ASA 8.3及更高版本：使用CLI和ASDM的可下載ACL進行VPN訪問的RADIUS授權(ACS 5.x)配置示例

目錄

簡介

本文檔介紹如何配置安全裝置以對使用者進行網路訪問身份驗證。由於您可以隱式啟用RADIUS授權，因此本文檔不包含有關在安全裝置上配置RADIUS授權的資訊。它提供關於安全裝置如何處理從RADIUS伺服器接收的訪問清單資訊的資訊。

您可以配置RADIUS伺服器將訪問清單下載到安全裝置或在身份驗證時下載訪問清單名稱。使用者僅有權執行使用者特定訪問清單中允許的行為。

使用思科安全存取控制伺服器(ACS)為每個使用者提供適當的存取清單時，可下載存取清單是最具擴充性的方式。如需可下載存取清單功能和Cisco Secure ACS的詳細資訊，請參閱設定RADIUS伺

服器以傳送可下載存取控制清單和可下載IP ACL。

請參閱ASA/PIX 8.x:使用可下載ACL和CLI進行網路訪問的RADIUS授權(ACS)和ASDM配置示例在8.2及更低版本的Cisco ASA上進行相同配置。

必要條件

需求

本文檔假設自適應安全裝置(ASA)完全可運行且配置為允許思科自適應安全裝置管理器(ASDM)或CLI進行配置更改。

注意：請參閱允許ASDM的HTTPS訪問，以允許通過ASDM或安全外殼(SSH)遠端配置裝置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA軟體8.3版及更高版本
- Cisco ASDM版本6.3及更高版本
- Cisco VPN客戶端5.x版及更高版本
- Cisco安全ACS 5.x

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

您可以使用可下載的IP ACL來建立可應用於許多使用者或使用者組的ACL定義集。這些ACL定義集稱為ACL內容。

可下載IP ACL的運作方式如下：

1. 當ACS向使用者授予網路訪問許可權時，ACS會確定可下載IP ACL是否分配給結果部分中的授權配置檔案。
2. 如果ACS找到分配給授權配置檔案的可下載IP ACL，則ACS會傳送指定命名ACL和命名ACL版本的屬性（作為使用者會話的一部分，在RADIUS訪問接受資料包中）。
3. 如果AAA客戶端響應其快取中沒有當前版本的ACL（即ACL是新的或已更改的），ACS會將ACL（新的或已更新）傳送到裝置。

可下載IP ACL是每個使用者或使用者組的RADIUS Cisco-av配對屬性[26/9/1]中設定ACL的替代方案。您可以建立一次可下載IP ACL，為其指定一個名稱，然後在引用其名稱時將可下載IP ACL分配給任何授權配置檔案。與為授權配置檔案配置RADIUS Cisco-av-pair屬性相比，此方法更有效。

在ACS Web介面中輸入ACL定義時，不要使用關鍵字或名稱條目；在所有其他方面，對於要應用可下載IP ACL的AAA客戶端，請使用標準ACL命令語法和語義。您在ACS中輸入的ACL定義包含一條

或多條ACL命令。每個ACL命令必須位於單獨的行上。

在ACS中，您可以定義多個可下載IP ACL，並在不同的授權配置檔案中使用它們。根據訪問服務授權規則中的條件，您可以將包含可下載IP ACL的不同授權配置檔案傳送到不同的AAA客戶端。

此外，您還可以變更ACL內容在可下載IP ACL中的順序。ACS從表頂部開始檢查ACL內容，並下載找到的第一個ACL內容。設定順序時，如果您將最廣泛適用的ACL內容放在清單的較高位置，就可以確保系統效率。

要在特定AAA客戶端上使用可下載IP ACL，AAA客戶端必須遵守以下規則：

- 使用RADIUS進行驗證
- 支援可下載的IP ACL

以下是支援可下載IP ACL的Cisco裝置範例：

- ASA
- 執行IOS版本12.3(8)T和更新版本的思科裝置

以下是在ACL定義框中輸入ASA ACL時必須使用的格式示例：

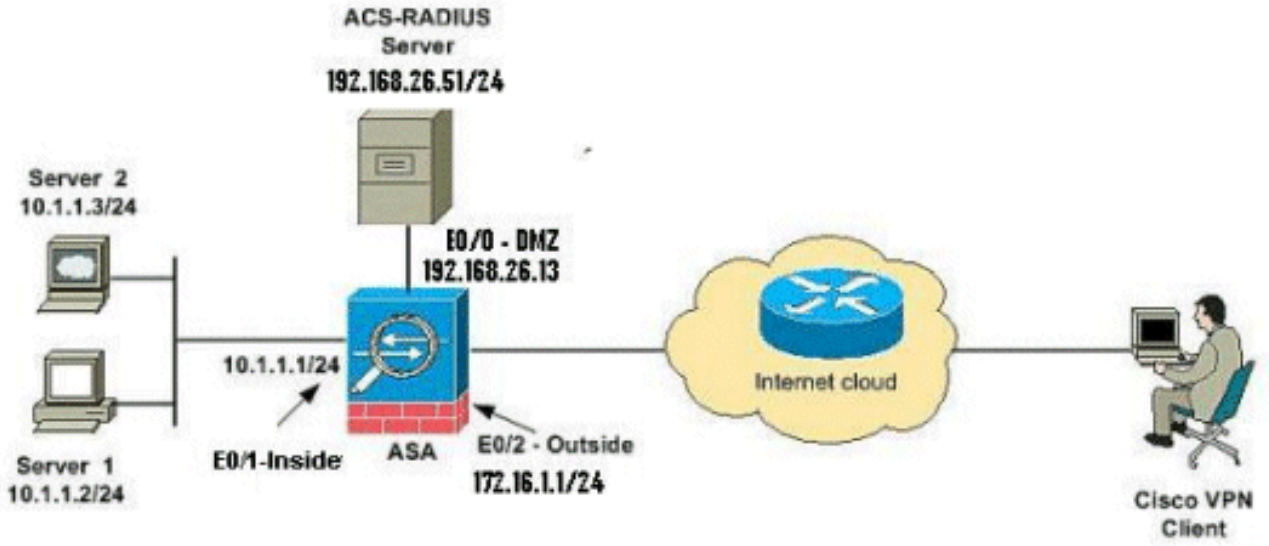
```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3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

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用以下網路設定：



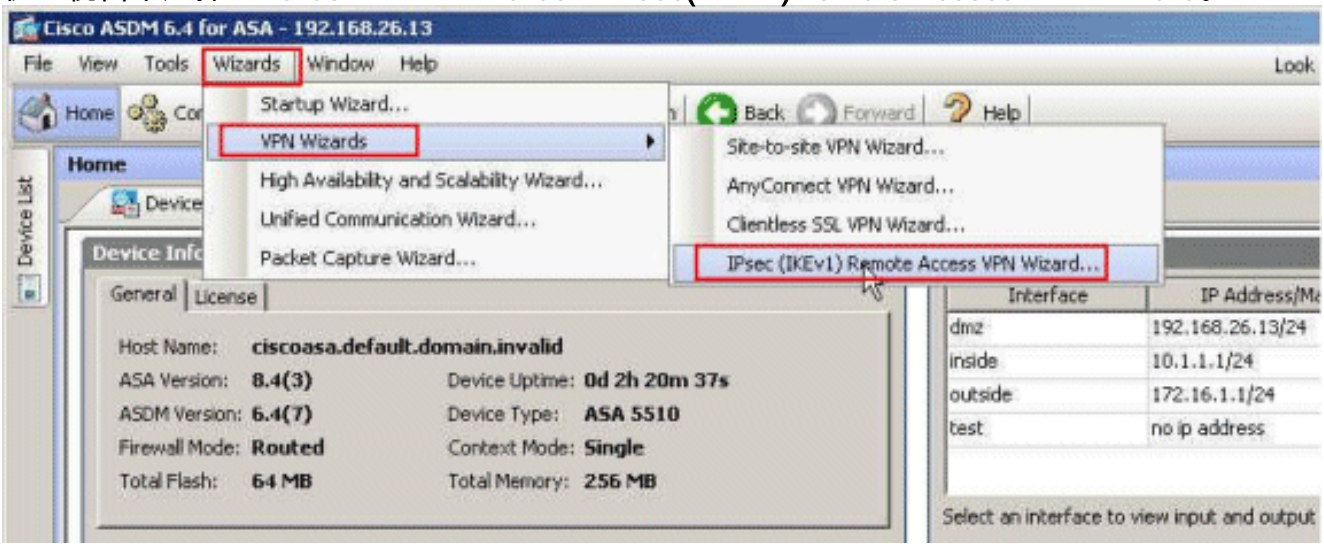
注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

設定遠端存取VPN(IPsec)

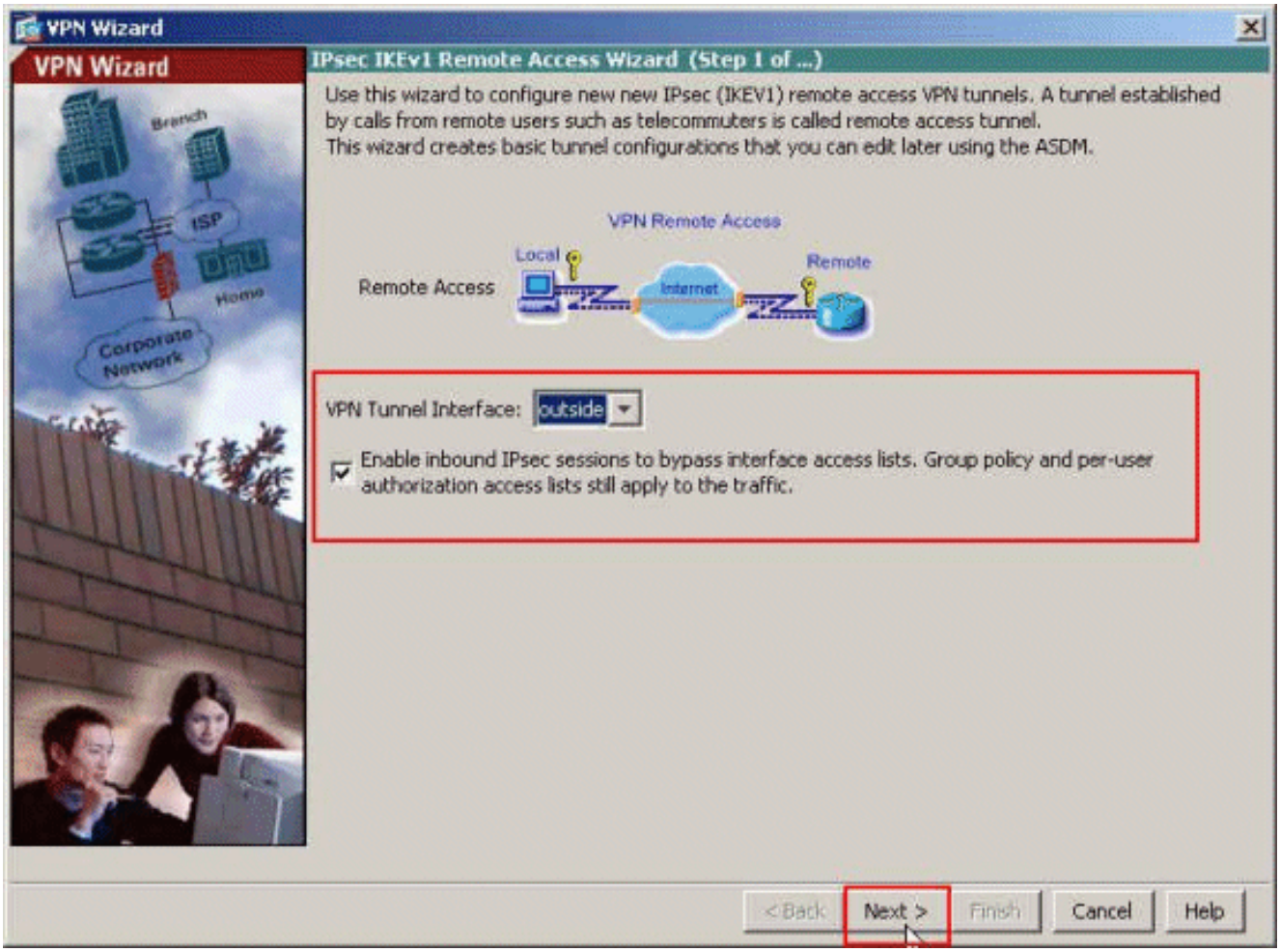
ASDM過程

完成以下步驟以配置遠端訪問VPN:

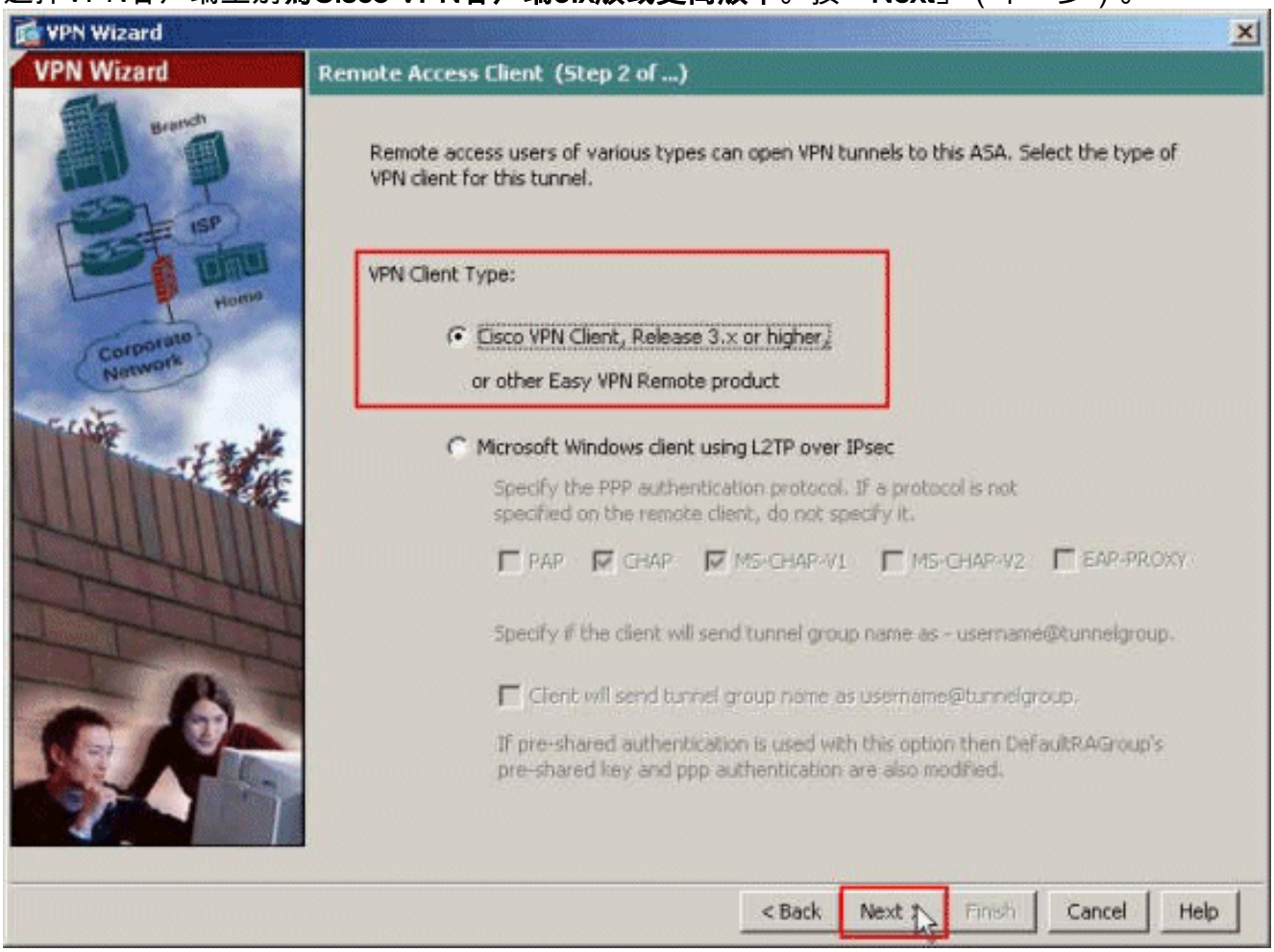
1. 從主視窗中選擇**Wizards > VPN Wizards > IPsec(IKEv1)Remote Access VPN Wizard**。



2. 根據需要選擇**VPN Tunnel Interface**(本例中為**Outside**)，並且還要確保**Enable inbound IPsec sessions to bypass interface access lists**旁邊的覈取方塊已選中。

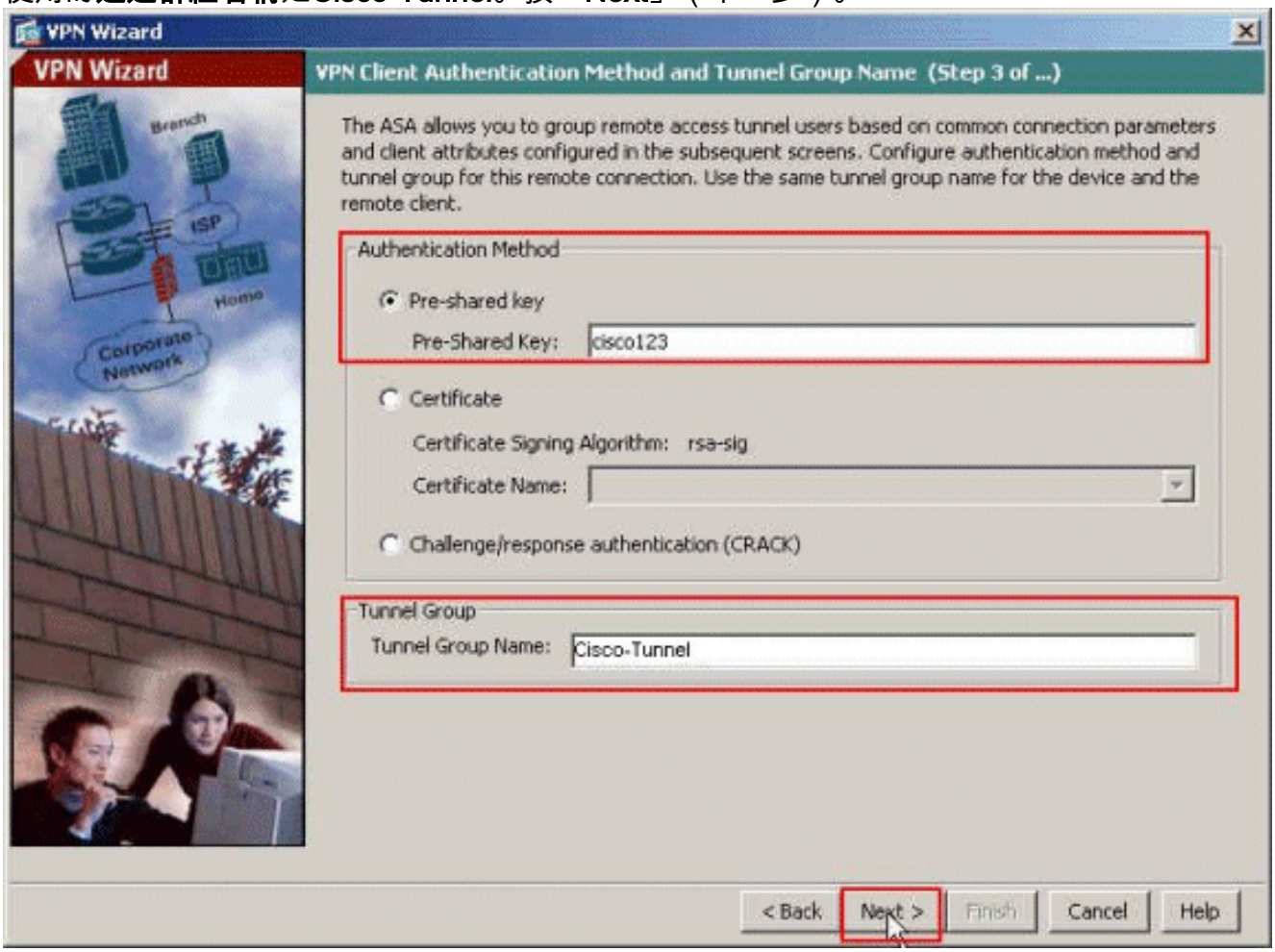


3. 選擇VPN客戶端型別**為Cisco VPN客戶端3.x版或更高版本**。按「**Next**」（下一步）。

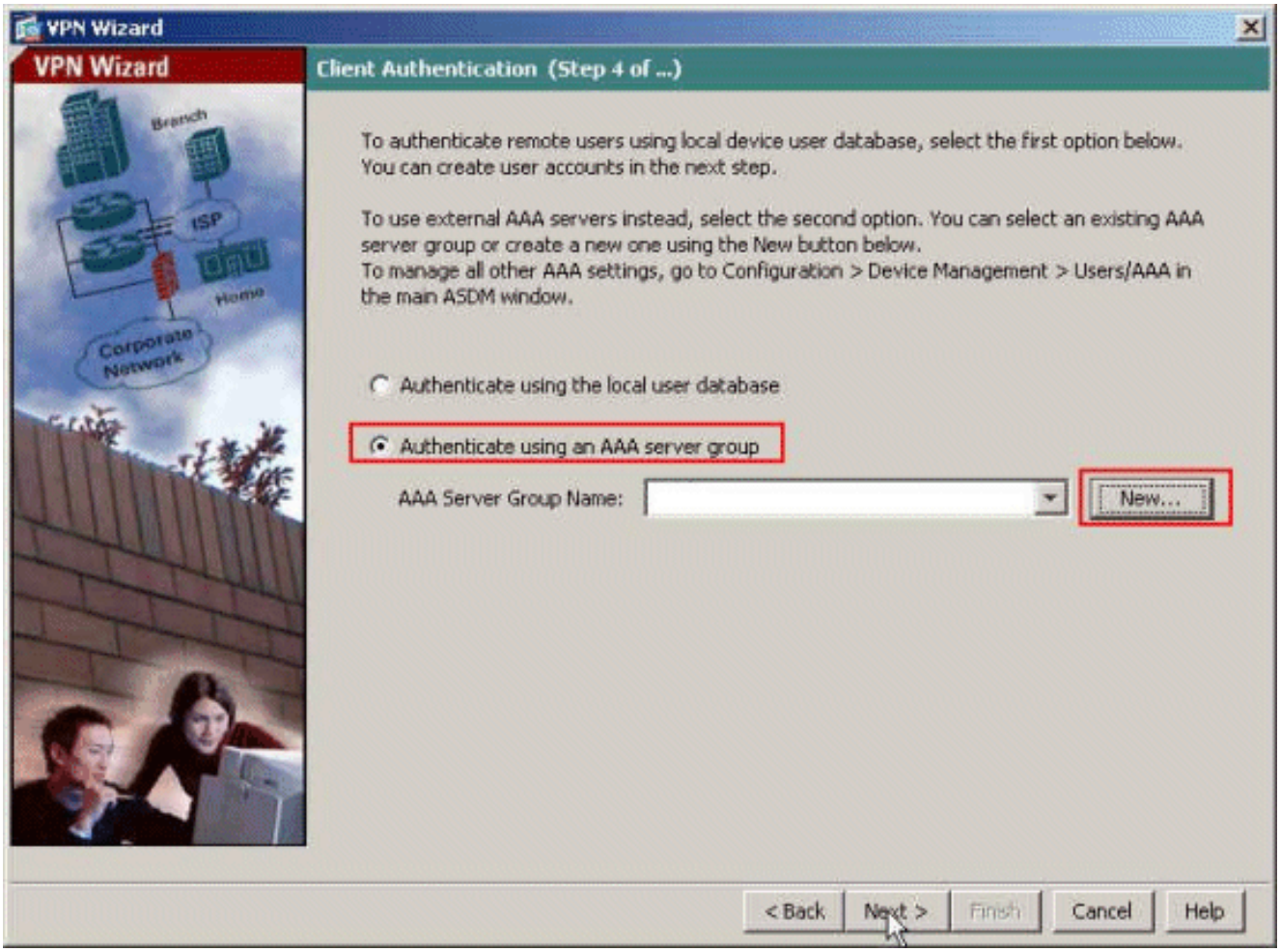


4. 選擇**Authentication Method**並提供身份驗證資訊。此處使用的身份驗證方法是**預共用金鑰**。此

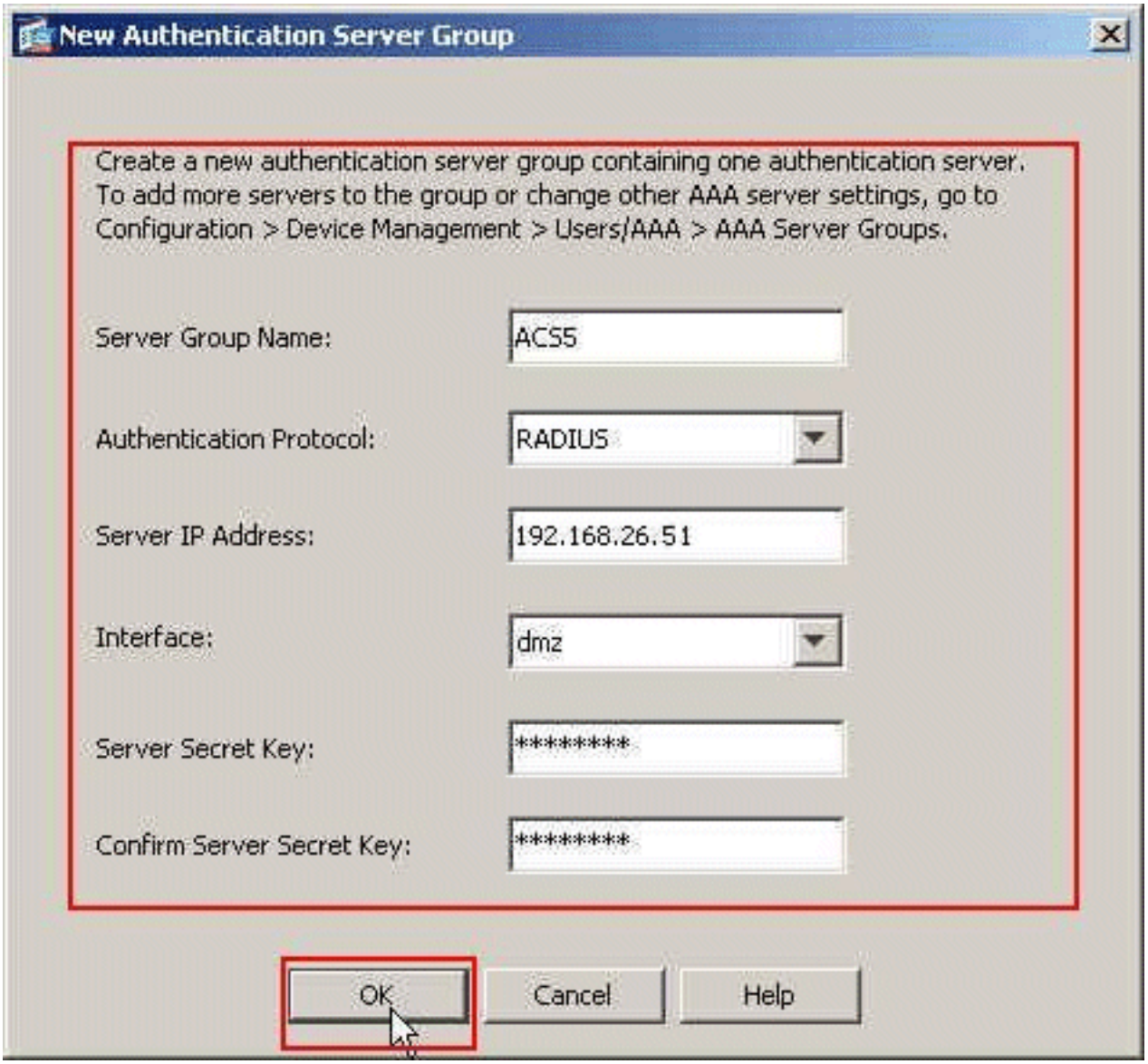
外，請在提供的空白處提供**Tunnel Group**名稱。此處使用的**預先共用金鑰**是**cisco123**，而此處使用的**通道群組名稱**是**Cisco-Tunnel**。按「**Next**」（下一步）。



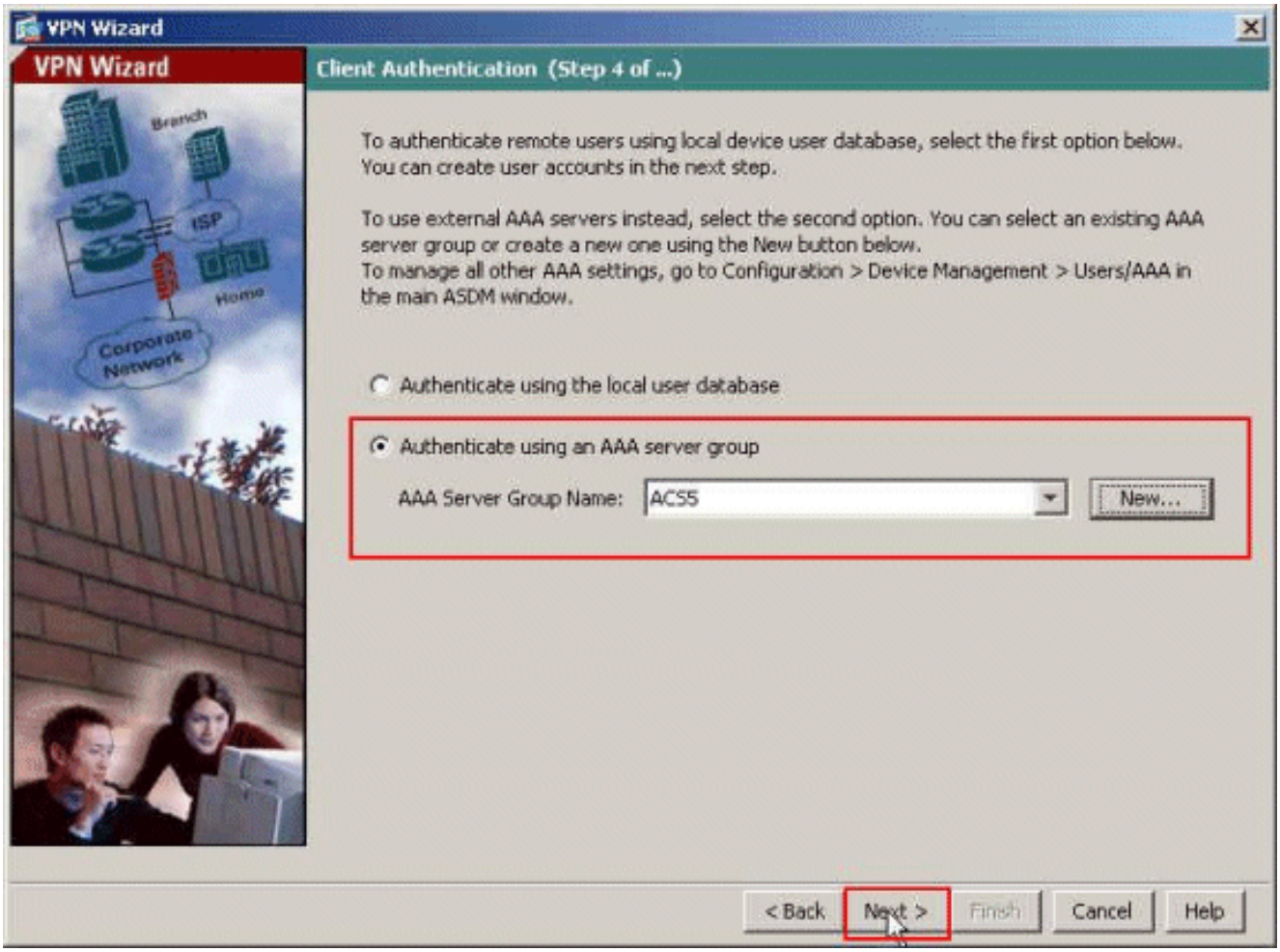
5. 選擇是要對本地使用者資料庫還是外部AAA伺服器組驗證遠端使用者。在這裡，我們選擇**Authenticate using an AAA server group**。按一下AAA Server Group Name欄位旁邊的**New**，以建立新的AAA Server Group Name。



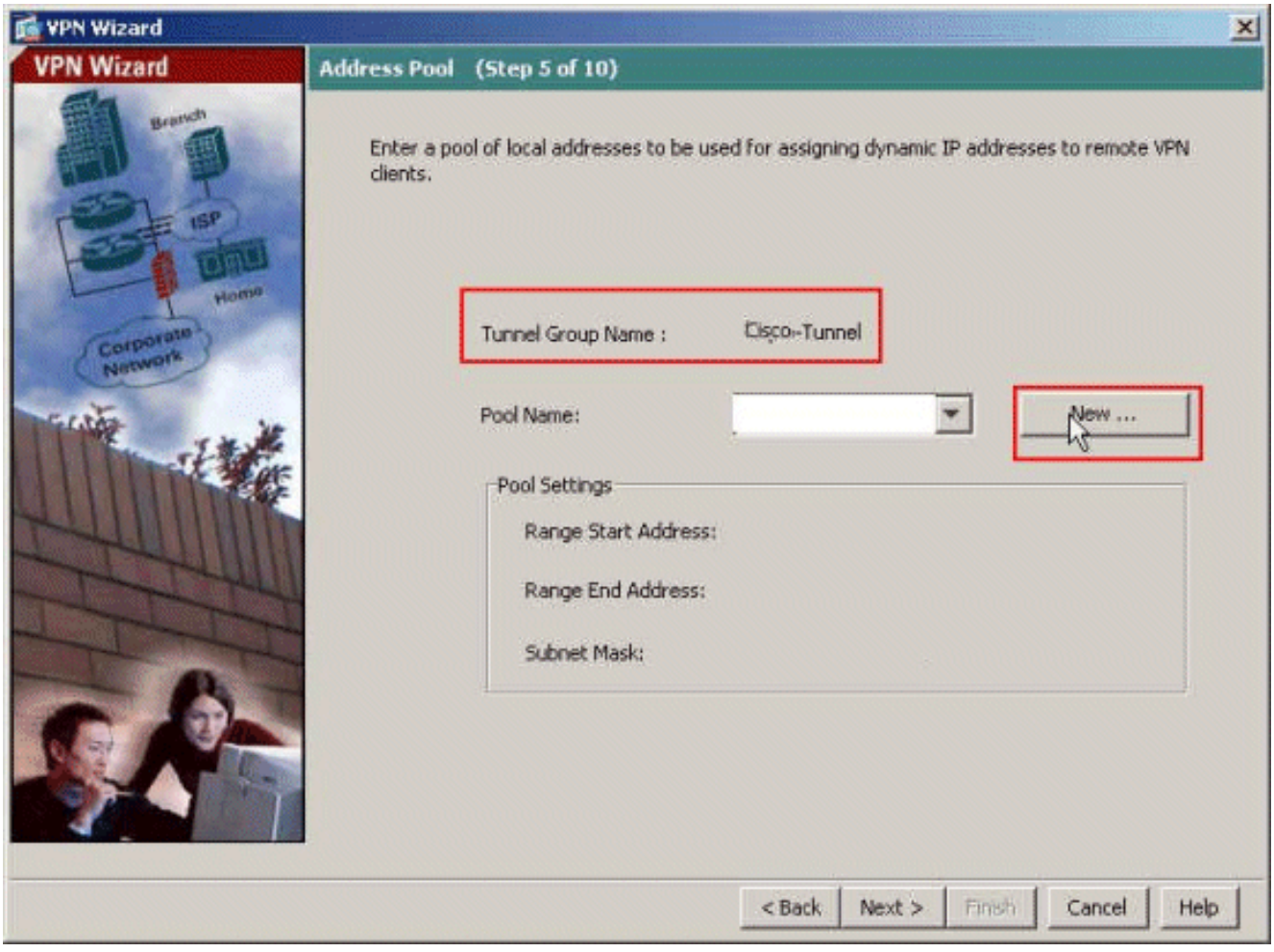
6. 在提供的相應空白處提供伺服器組名稱、身份驗證協定、伺服器IP地址、介面名稱和伺服器金鑰，然後按一下**確定**。


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

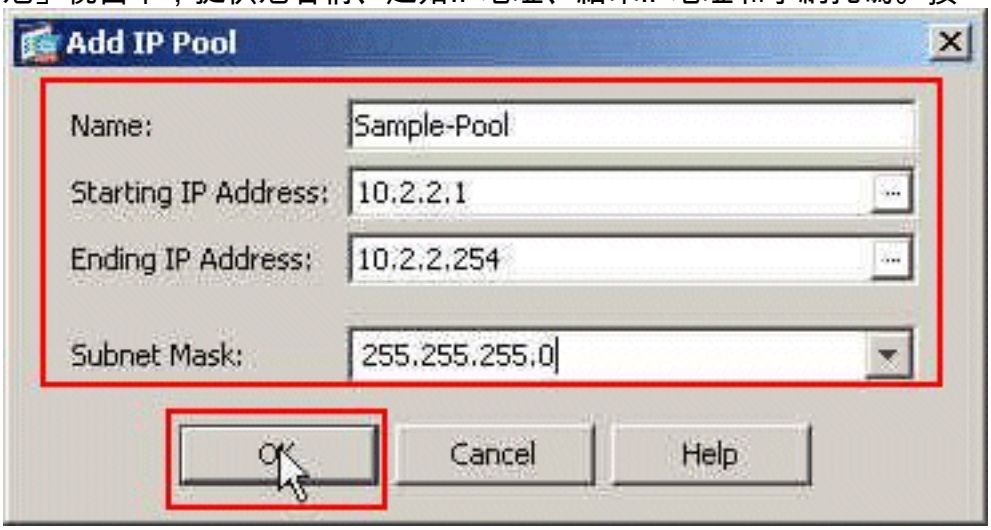
7. 按「**Next**」（下一步）。



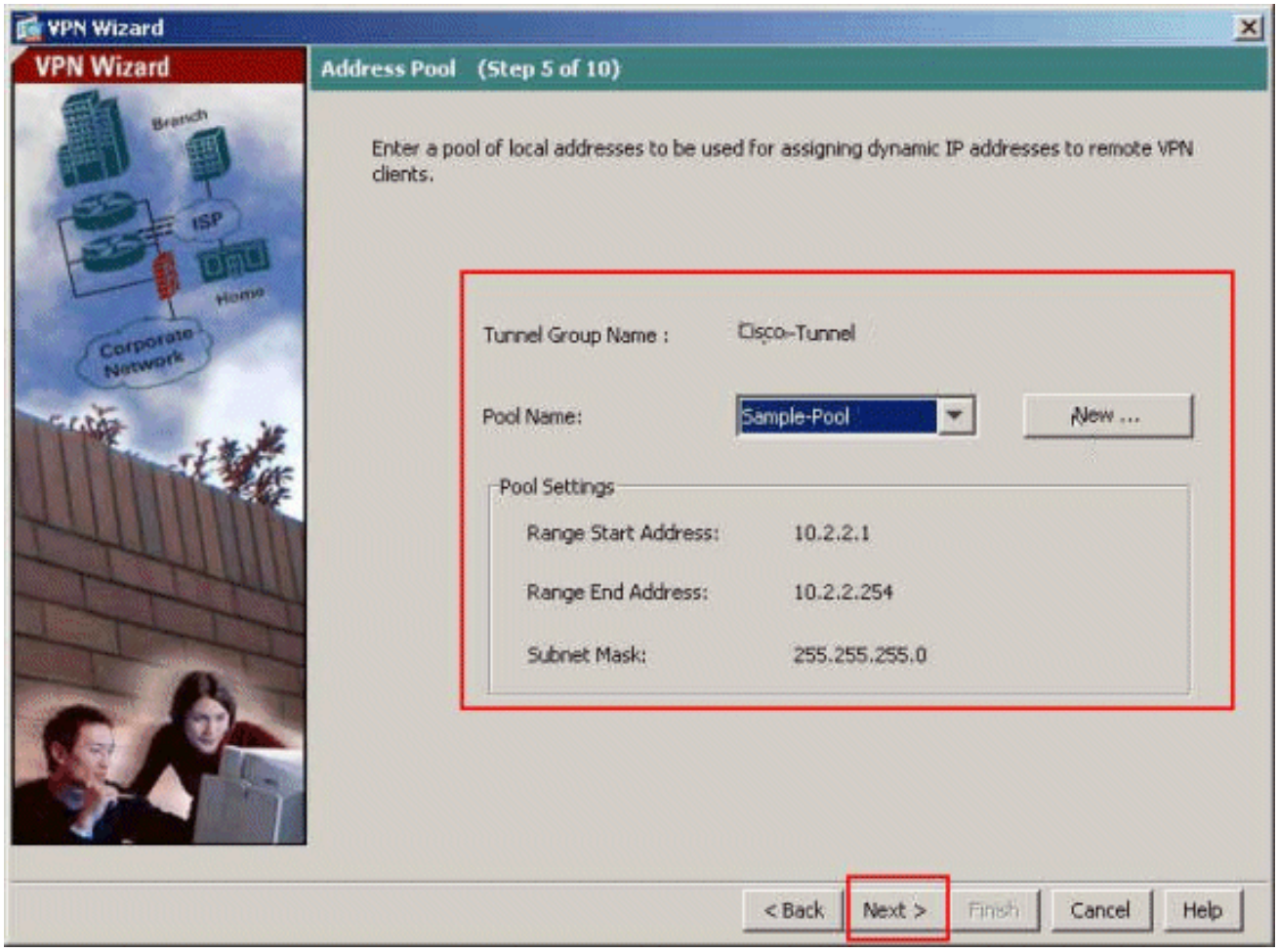
8. 定義一個本地地址池，在遠端VPN客戶端連線時將其動態分配給它們。按一下**New**以建立新的本地地址池。



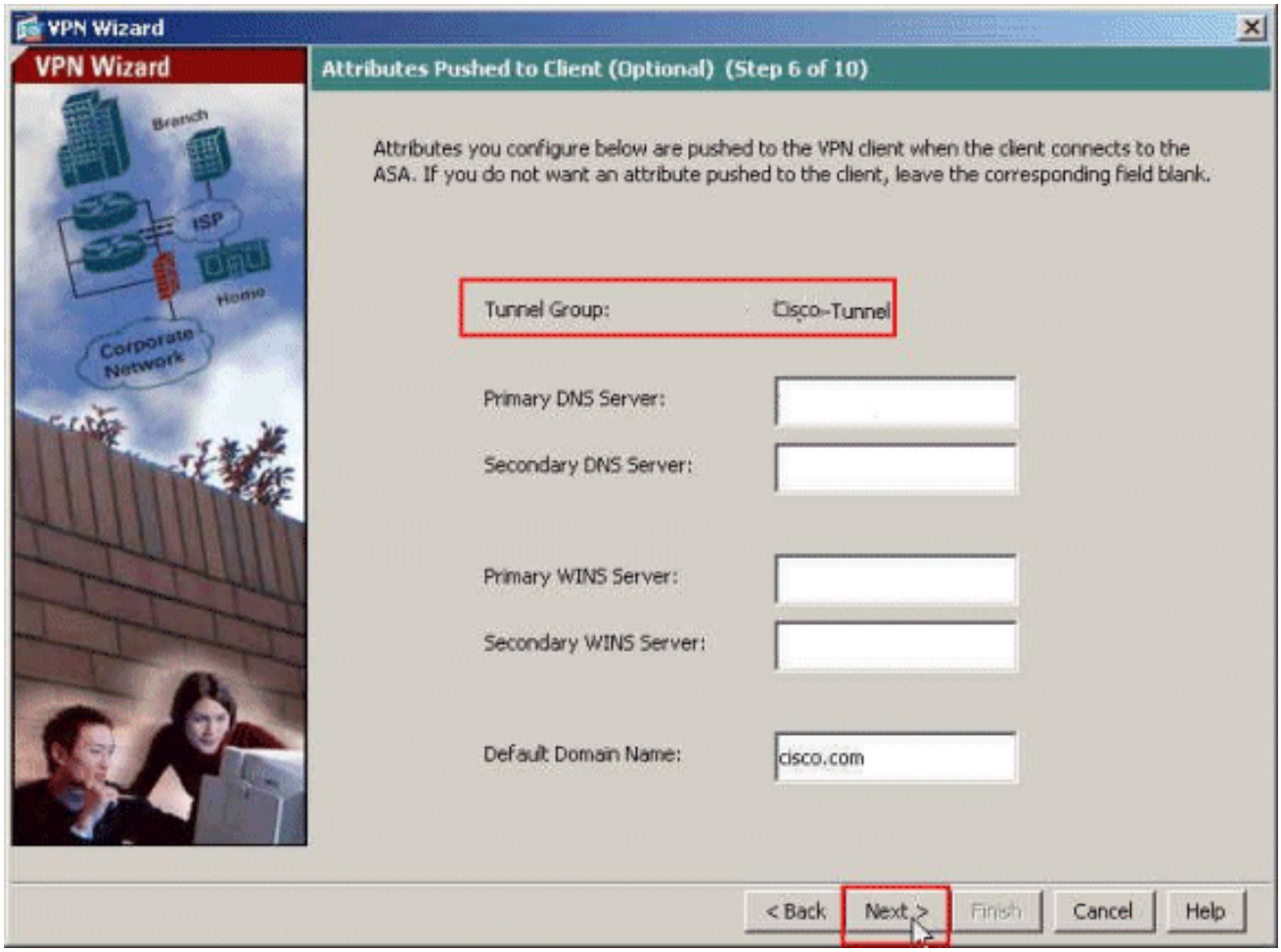
9. 在「新增IP池」視窗中，提供池名稱、起始IP地址、結束IP地址和子網掩碼。按一下「**OK**」（確定）。



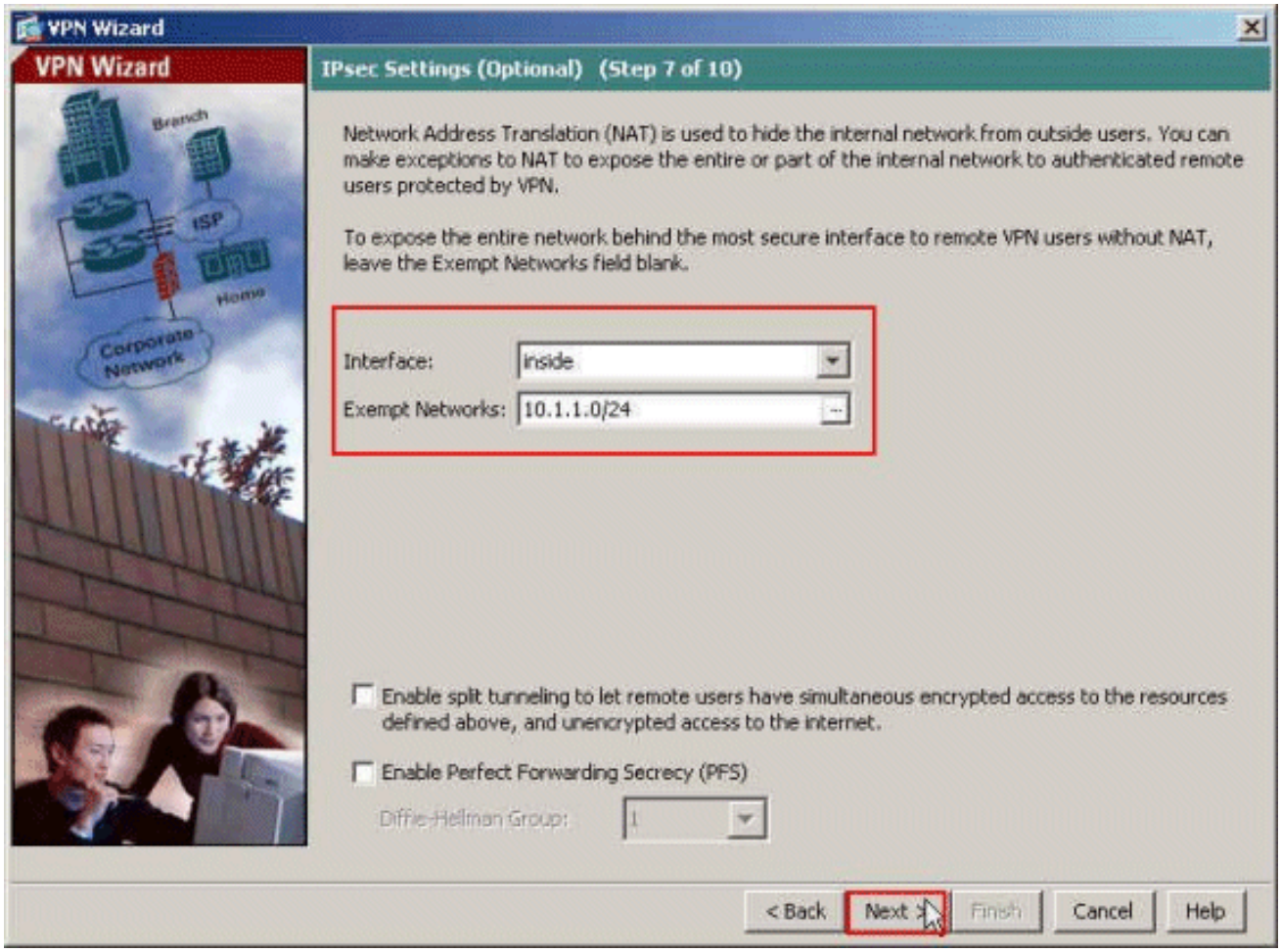
10. 從下拉選單中選擇池名稱，然後點選**下一步**。此示例的池名稱是在步驟9中建立的**Sample-Pool**。



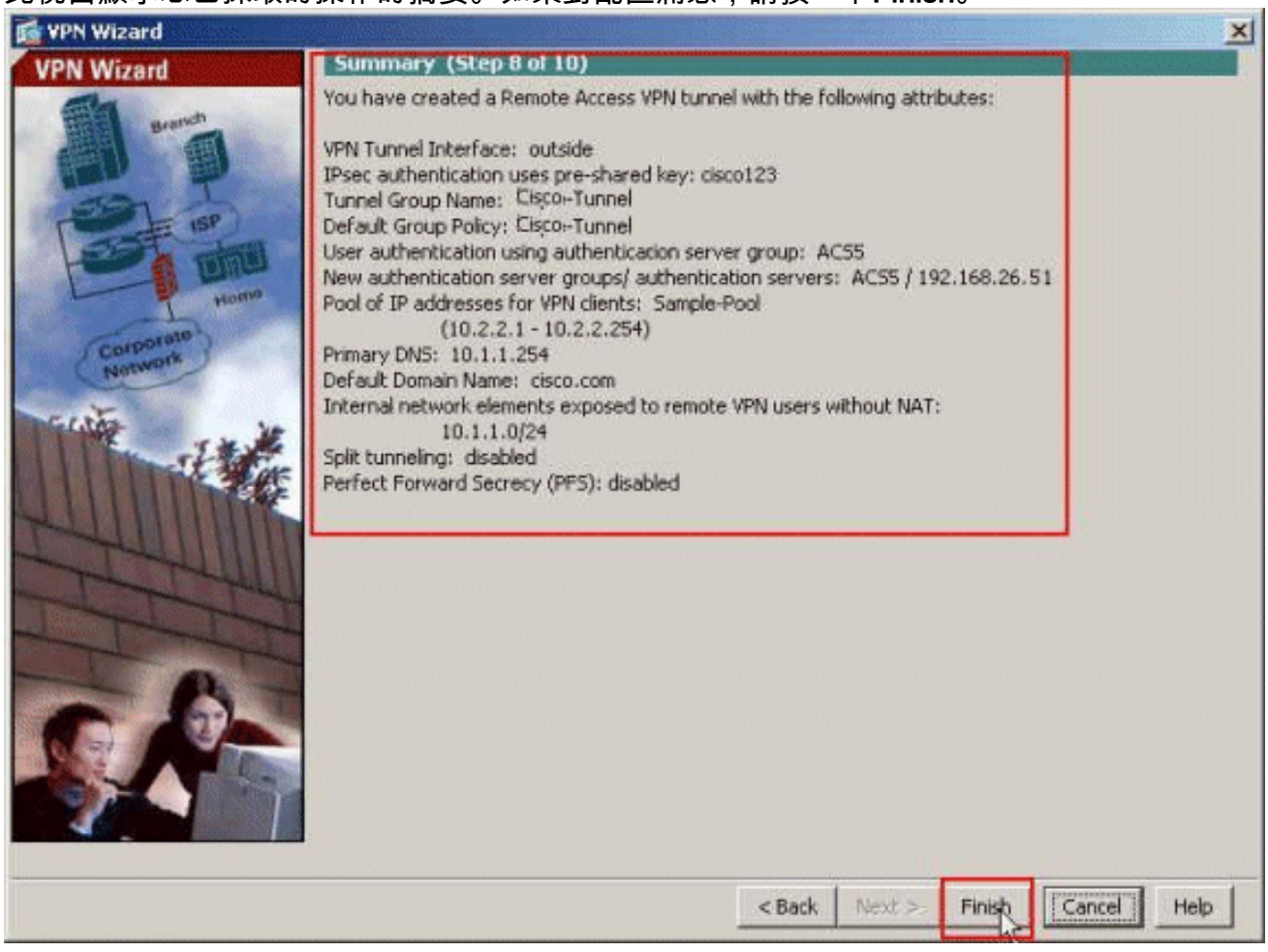
11. *可選：*指定要推送到遠端VPN客戶端的DNS和WINS伺服器資訊以及預設域名。



12. 指定應向遠端VPN使用者公開哪些內部主機或網路（如果有）。在Exempt Networks欄位中提供介面名稱和要免除的網路，然後按一下**Next**。如果將此清單留空，則遠端VPN使用者可訪問ASA的整個內部網路。您還可以在此視窗中啟用分割隧道。分割隧道可加密流向此過程前面定義的資源的流量，並通過不對該流量進行隧道傳輸來提供對一般網際網路的未加密訪問。如果未啟用*拆分隧道*，則所有來自遠端VPN使用者的流量都會通過隧道連線到ASA。根據您的配置，這會佔用大量頻寬和處理器。



13. 此視窗顯示您已採取的操作的摘要。如果對配置滿意，請按一下**Finish**。



使用CLI配置ASA

以下是CLI組態：

在ASA裝置上運行配置

