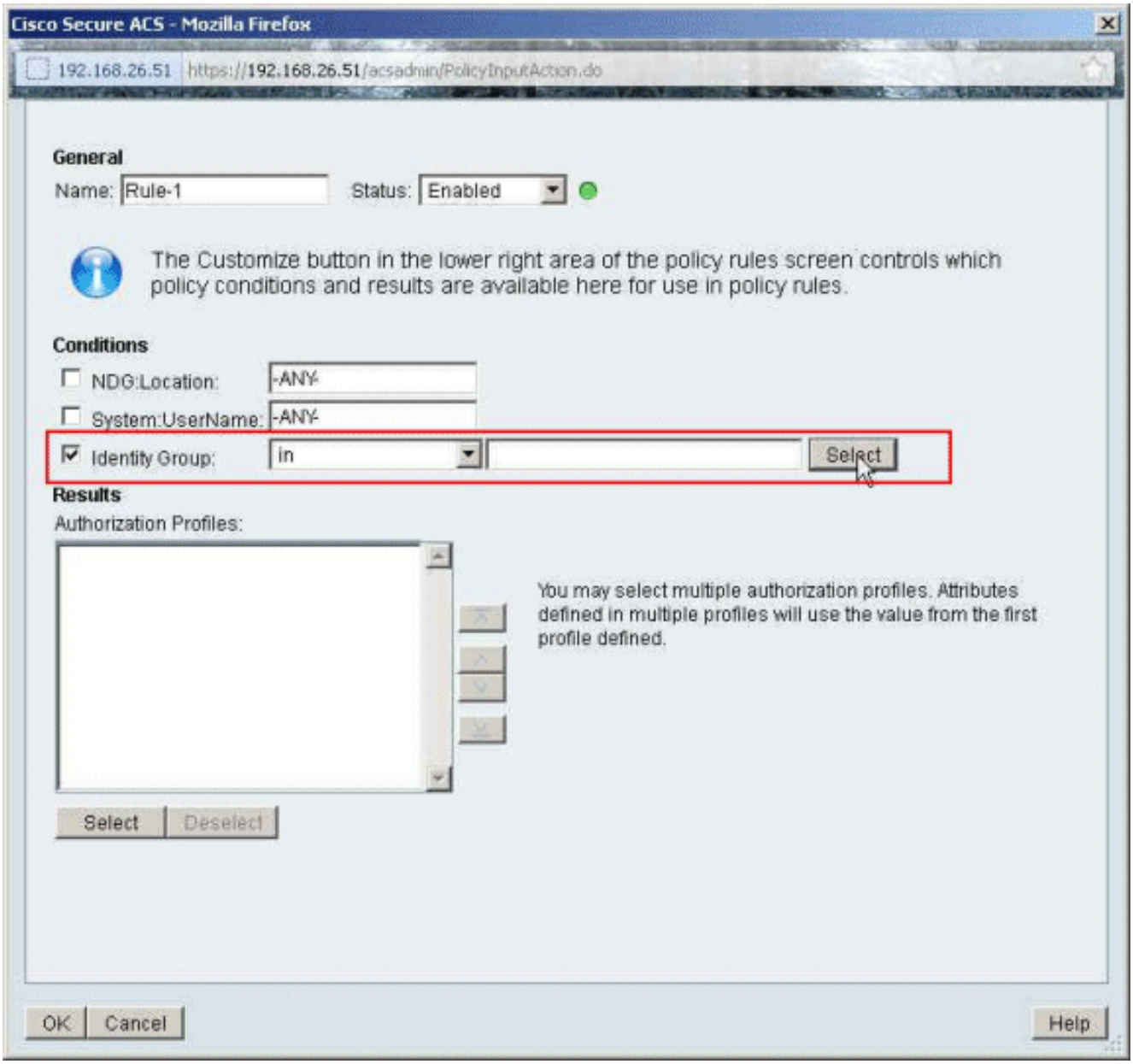
3. Click the **Common Tasks** tab, and choose **Static** from the drop-down list for **Filter-ID ACL**. Enter the access list name as **new** in the Value field, and click **Submit**.