```
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#
```

為個人使用者的可下載ACL配置ACS

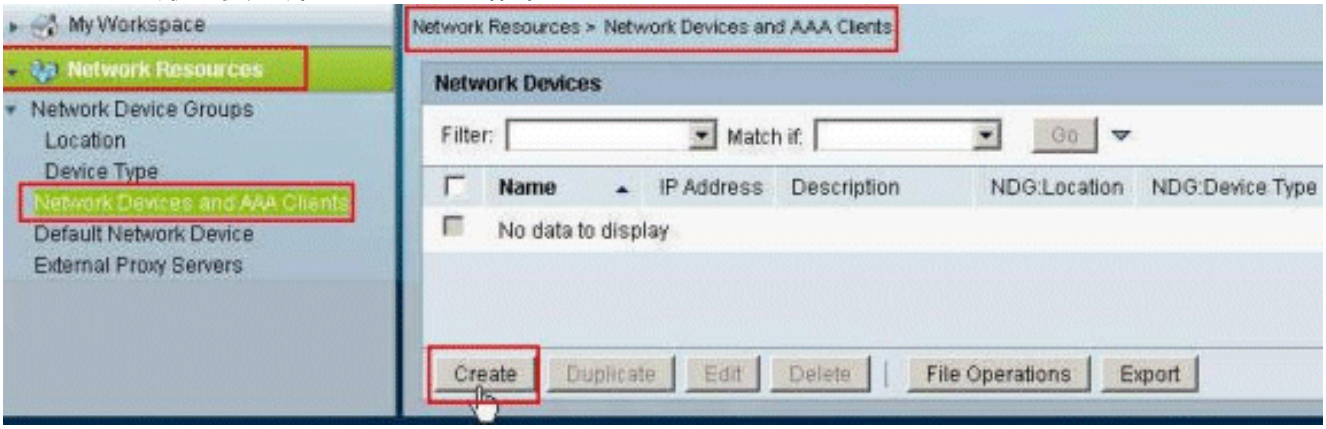
您可以將Cisco Secure ACS 5.x上的可下載訪問清單配置為命名許可權對象，然後將其分配給將在Access-Service規則的結果部分中選擇的授權配置檔案。

在此示例中，IPsec VPN使用者**cisco**成功進行身份驗證，並且RADIUS伺服器向安全裝置傳送可下載訪問清單。使用者「cisco」只能訪問10.1.1.2伺服器並拒絕所有其他訪問。要驗證ACL，請參閱

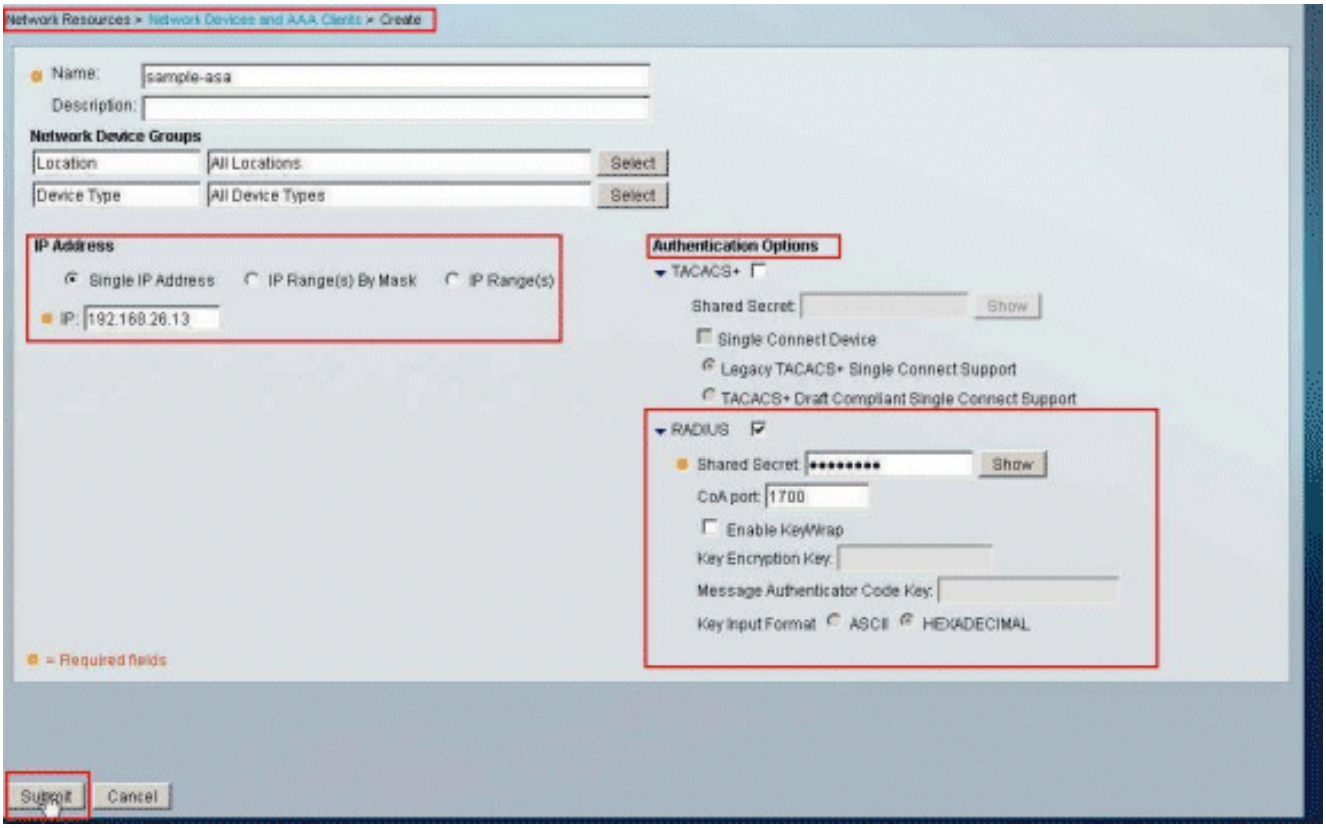
使用者/組的可下載ACL部分。

完成以下步驟，以便在Cisco Secure ACS 5.x中配置RADIUS客戶端：

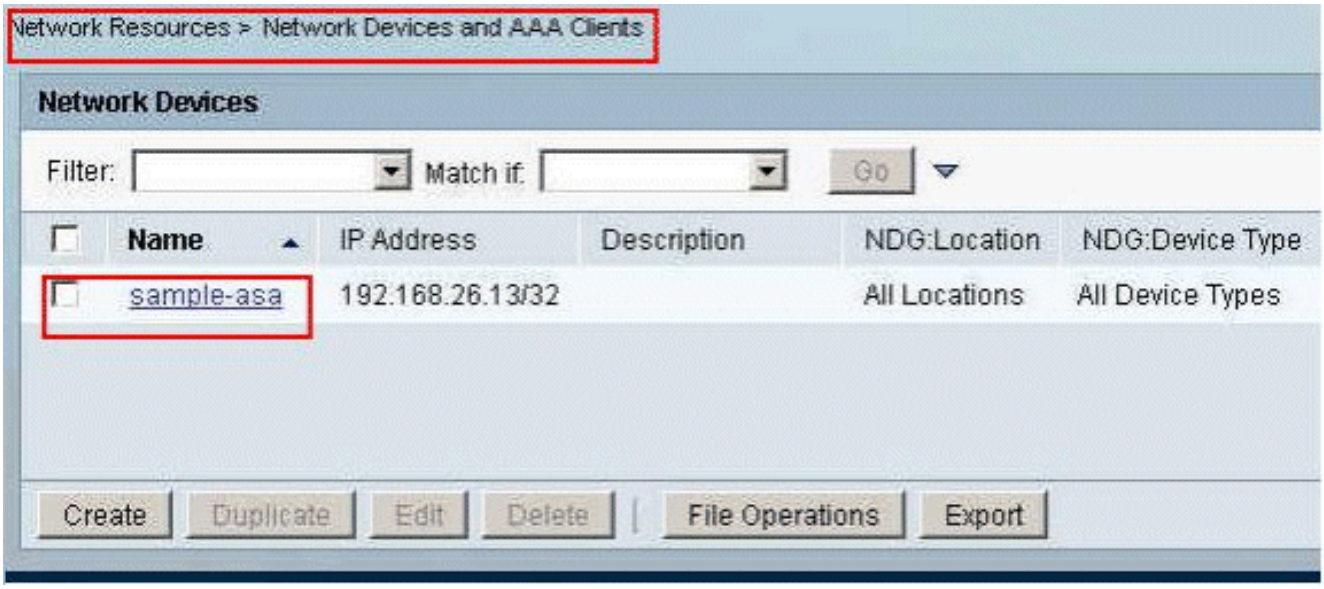
1. 選擇**Network Resources > Network Devices and AAA Clients**，然後按一下**Create**以在RADIUS伺服器資料庫中為ASA新增條目。



2. 為ASA輸入本地有效的Name(在本例中為**sample-asa**)，然後在IP address欄位中輸入**192.168.26.13**。在「驗證選項」區段中選擇**RADIUS**，方法是勾選「**RADIUS**」覈取方塊，然後在「共用密碼」欄位中輸入**cisco123**。按一下「**Submit**」。

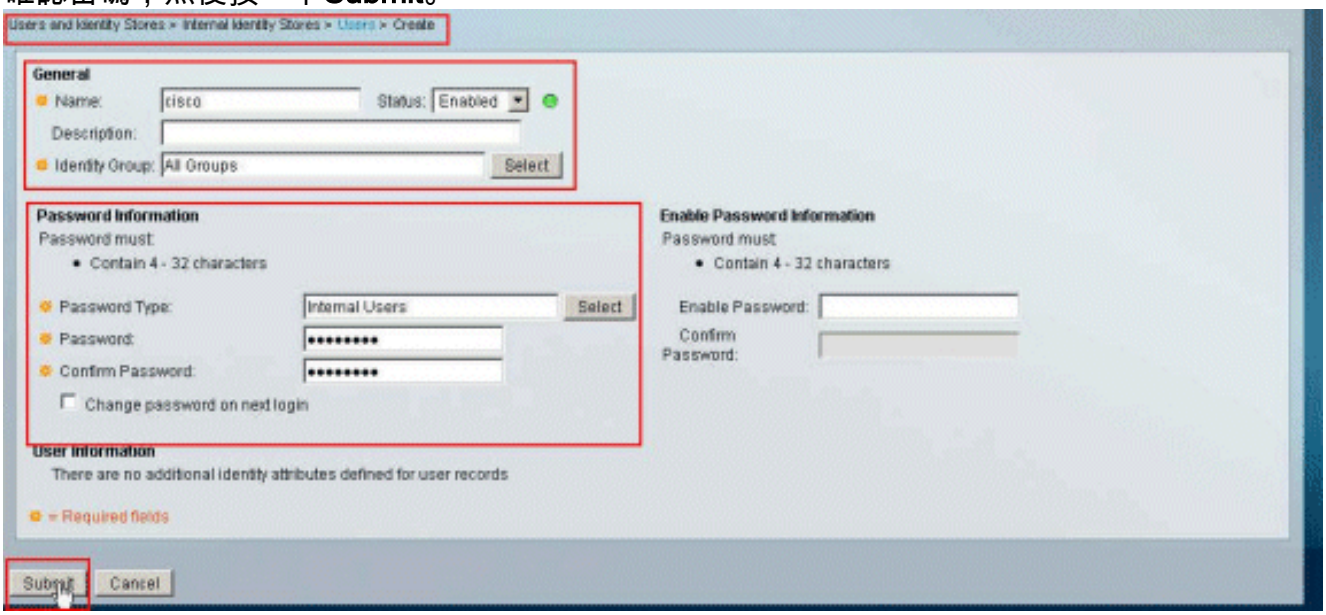


3. ASA已成功新增到RADIUS伺服器(ACS)資料庫。

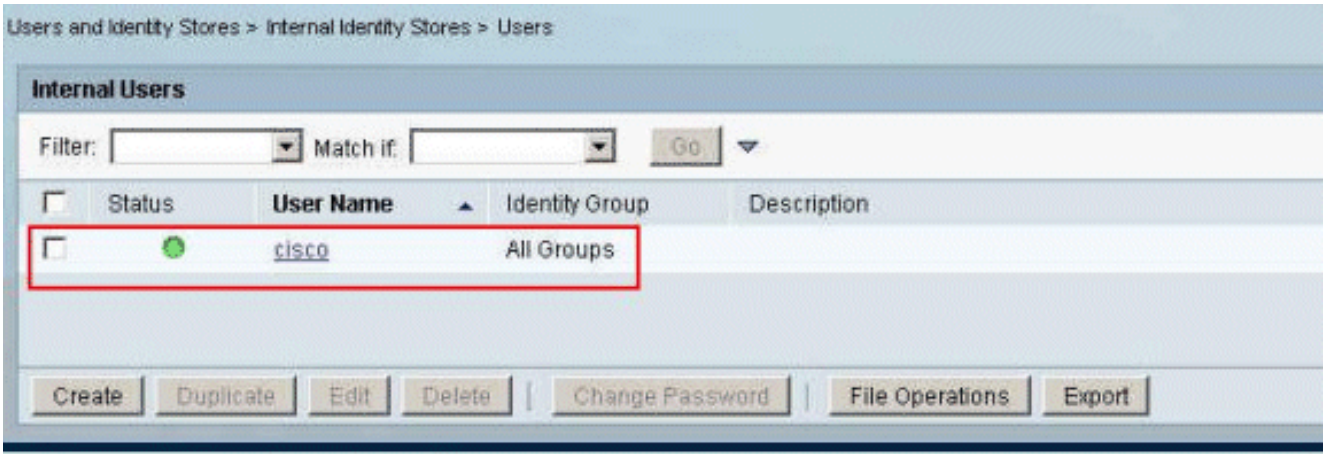


4. 選擇**Users and Identity Stores > Internal Identity Stores > Users**，然後按一下**Create**，以便在ACS的本地資料庫中為VPN身份驗證建立使用者。

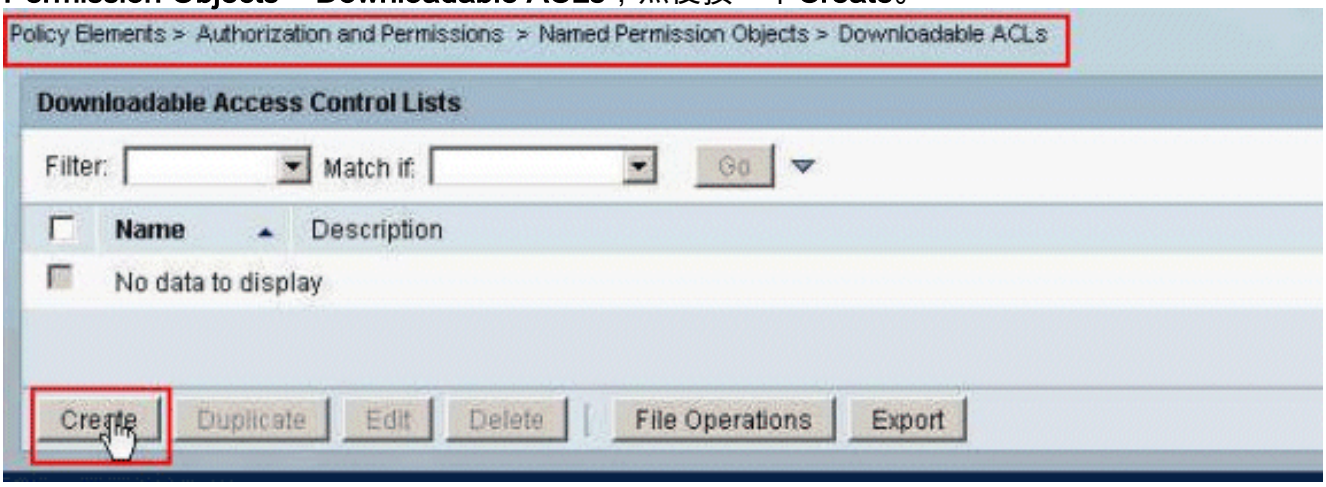
5. 輸入使用者名稱**cisco**。將密碼型別選擇為**Internal Users**，然後輸入密碼(本例中為**cisco123**)。確認密碼，然後按一下**Submit**。



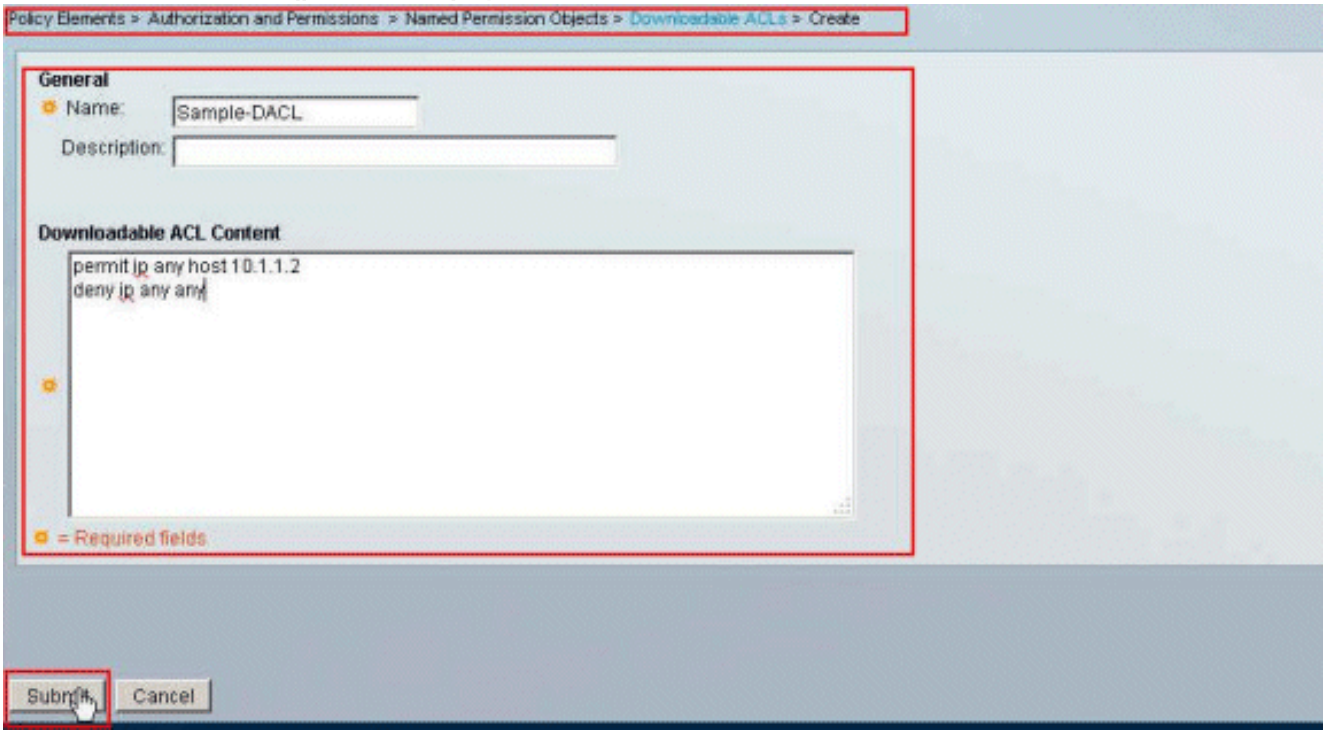
6. 已成功建立使用者**cisco**。



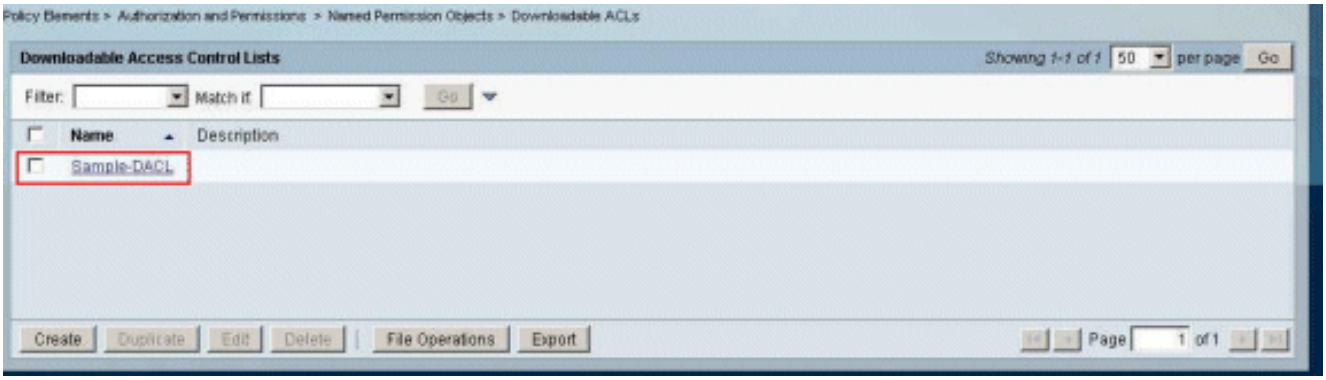
7. 要建立可下載ACL，請選擇Policy Elements > **Authorization and Permissions > Named Permission Objects > Downloadable ACLs**，然後按一下**Create**。



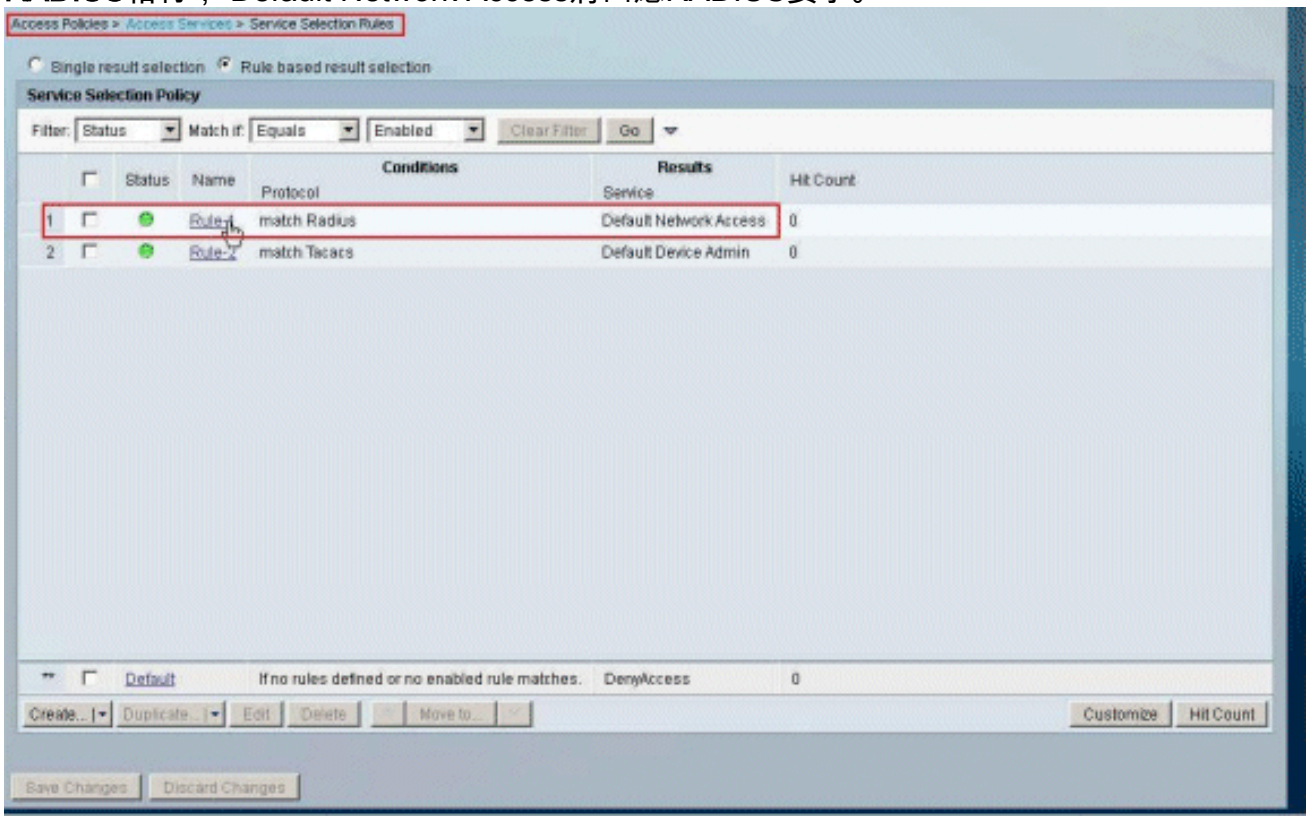
8. 提供可下載ACL的**名稱**以及**ACL內容**。按一下「**Submit**」。



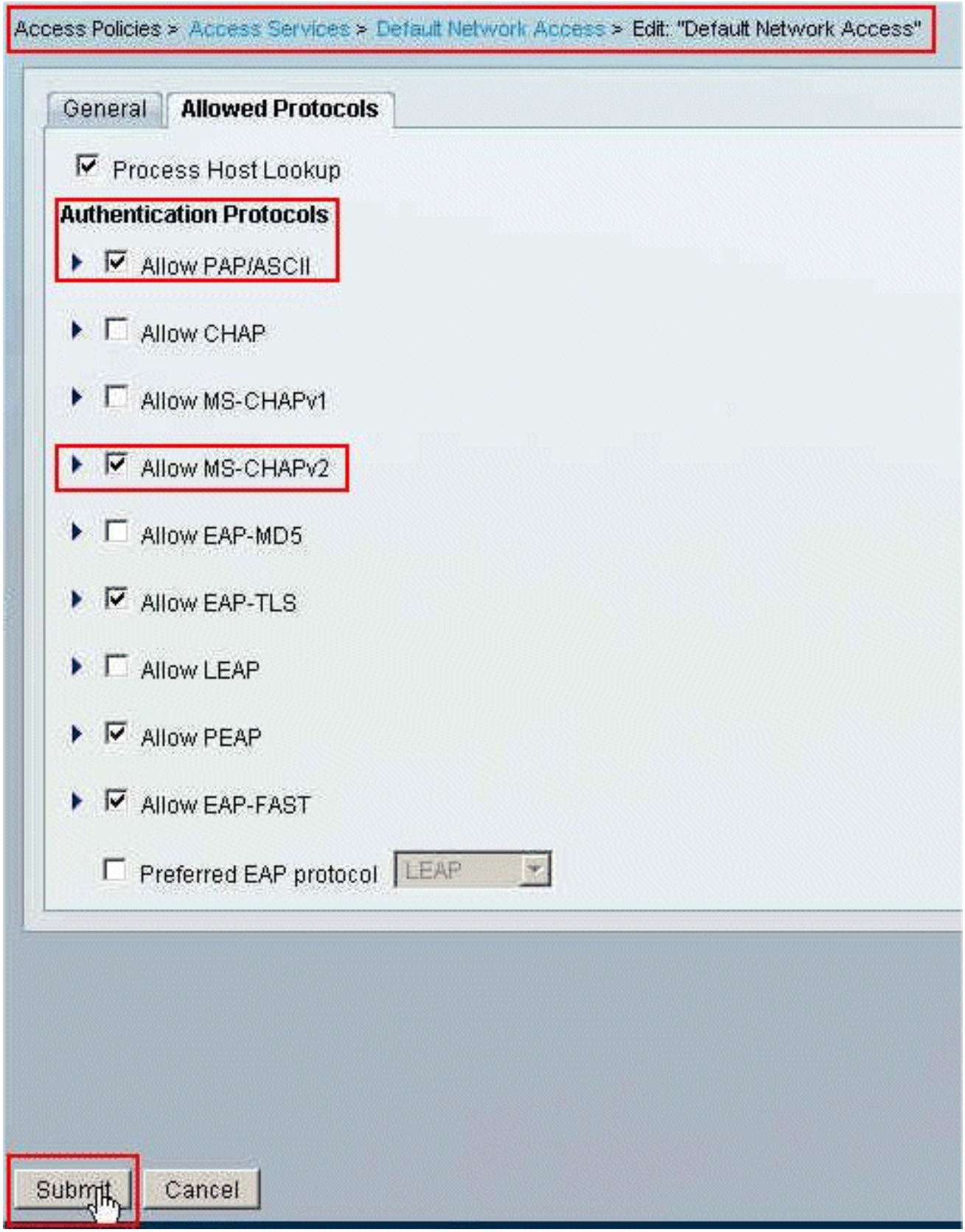
9. 可下載ACL **Sample-DACL**已成功建立。



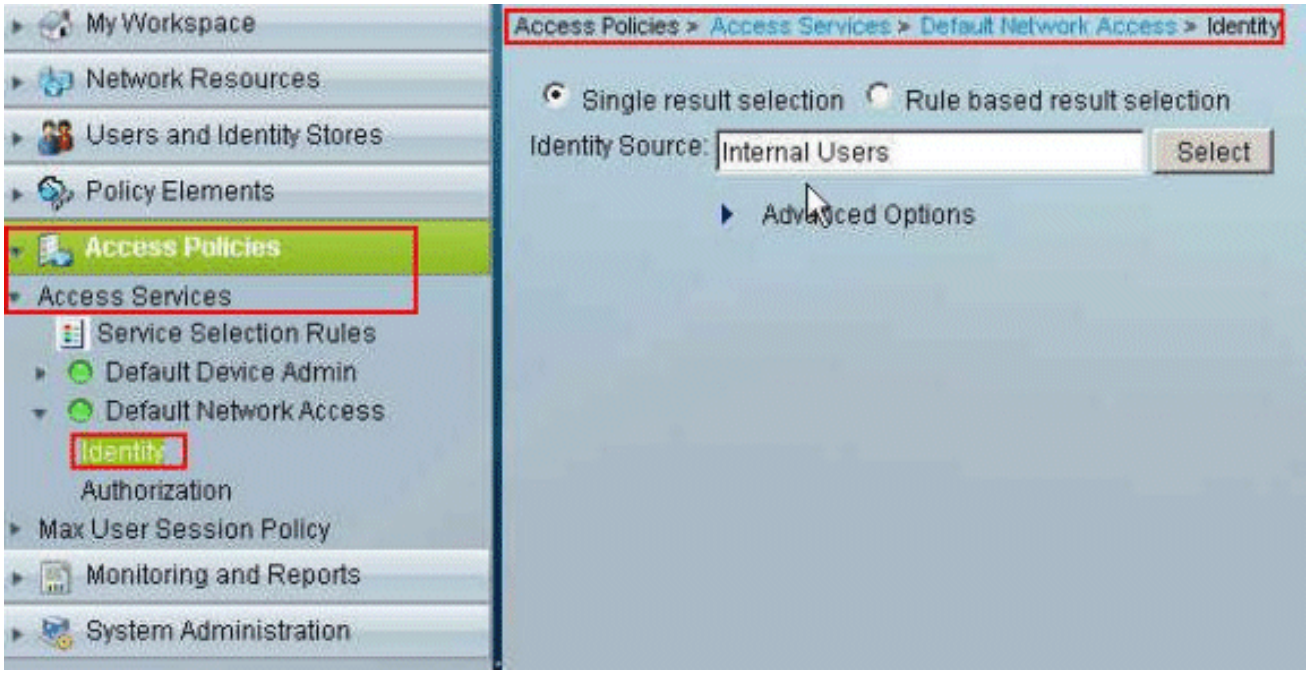
10. 若要針對VPN驗證設定Access-Policies，請選擇**Access Policies > Access Services > Service Selection Rules**，然後判斷哪個服務符合RADIUS通訊協定。在本範例中， **Rule 1**與**RADIUS**相符， Default Network Access將回應RADIUS要求。



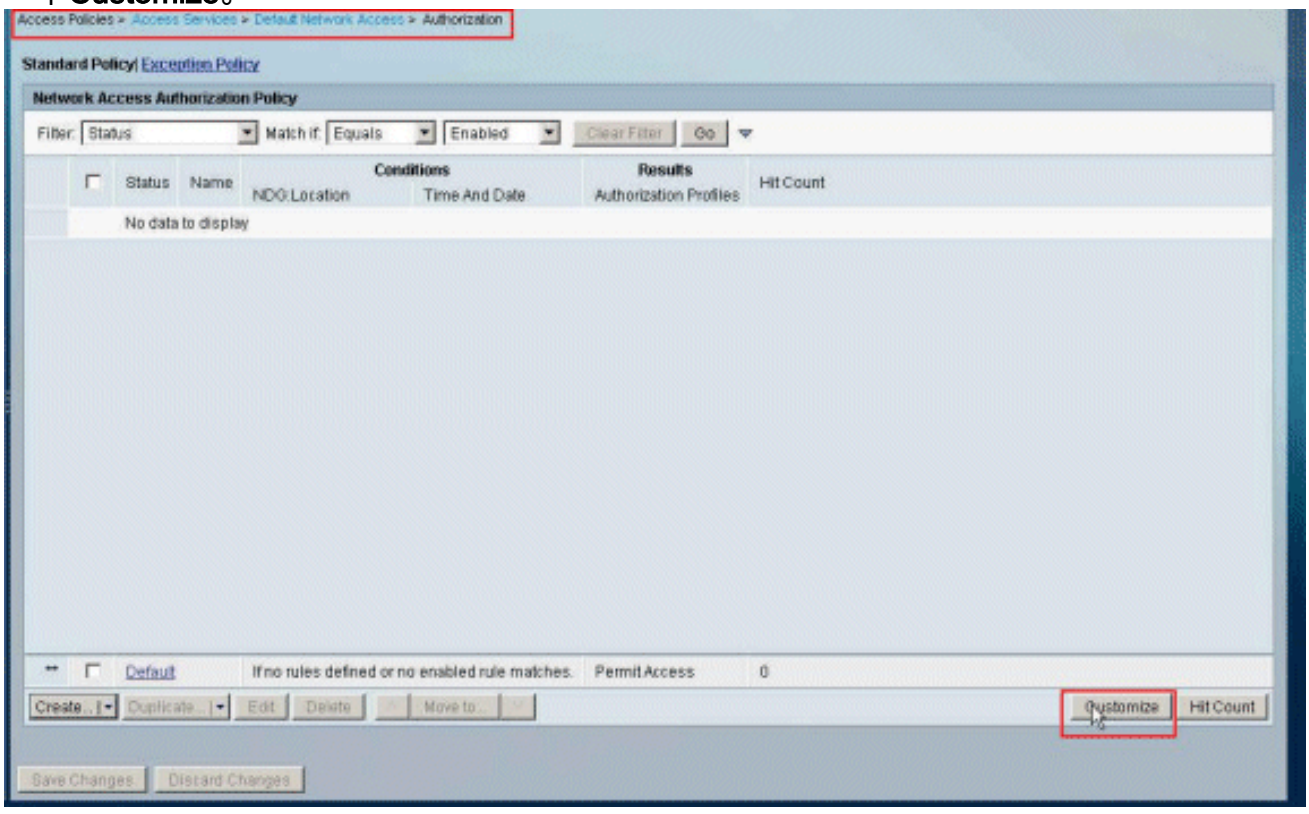
11. 選擇步驟10中決定的**Access Service**。在本範例中使用的是**Default Network Access**。選擇**Allowed Protocols**頁籤，並確保**Allow PAP/ASCII**和**Allow MS-CHAPv2**已選中。按一下**Submit**。



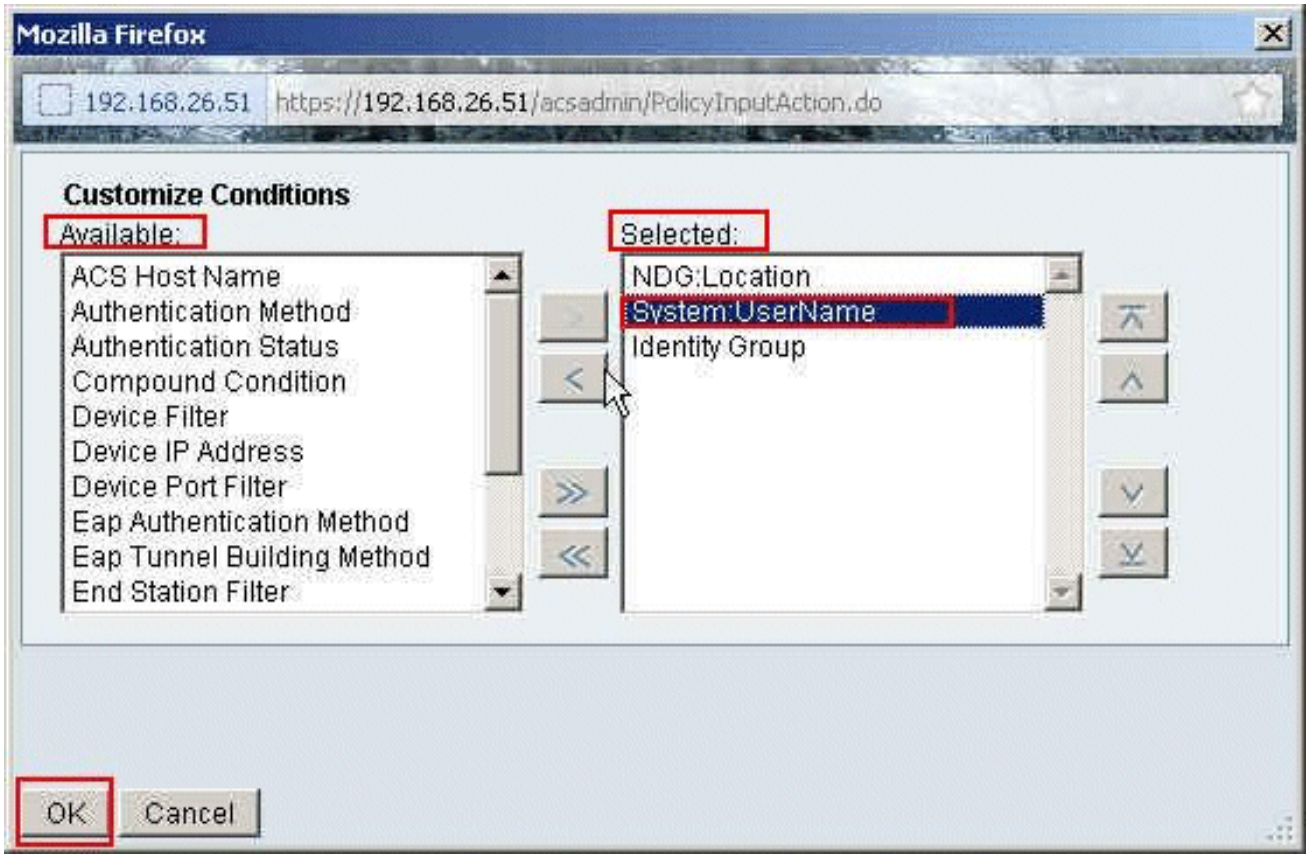
12. 按一下**Access Services**的**Identity Section**，並確保已選擇**Internal Users**作為身份源。在本例中，我們採用了預設的網路訪問。



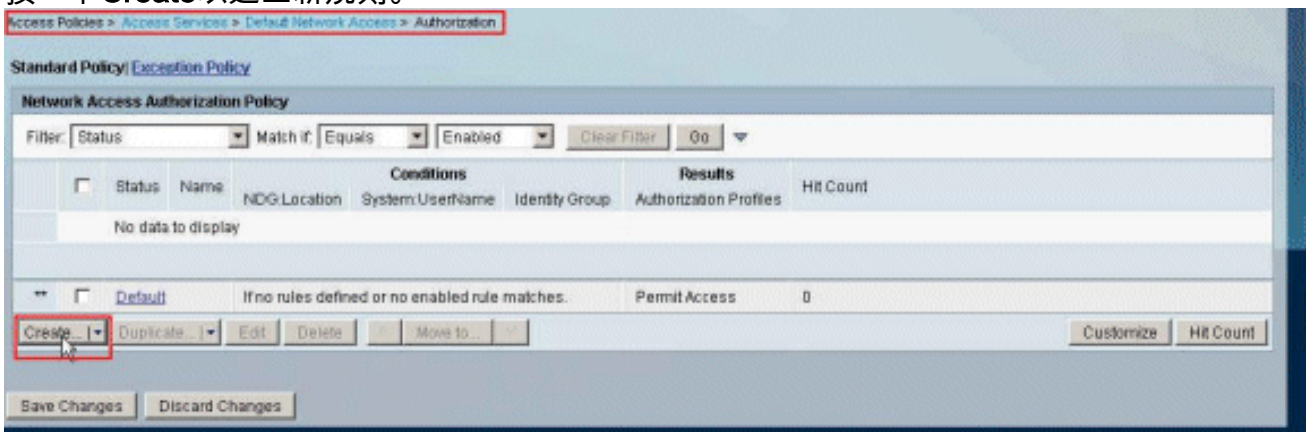
13. 選擇Access Policies > **Access Services > Default Network Access > Authorization**，然後按一下**Customize**。



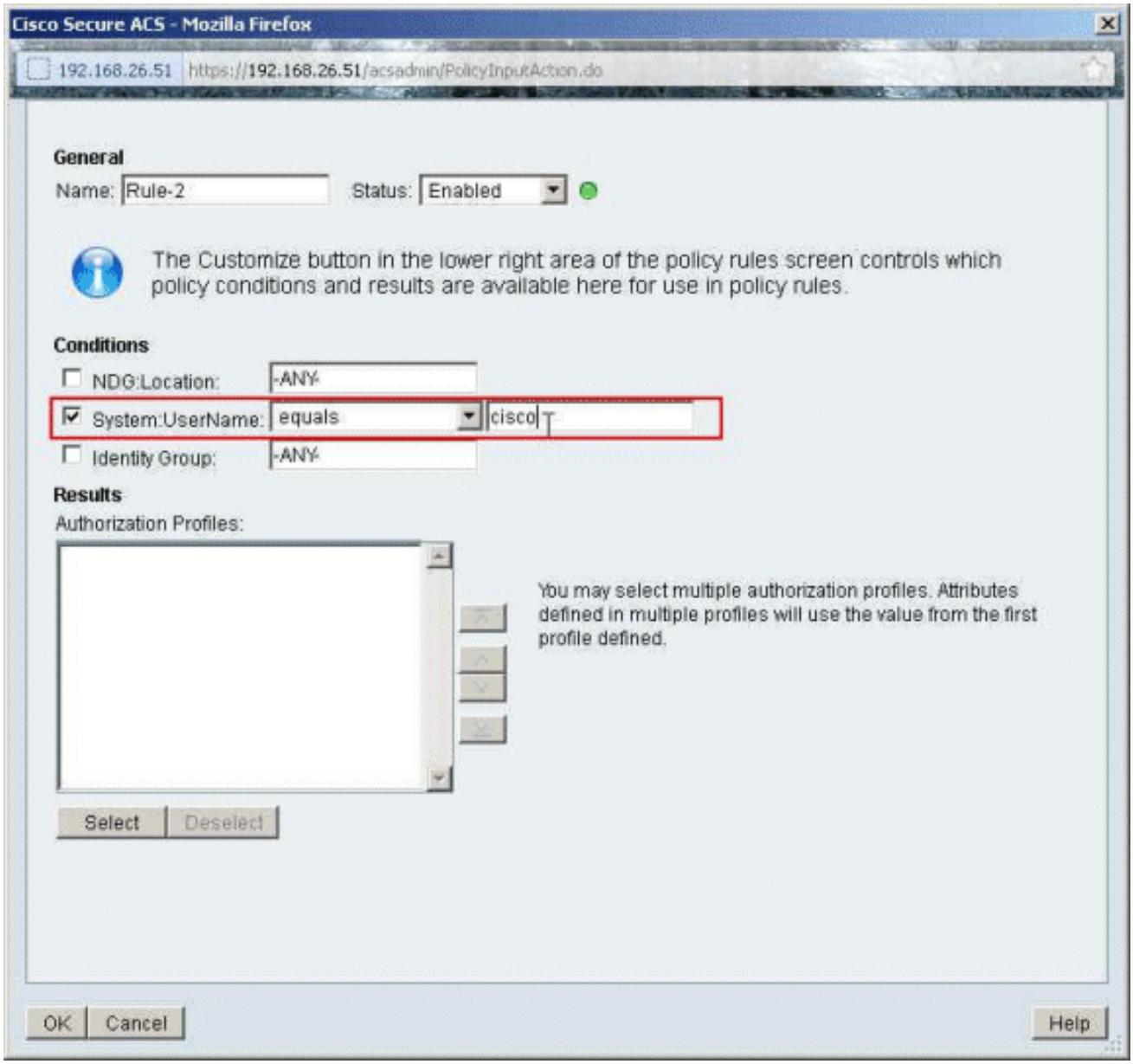
14. 將**System:UserName**從**Available**列移動到**Selected**列，然後按一下**OK**。



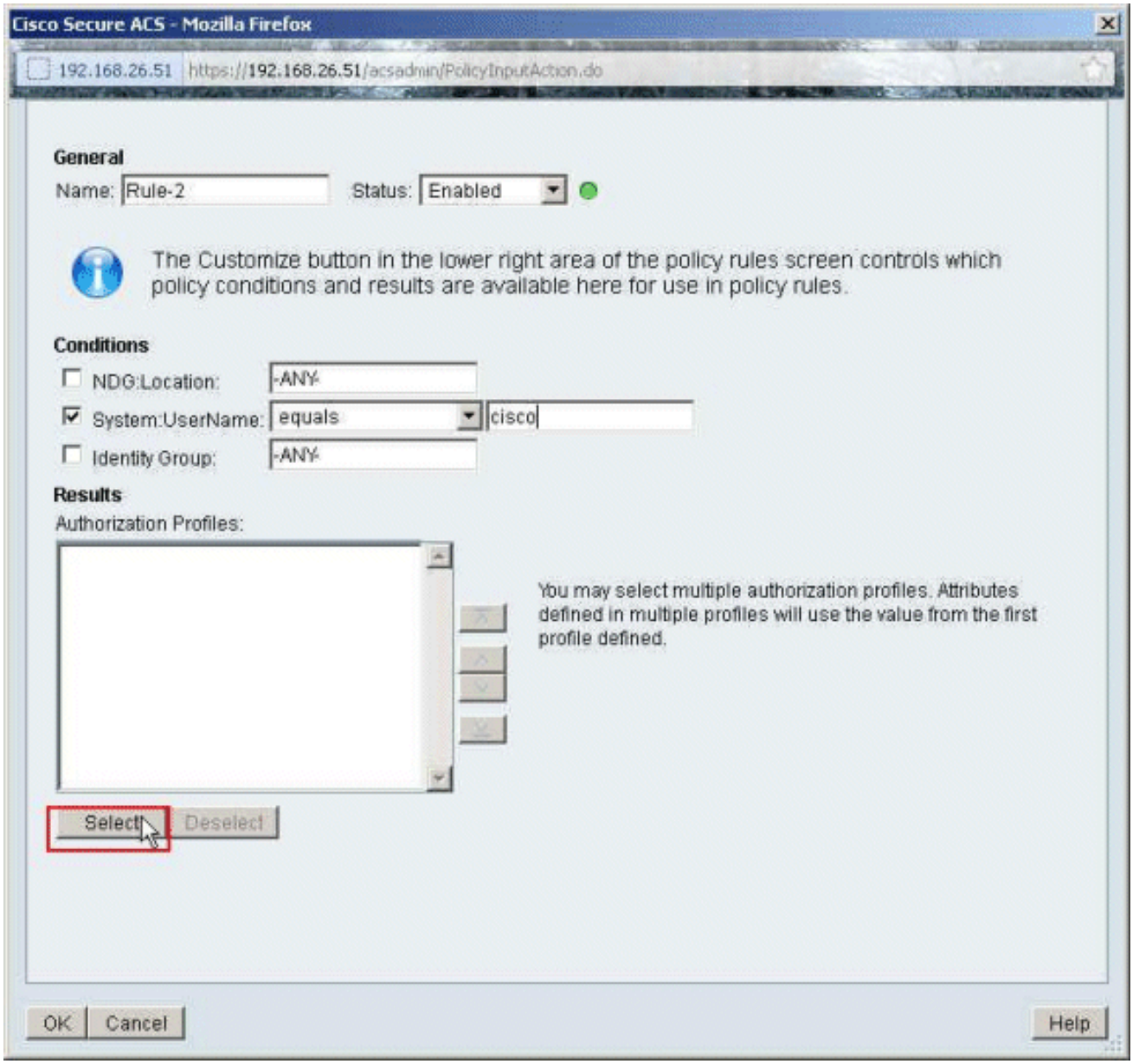
15. 按一下**Create**以建立新規則。



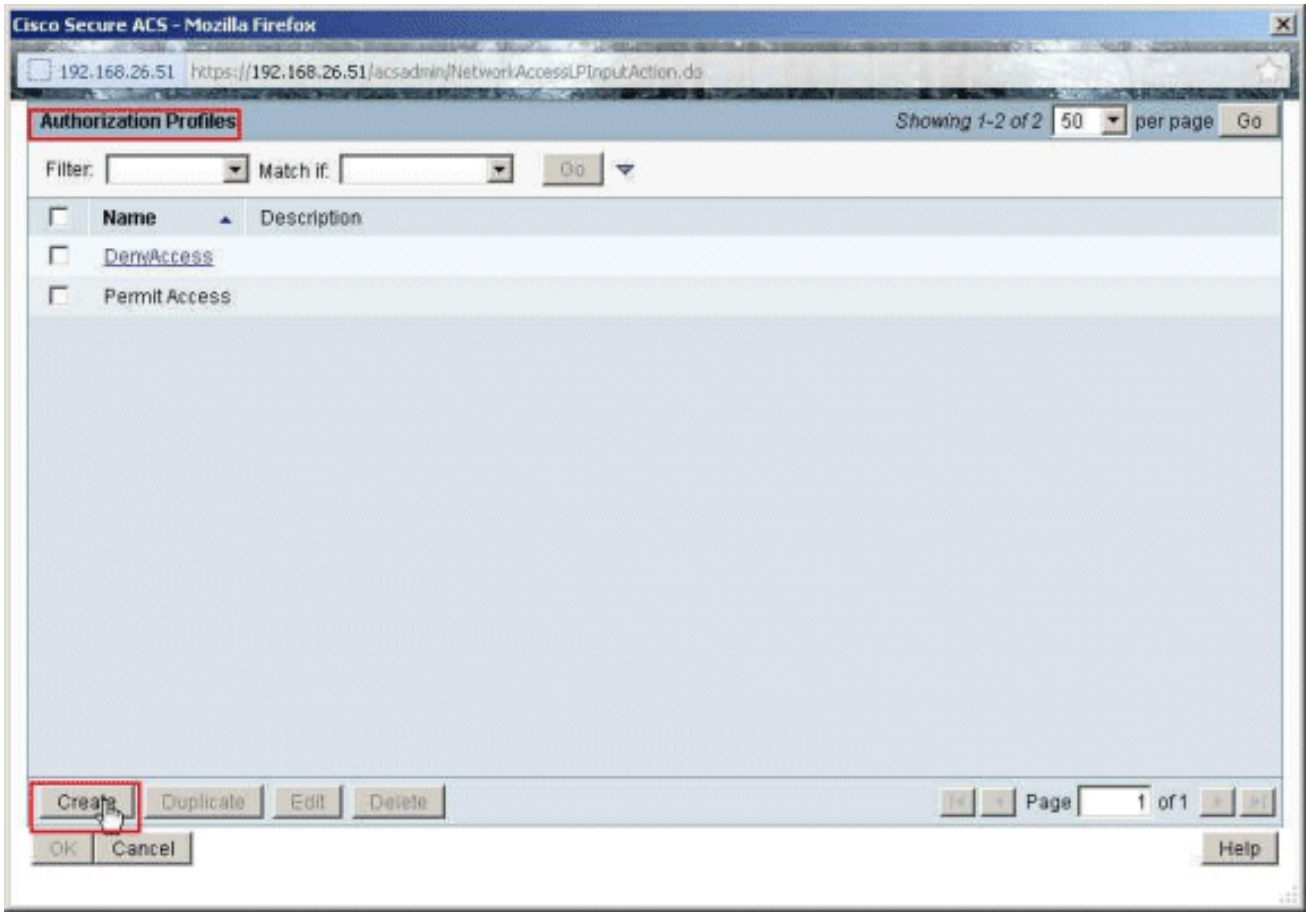
16. 確保選中**System:UserName**旁邊的覈取方塊，從下拉選單中選擇**equals**，然後輸入使用者名稱**cisco**。



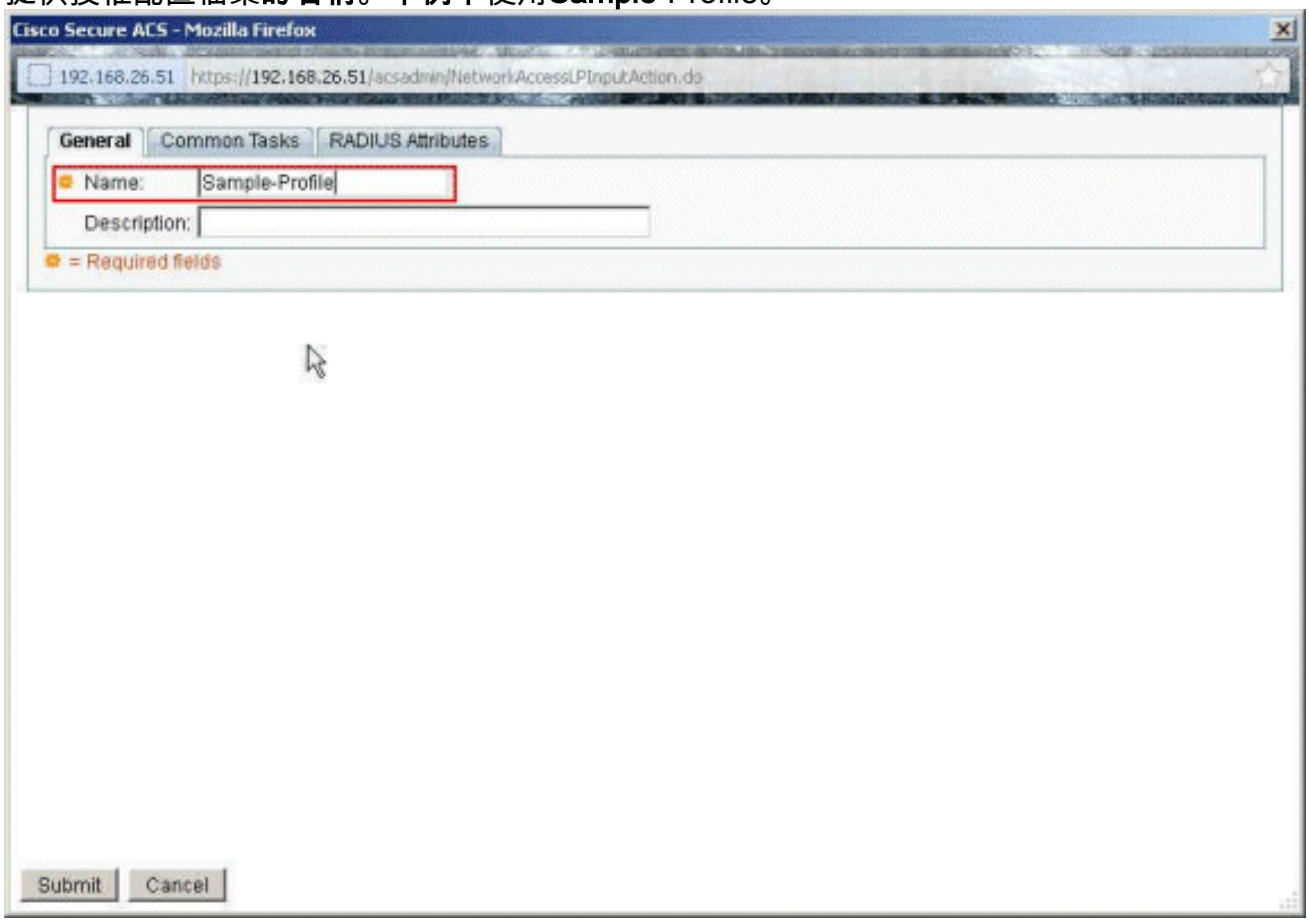
17. 按一下「**Select**」。



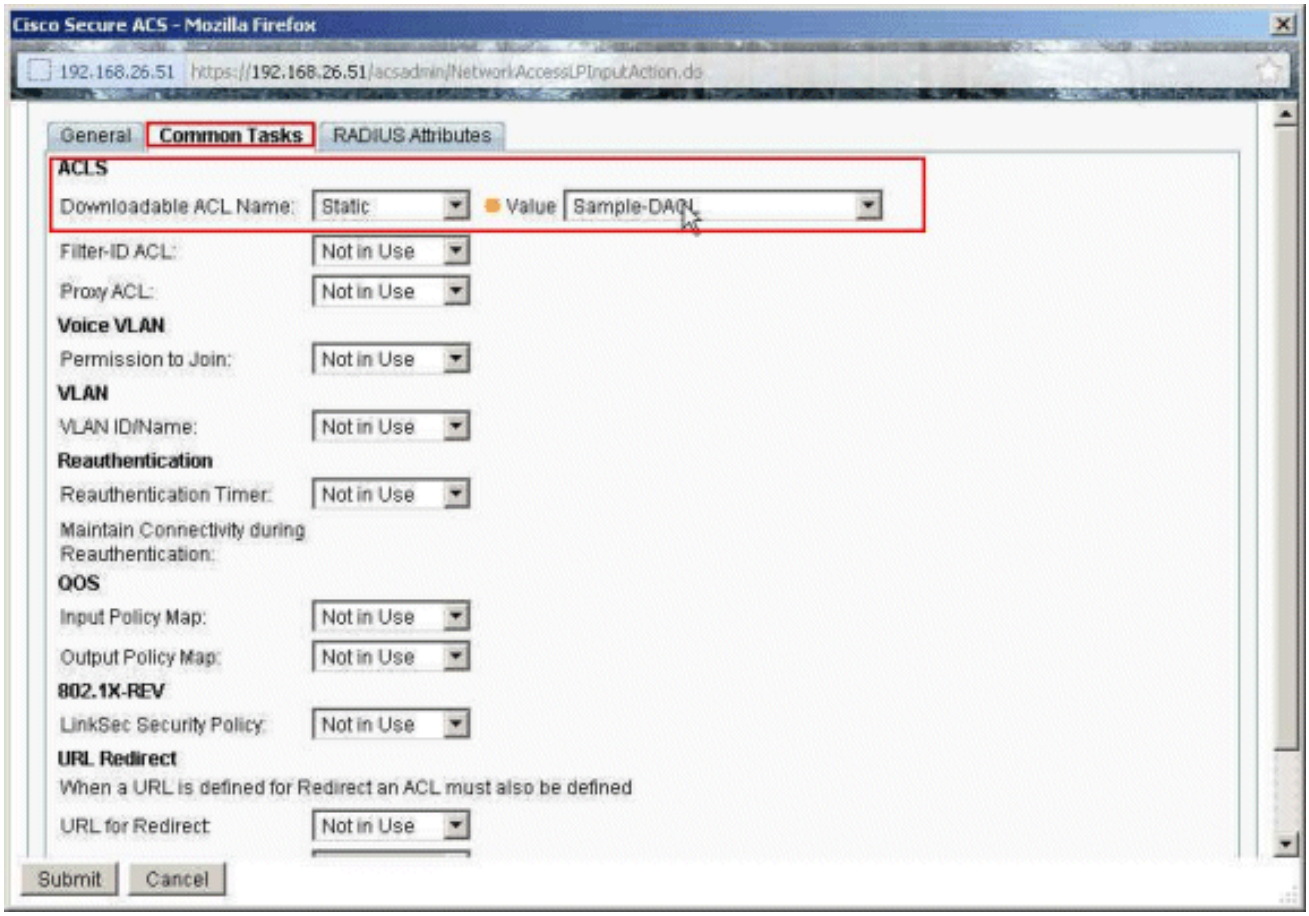
18. 按一下「**Create**」以建立一個新的授權設定檔。



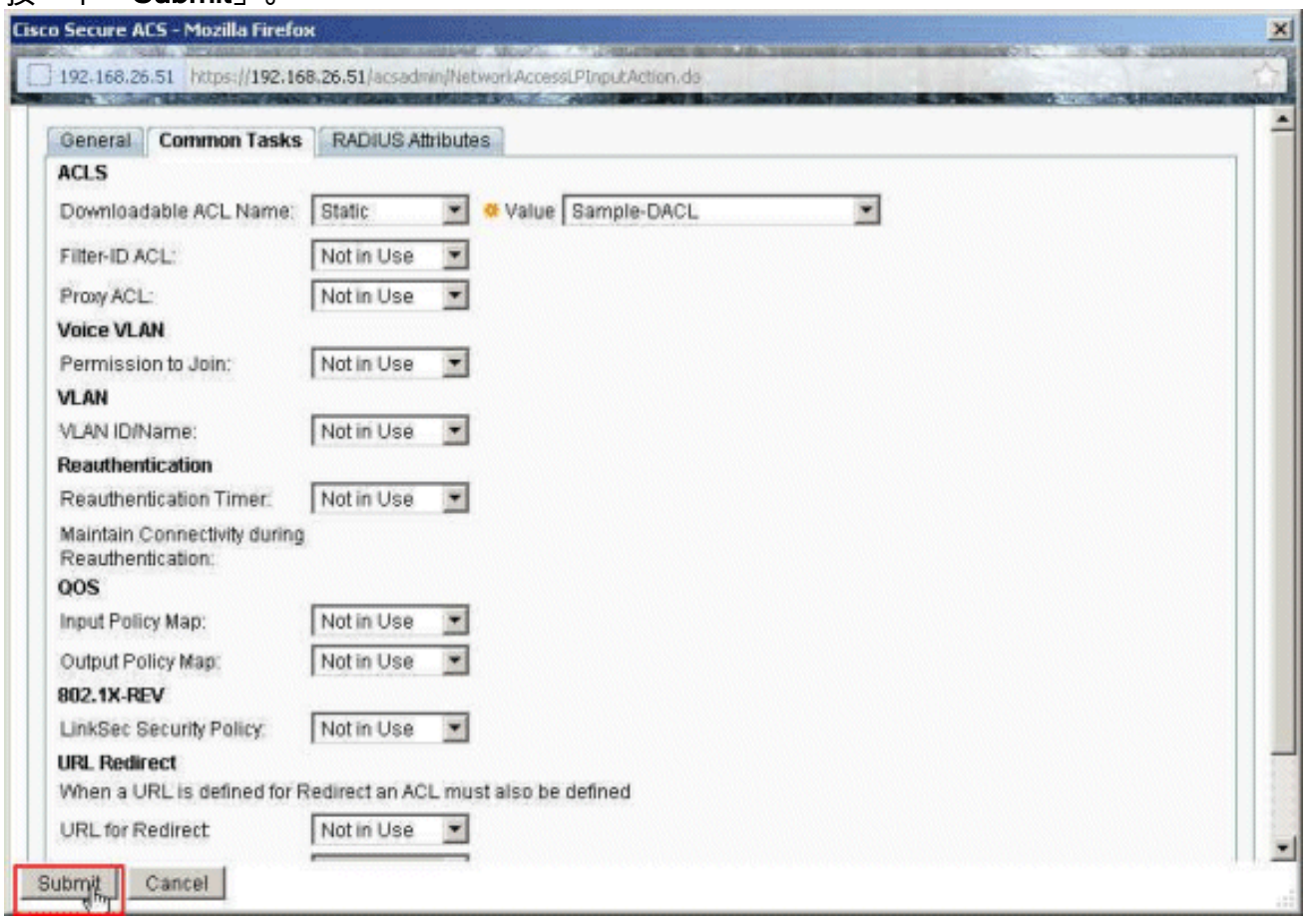
19. 提供授權配置檔案**的名稱。本例中**使用**Sample**-Profile。



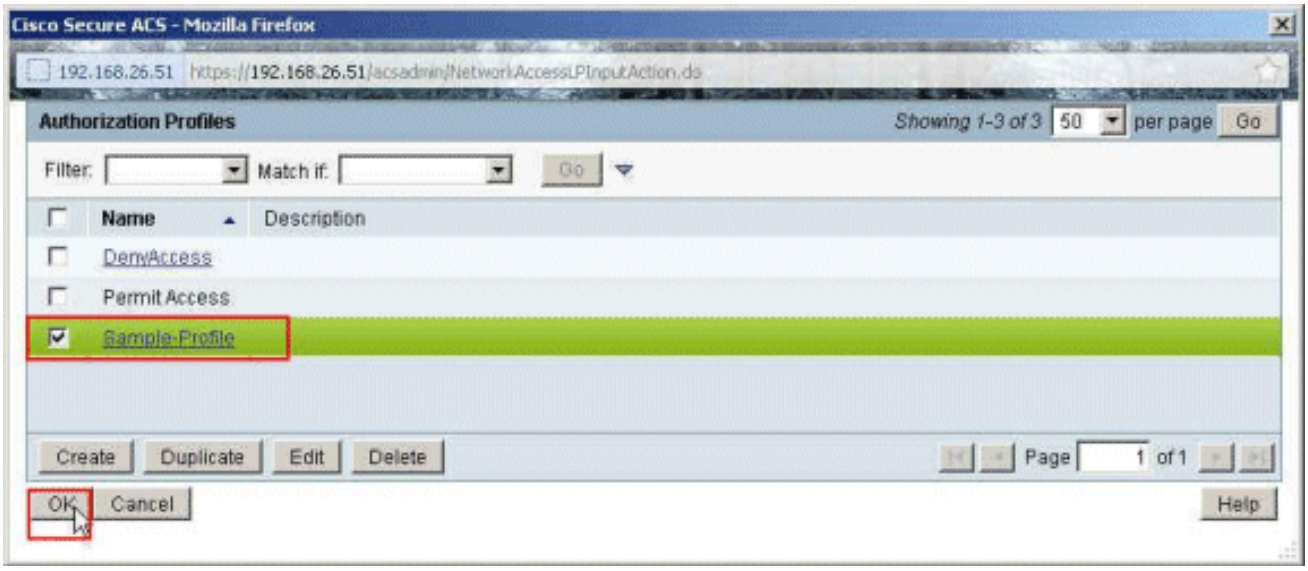
20. 選擇**Common Tasks**頁籤，然後從**Downloadable ACL Name**的下拉選單中選擇**Static**。從值下拉列**表中選擇新建**立的**DACL**（示例 — DACL）。



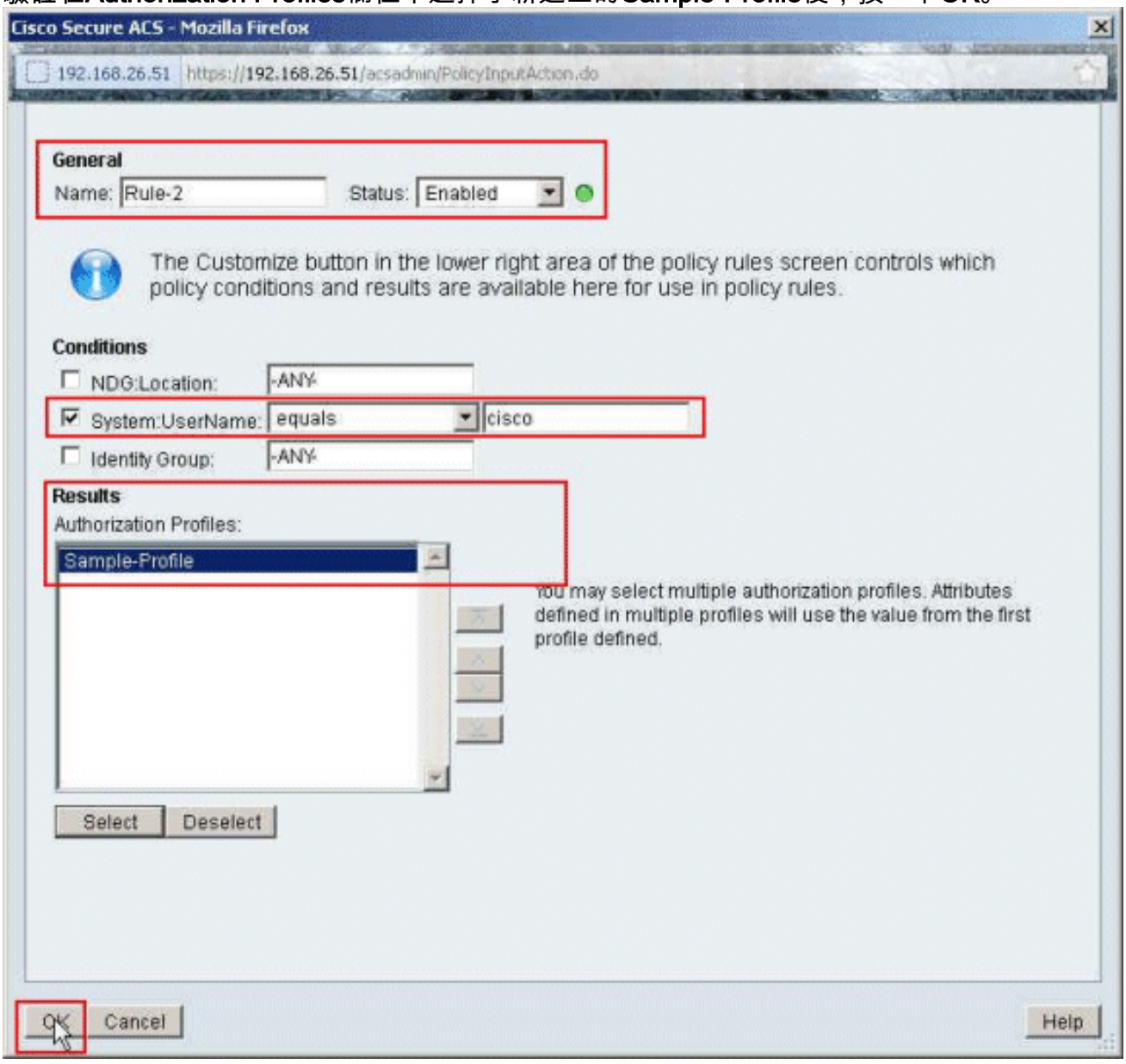
21. 按一下「**Submit**」。



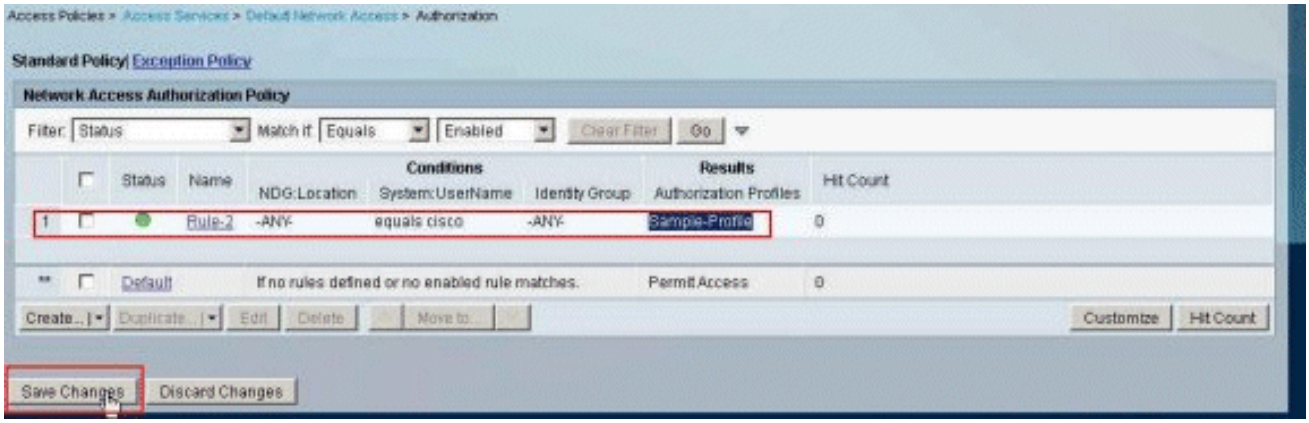