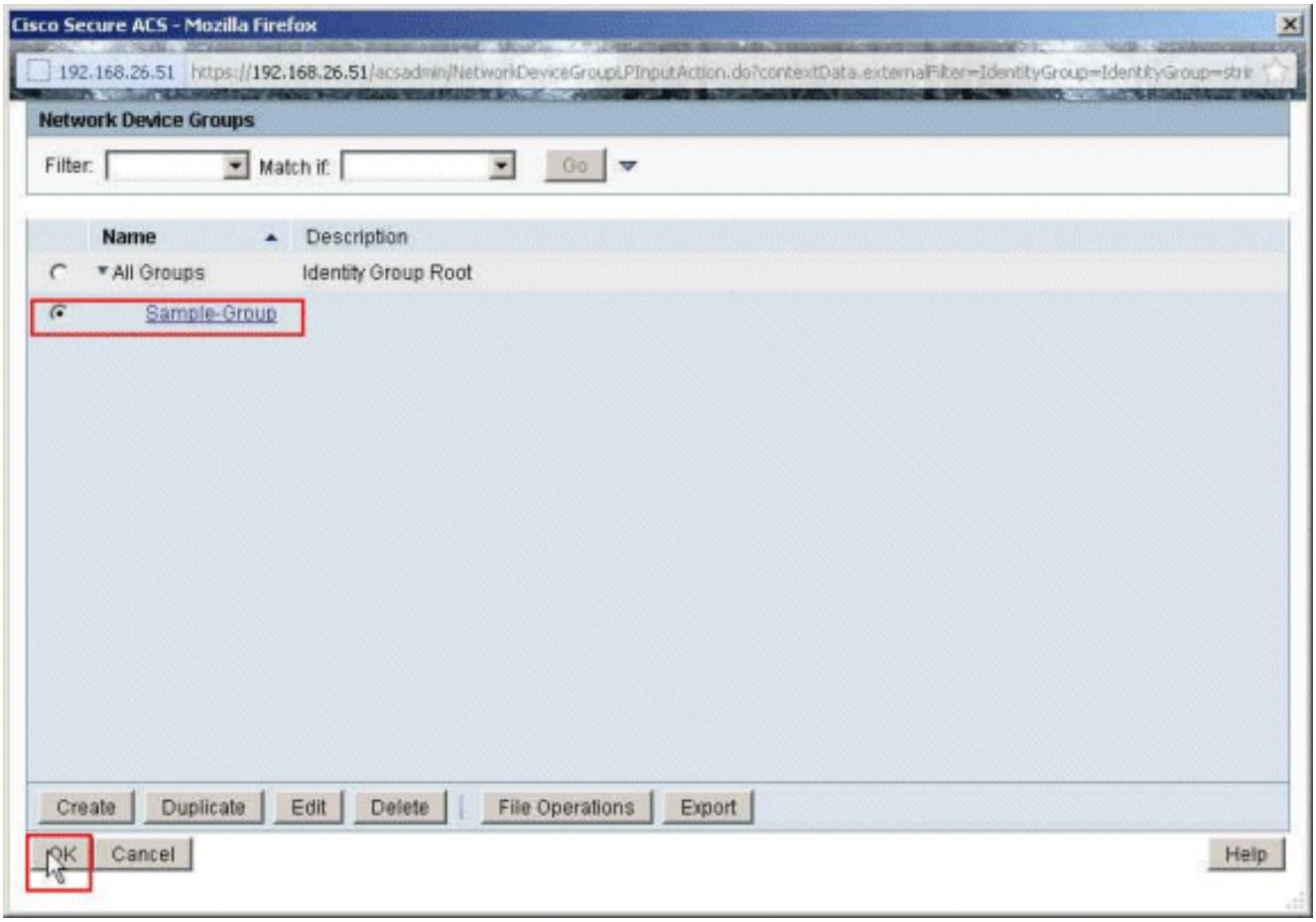
4. Choose **Access Policies** > **Access Services** > **Default Network Access** > **Authorization**, and click **Create** in order to create a new Rule.