22. 確保選中**Sample-Profile**（新建立的授權配置檔案）旁邊的覈取方塊，然後按一下**OK**。



23. 驗證在**Authorization Profiles**欄位中選擇了新建立的**Sample-Profile**後，按一下**OK**。



24. 驗證新規則(**Rule-2**)是否使用System:UserName **等於cisco**條件和**Sample-Profile** 作為結果建立。按一下「**Save Changes**」。已成功建立規則2。



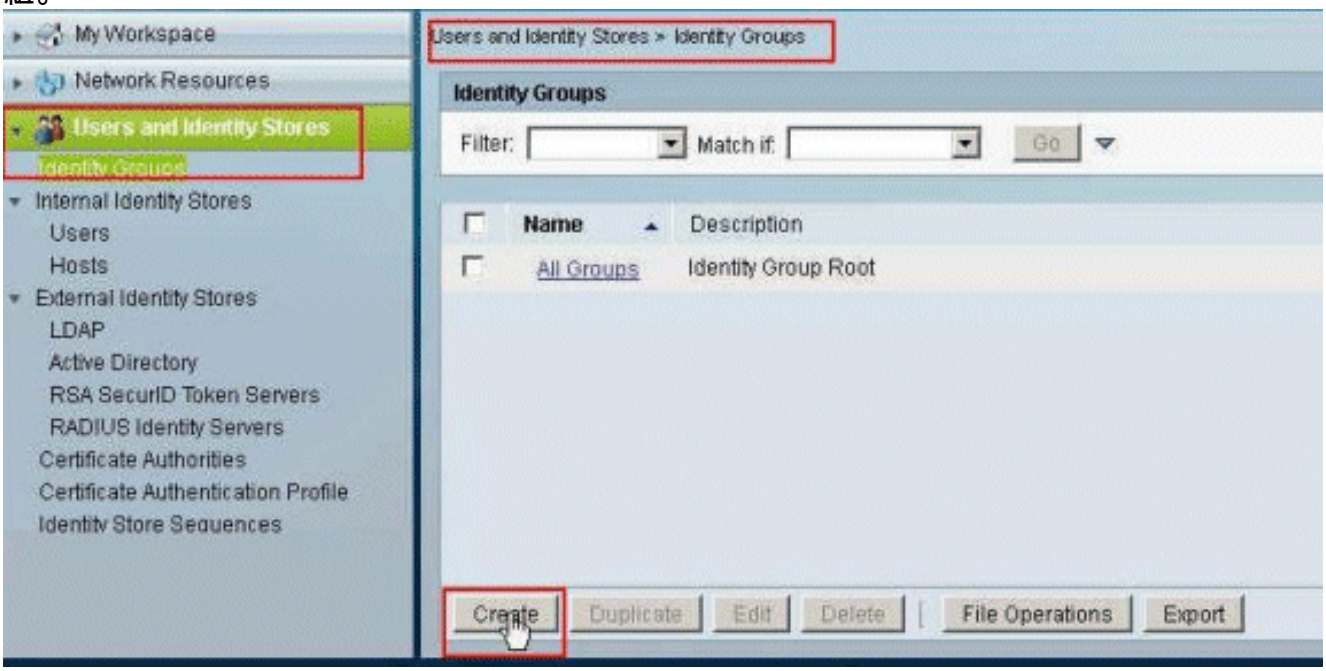
為組的可下載ACL配置ACS

完成為個人使用者的可下載ACL配置ACS的步驟1至12，並執行這些步驟，以便為Cisco Secure ACS中的組配置可下載ACL。

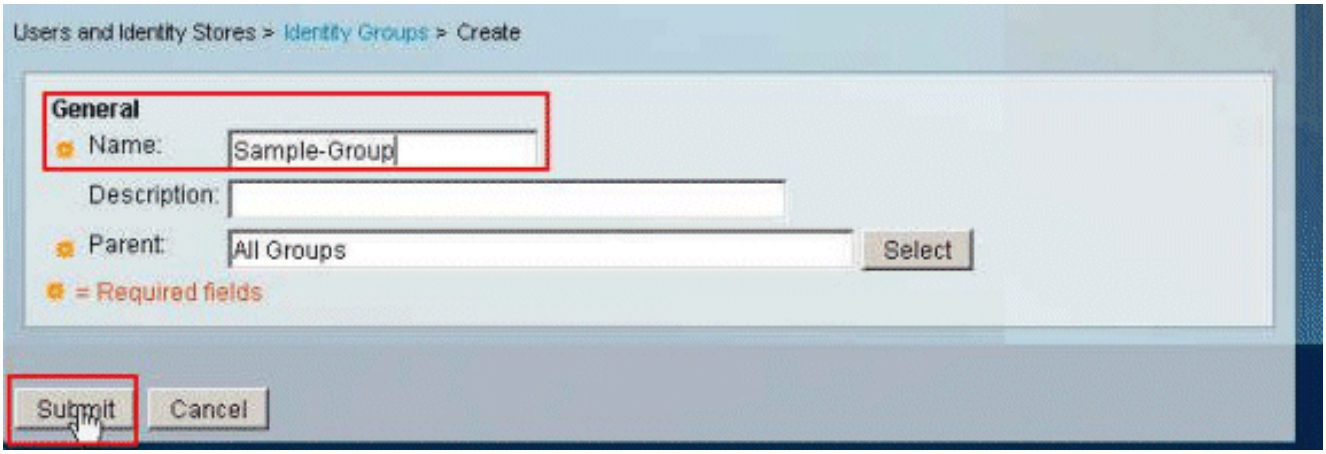
在本示例中，IPsec VPN使用者「cisco」屬於**Sample-Group**。

Sample-Group使用者**cisco**身份驗證成功，RADIUS伺服器向安全裝置傳送可下載的訪問清單。使用者「cisco」只能訪問10.1.1.2伺服器並拒絕所有其他訪問。若要驗證ACL，請參閱使用者/群組的可下載ACL一節。

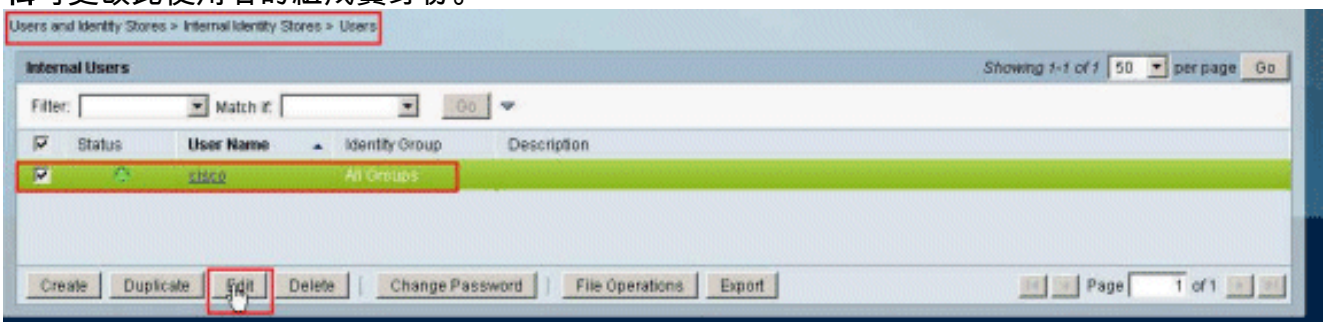
1. 在導航欄中，按一下**Users and Identity Stores > Identity Groups**，然後按一下**Create**以建立新組。



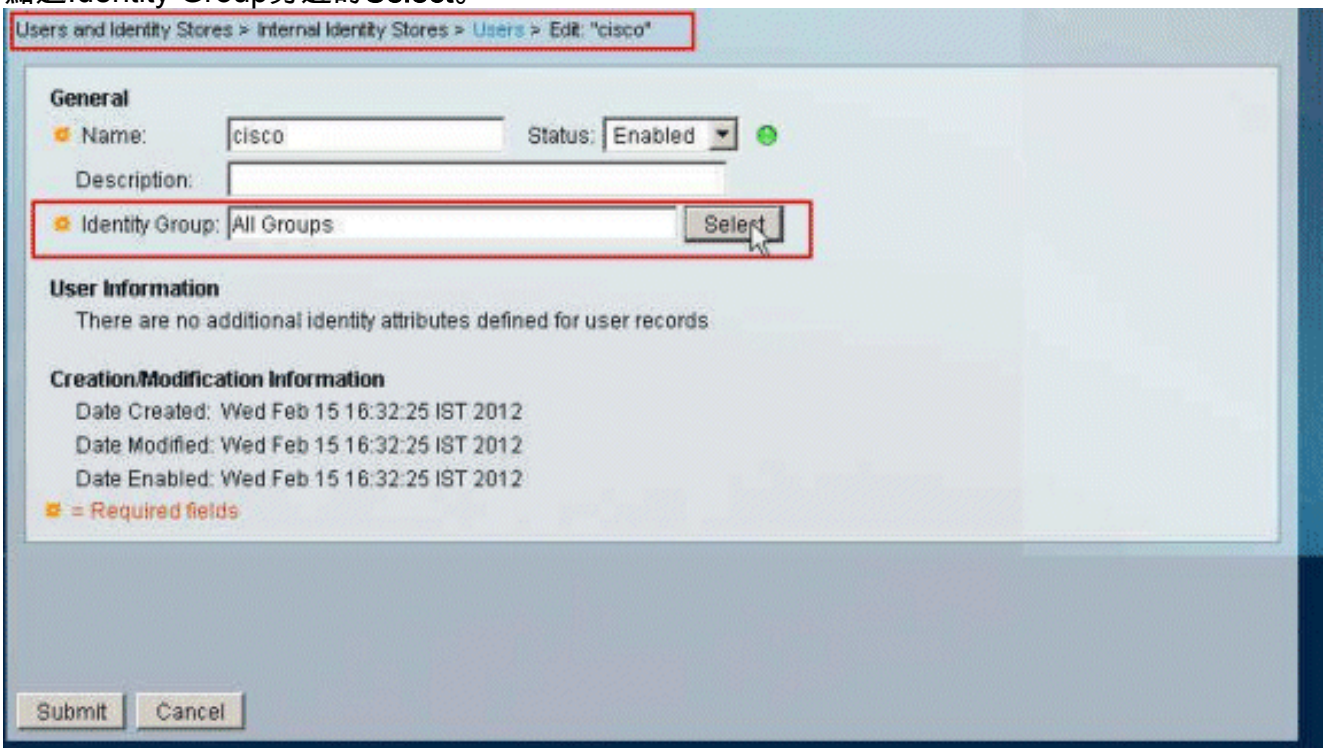
2. 提供組名稱(**Sample-Group**)，然後按一下**Submit**。



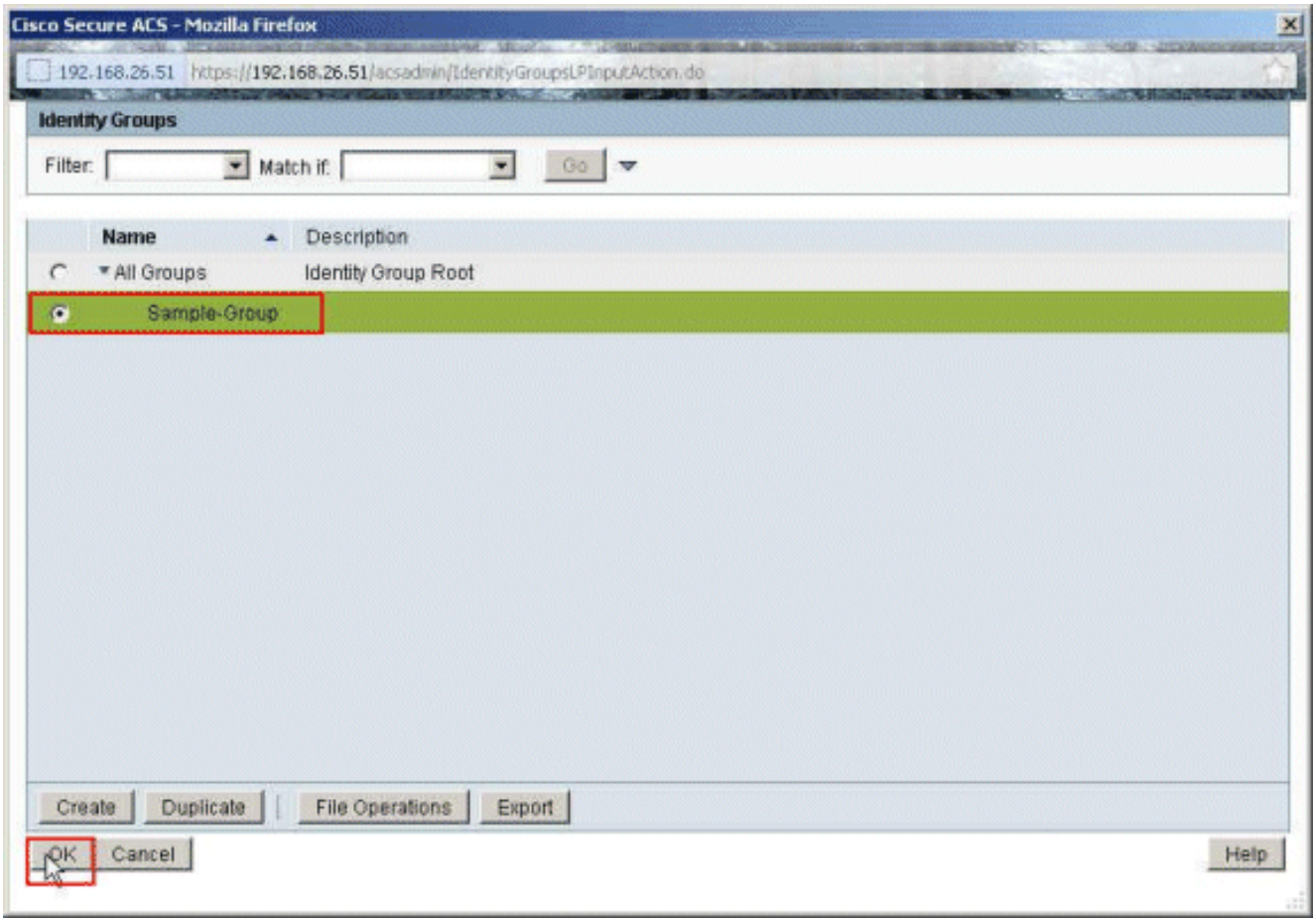
3. 選擇**User Identity Stores > Internal Identity Stores > Users**，然後選擇使用者**cisco**。按一下**編輯**可更改此使用者的組成員身份。



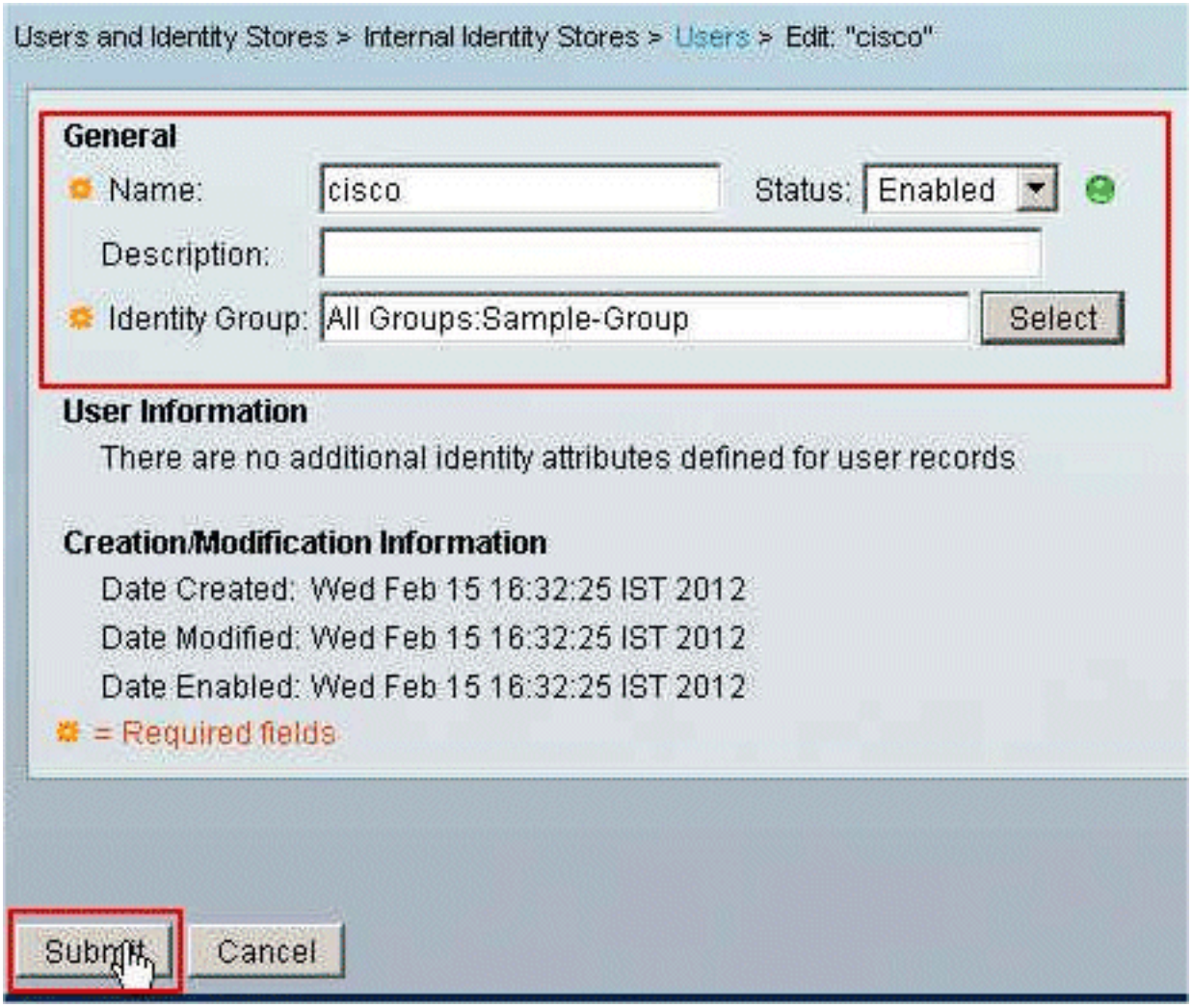
4. 點選Identity Group旁邊的**Select**。



5. 選擇新建立的組(即**Sample-Group**)，然後按一下**OK**。

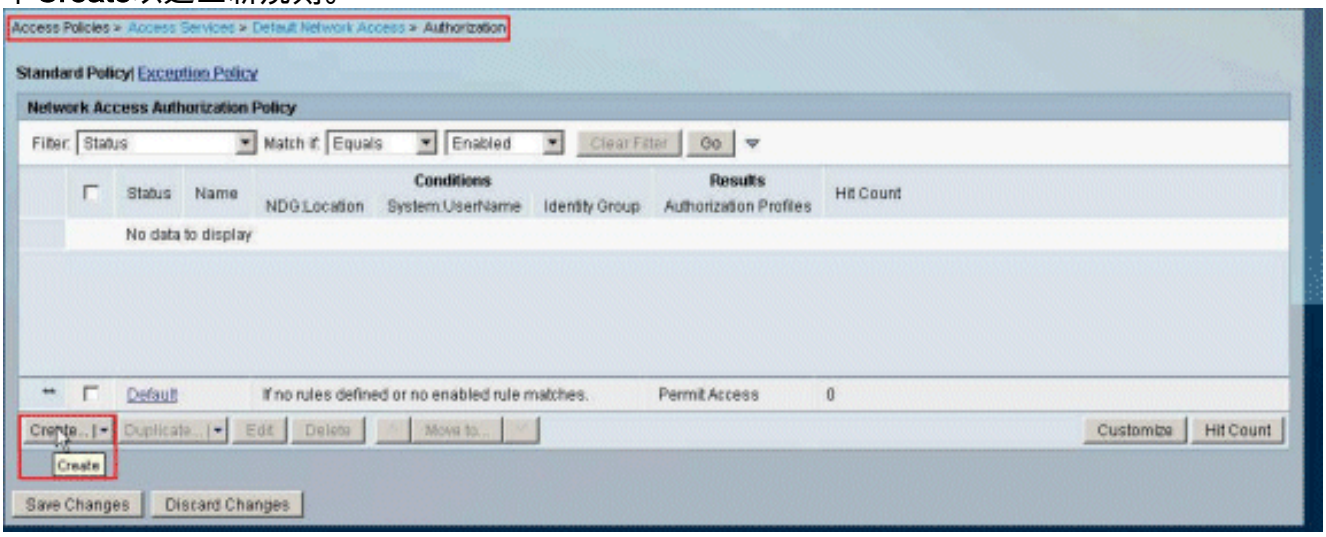


6. 按一下「**Submit**」。

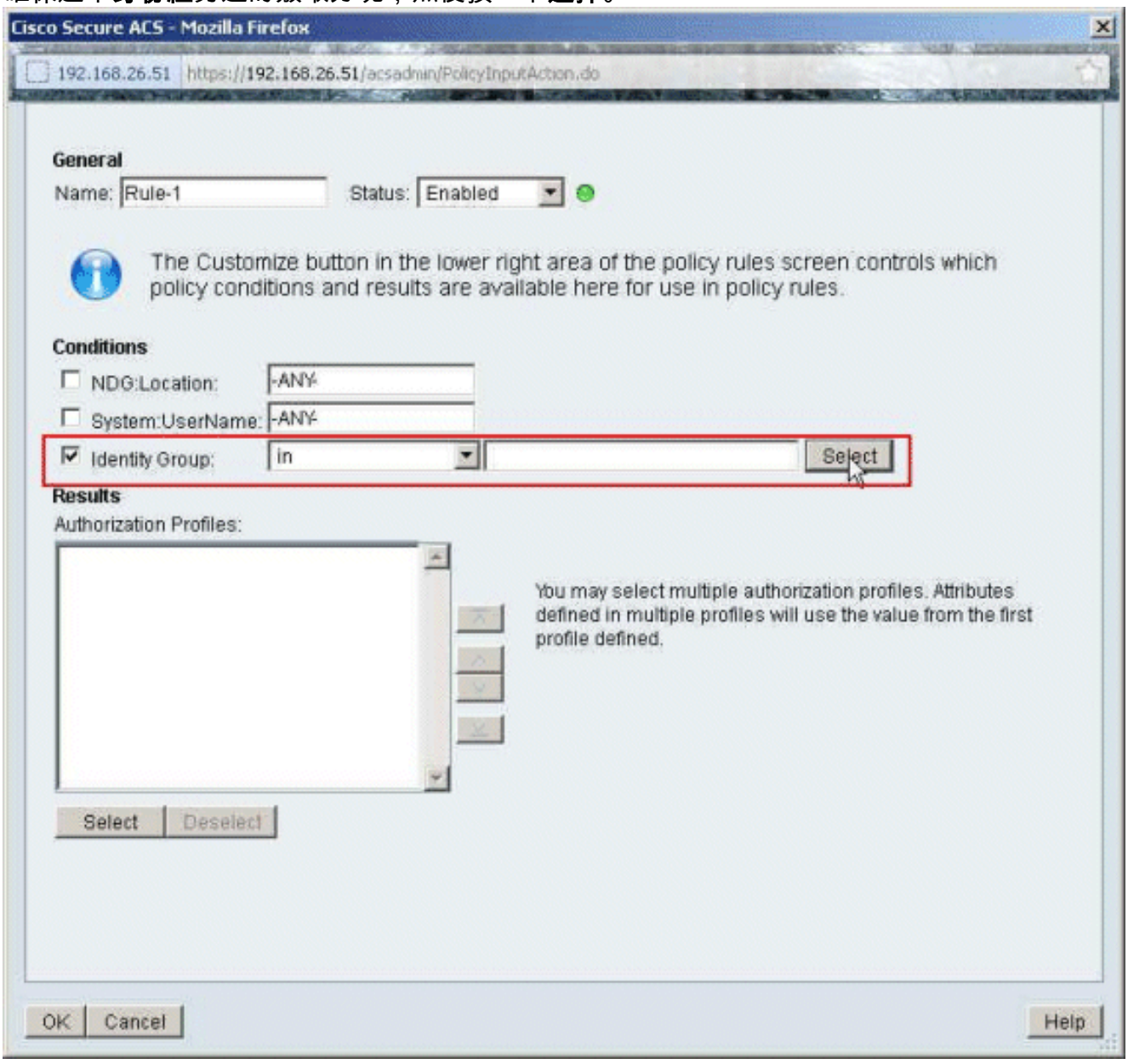


7. 選擇Access Policies > **Access Services** > **Default Network Access** > **Authorization**，然後按一

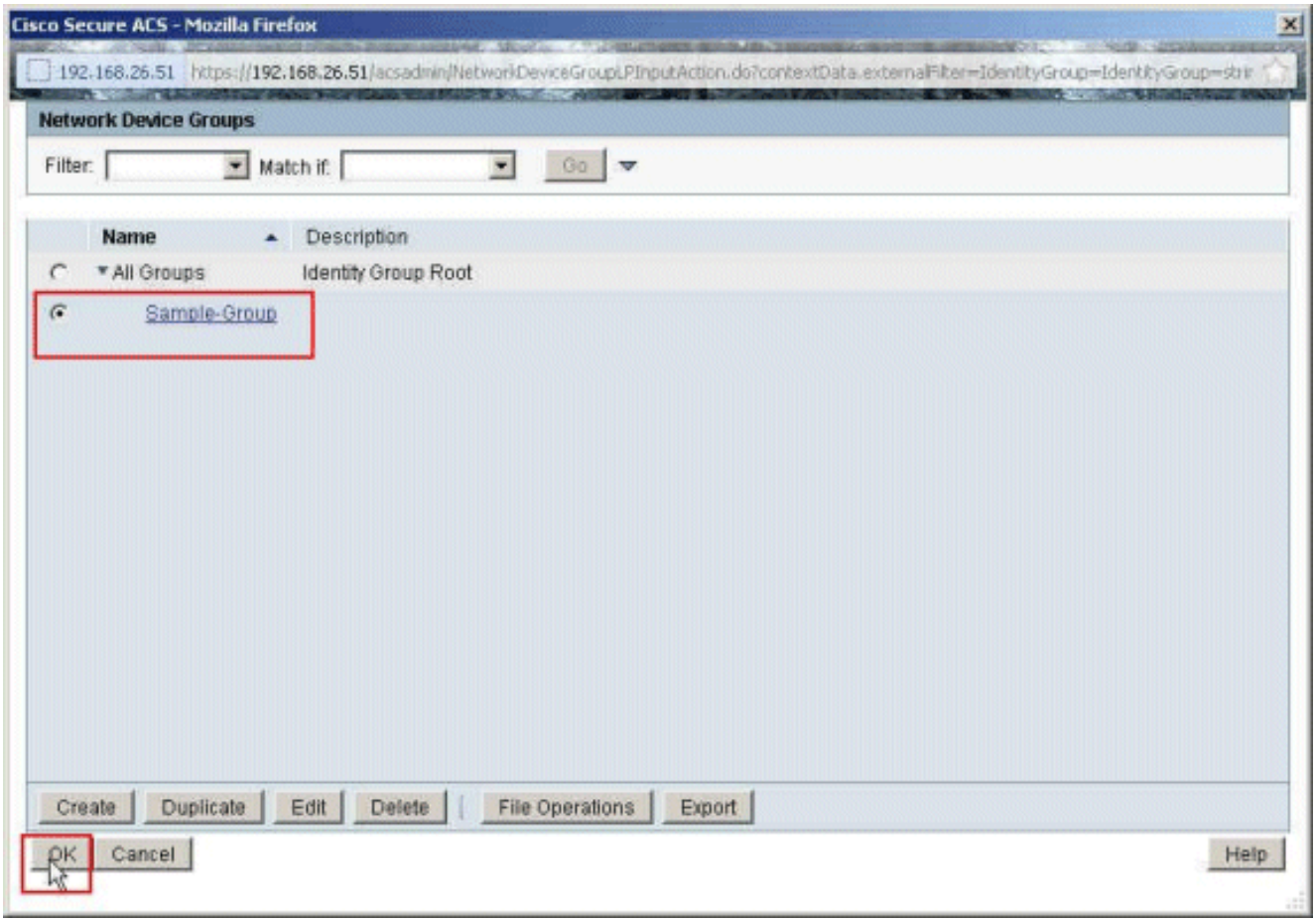
下Create以建立新規則。



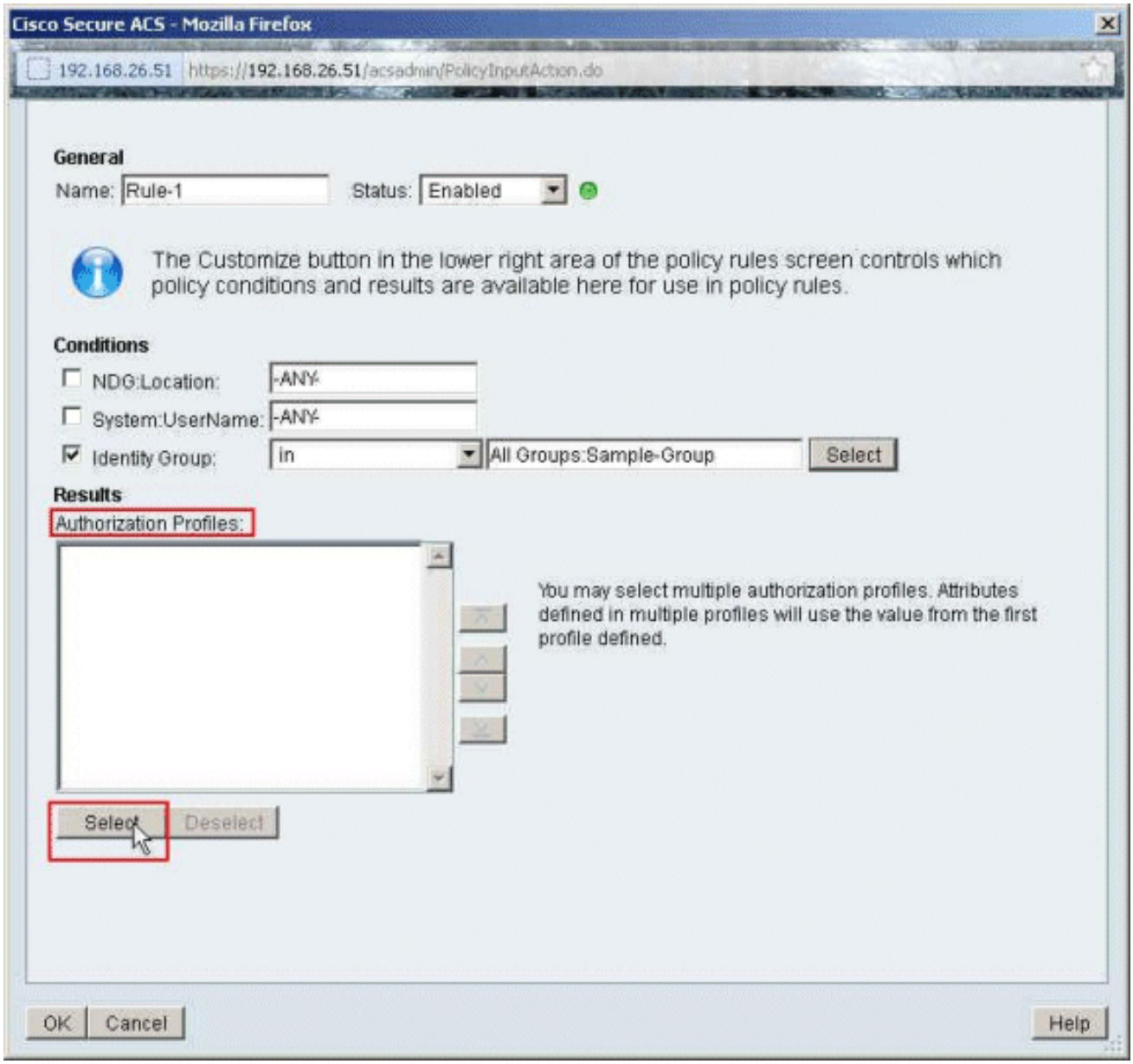
8. 確保選中**身份組**旁邊的覈取方塊，然後按一下**選擇**。



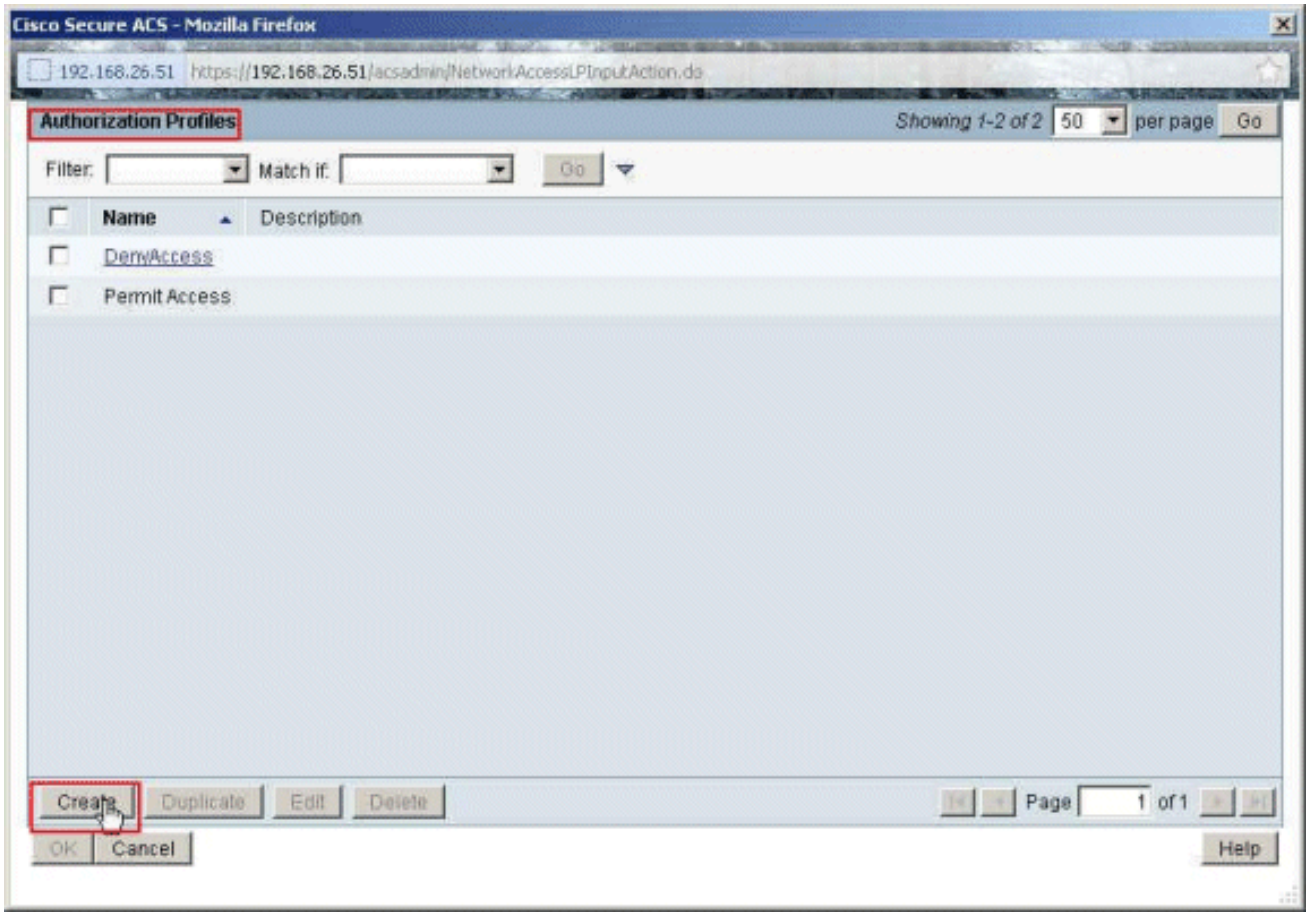
9. 選擇Sample-Group，然後按一下OK。



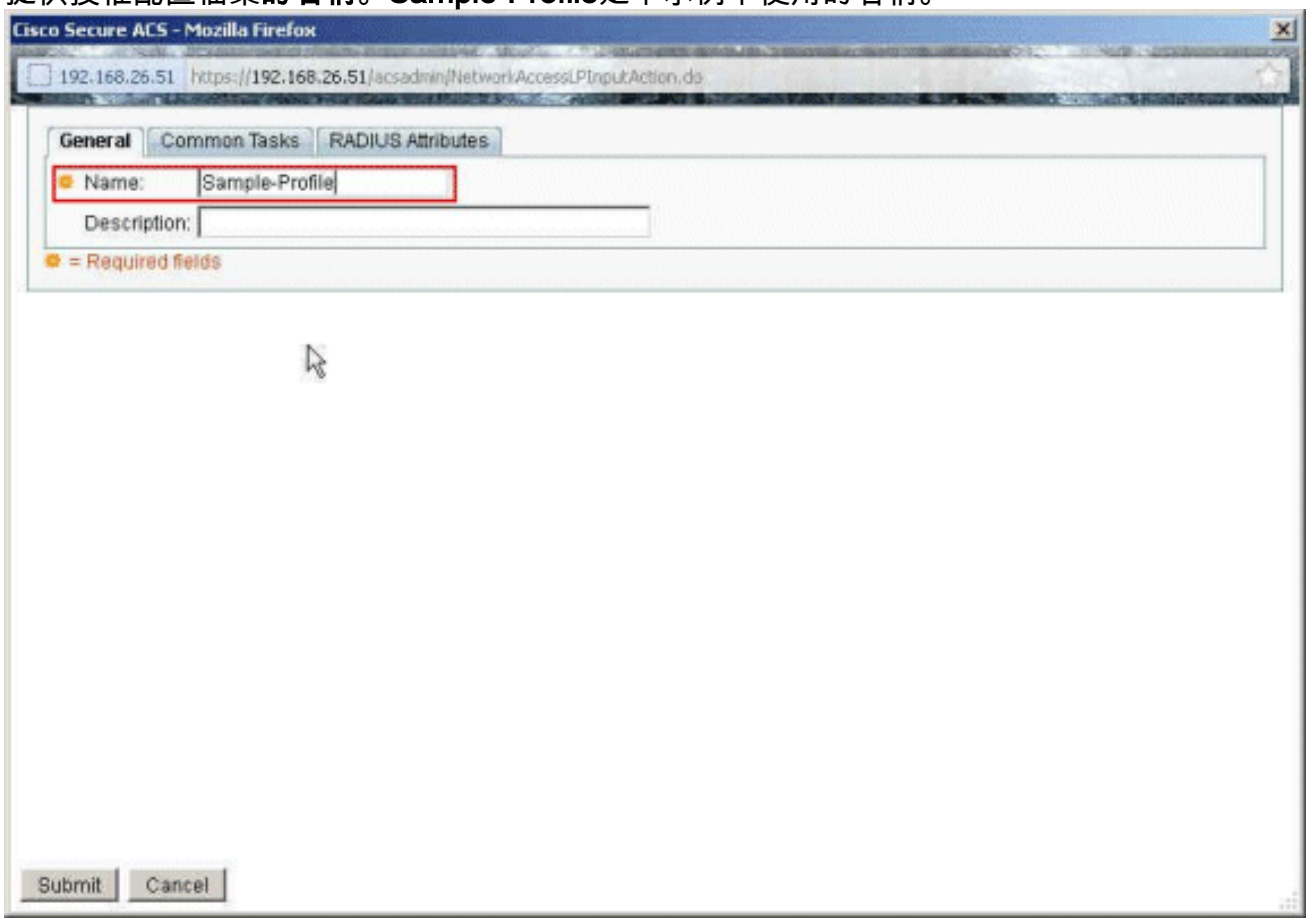
10. 在Authorization Profiles部分中按一下**Select**。



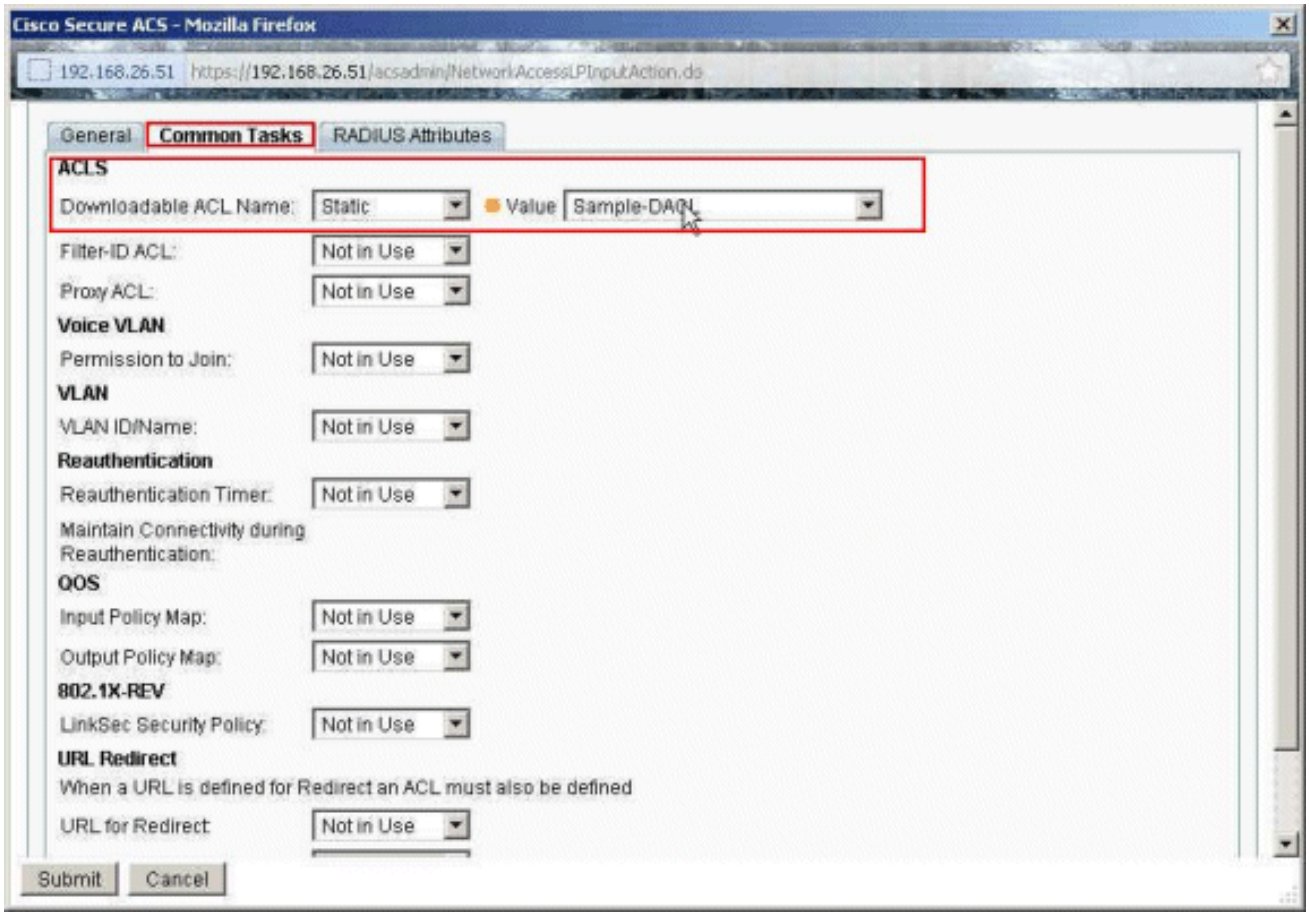
11. 按一下「**Create**」以建立一個新的授權設定檔。



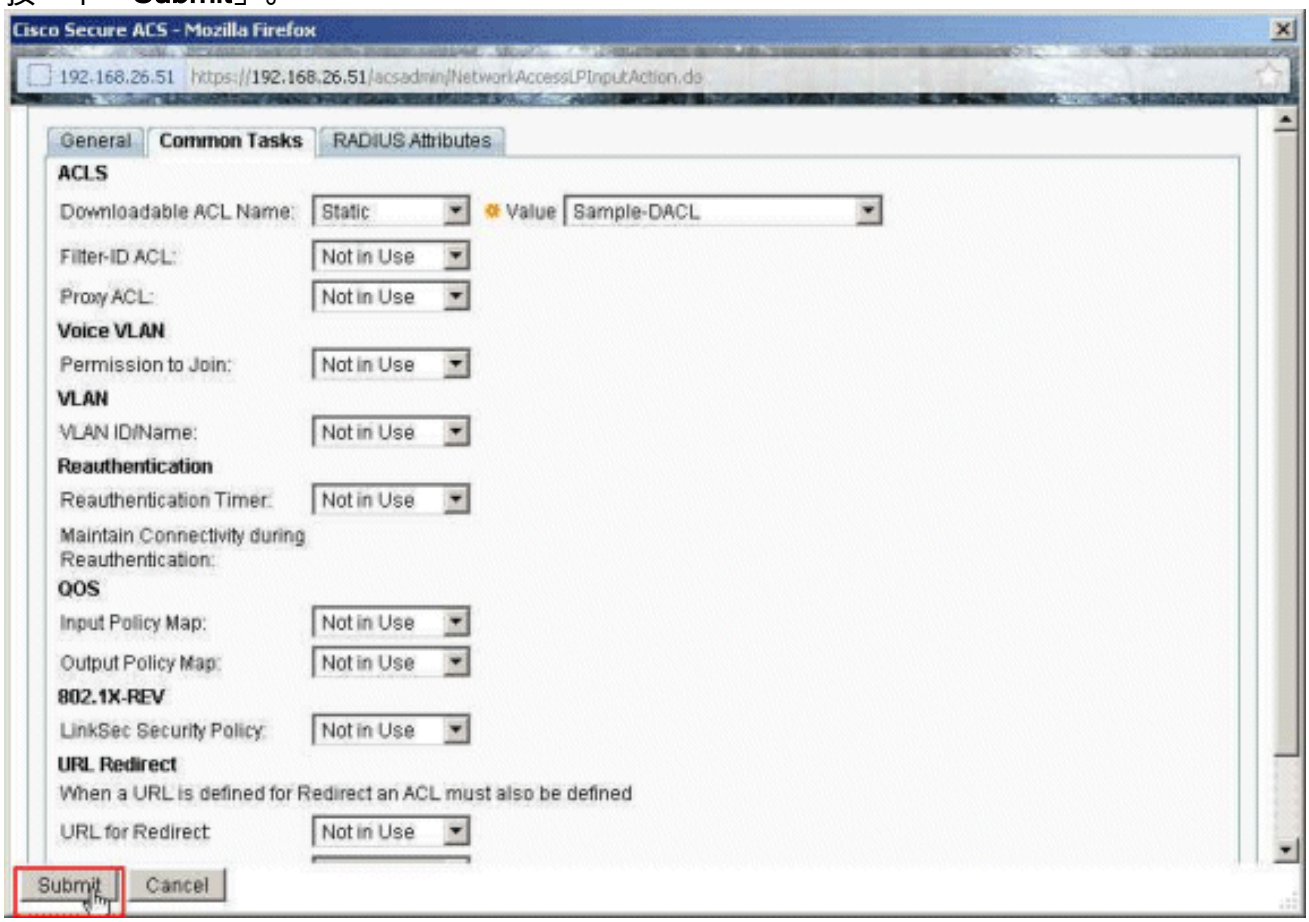
12. 提供授權配置檔案**的名稱。Sample-Profile**是本示例中使用的名稱。



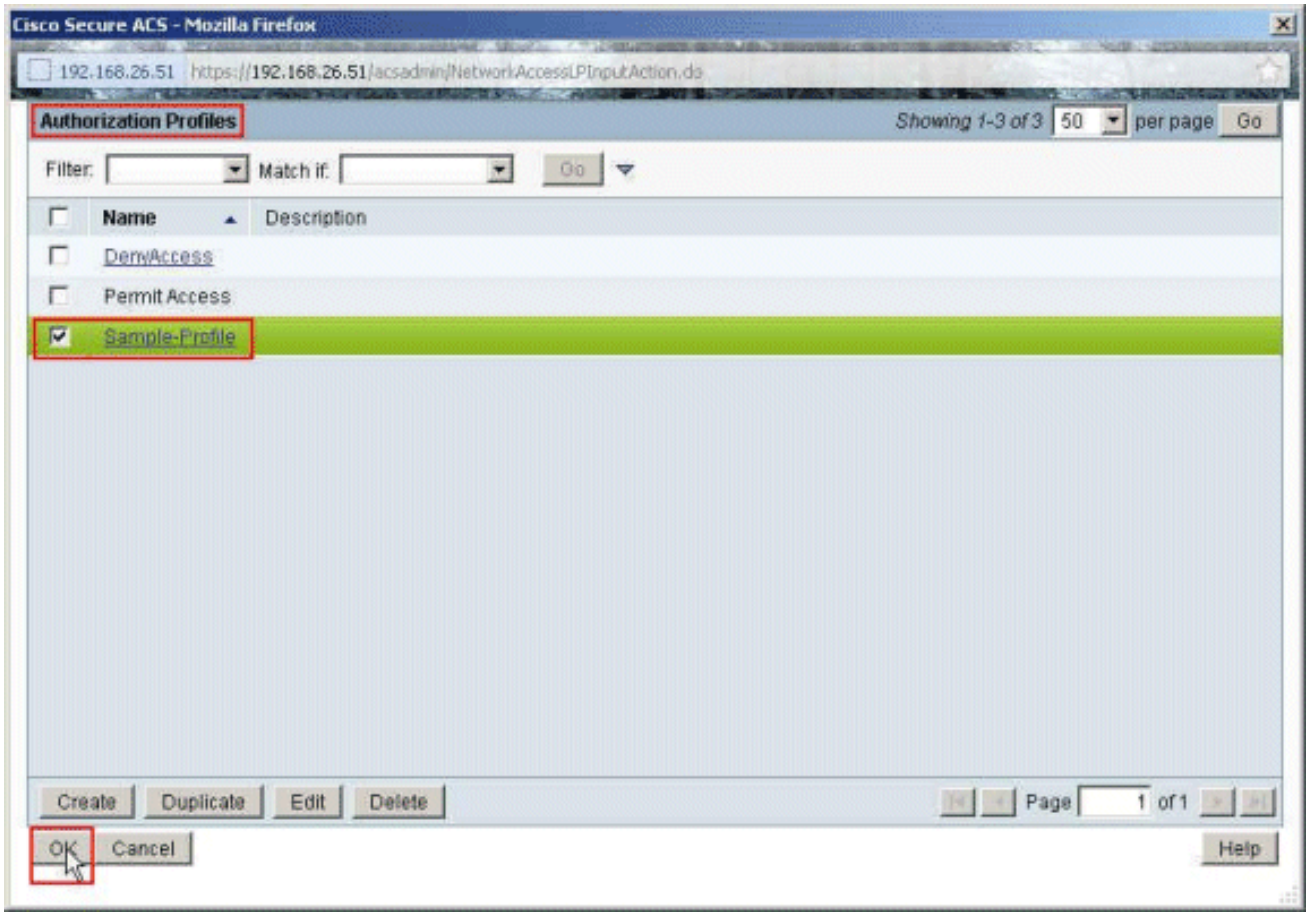
13. 選擇**Common Tasks**頁籤，然後從**Downloadable ACL Name**的下拉選單中選擇**Static**。從值下拉列**表中選擇新創**建的**DACL**（示例 — DACL）。



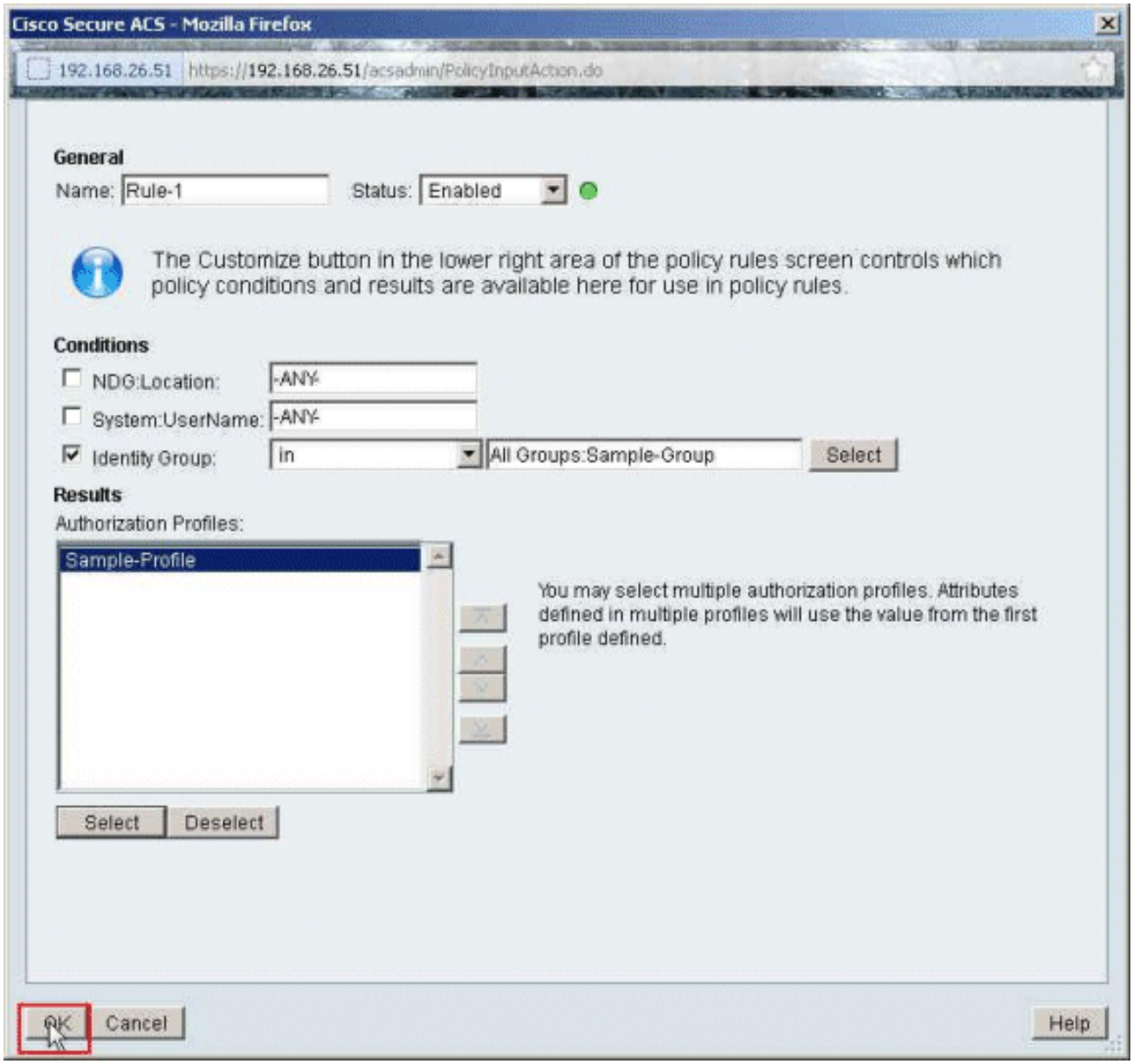
14. 按一下「**Submit**」。



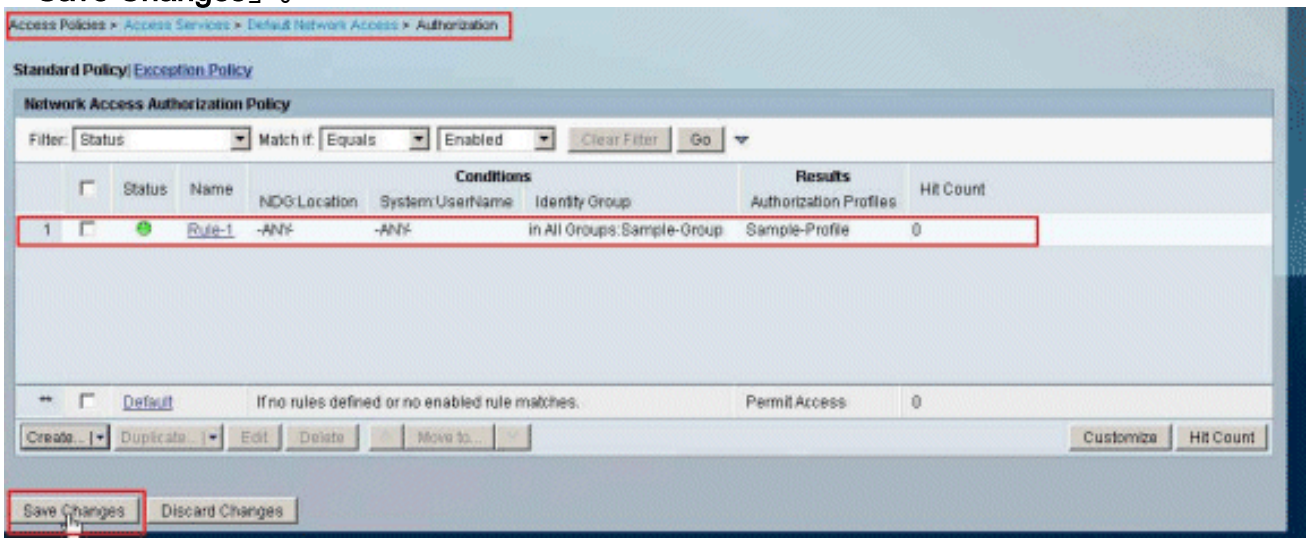
15. 選擇先前建立的Authorization Profile **Sample-Profile**，然後按一下**OK**。


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. 按一下「**OK**」（確定）。



17. 驗證是否建立了**Rule-1**，其中條件為身份組**Sample-Group**，結果為**Sample-Profile**。按一下「**Save Changes**」。

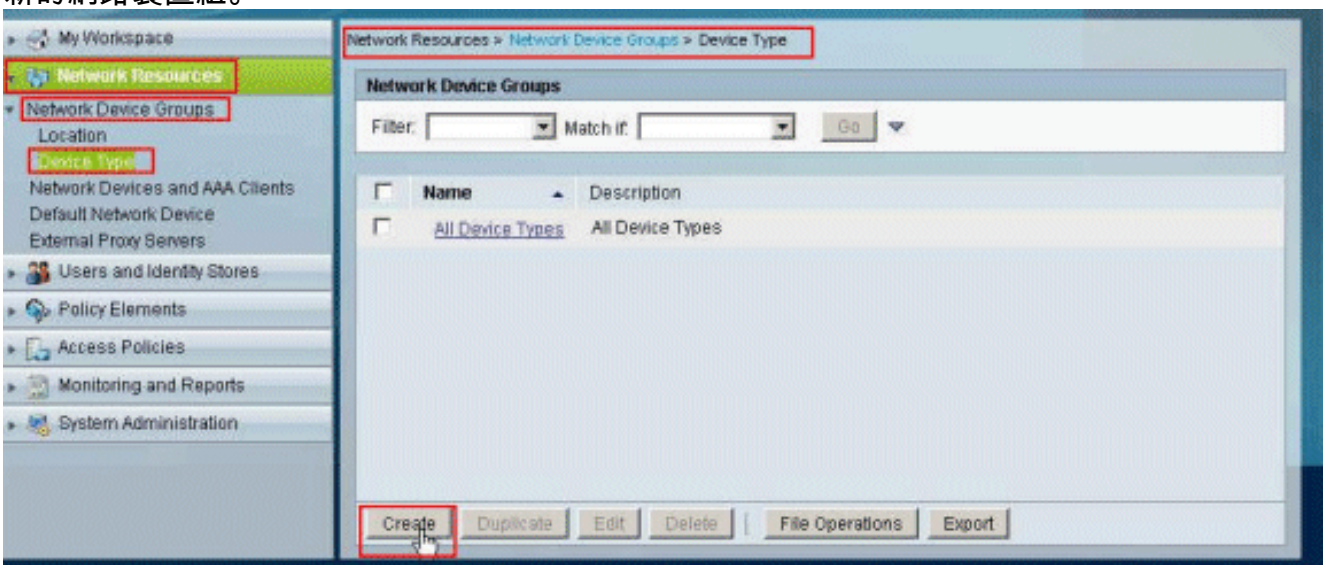


為網路裝置組的可下載ACL配置ACS

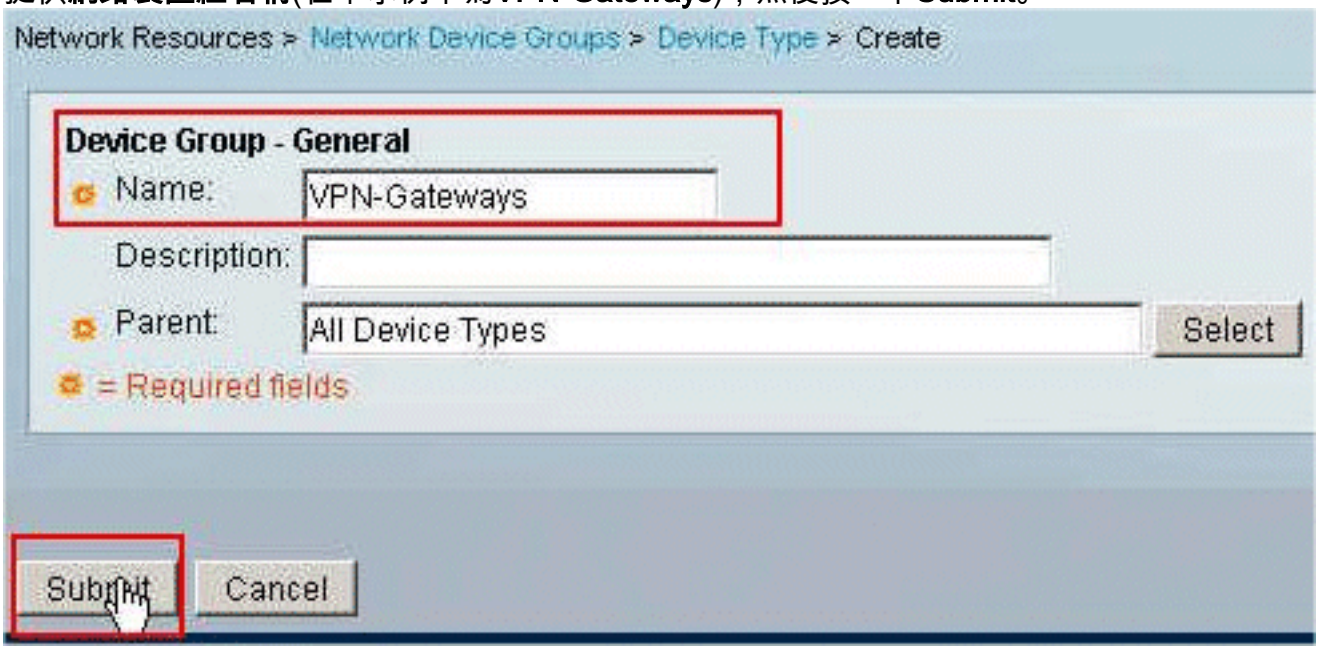
完成為個人使用者的可下載ACL配置ACS的步驟1至12，並執行這些步驟，以便為Cisco Secure ACS中的網路裝置組配置可下載ACL。

在本示例中，RADIUS客戶端(ASA)屬於網路裝置組**VPN-Gateways**。來自ASA的使用者「cisco」的VPN身份驗證請求成功進行身份驗證，並且RADIUS伺服器向安全裝置傳送可下載訪問清單。使用者「cisco」只能訪問10.1.1.2伺服器並拒絕所有其他訪問。若要驗證ACL，請參閱使用者/群組的可下載ACL一節。

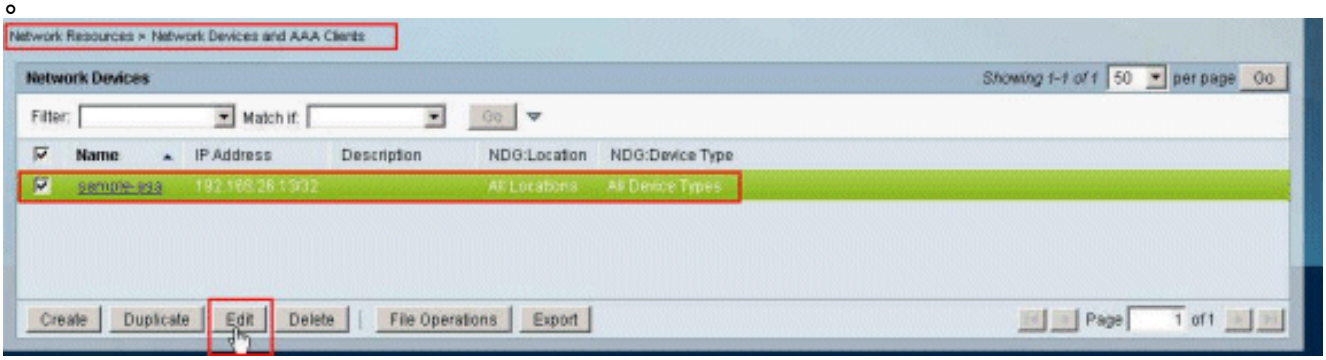
1. 選擇**Network Resources > Network Device Groups > Device Type**，然後按一下**Create**以建立新的網路裝置組。



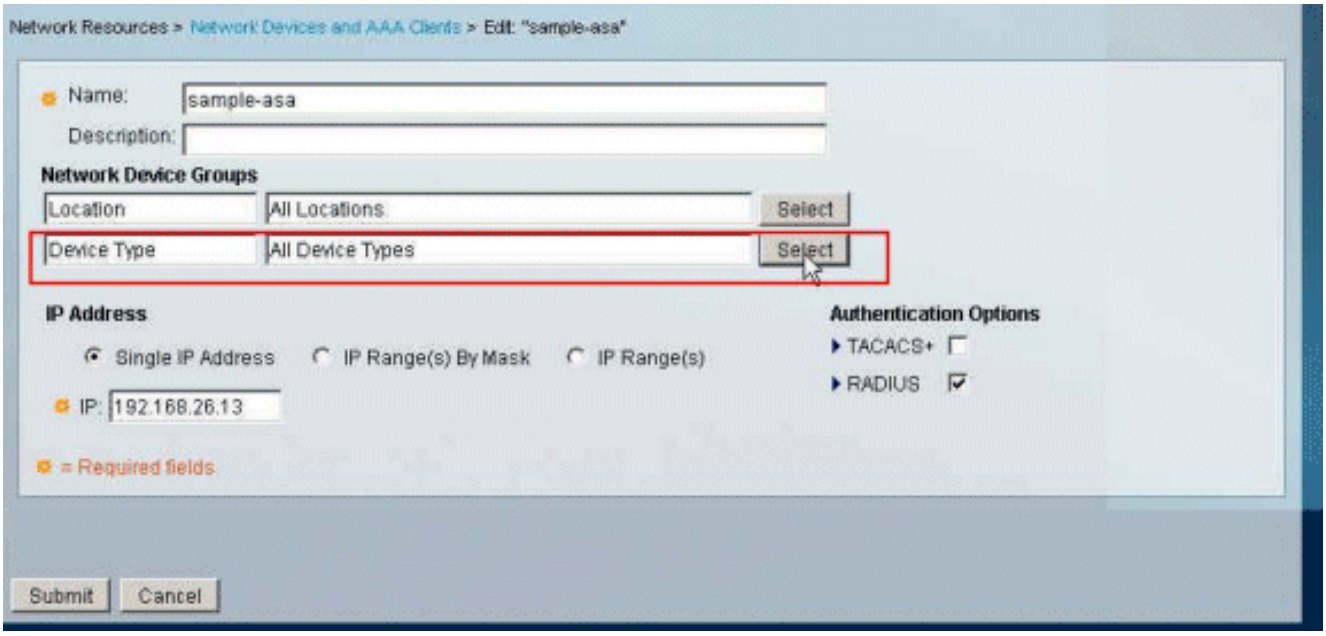
2. 提供**網路裝置組名稱**(在本示例中為**VPN-Gateways**)，然後按一下**Submit**。



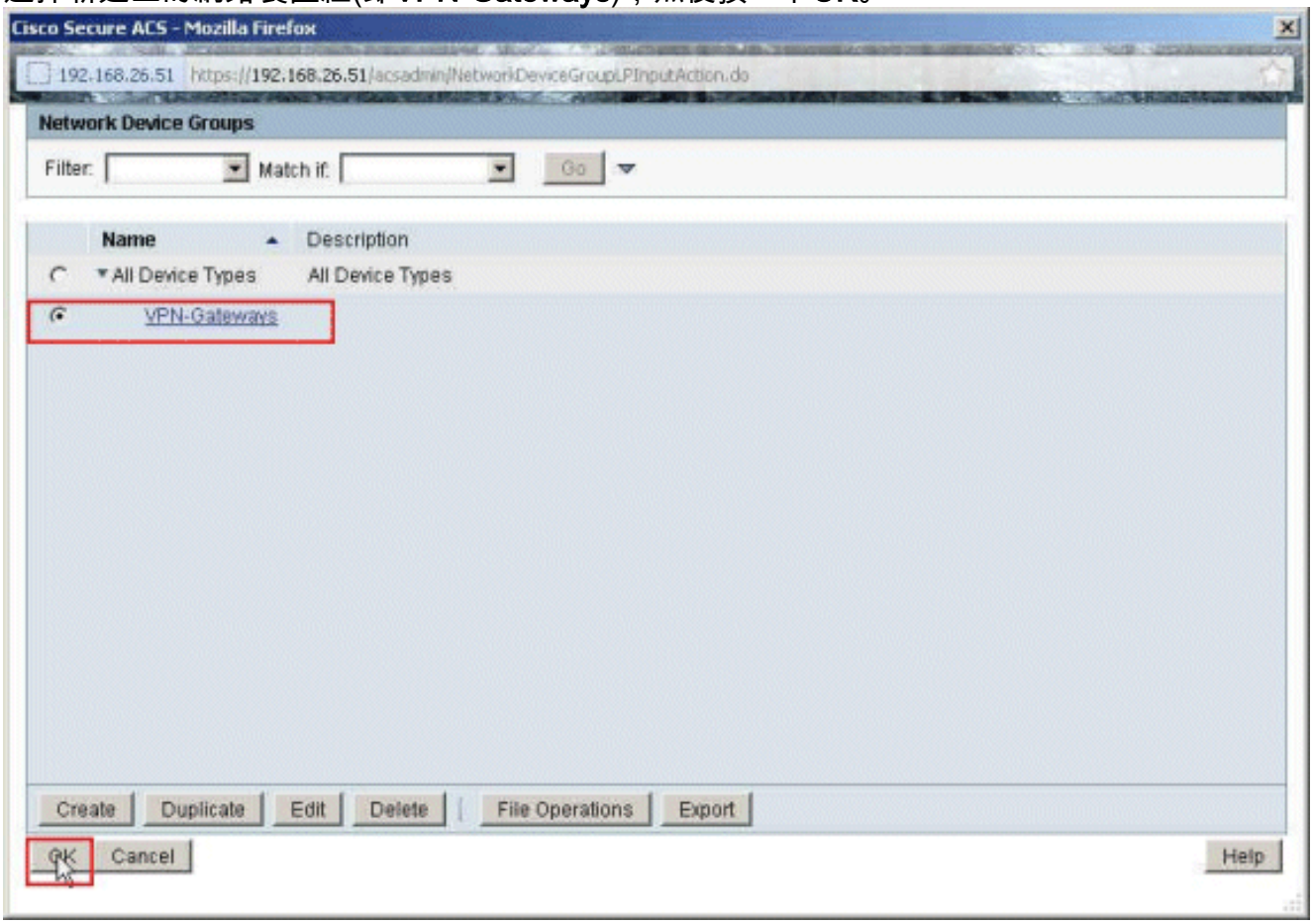
3. 選擇**Network Resources > Network Devices and AAA Clients**，然後選擇之前建立的**RADIUS** Client **sample-asa**。按一下「**Edit**」以變更此RADIUS使用者端(asa)的**網路裝置群組**成員身分。



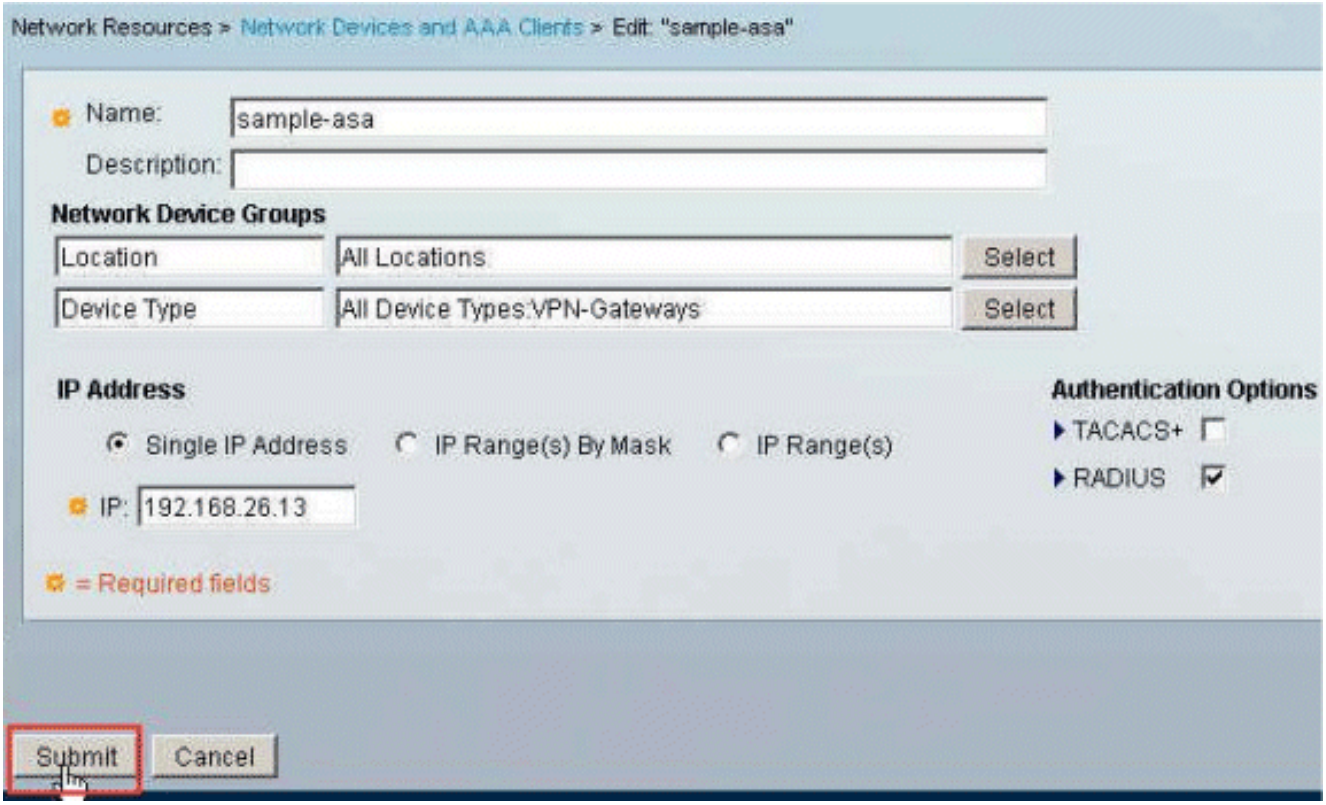