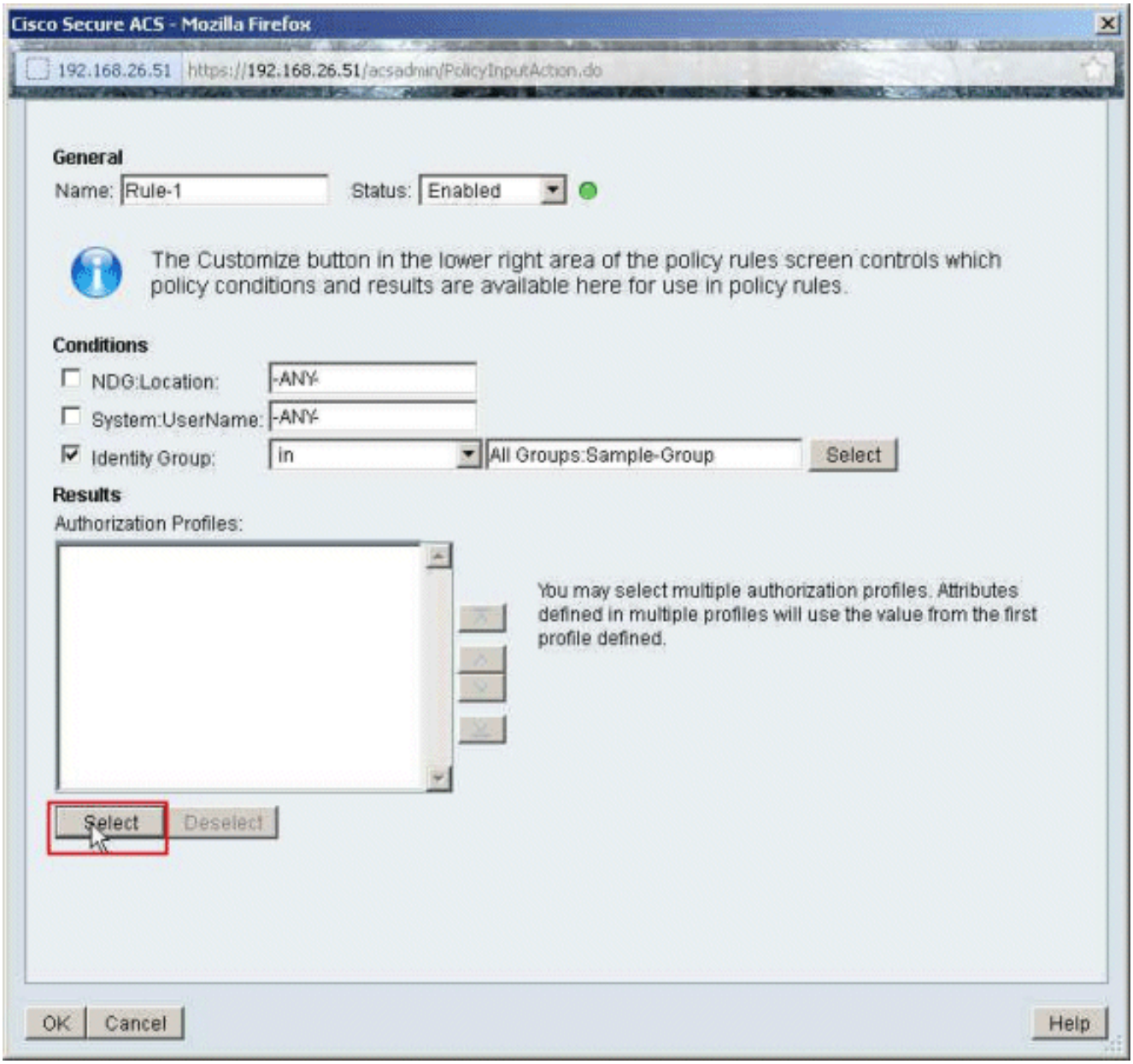
5. Make sure that the checkbox next to **Identity Group** is checked, and click **Select**.



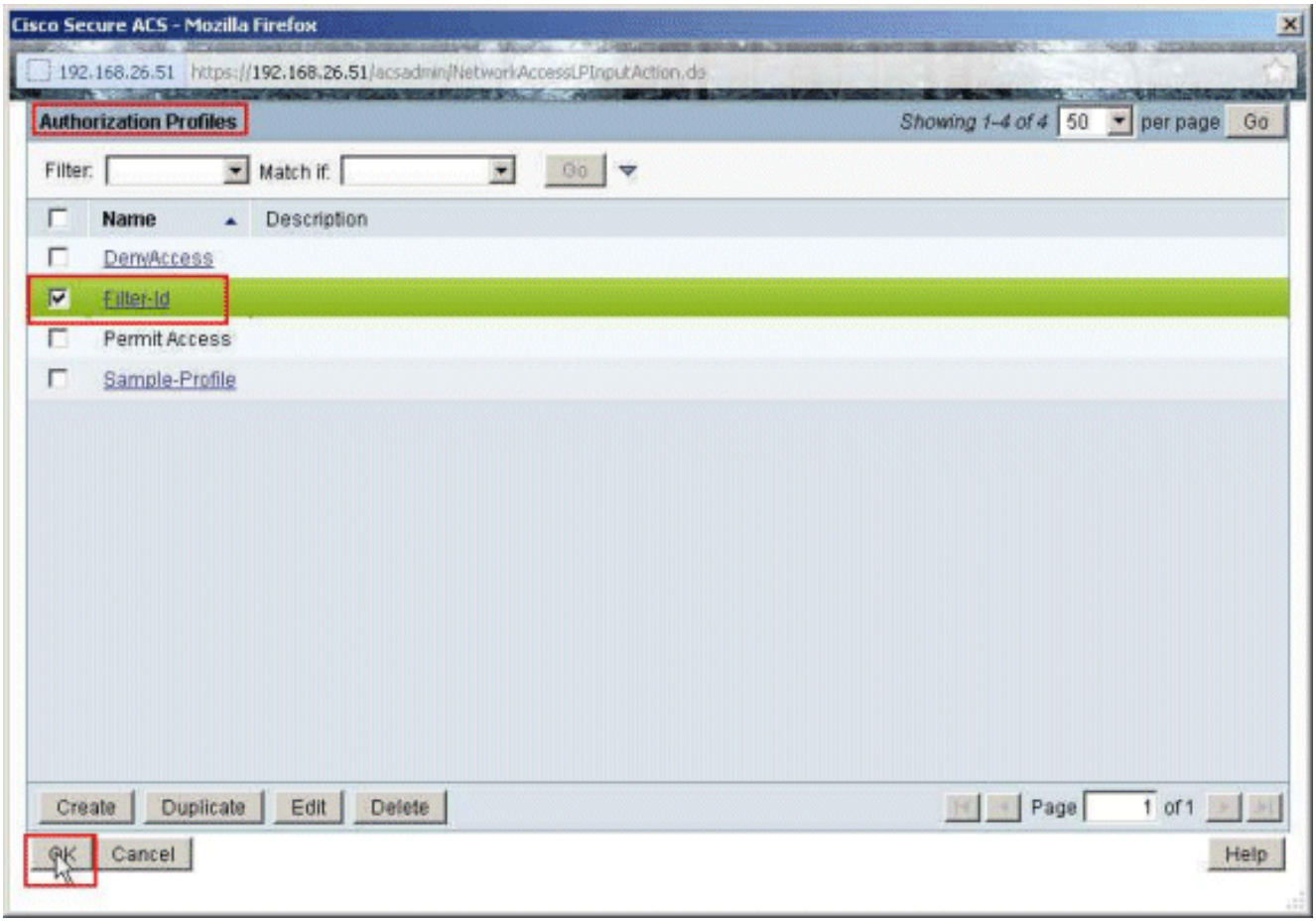
6. Choose **Sample-Group**, and click **OK**.