4. 按一下「Device Type（裝置型別）」旁邊的**Select**。



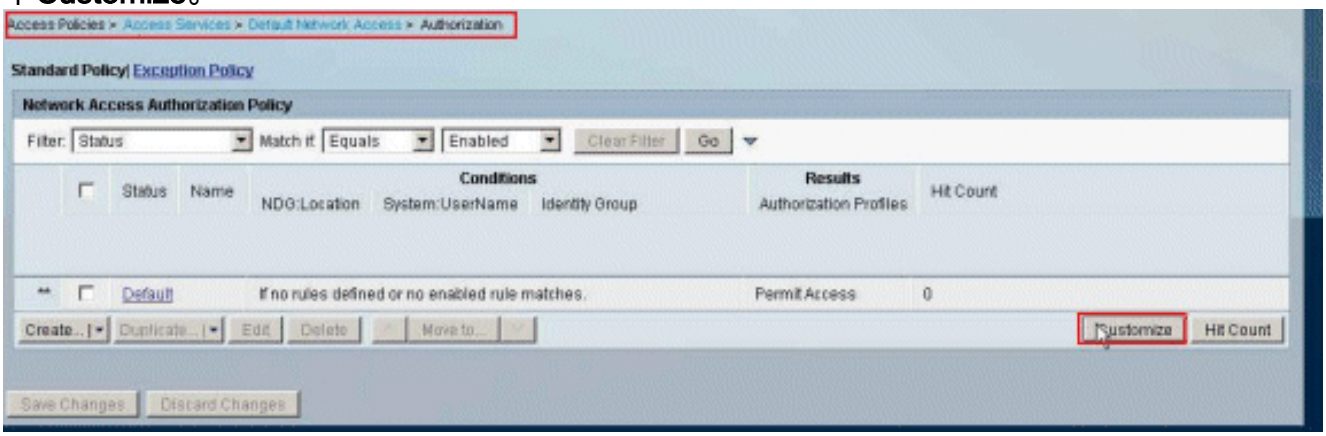
5. 選擇新建立的網路裝置組(即VPN-Gateways)，然後按一下OK。



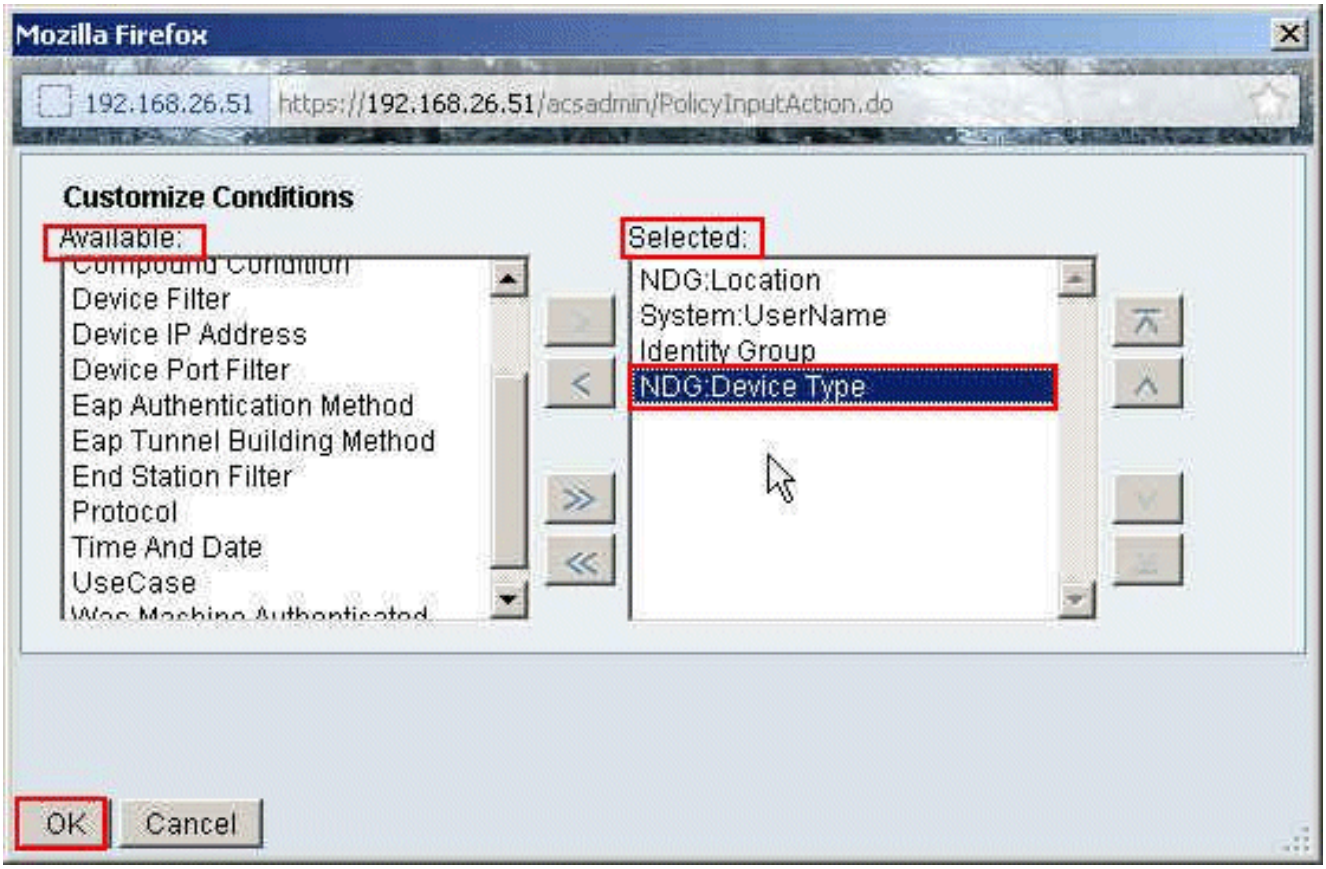
6. 按一下「Submit」。



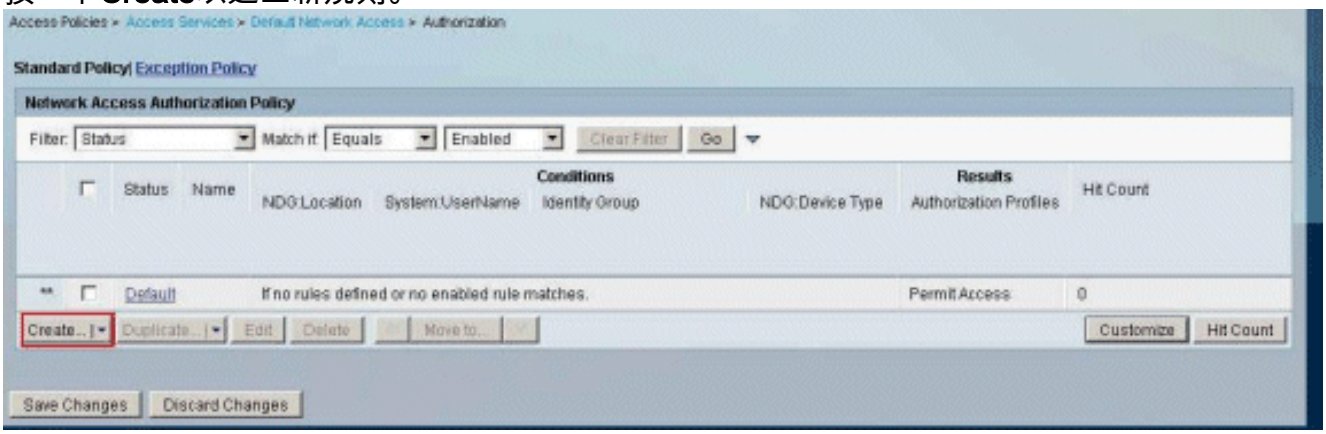
7. 選擇Access Policies > **Access Services > Default Network Access > Authorization**，然後按一下**Customize**。



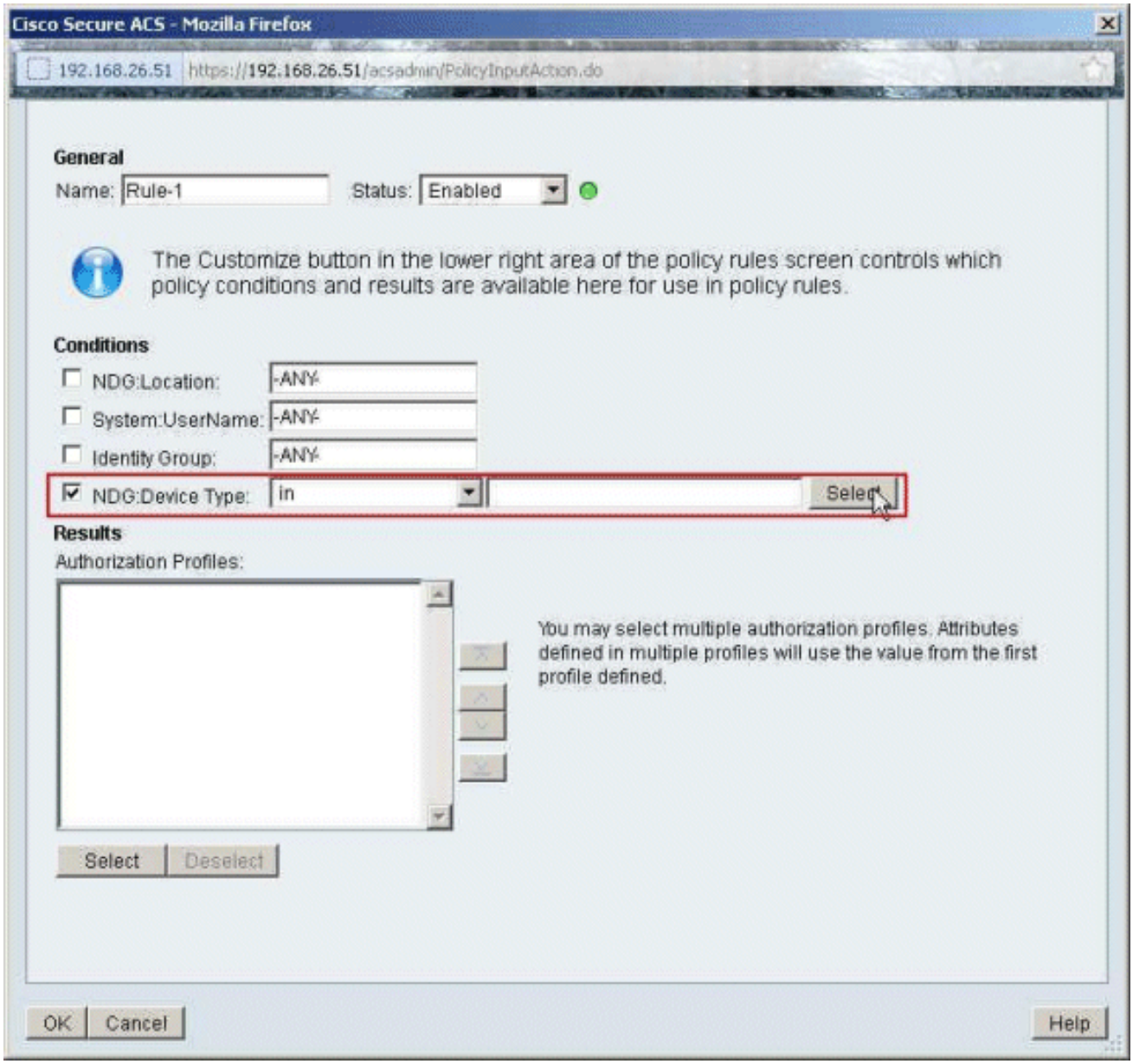
8. 將**NDG:Device Type**從**Available**部分移動到**Selected**部分，然後按一下**OK**。



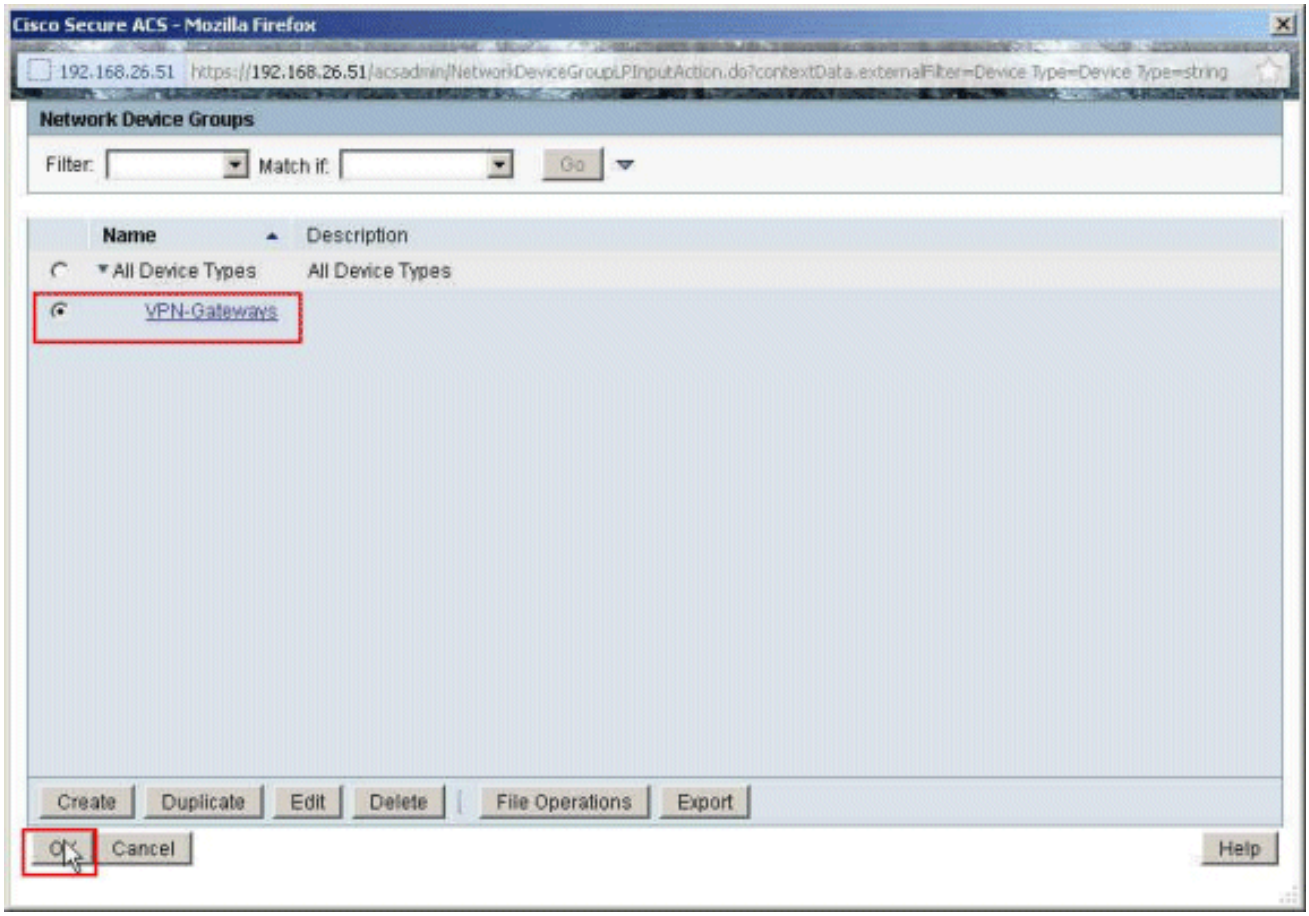
9. 按一下**Create**以建立新規則。



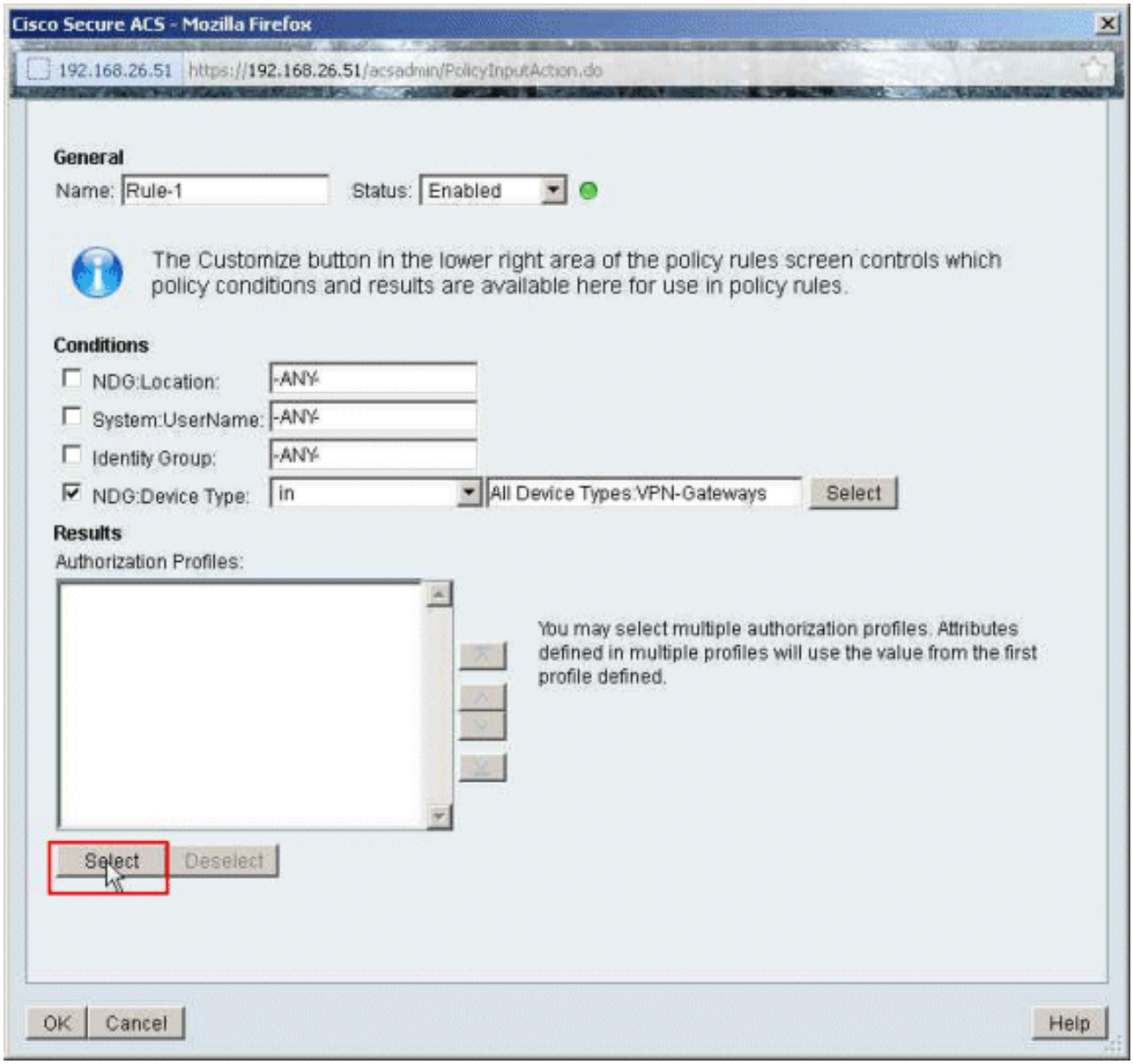
10. 確保選中**NDG:Device Type**旁邊的覈取方塊，然後從下拉選單中選擇**in**。按一下「**Select**」。



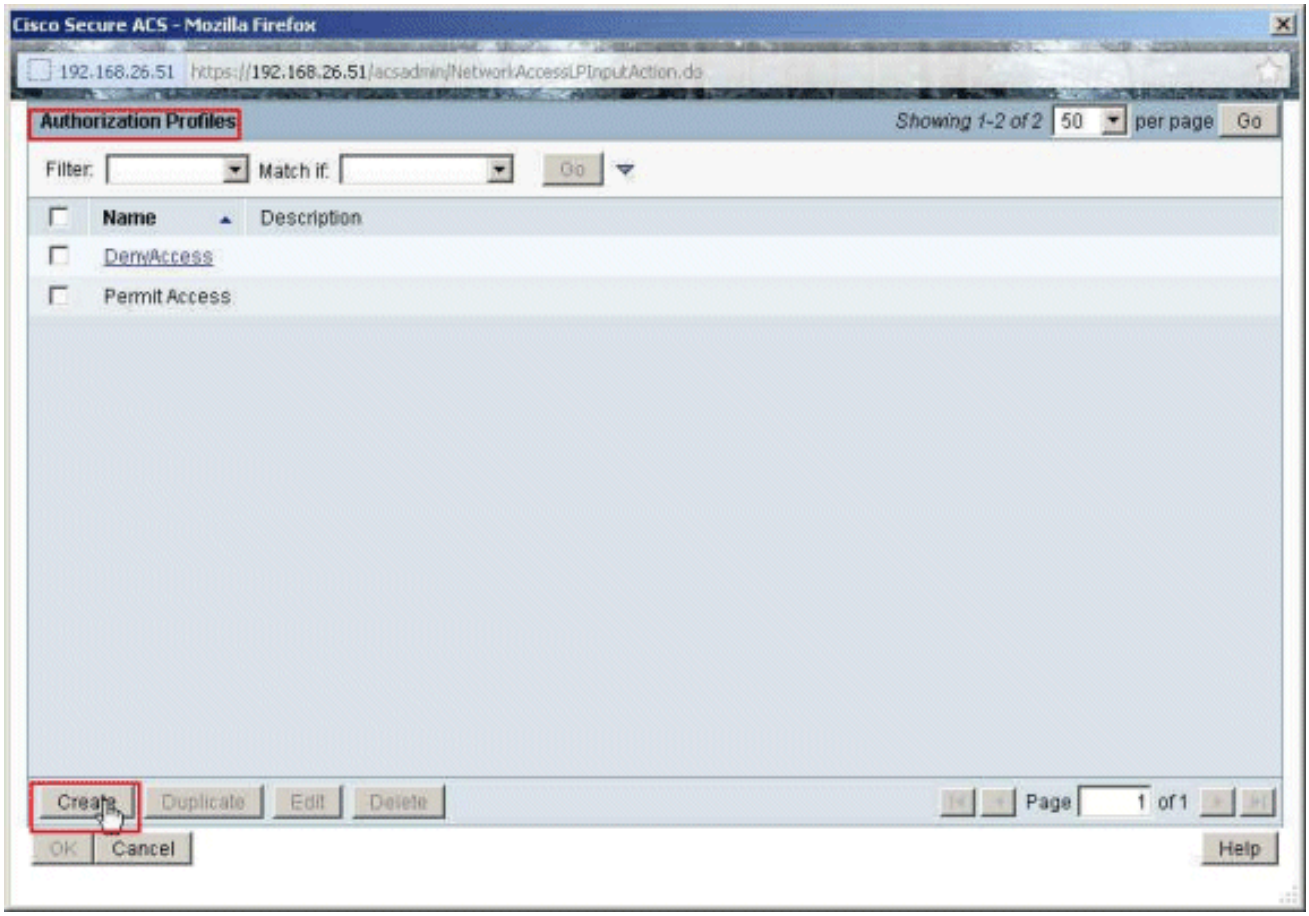
11. 選擇之前建立的**Network Device Group VPN-Gateways**，然後按一下**OK**。



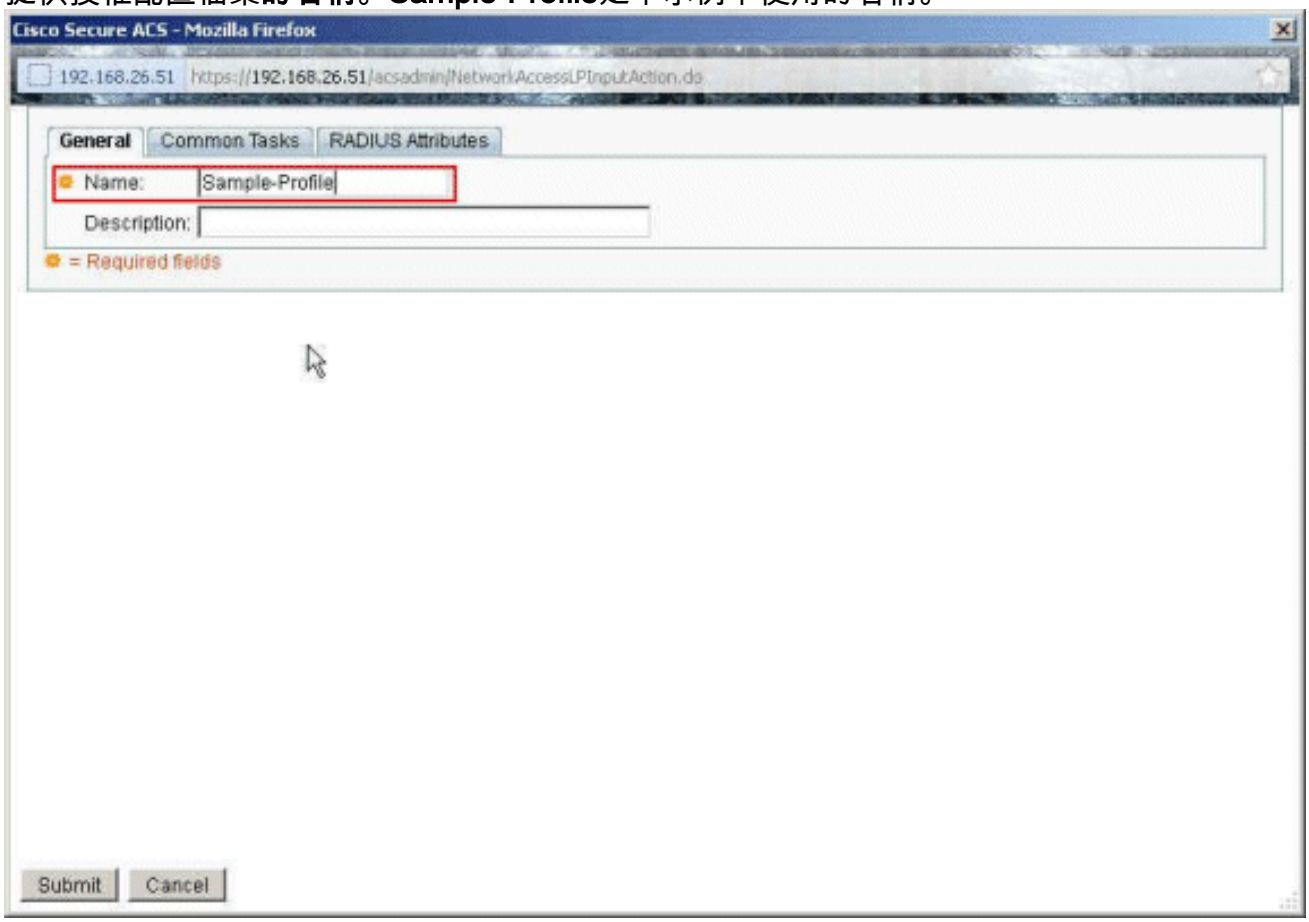
12. 按一下「**Select**」。



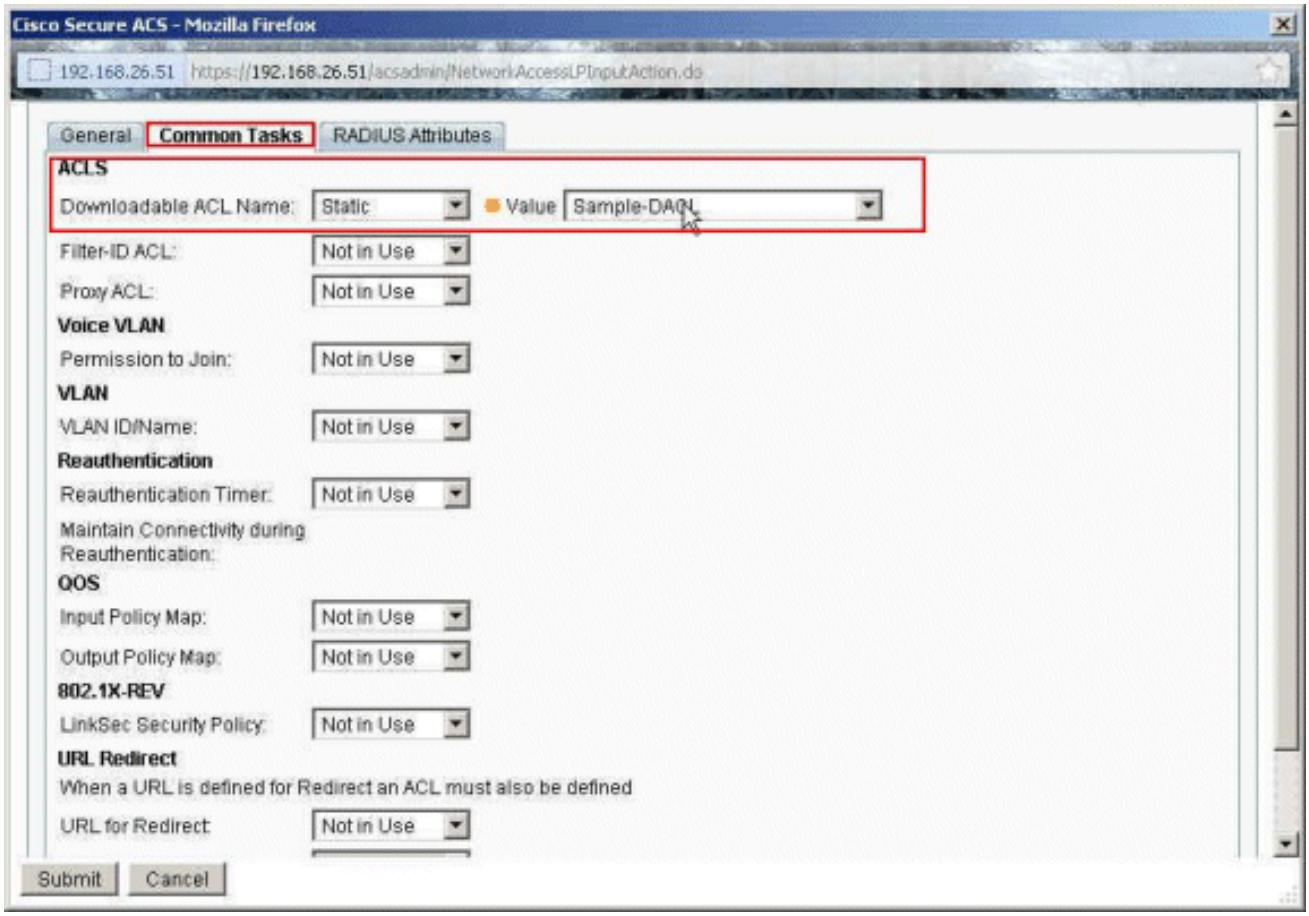
13. 按一下「**Create**」以建立一個新的授權設定檔。



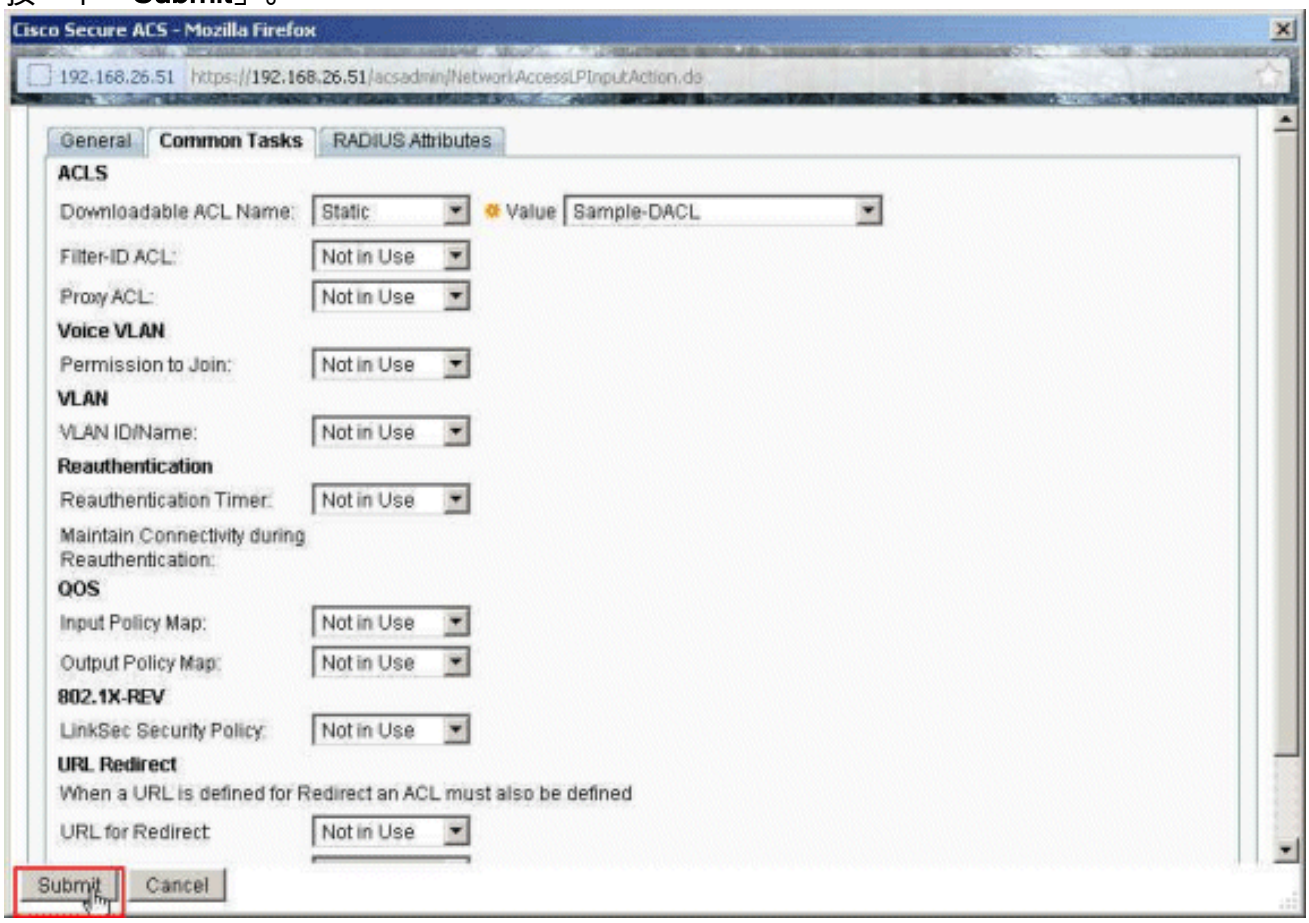
14. 提供授權配置檔案**的名稱。Sample-Profile**是本示例中使用的名稱。



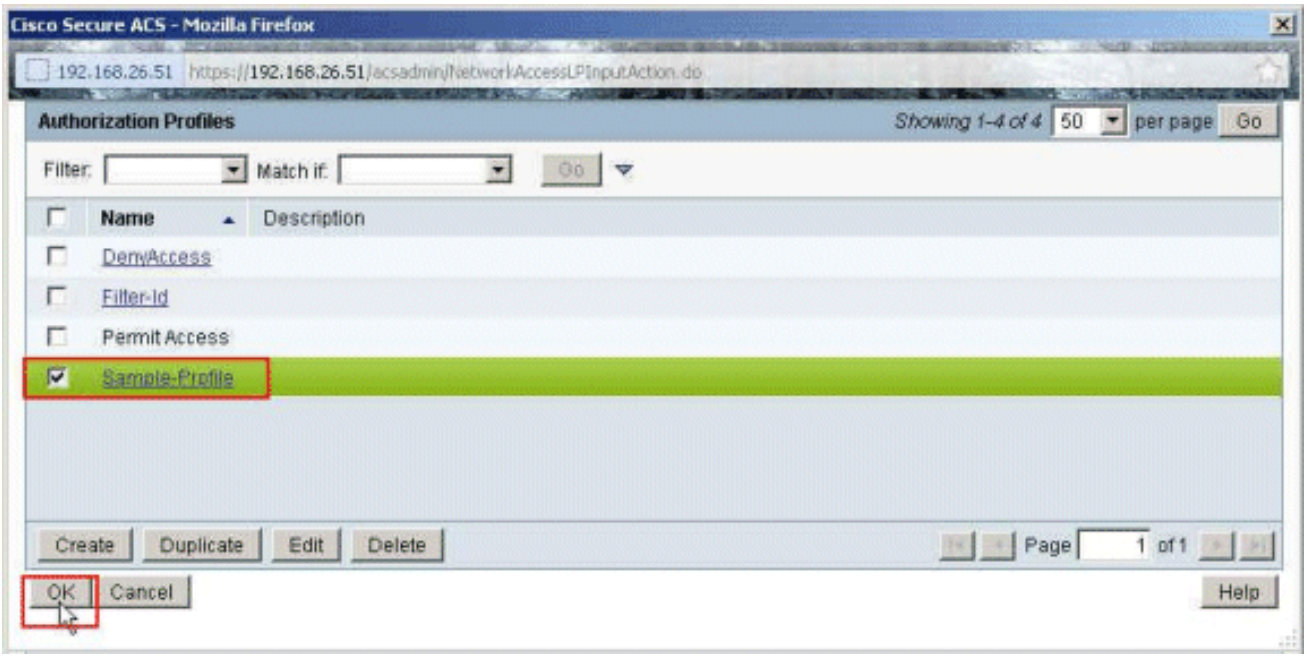
15. 選擇**Common Tasks**頁籤，然後從Downloadable ACL Name的下拉選單中選擇**Static**。從值下拉列**表中選擇新建立的DACL(Sample**-DACL)。



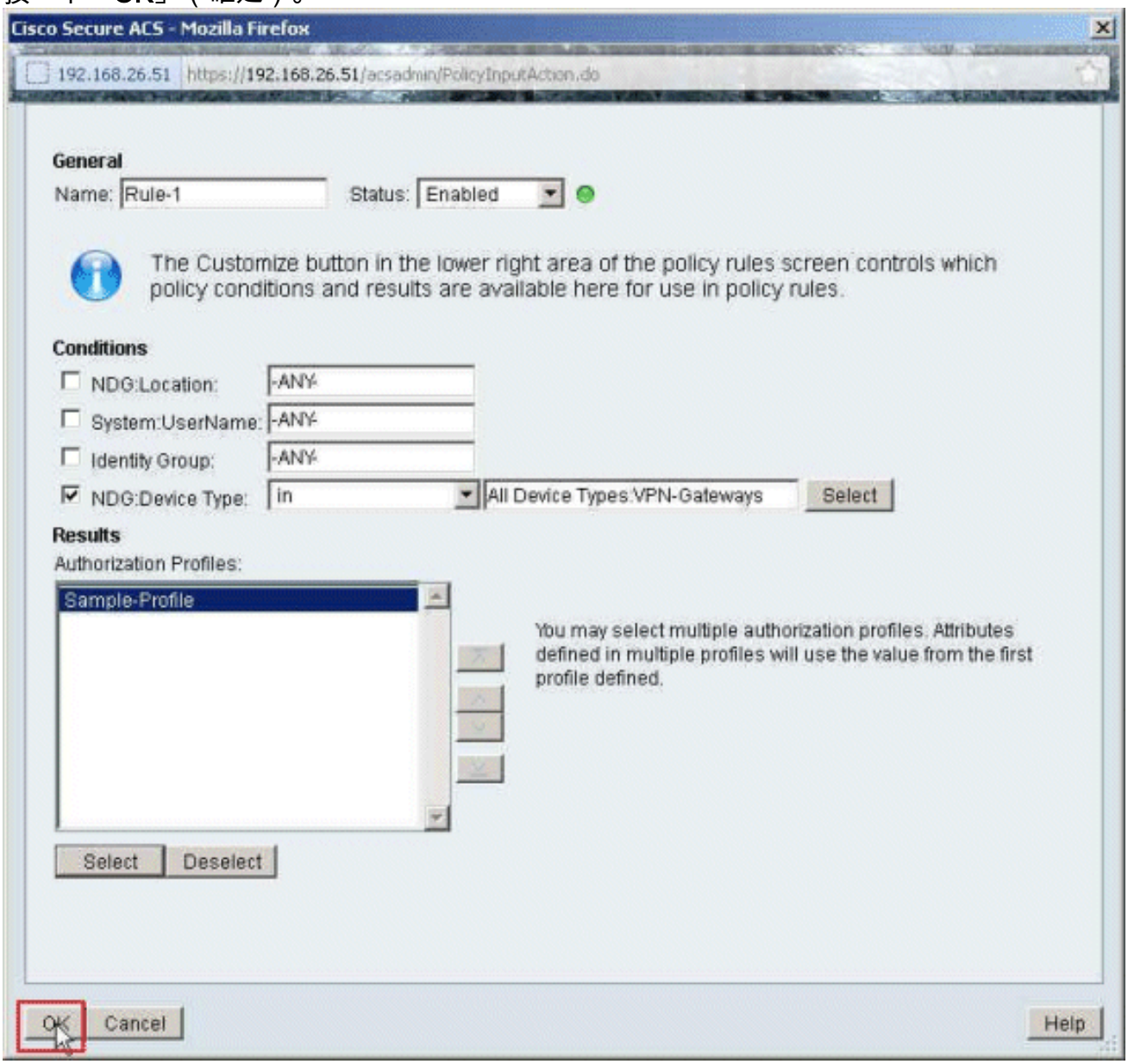
16. 按一下「**Submit**」。



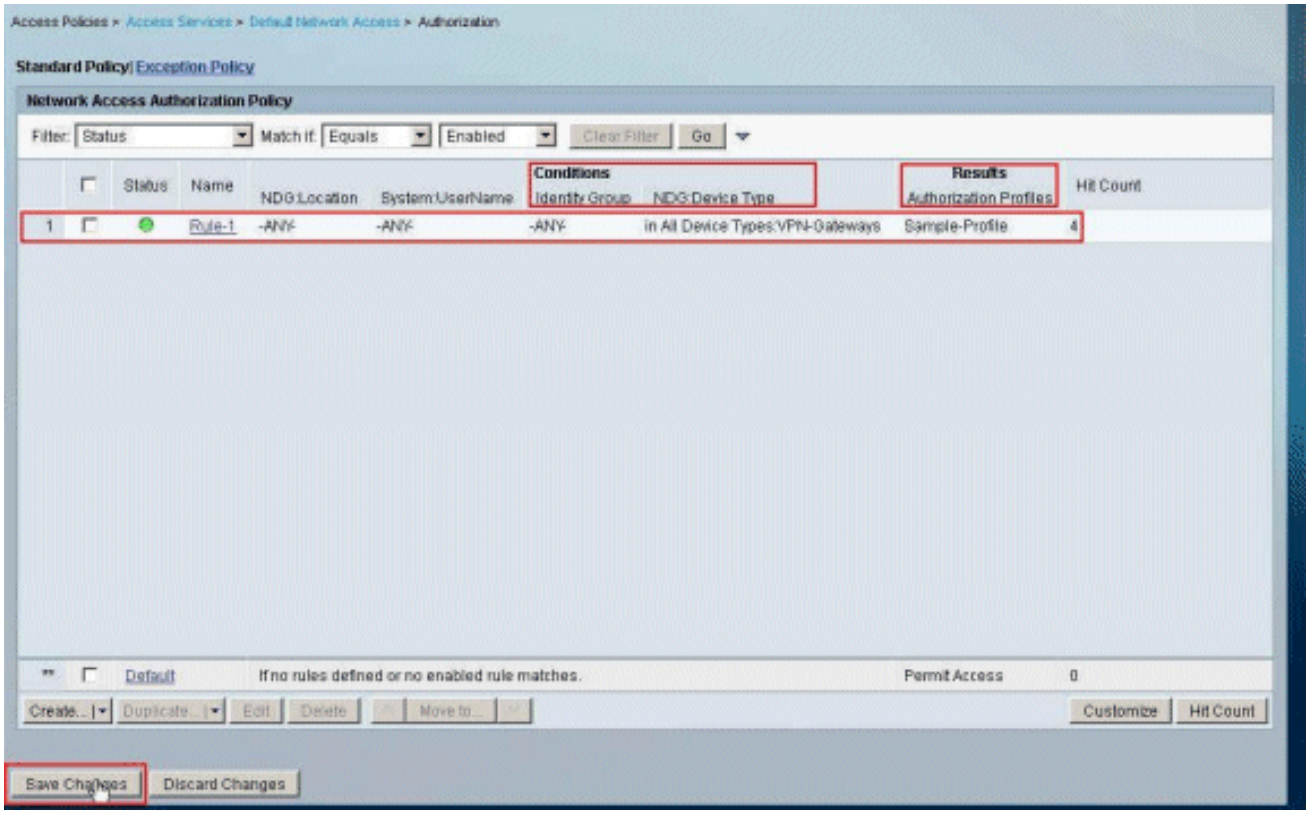
17. 選擇**Sample-Profile**（先前建立），然後按一下**OK**。



18. 按一下「**OK**」（確定）。



19. 驗證是否使用**VPN-Gateways**作為NDG:Device Type作為條件，使用**Sample-Profile**作為結果建立了**Rule-1**。按一下「**Save Changes**」。



為使用者組配置IETF RADIUS設定

要在使用者進行身份驗證時從RADIUS伺服器下載已在安全裝置上建立的訪問清單的名稱，請配置IETF RADIUS filter-id屬性（屬性編號11）：

```
filter-id=acl_name
```

樣例組使用者cisco身份驗證成功，RADIUS伺服器下載已在安全裝置上建立的訪問清單的ACL名稱（新）。使用者「cisco」可以訪問ASA **10.1.1.2伺服器以外的所有網路內的裝置。**若要驗證ACL，請參閱Filter-Id ACL部分。

根據示例，名為**new**的ACL配置為在ASA中進行過濾：

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

僅當這些引數為真時，才會顯示這些引數。您已設定：

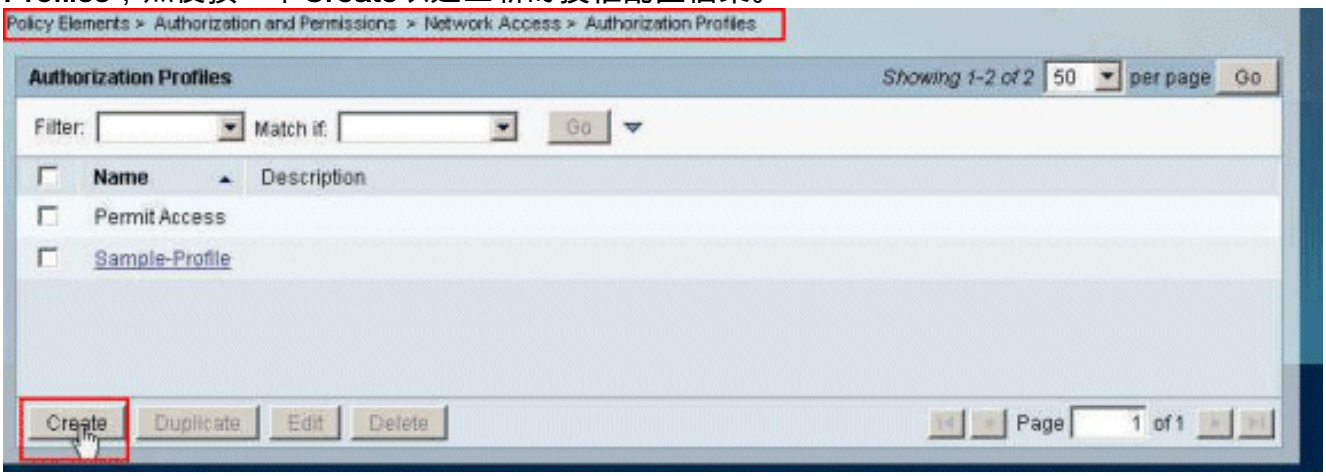
- AAA客戶端在網路配置中使用其中一個RADIUS協定
- 在Access-Service中規則的結果部分下選擇具有RADIUS(IETF)Filter-Id的授權配置檔案。

RADIUS屬性作為每個使用者的配置檔案從ACS傳送到請求AAA客戶端。

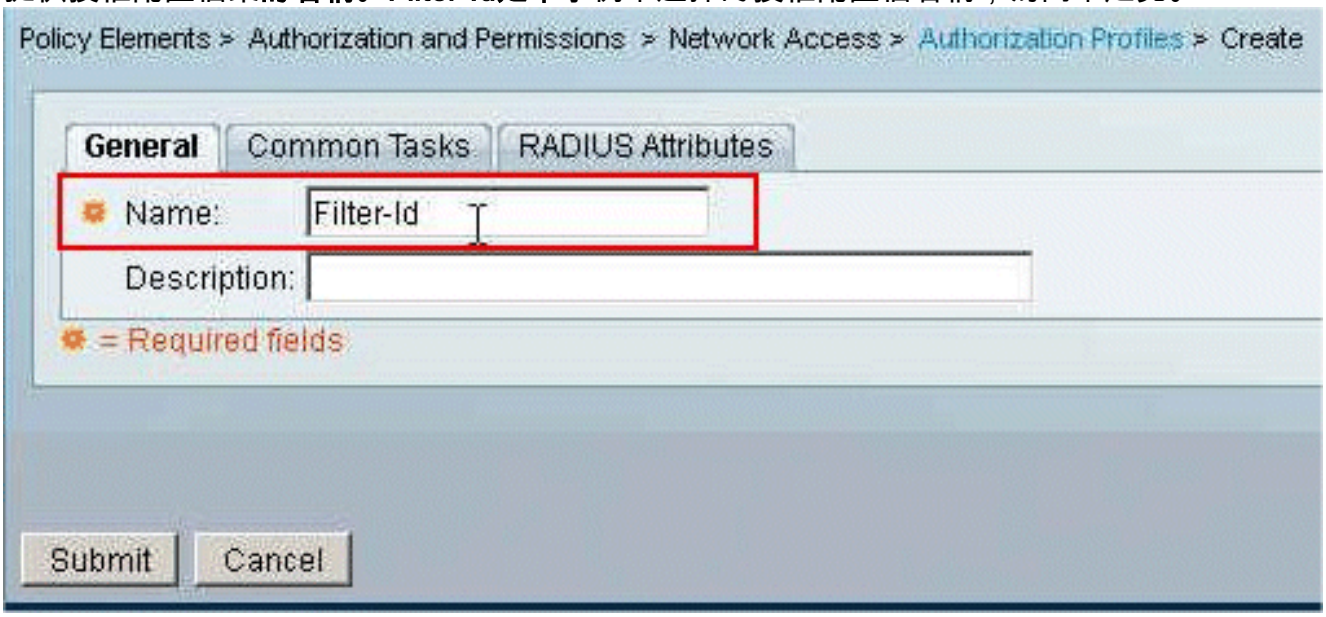
完成為單個使用者的可下載ACL配置ACS的步驟1至6和10至12，然後完成為組的可下載ACL配置ACS的步驟1至6，在本部分執行這些步驟，以便在Cisco安全ACS中配置Filter-Id。

若要將**IETF RADIUS屬性設**置配置為按授權配置檔案中的方式應用，請執行以下步驟：

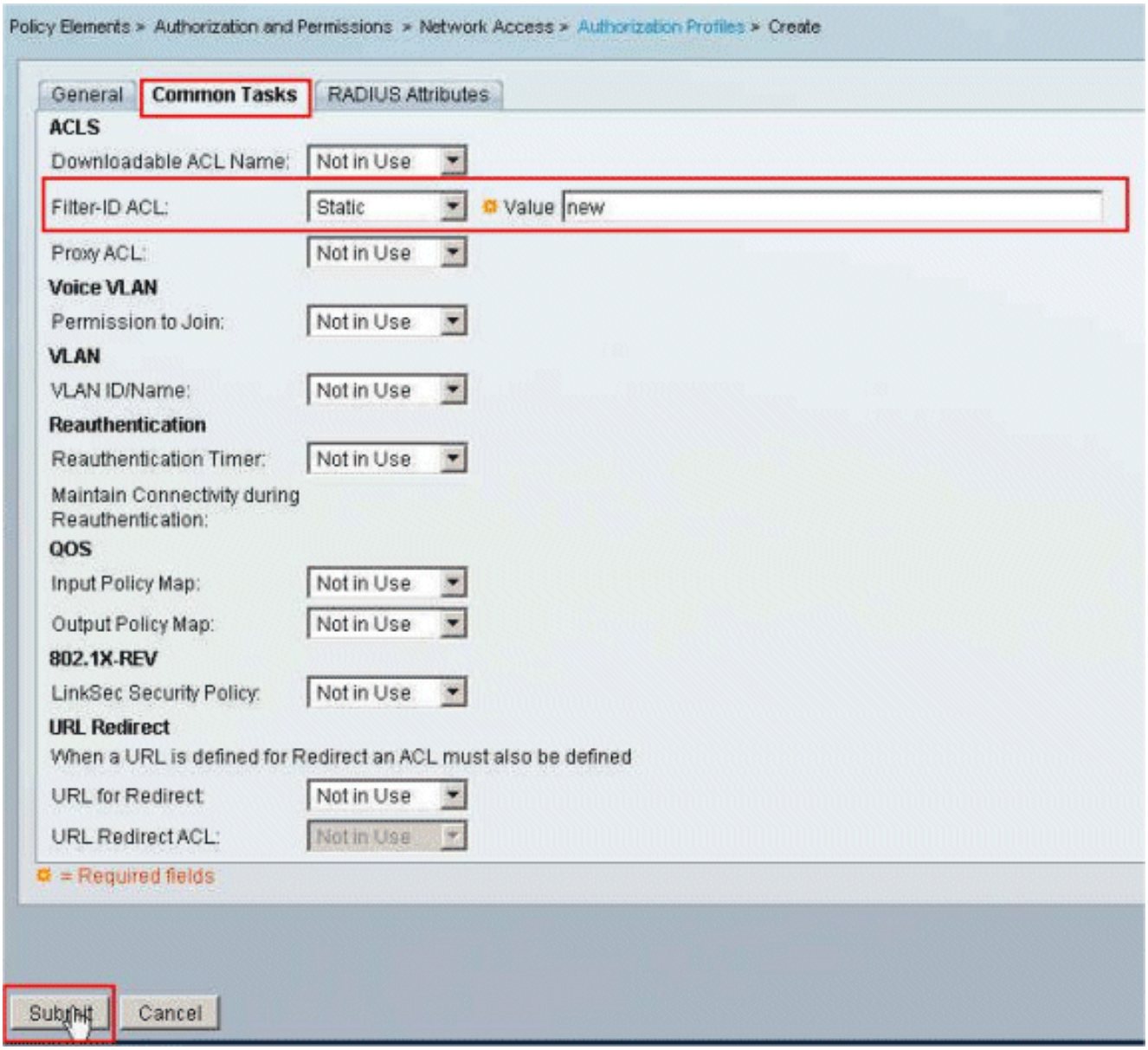
1. 選擇Policy Elements > **Authorization and Permissions > Network Access > Authorization Profiles**，然後按一下**Create**以建立新的授權配置檔案。



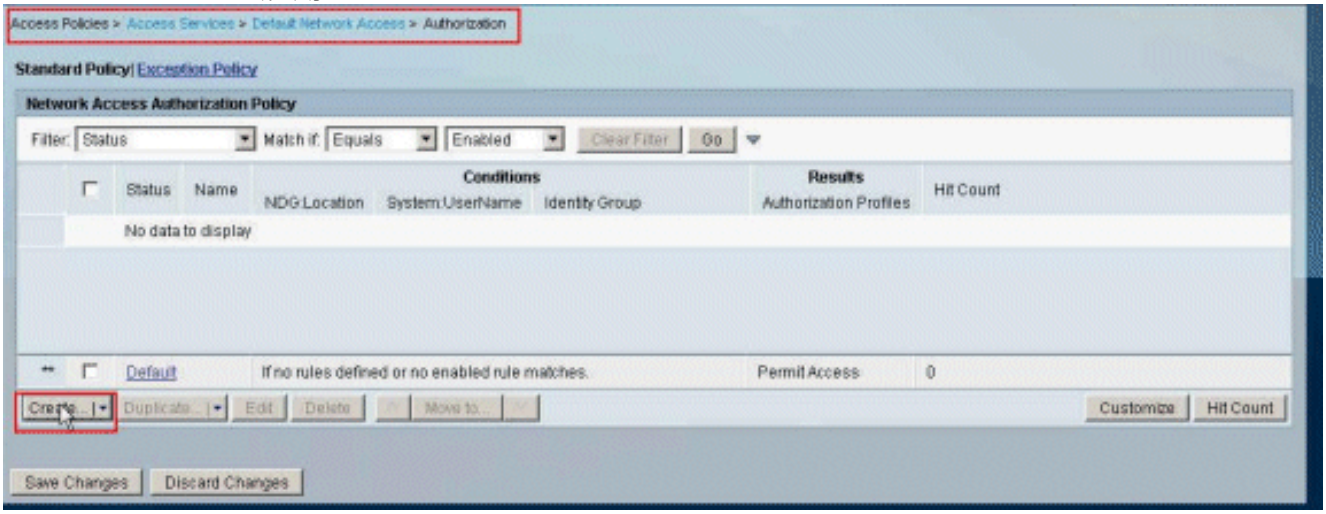
2. 提供授權配置檔案**的名稱。Filter-Id是本**示例中選擇的授權配置檔名稱，為簡單起見。



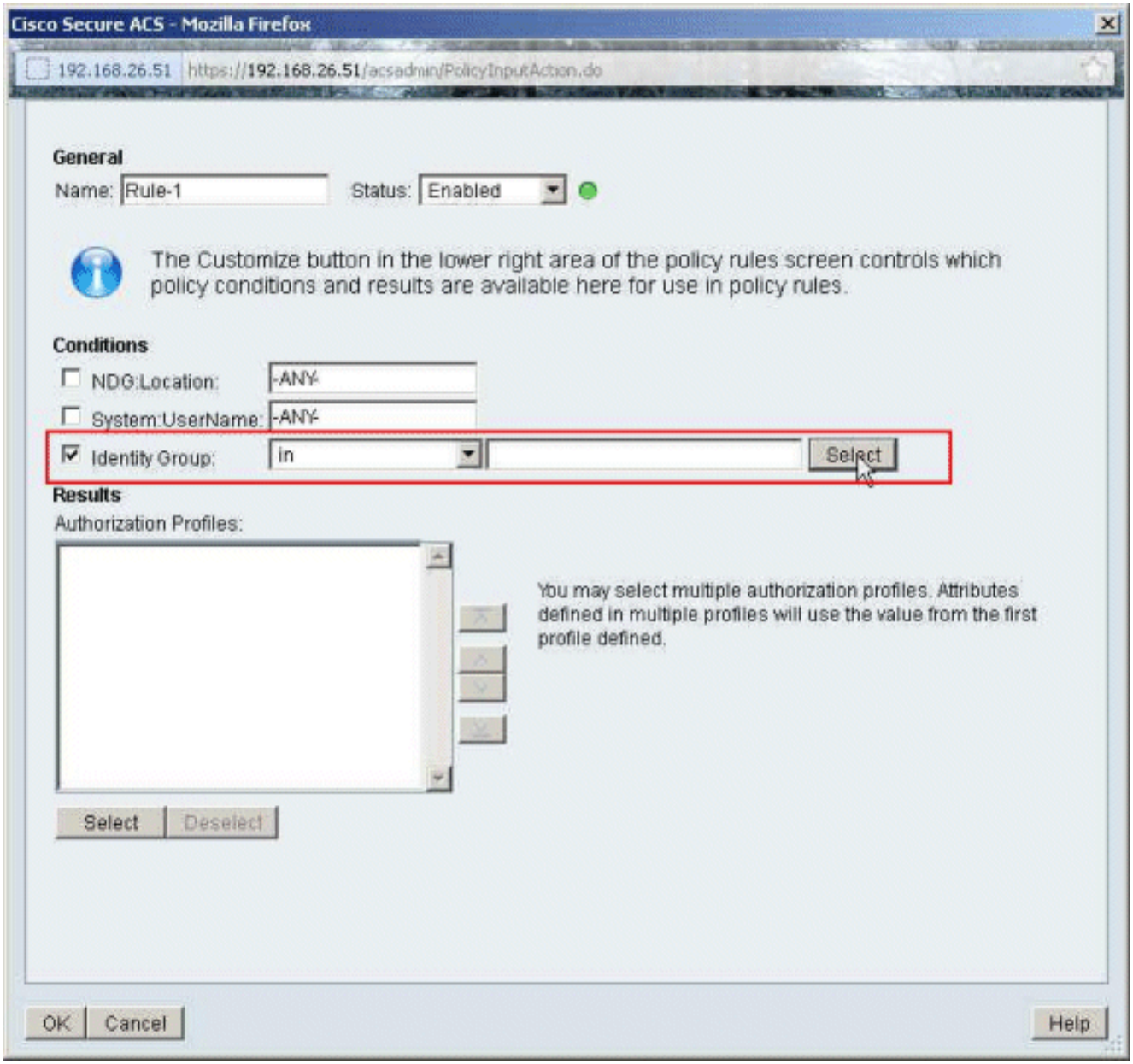
3. 按一下**Common Tasks**頁籤，然後從**Filter-ID ACL**的下拉選單中選擇**Static**。在「值」欄位中輸入新的訪問清單名稱，然後按一下**提交**。



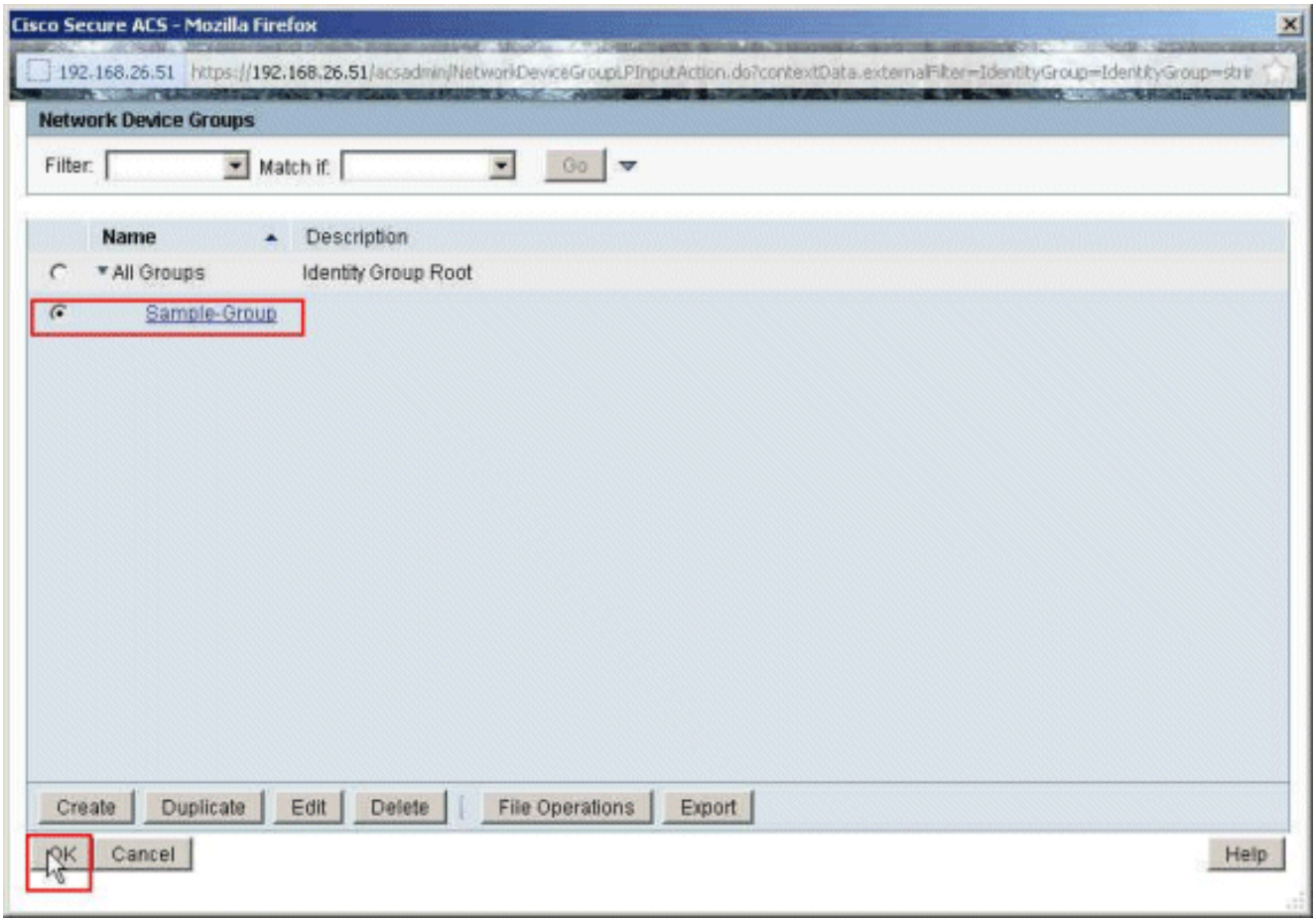
4. 選擇Access Policies > **Access Services** > **Default Network Access** > **Authorization**，然後按一下**Create**以建立新規則。



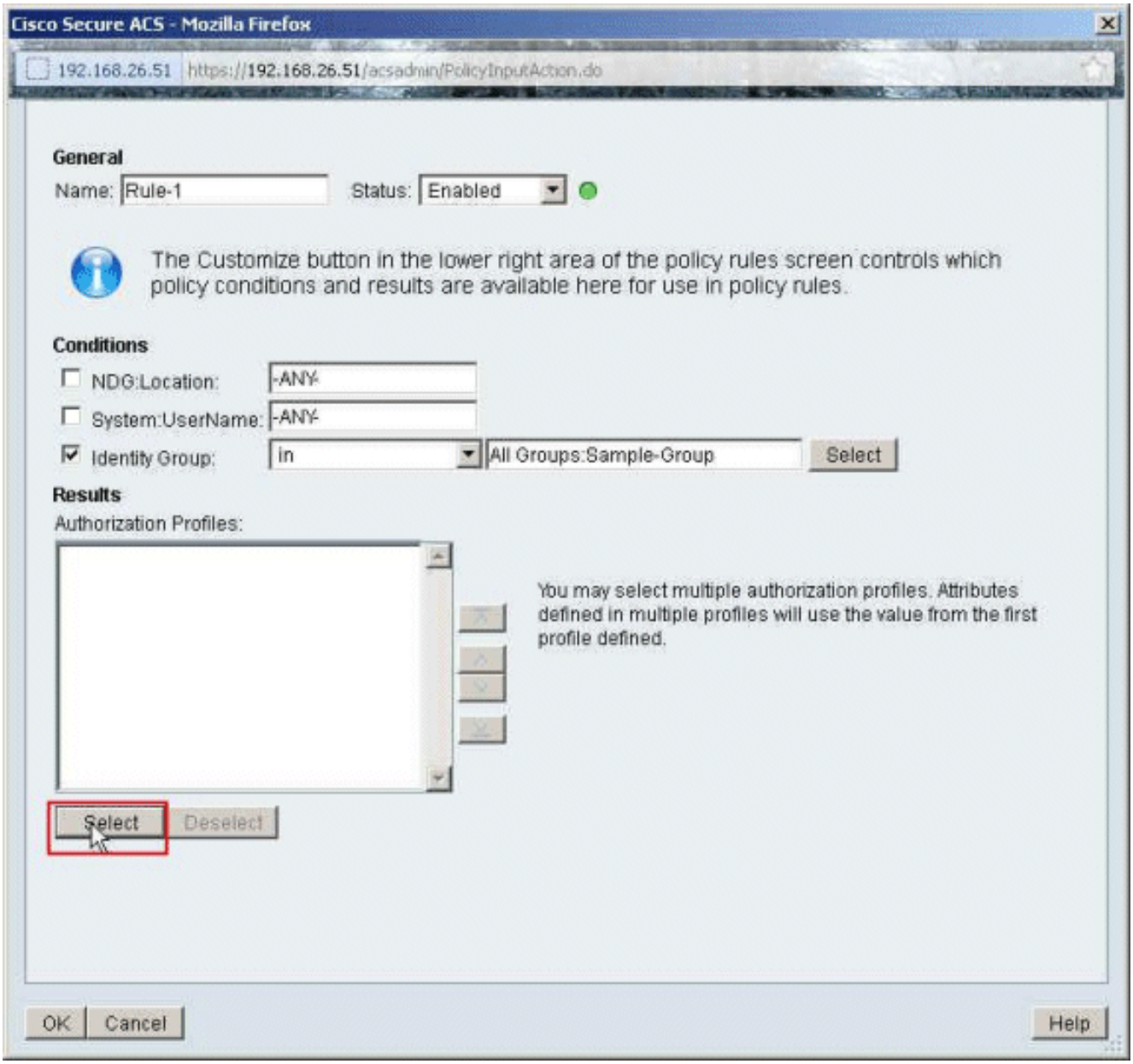
5. 確保選中**身份組**旁邊的覈取方塊，然後按一下**選擇**。



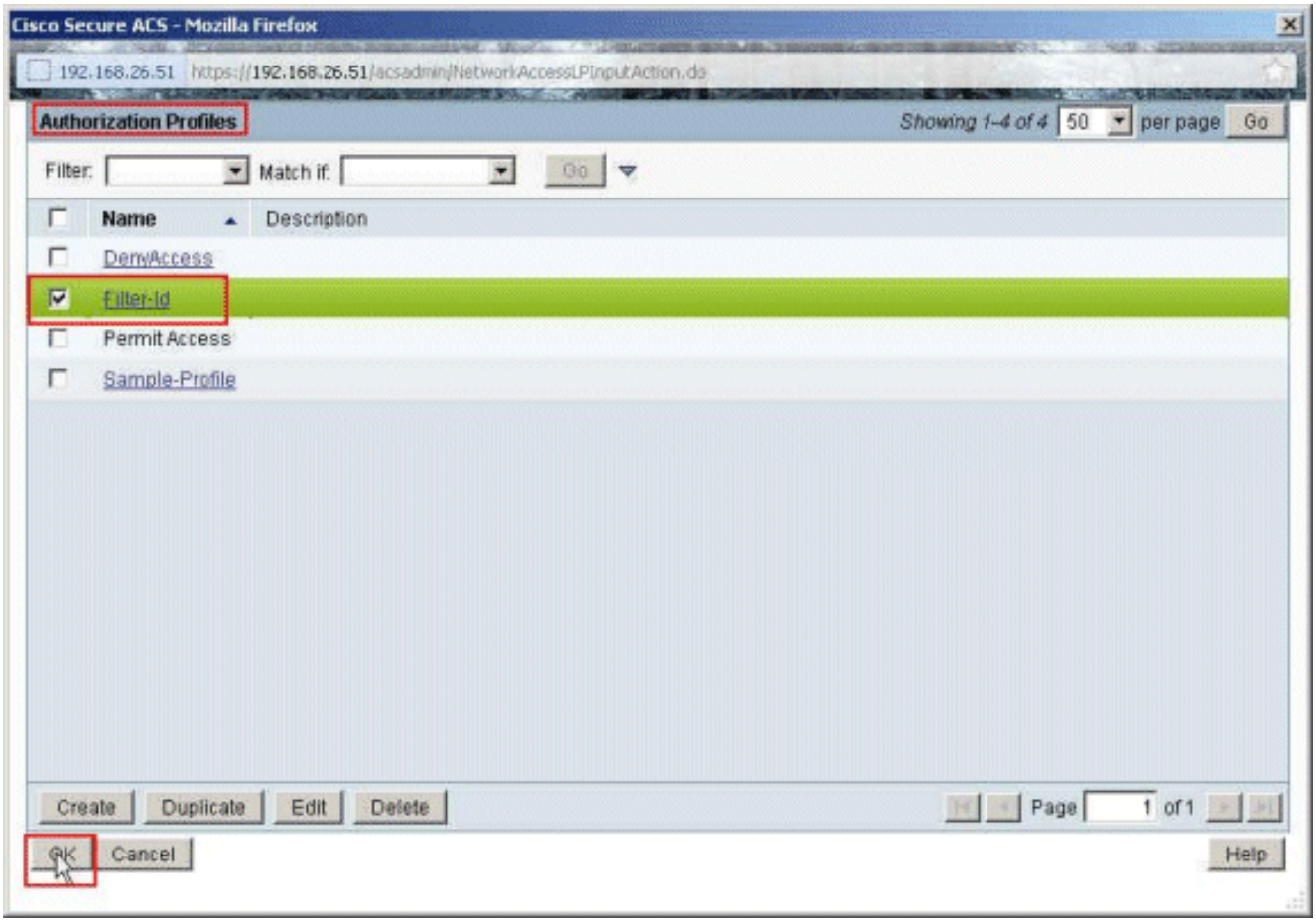
6. 選擇**Sample-Group**，然後按一下**OK**。



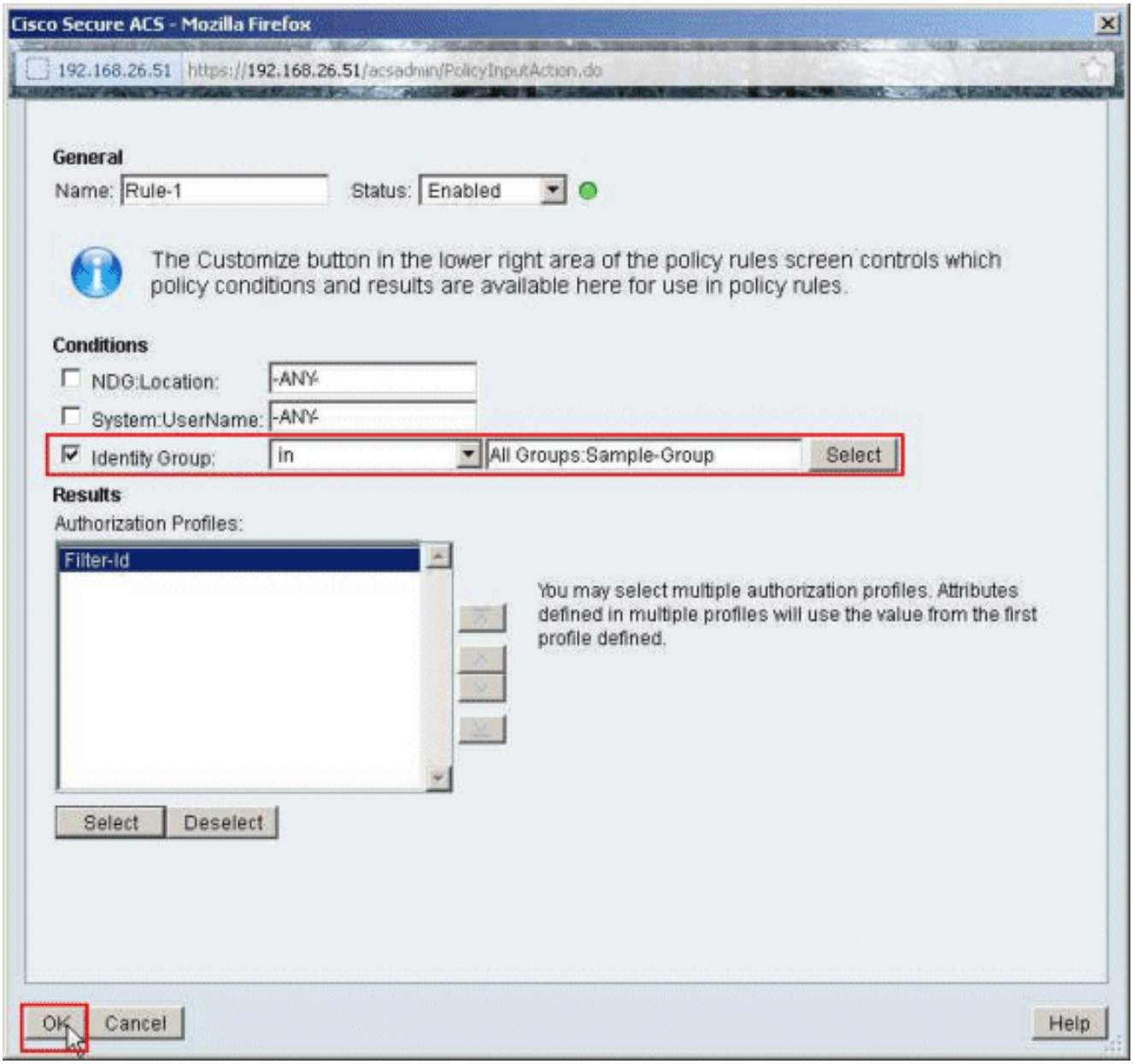
7. 在Authorization Profiles部分中按一下**Select**。



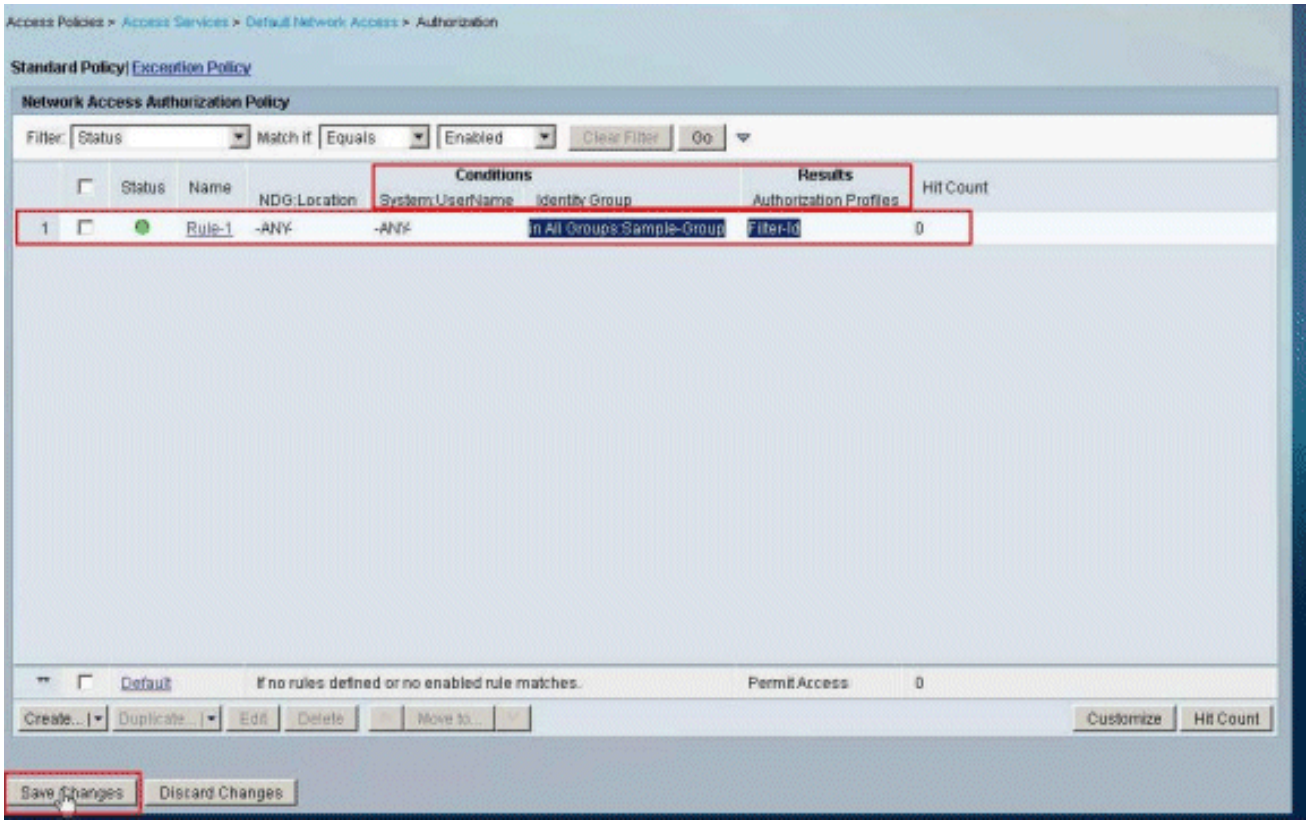
8. 選擇之前建立的Authorization Profile **Filter-Id**，然後按一下**OK**。


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. 按一下「**OK**」（確定）。



10. 驗證是否以身份組**Sample-Group**作為條件，以**Filter-Id**作為結果建立了**Rule-1**。按一下「**Save Changes**」。

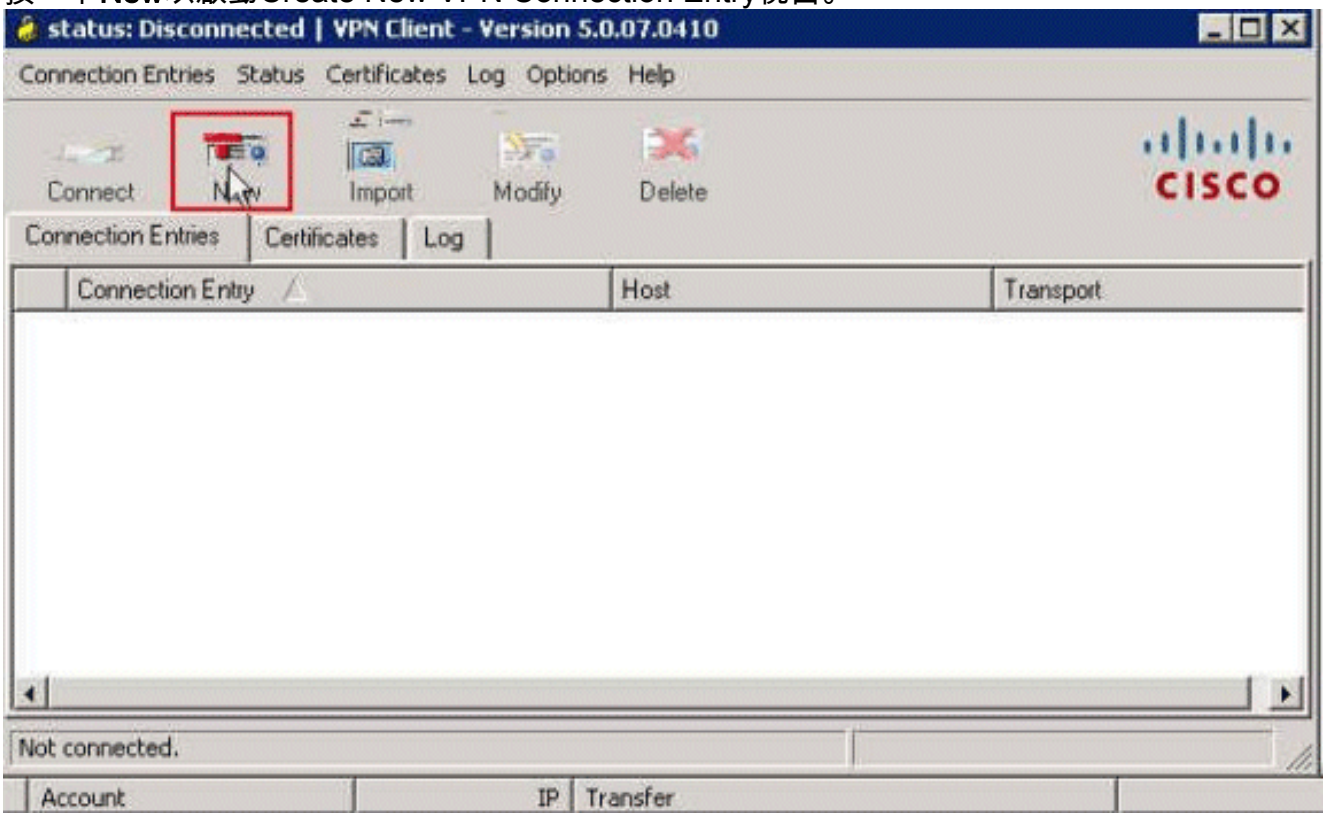


Cisco VPN客戶端配置

使用Cisco VPN客戶端連線到Cisco ASA，以驗證ASA配置是否成功。

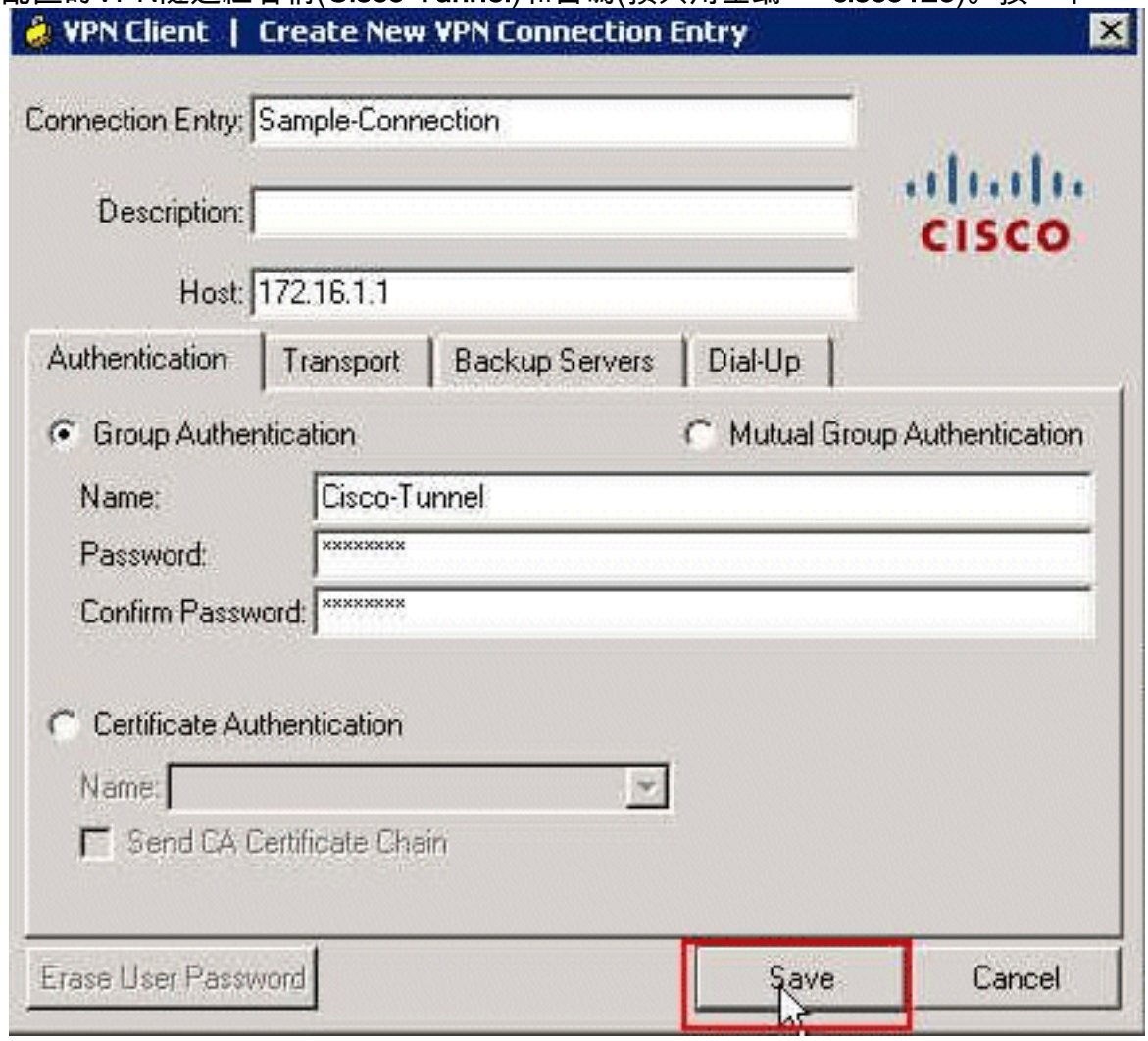
請完成以下步驟：

1. 選擇**Start > Programs > Cisco Systems VPN Client > VPN Client**。
2. 按一下**New**以啟動Create New VPN Connection Entry視窗。

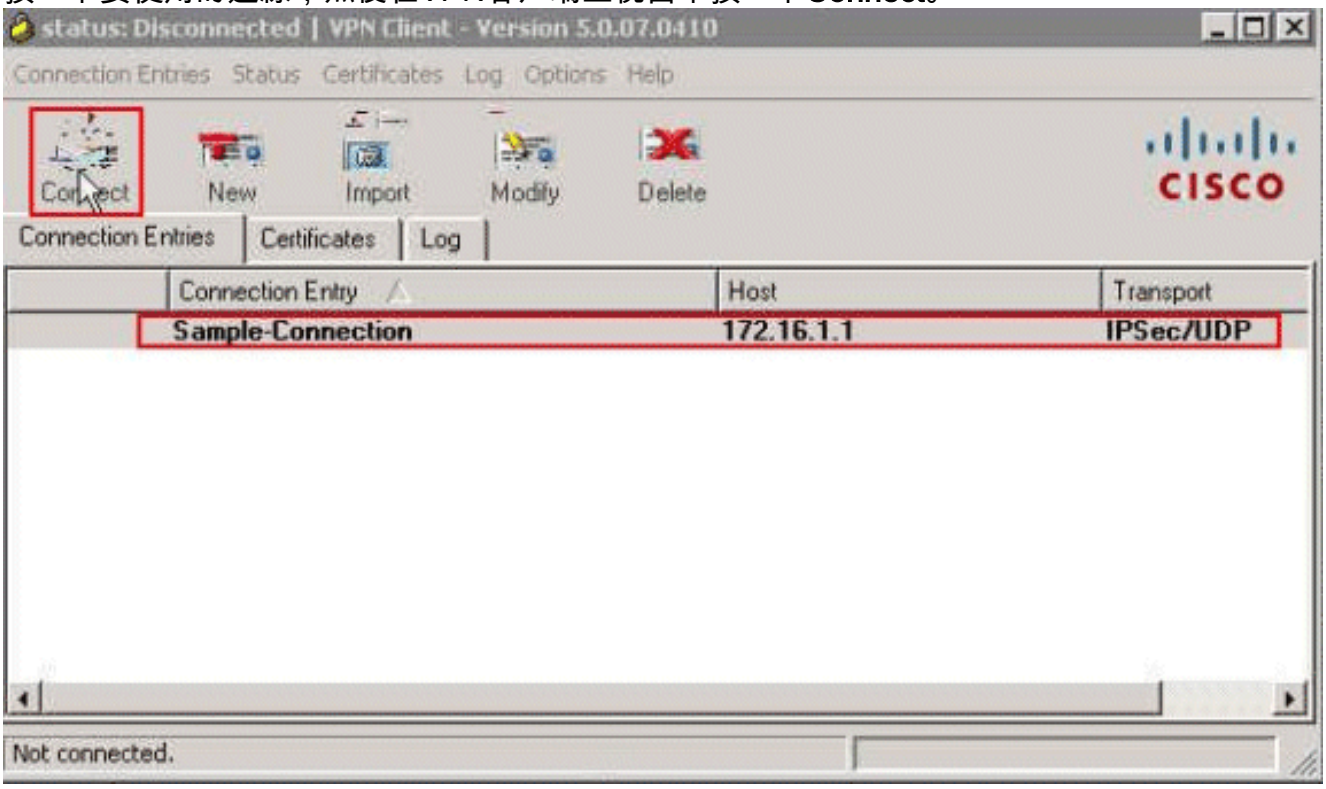


3. 填寫新連線的詳細資訊：輸入連線條目的名稱和說明。在Host**框中輸入ASA的**外部IP地址。輸

入ASA中配置的VPN隧道組名稱(**Cisco-Tunnel**)和密碼(預共用金鑰 — **cisco123**)。按一下「**Save**」。

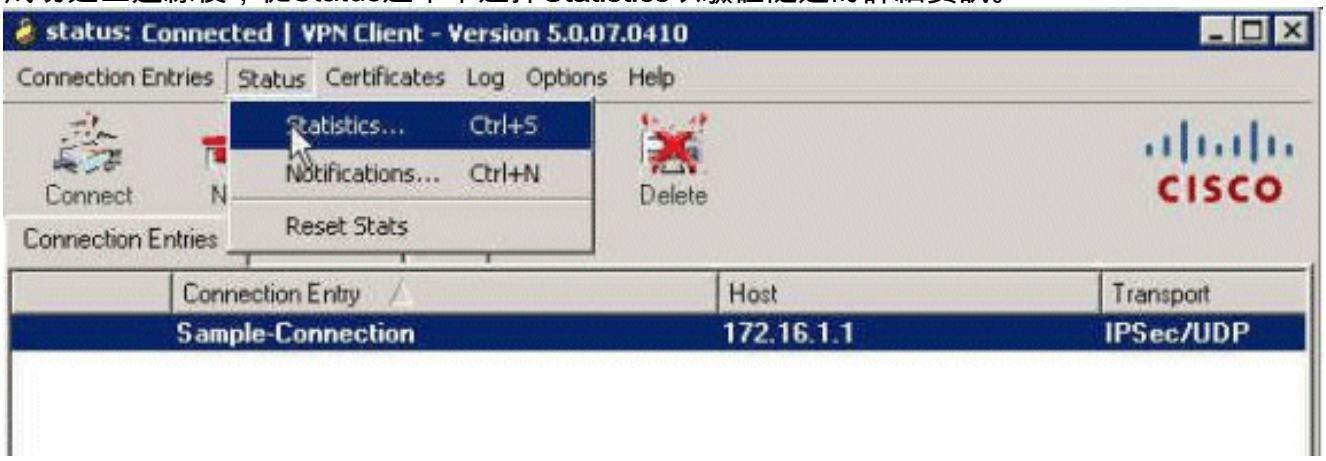


4. 按一下要使用的連線，然後在VPN客戶端主視窗中按一下**Connect**。



5. 出現提示時，輸入**使用者名稱cisco**和密碼**cisco123**（如在ASA中配置進行身份驗證），然後按一下**OK**以連線到遠端網路。

6. 成功建立連線後，從Status選單中選擇**Statistics**以驗證隧道的詳細資訊。



驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

Show Crypto命令

- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE安全關聯(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** — 顯示當前SA使用的設定。