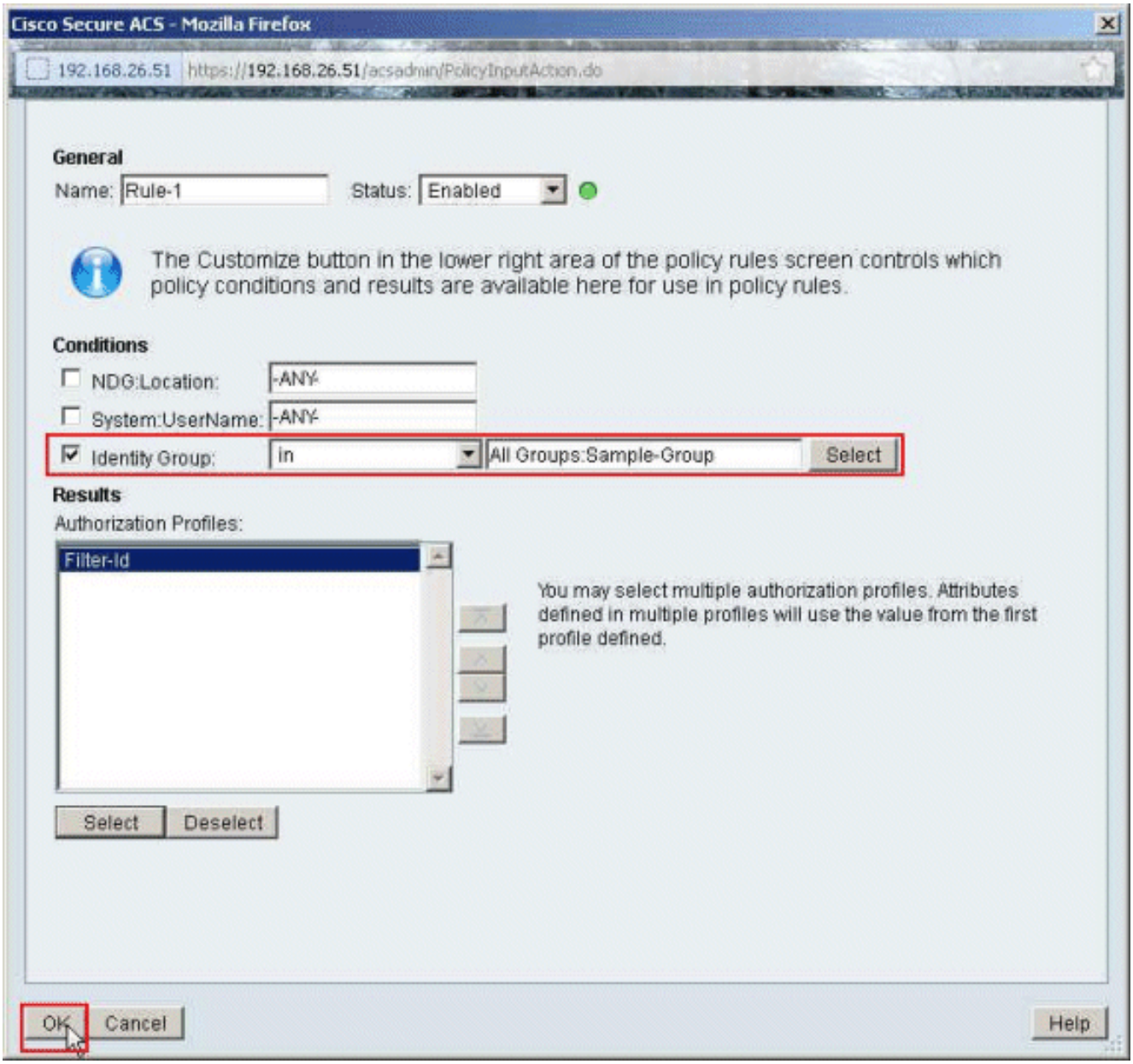
7. Click **Select** in the Authorization Profiles section.



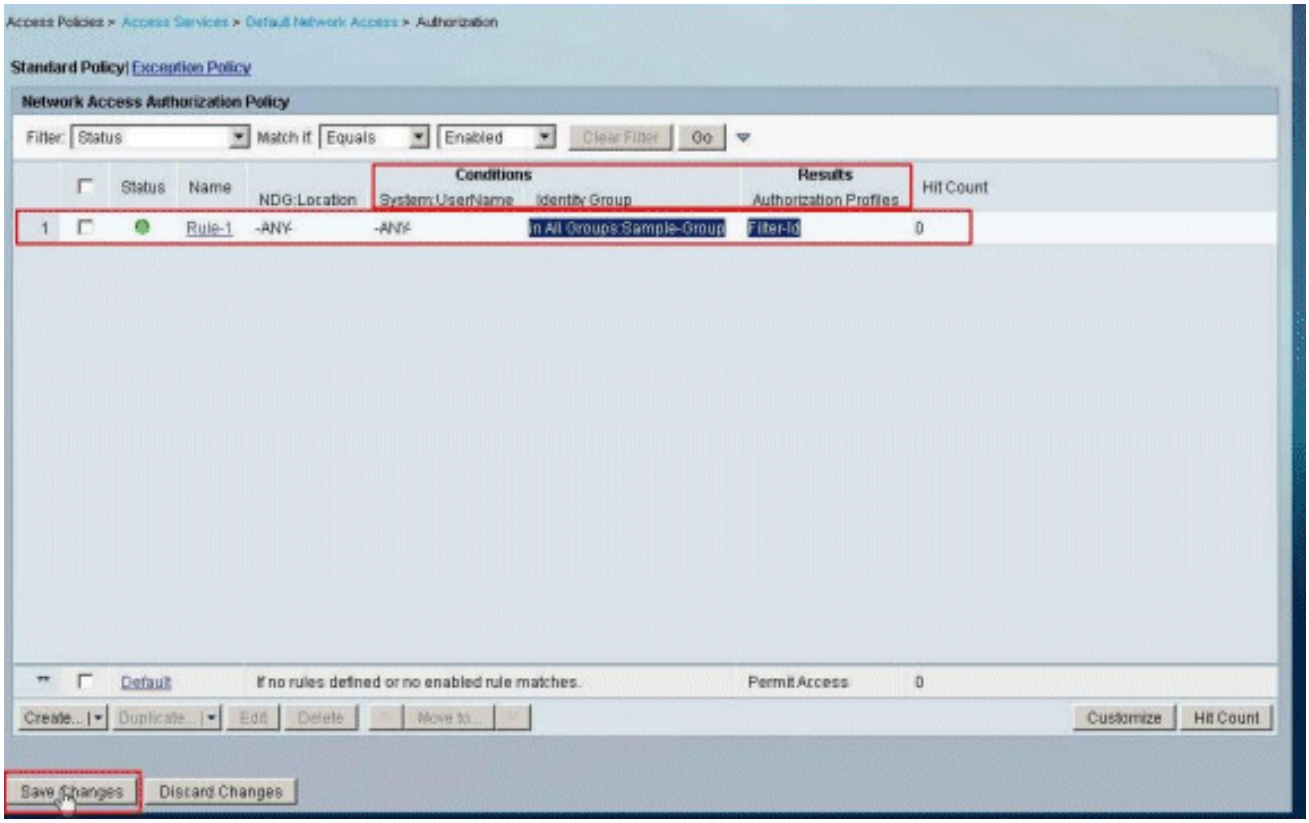
8. Choose the Authorization Profile **Filter-Id** created earlier, and click **OK**.


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. Verify that **Rule-1** is created with Identity Group **Sample-Group** as condition and **Filter-Id** as Result. Click **Save Changes**.

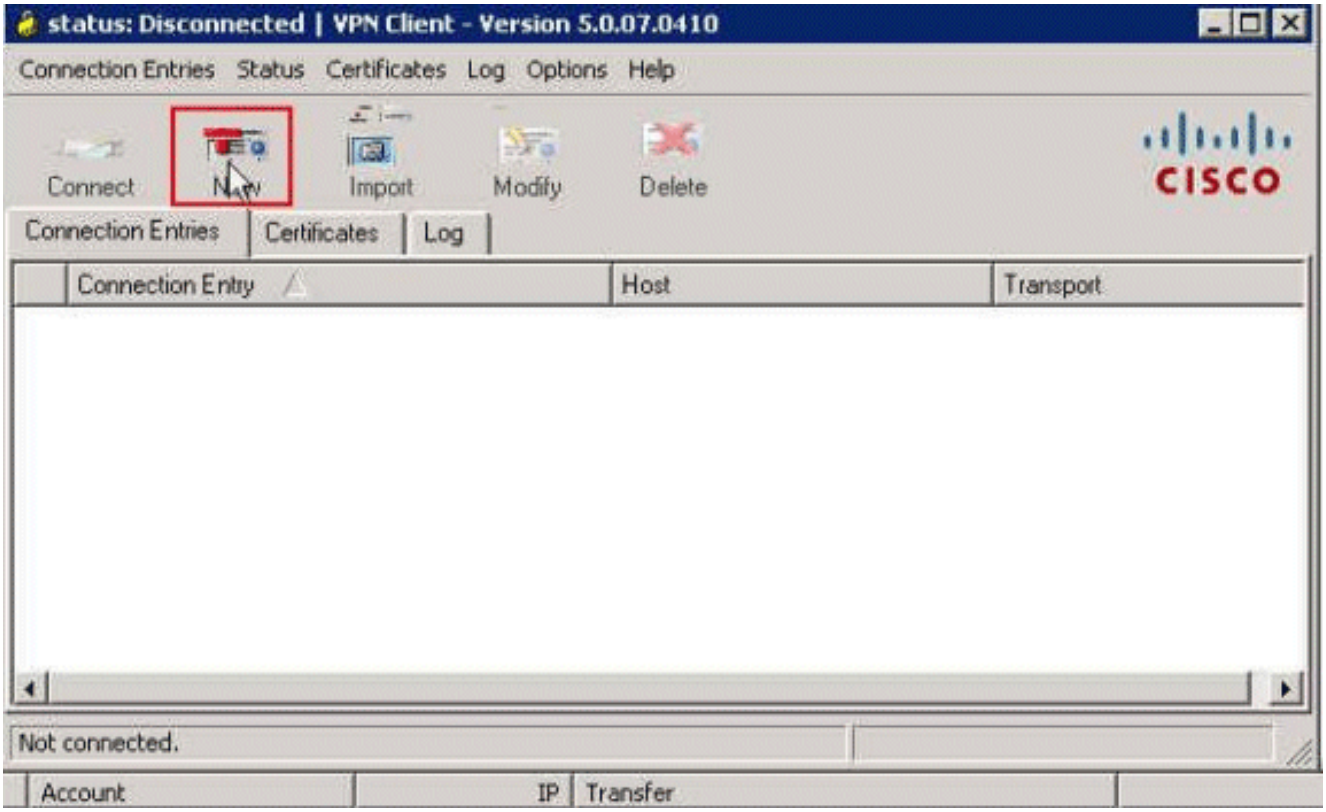


Cisco VPN Client Configuration

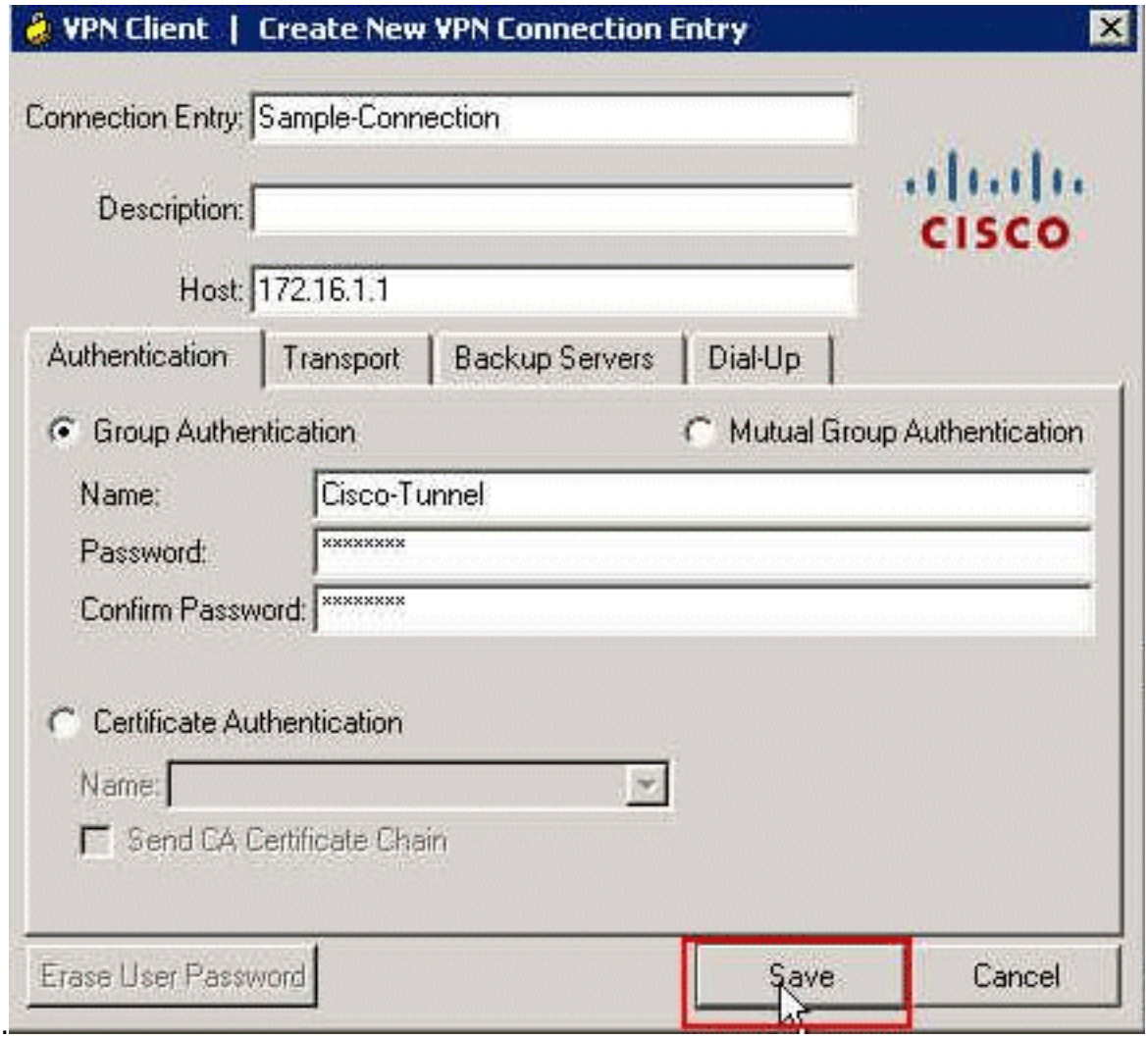
Connect to the Cisco ASA with the Cisco VPN Client in order to verify that the ASA is successfully configured.

Complete these steps:

1. Choose **Start** > **Programs** > **Cisco Systems VPN Client** > **VPN Client**.
2. Click **New** in order to launch the Create New VPN Connection Entry window.

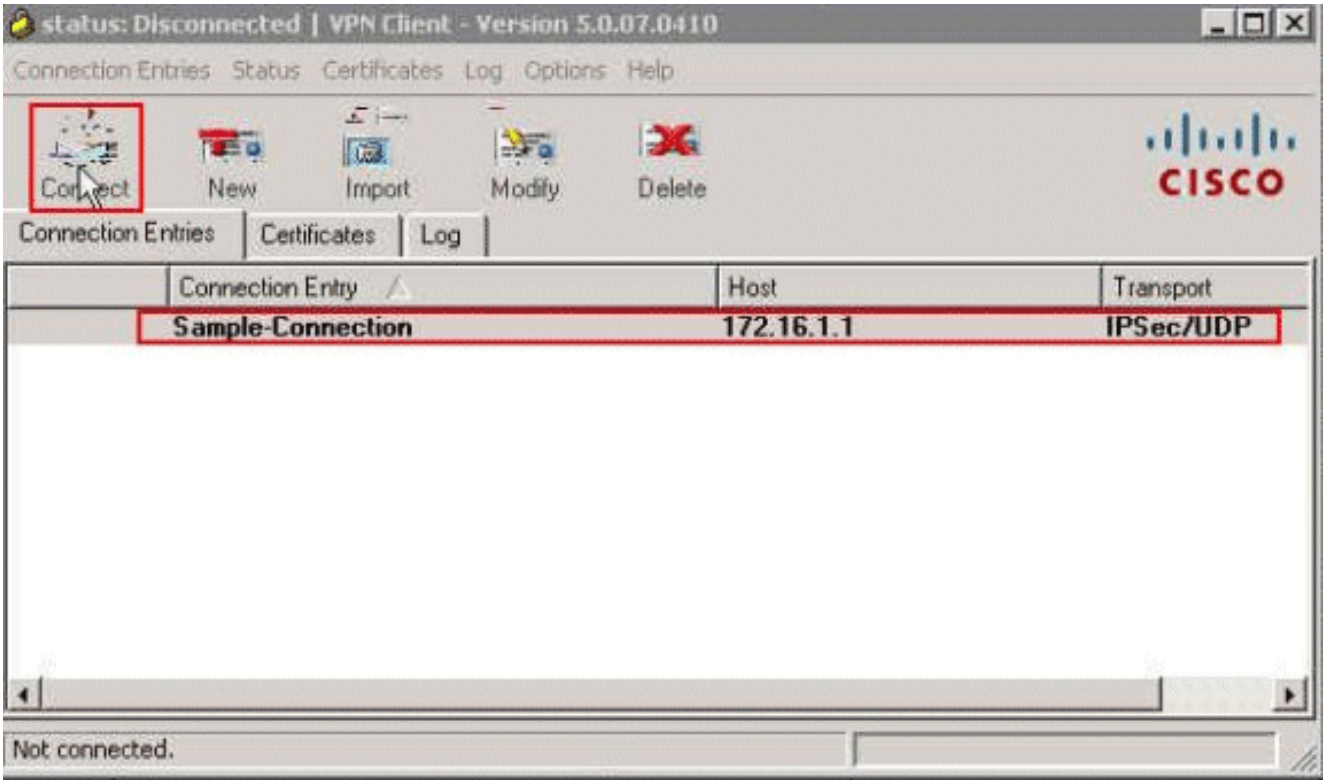


3. Fill in the details of your new connection:Enter the name of the Connection Entry along with a description.Enter the **outside IP address of the ASA** in the Host box.Enter the VPN Tunnel Group Name (**Cisco-Tunnel**) and password (Pre-shared Key - **cisco123**) as configured in the ASA.Click



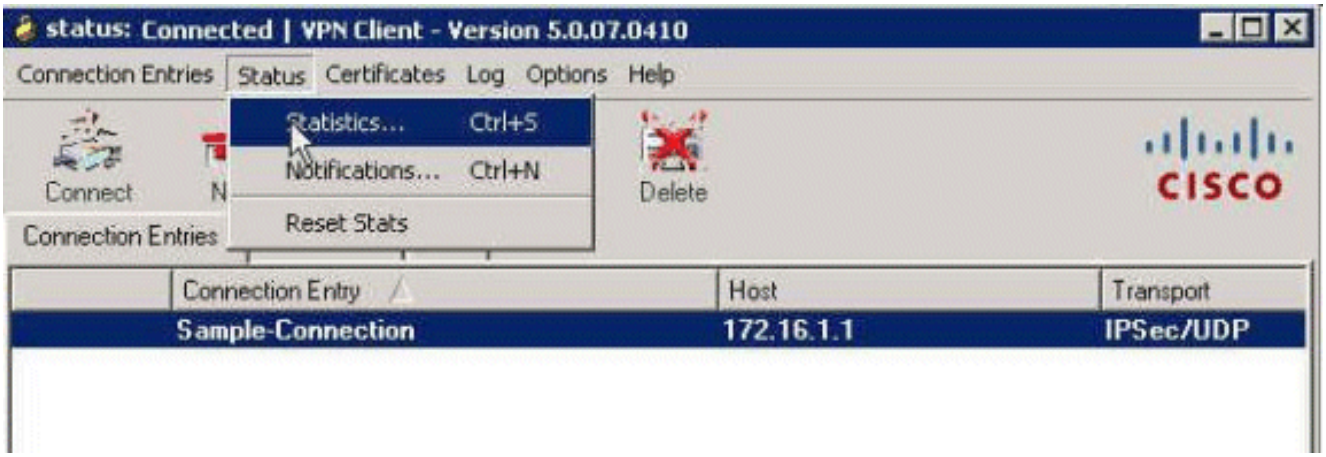
Save.

4. Click the connection that you want to use, and click **Connect** from the VPN Client main window.



5. When prompted, enter the Username **cisco** and Password **cisco123** as configured in the ASA for authentication, and click **OK** in order to connect to the remote network.

6. Once the connection is successfully established, choose **Statistics** from the Status menu in order to verify the details of the tunnel.



Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Show Crypto Commands

- **show crypto isakmp sa** - Shows all current IKE Security Associations (SAs) at a peer.`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** - Shows the settings used by current SAs.`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`

Downloadable ACL for User/Group

Verify the Downloadable ACL for the user Cisco. ACLs are downloaded from the CSACS.

```
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

The [011] Filter-Id has applied for the Group - Sample-Group, and users of the group are filtered as per the ACL (new) defined in the ASA.

```
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
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration. Sample **debug** output is also shown.

Note: For more information on troubleshooting Remote Access IPsec VPN, refer to Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions.

Clear Security Associations

When you troubleshoot, make sure to clear existent SAs after you make a change. In the privileged mode of the PIX, use these commands:

- **clear [crypto] ipsec sa** - Deletes the active IPsec SAs. The keyword crypto is optional.
- **clear [crypto] isakmp sa** - Deletes the active IKE SAs. The keyword crypto is optional.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec 7** - Displays the IPsec negotiations of Phase 2.
- **debug crypto isakmp 7** - Displays the ISAKMP negotiations of Phase 1.

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances Support Page**
- **Cisco ASA 5500 Series Adaptive Security Appliances Command References**
- **Cisco Adaptive Security Device Manager**
- **IPsec Negotiation/IKE Protocols Support Page**
- **Cisco VPN Client Support Page**
- **Cisco Secure Access Control System**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation - Cisco Systems**