```
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
```

使用者/組的可下載ACL

驗證使用者Cisco的可下載ACL。ACL會從CSACS下載。

```
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已應用於Group - Sample-Group，並且根據ASA中定義的ACL（新）過濾該組的使用者。

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。還顯示了**debug**輸出示例。

注意：有關遠端訪問IPsec VPN故障排除的詳細資訊，請參閱最常見的L2L和遠端訪問IPsec VPN故障排除解決方案。

清除安全關聯

進行故障排除時，請確保在進行更改後清除現有的SA。在PIX的特權模式下，使用以下命令：

- **clear [crypto] ipsec sa** -刪除活動的IPsec SA。關鍵字crypto是可選的。
- **clear [crypto] isakmp sa** — 刪除活動的IKE SA。關鍵字crypto是可選的。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug crypto ipsec 7** — 顯示第2階段的IPsec協商。
- **debug crypto isakmp 7** — 顯示第1階段的ISAKMP協商。

相關資訊

- Cisco ASA 5500系列自適應安全裝置支援頁
- Cisco ASA 5500系列自適應安全裝置命令參考
- 思科調適型資安裝置管理員
- IPsec協商/IKE通訊協定支援頁面
- Cisco VPN使用者端支援頁面
- 思科安全存取控制系統
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems