ASA 8.3 et plus tard : Autorisation RADIUS (ACS 5.x) pour l'accès VPN utilisant l'ACL téléchargeable avec l'exemple de configuration CLI et ASDM

Contenu

Introduction

Ce document décrit comment configurer l’appliance de sécurité pour authentifier des utilisateurs pour l’accès au réseau. Puisque vous pouvez implicitement activer des autorisations RADIUS, ce document ne contient aucune information sur la configuration de l'autorisation RADIUS sur les dispositifs de sécurité. Elle fournit néanmoins des renseignements sur la façon dont l’appliance de sécurité gère les renseignements de liste d’accès reçus des serveurs RADIUS.

Vous pouvez configurer un serveur de RADIUS pour télécharger une liste d'accès aux dispositifs

de sécurité ou un nom de liste d'accès au moment de l'authentification. L'utilisateur est autorisé à faire seulement ce qui est permis dans la liste d'accès d'utilisateur-particularité.

Les Listes d'accès téléchargeables sont les moyens les plus extensibles quand vous utilisez le Cisco Secure Access Control Server (ACS) pour fournir les Listes d'accès appropriées pour chaque utilisateur. Pour plus d'informations sur les caractéristiques téléchargeables de liste d'accès et le Cisco Secure ACS, référez-vous à configurer un serveur de RADIUS pour envoyer les listes de contrôle d'accès téléchargeables et l'IP téléchargeable ACLs.

Référez-vous à ASA/PIX 8.x : Autorisation RADIUS (ACS) pour l'accès de réseau utilisant l'ACL téléchargeable avec l'exemple de configuration CLI et ASDM pour la configuration identique sur Cisco ASA avec des versions 8.2 et antérieures.

Conditions préalables

Conditions requises

Ce document suppose que l'appliance de sécurité adaptable (ASA) est complètement opérationnelle et configurée pour permettre au Cisco Adaptive Security Device Manager (ASDM) ou au CLI pour apporter des modifications de configuration.

Remarque: Référez-vous à permettre à HTTPS Access pour l'ASDM afin de permettre le périphérique à configurer à distance par l'ASDM ou Protocole Secure Shell (SSH).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de logiciel 8.3 de Cisco ASA et plus tard
- Version 6.3 et ultérieures de Cisco ASDM
- Version 5.x et ultérieures de Client VPN Cisco
- Cisco Secure ACS 5.x

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Vous pouvez employer IP téléchargeable ACLs afin de créer des ensembles de définitions d'ACL que vous pouvez s'appliquer à beaucoup d'utilisateurs ou de groupes d'utilisateurs. Ces ensembles de définitions d'ACL s'appellent le contenu d'ACL.

IP téléchargeable ACLs actionnent de cette façon :

1. Quand ACS accorde un accès client au réseau, ACS détermine si un ACL IP téléchargeable est assigné au profil d'autorisation dans la section de résultat.
2. Si ACS localise un ACL IP téléchargeable qui est assigné au profil d'autorisation, ACS envoie un attribut (en tant qu'élément de la session d'utilisateur, dans le paquet d'acceptation d'accès de RADIUS) qui spécifie ACL Désigné, et la version d'ACL Désigné.
3. Si le client d'AAA répond qu'il n'a pas la version en cours de l'ACL dans son cache (c'est-à-dire, l'ACL est nouveau ou a changé), ACS envoie l'ACL (nouveau ou mis à jour) au périphérique.

IP téléchargeable ACLs sont une alternative à la configuration d'ACLs dans l'attribut [26/9/1] de Cisco-poids du commerce-paires de RADIUS Cisco de chaque utilisateur ou groupe d'utilisateurs. Vous pouvez créer un ACL IP téléchargeable une fois, lui donnez un nom, et puis assignez l'ACL IP téléchargeable à n'importe quel profil d'autorisation si vous mettez en référence son nom. Cette méthode est plus efficace que si vous configurez l'attribut de Cisco-poids du commerce-paires de RADIUS Cisco pour le profil d'autorisation.

Quand vous écrivez les définitions d'ACL dans l'interface web ACS, n'utilisez pas les entrées de mot clé ou de nom ; en outre, utilisez la syntaxe de commande d'ACL et la sémantique standard pour le client d'AAA sur lequel vous avez l'intention d'appliquer l'ACL IP téléchargeable. Les définitions d'ACL que vous écrivez dans ACS comportent un ou plusieurs commandes d'ACL. Chaque commande d'ACL doit être sur une ligne distincte.

Dans ACS, vous pouvez définir plusieurs IP téléchargeable ACLs et les utiliser dans différents profils d'autorisation. Basé sur les conditions dans les règles d'autorisation de service d'accès, vous pouvez envoyer différents profils d'autorisation contenant IP téléchargeable ACLs à différents clients d'AAA.

De plus, vous pouvez changer la commande du contenu d'ACL dans un ACL IP téléchargeable. ACS examine le contenu d'ACL, à partir du dessus de la table, et télécharge le premier contenu d'ACL qu'elle trouve. Quand vous placez la commande, vous pouvez assurer l'efficacité de système si vous placez le plus largement le contenu applicable d'ACL plus élevé sur la liste.

Afin d'utiliser un ACL IP téléchargeable sur un client particulier d'AAA, le client d'AAA doit adhérer à ces règles :

- Utilisation RADIUS pour l'authentification
- IP téléchargeable ACLs de support

Ce sont des exemples des périphériques de Cisco qui prennent en charge IP téléchargeable ACLs :

- ASA
- Périphériques de Cisco qui exécutent la version IOS 12.3(8)T et plus tard

C'est un exemple du format que vous devez employer afin d'écrire ASA ACLs dans la case de définitions d'ACL :

```
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
```

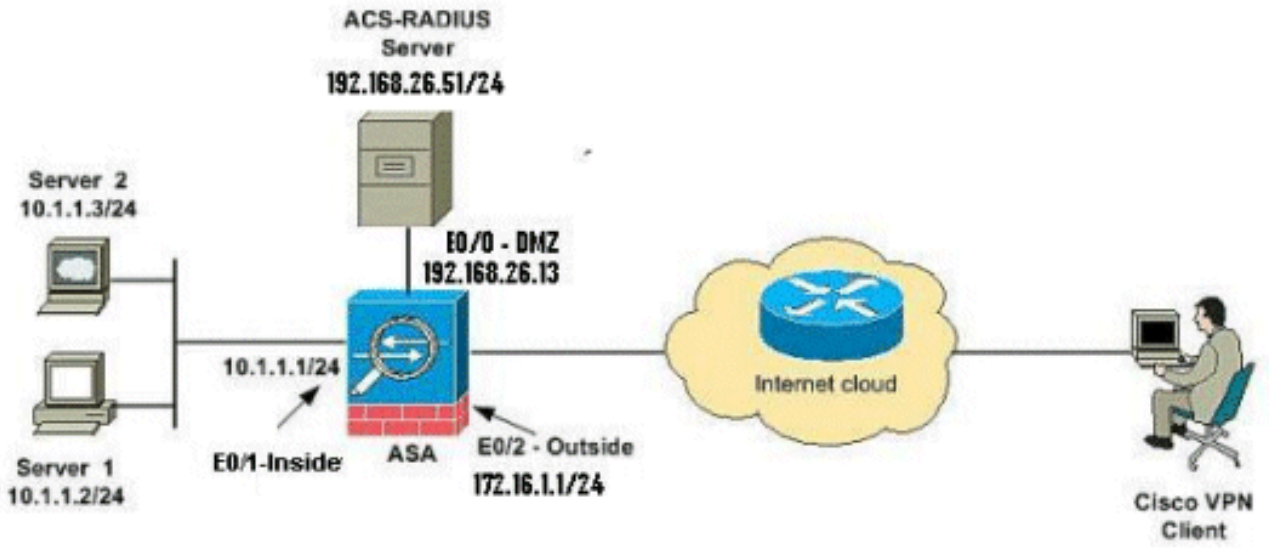
```
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



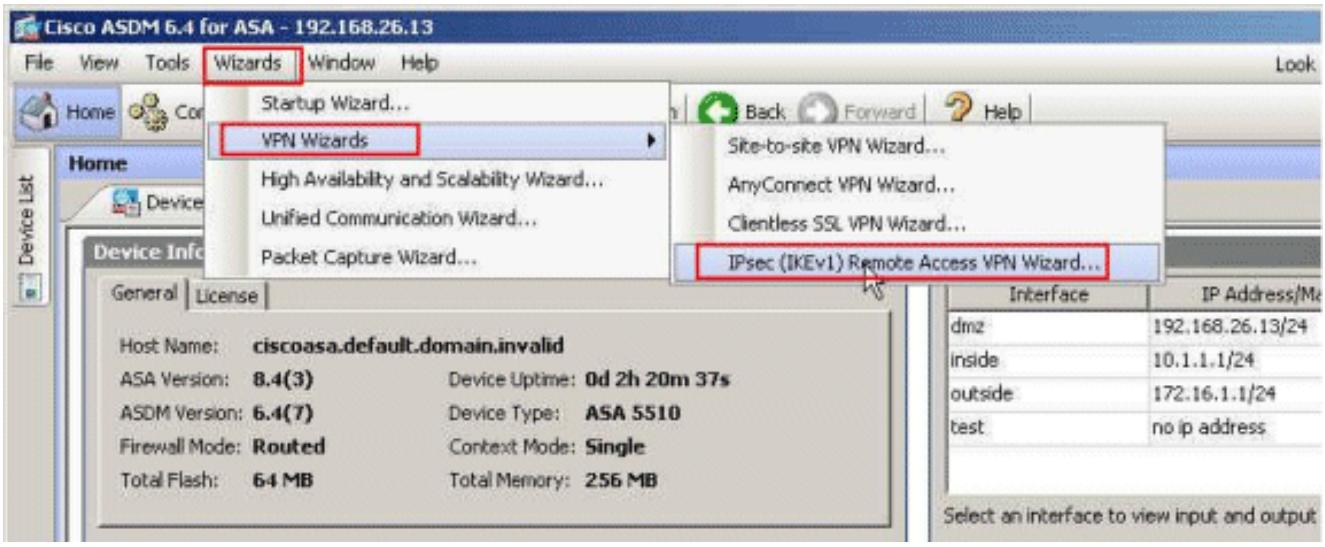
Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurez l'Accès à distance VPN (IPsec)

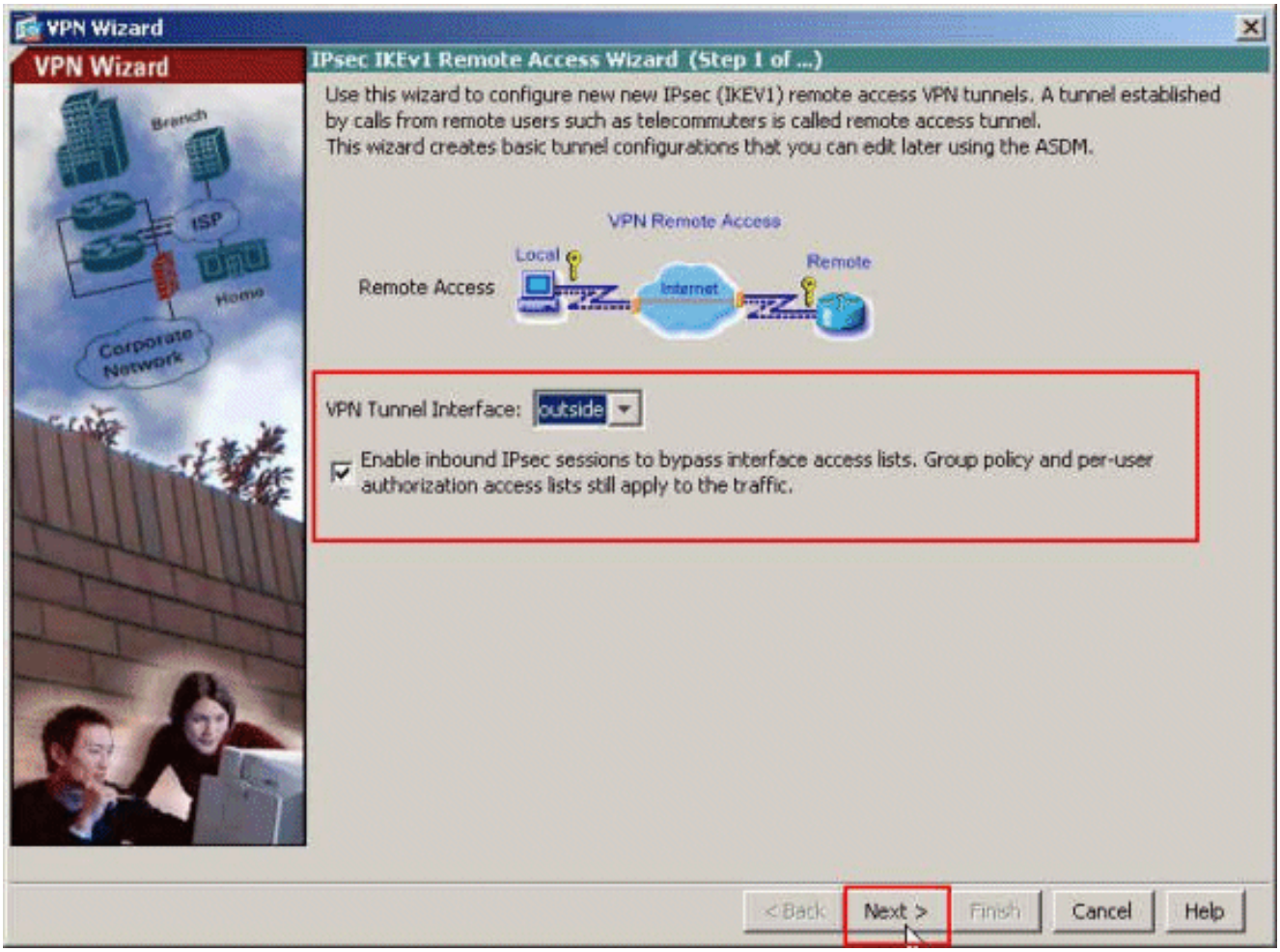
Procédure ASDM

Complétez ces étapes afin de configurer le VPN d'accès à distance :

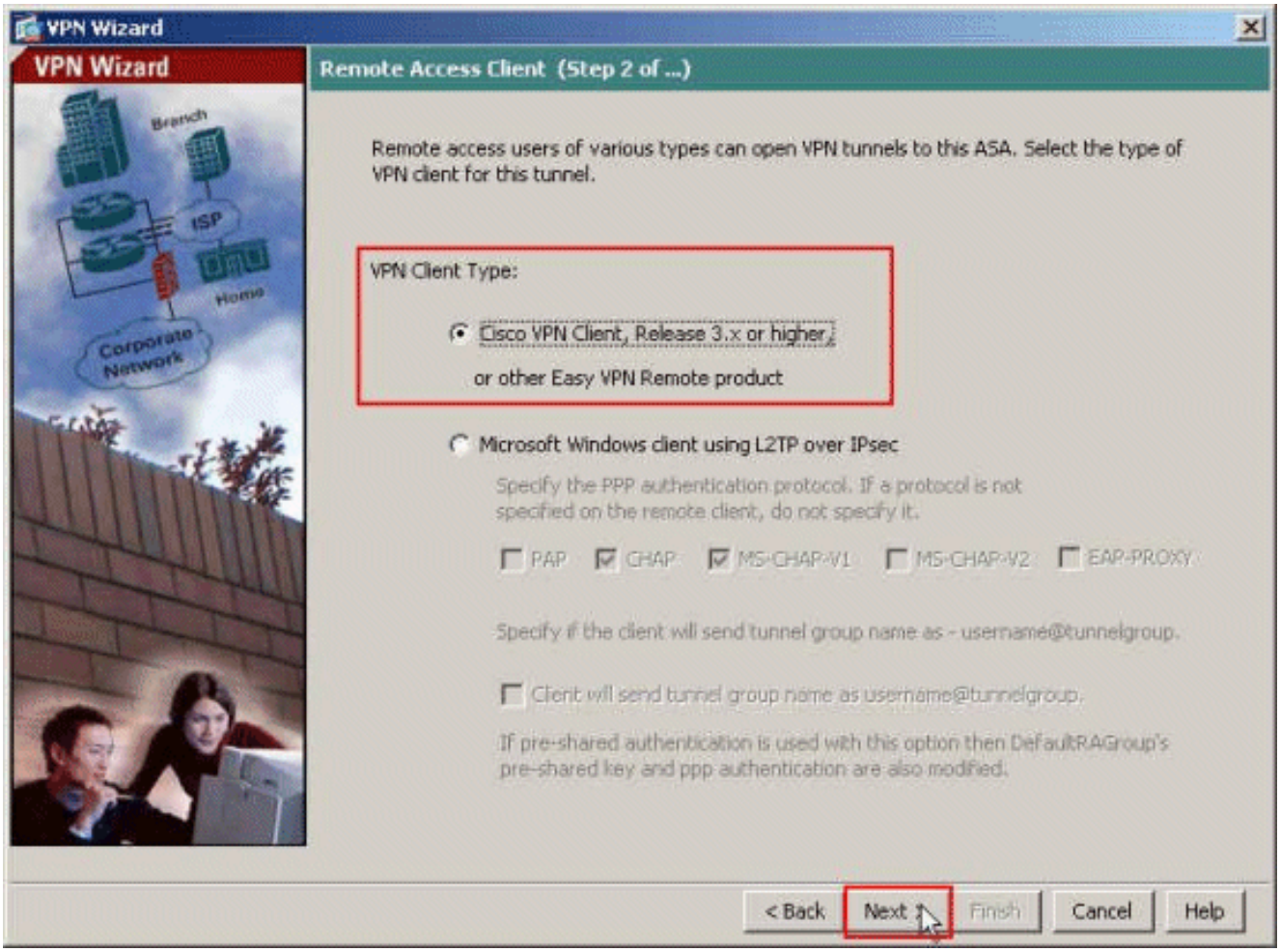
1. **Assistants** choisis > **assistants VPN > IPsec(IKEv1) assistant de l'Accès à distance VPN de la** fenêtre
d'accueil.



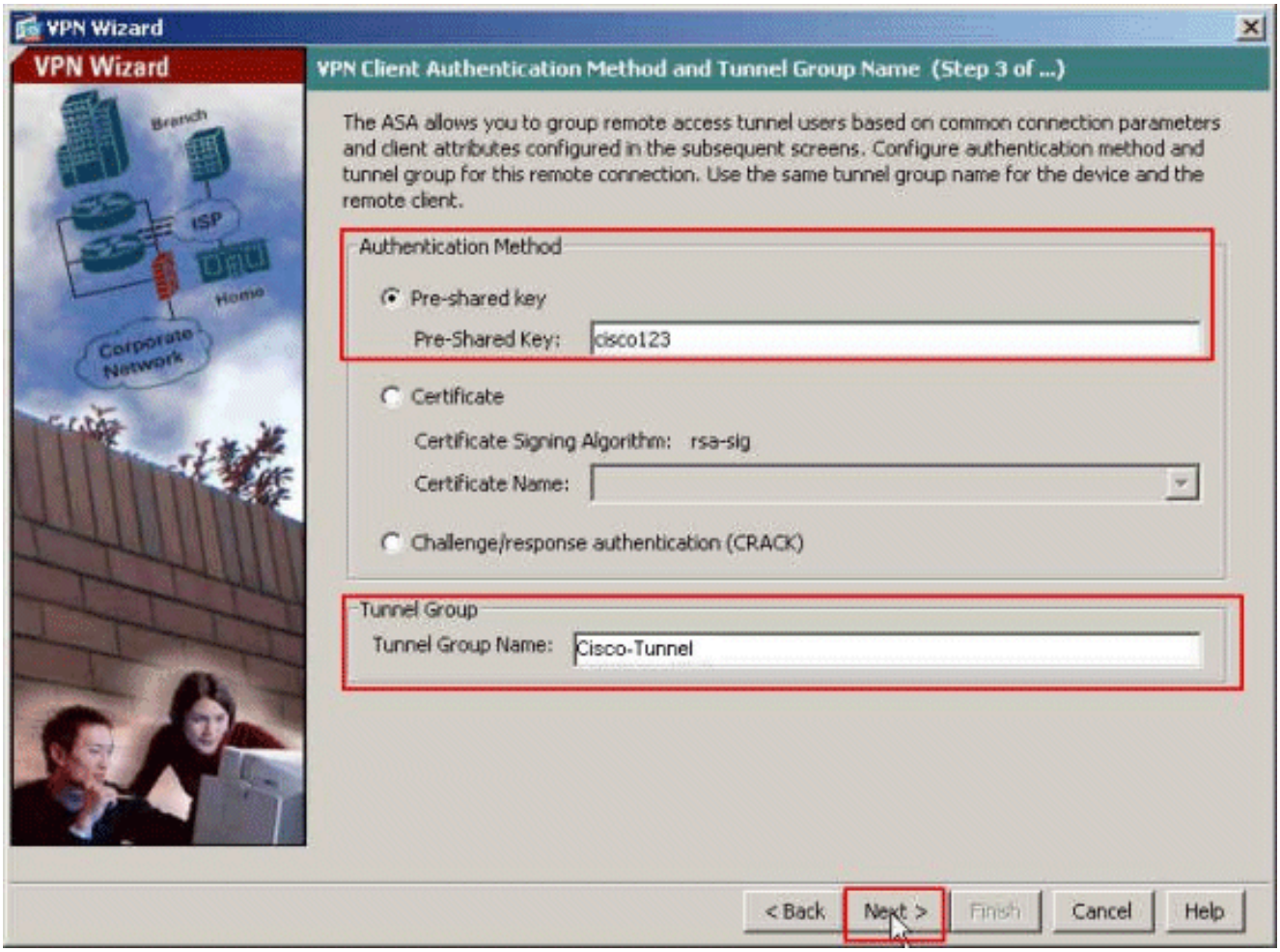
2. Sélectionnez l'**interface de tunnel VPN** au besoin (**dehors**, dans cet exemple), et assurez-vous également que la case à cocher à côté des **sessions d'arrivée d'IPsec d'enable pour sauter des Listes d'accès d'interface** est
vérifiée.



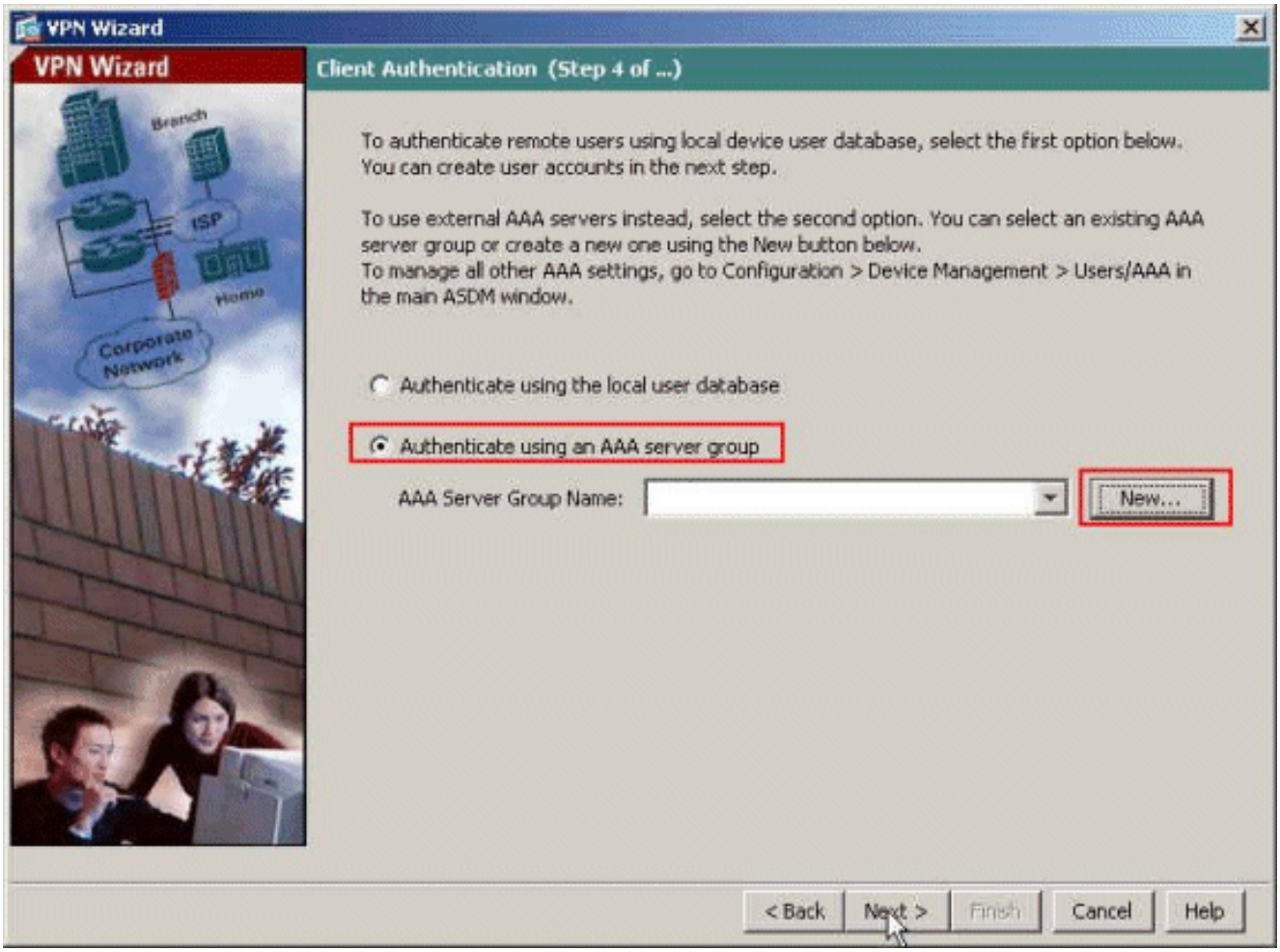
3. Choisissez le type de client vpn comme **Client VPN Cisco, la release 3.x ou plus élevé**. Cliquez sur **Next**
(Suivant).



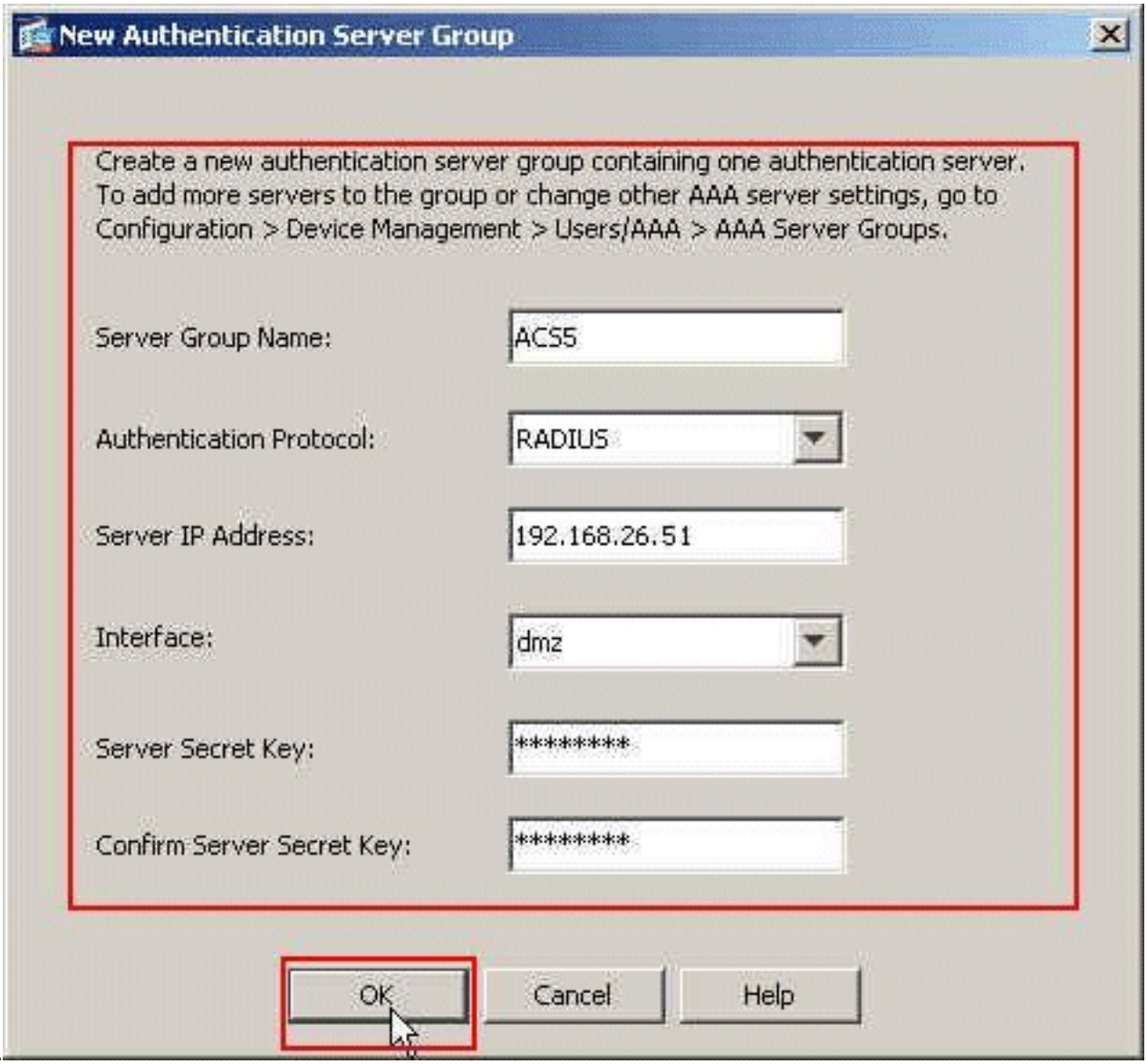
4. Choisissez la **méthode d'authentification** et fournissez les informations d'authentification. La méthode d'authentification utilisée ici est **clé pré-partagée**. En outre, fournissez un nom de **groupe de tunnel** dans l'espace prévu. **La clé pré-partagée** utilisée ici est **cisco123** et le **Tunnel Group Name** utilisé ici est Cisco-**tunnel**. Cliquez sur **Next** (Suivant).



5. Choisissez si vous voulez que des utilisateurs distants soient authentifiés à la base de données des utilisateurs locaux ou à un groupe de serveurs AAA externe. Ici, nous choisissons **authentifions utilisant un Groupe de serveurs AAA**. Cliquez sur New à côté de la zone d'identification de Groupe de serveurs AAA afin de créer un nouveau nom de Groupe de serveurs
AAA.

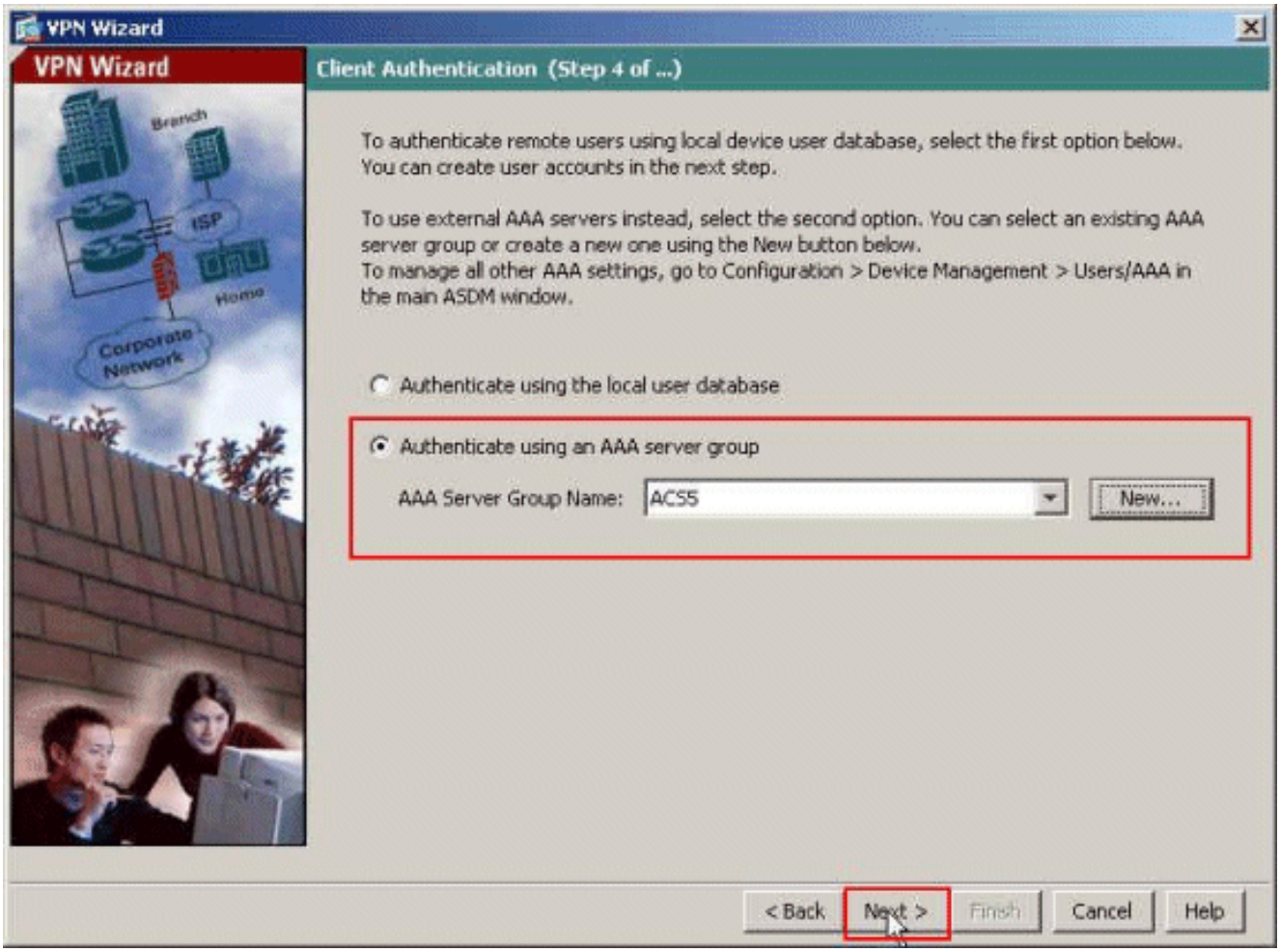


6. Fournissez le nom de nom de groupe de serveurs, d'authentification Protocol, d'adresse IP du serveur, d'interface, et la clé secrète de serveur dans les espaces respectifs fournis, et cliquez sur

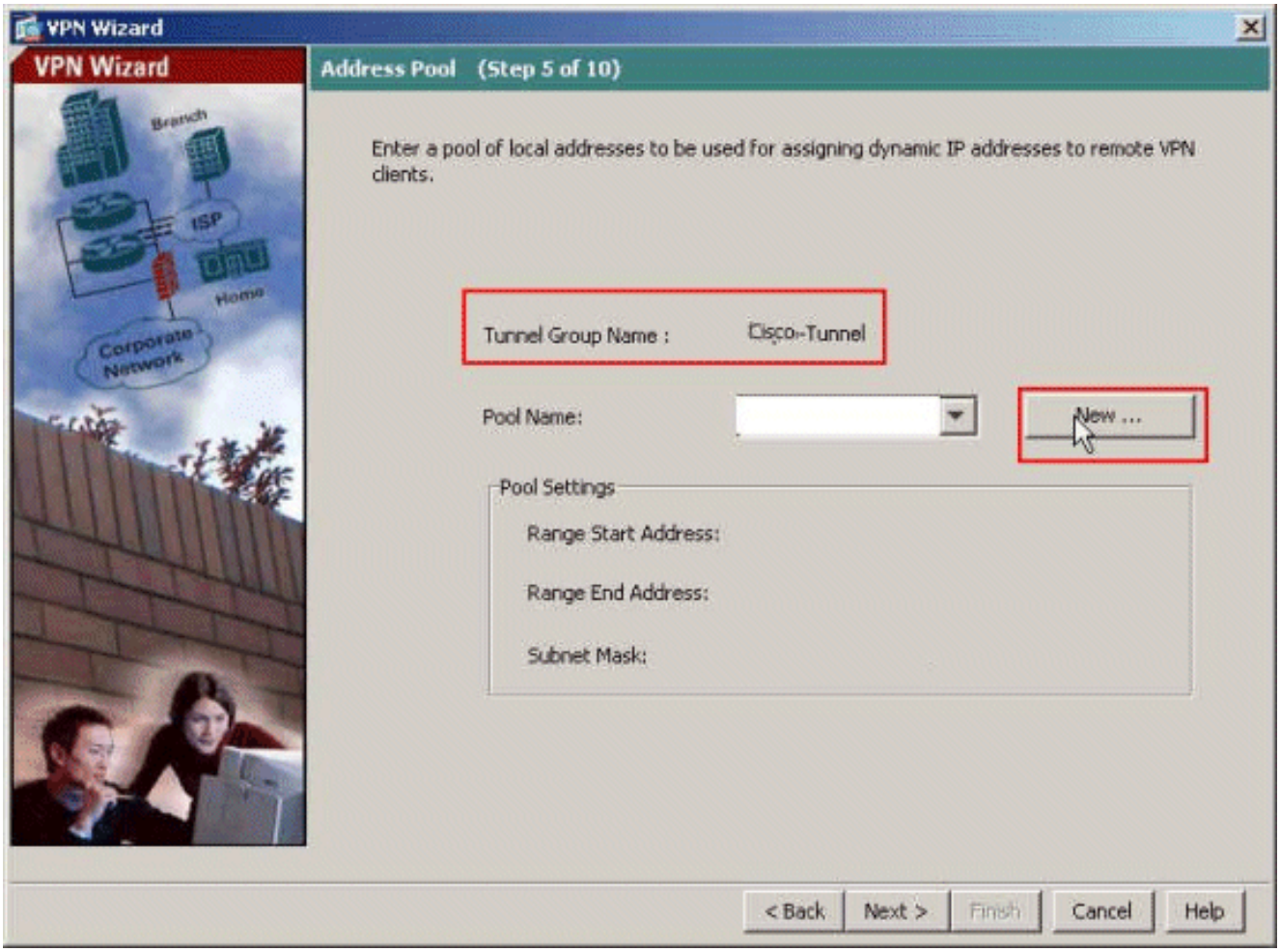


OK.

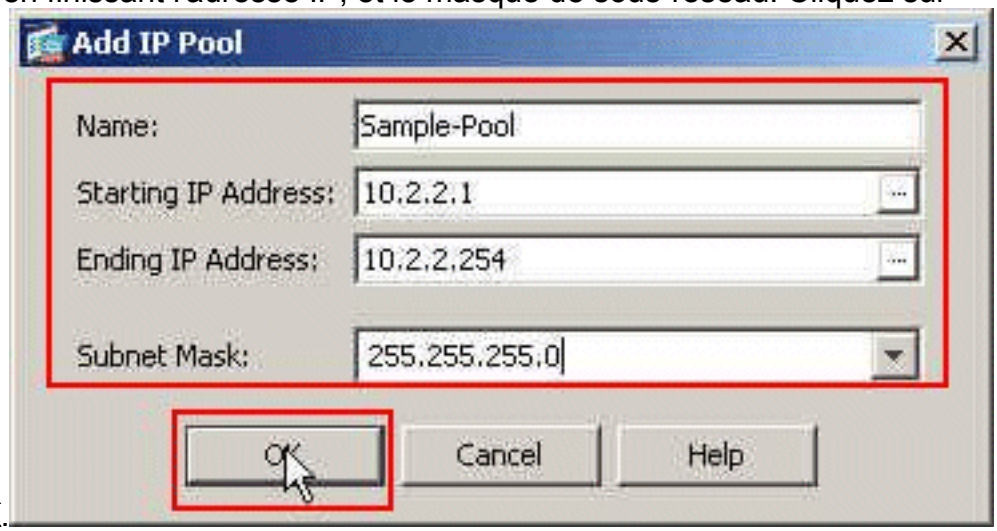
7. Cliquez sur **Next** (Suivant).



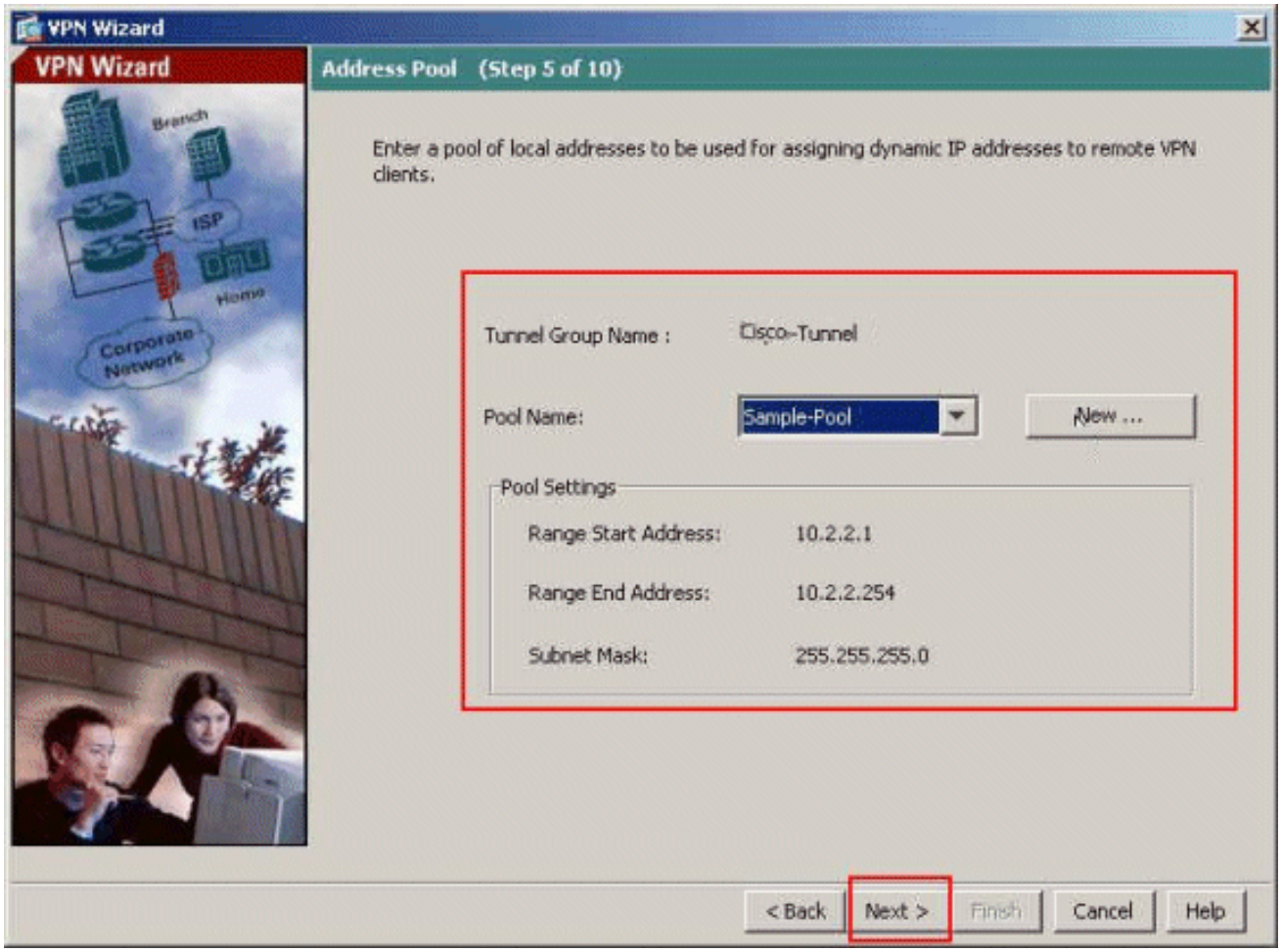
8. Définissez un pool des adresses locales à assigner dynamiquement aux clients VPN distants quand elles se connectent. Cliquez sur New afin de créer un nouveau groupe d'adresse locale.



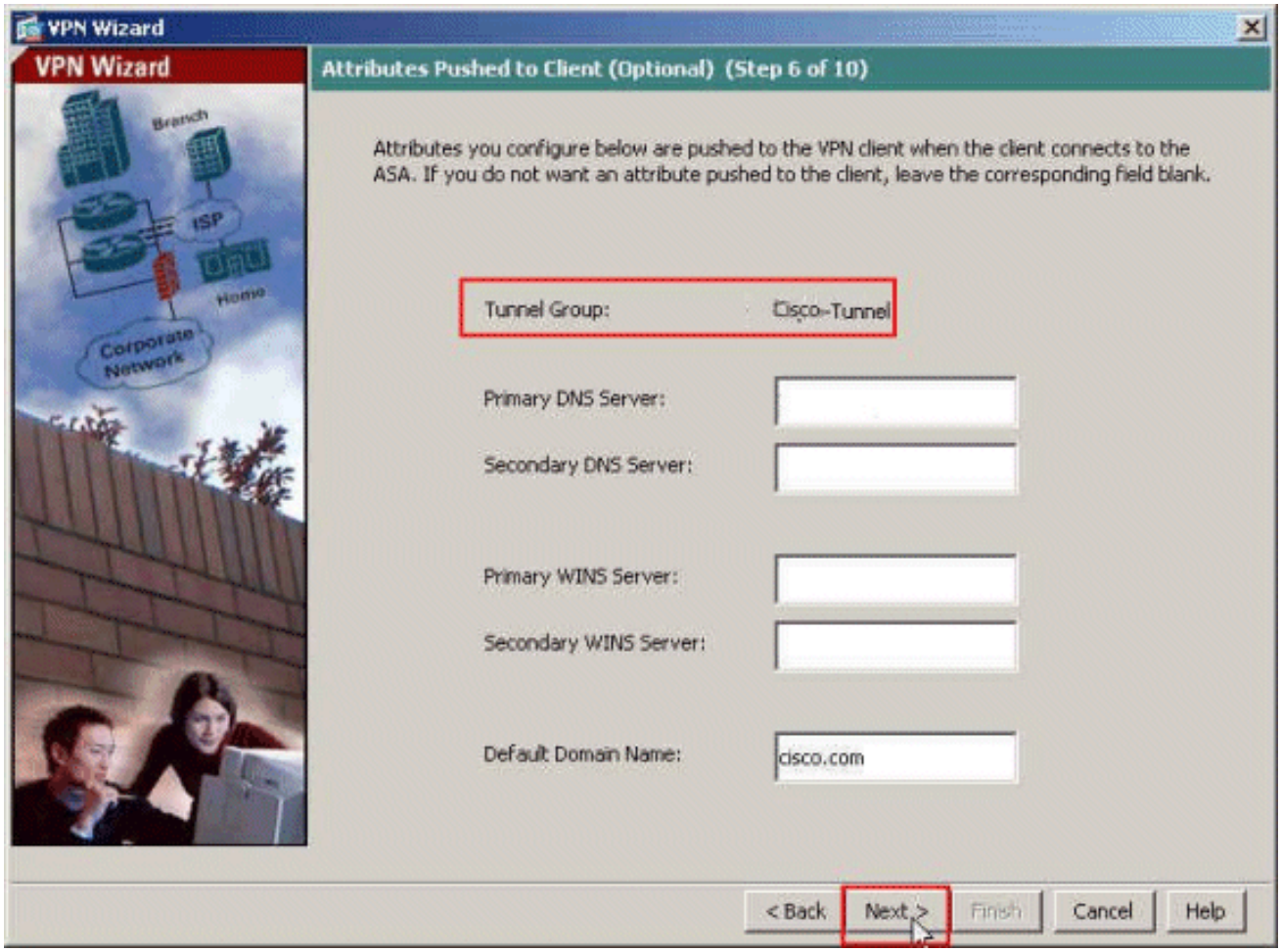
9. Dans la fenêtre de pool d'IP d'ajouter, fournissez le nom du pool, en commençant l'adresse IP, en finissant l'adresse IP, et le masque de sous-réseau. Cliquez sur OK.



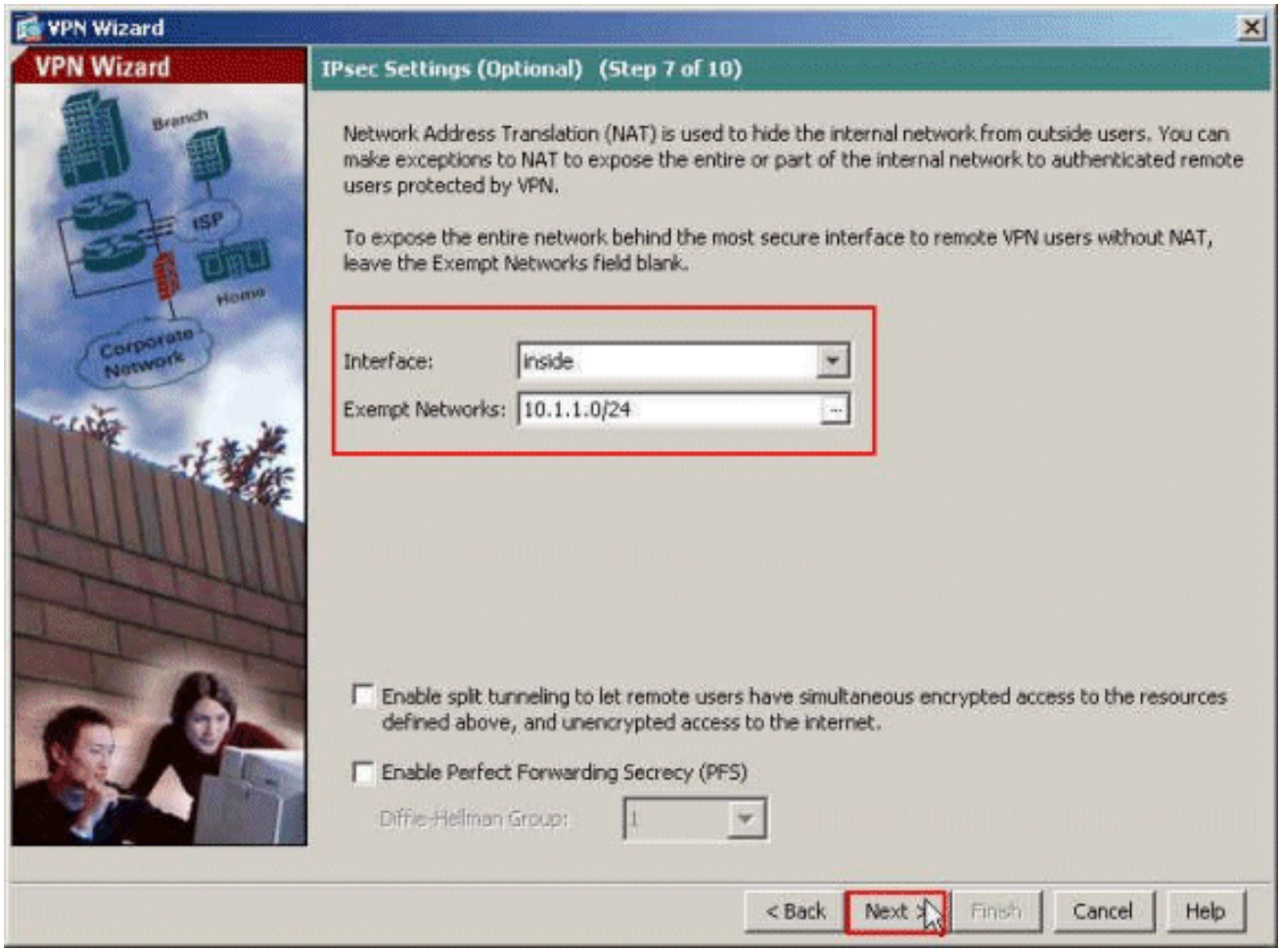
10. Sélectionnez le nom du pool de la liste déroulante, et cliquez sur Next. Le nom du pool pour cet exemple est l'Échantillon-**groupe** qui a été créé dans l'étape 9.



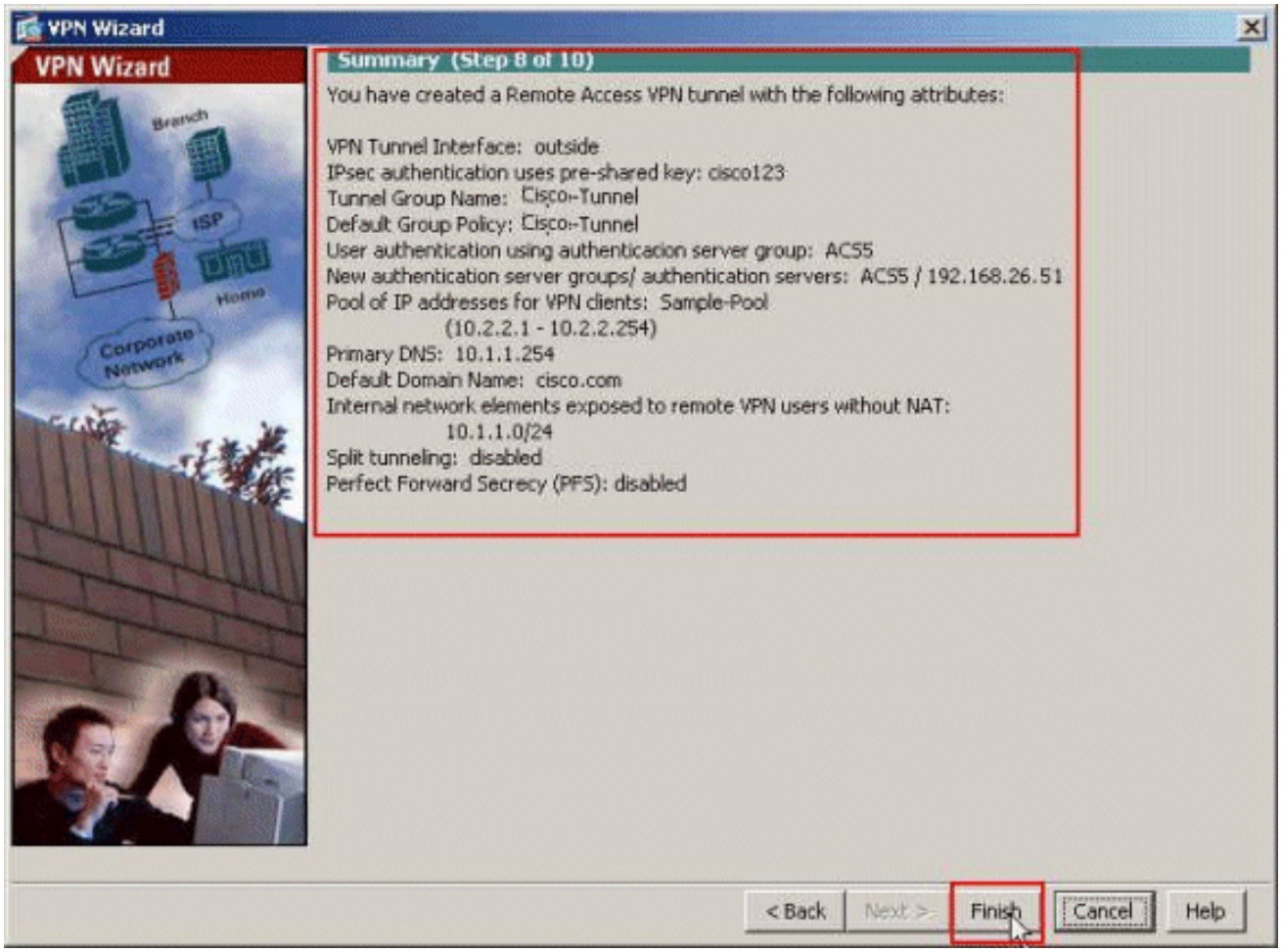
11. *Facultatif :* Spécifiez les informations du serveur DNS et WINS et un nom de Domaine par défaut à diffuser aux clients VPN
distants.



12. Spécifiez lequel, le cas échéant, des hôtes ou des réseaux internes devraient être exposés aux utilisateurs distants de VPN. Cliquez sur Next après fourniture du nom d'interface et les réseaux à exempter dans les réseaux exempts mettent en place.Si vous laissez cette liste vide, elle permet à des utilisateurs distants de VPN d'accéder au réseau interne en entier de l'ASA.Vous pouvez également activer split tunneling sur cette fenêtre. Split tunneling crypte le trafic aux ressources définies précédemment dans cette procédure et fournit un accès non crypté à l'ensemble de l´Internet en ne tunnellisant pas ce trafic. Si la Transmission tunnel partagée n'est *pas* activée, tout le trafic des utilisateurs distants de VPN est tunnellisé à l'ASA. Ceci peut devenir très intensif en largeur de bande et processeur intensif, basé sur votre configuration.



13. Cette fenêtre montre un résumé des actions que vous avez prises. Cliquez sur **Finish** si vous êtes satisfait de votre configuration.



Configurez l'ASA avec le CLI

C'est la configuration CLI :

Configuration en cours sur le périphérique ASA

```
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#
```

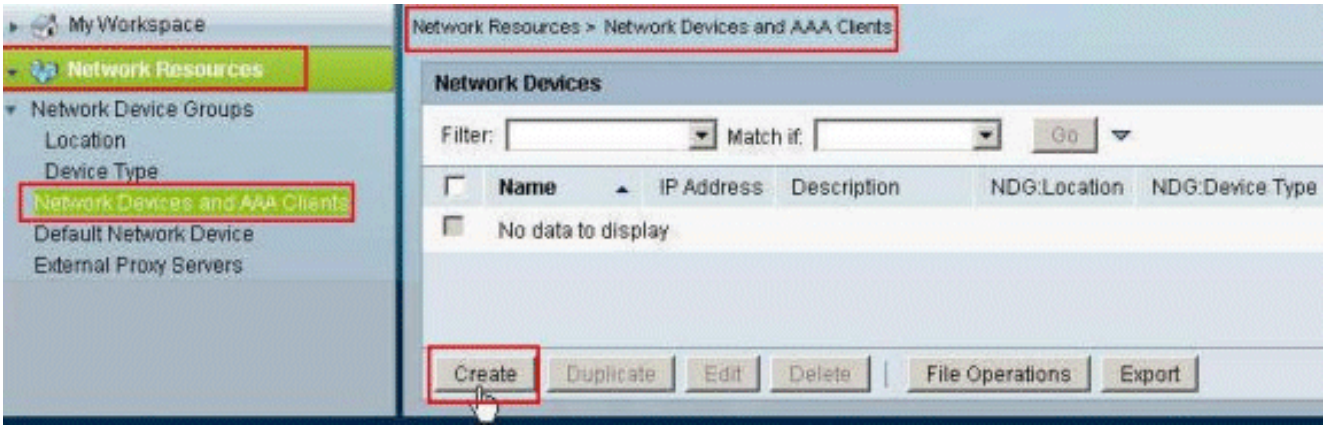
Configurez ACS pour l'ACL téléchargeable pour l'utilisateur individuel

Vous pouvez configurer les Listes d'accès téléchargeables sur le Cisco Secure ACS 5.x car Permissions Object Désignée et puis l'assignez à un profil d'autorisation qui sera choisi dans la section de résultat de la règle au service d'accès.

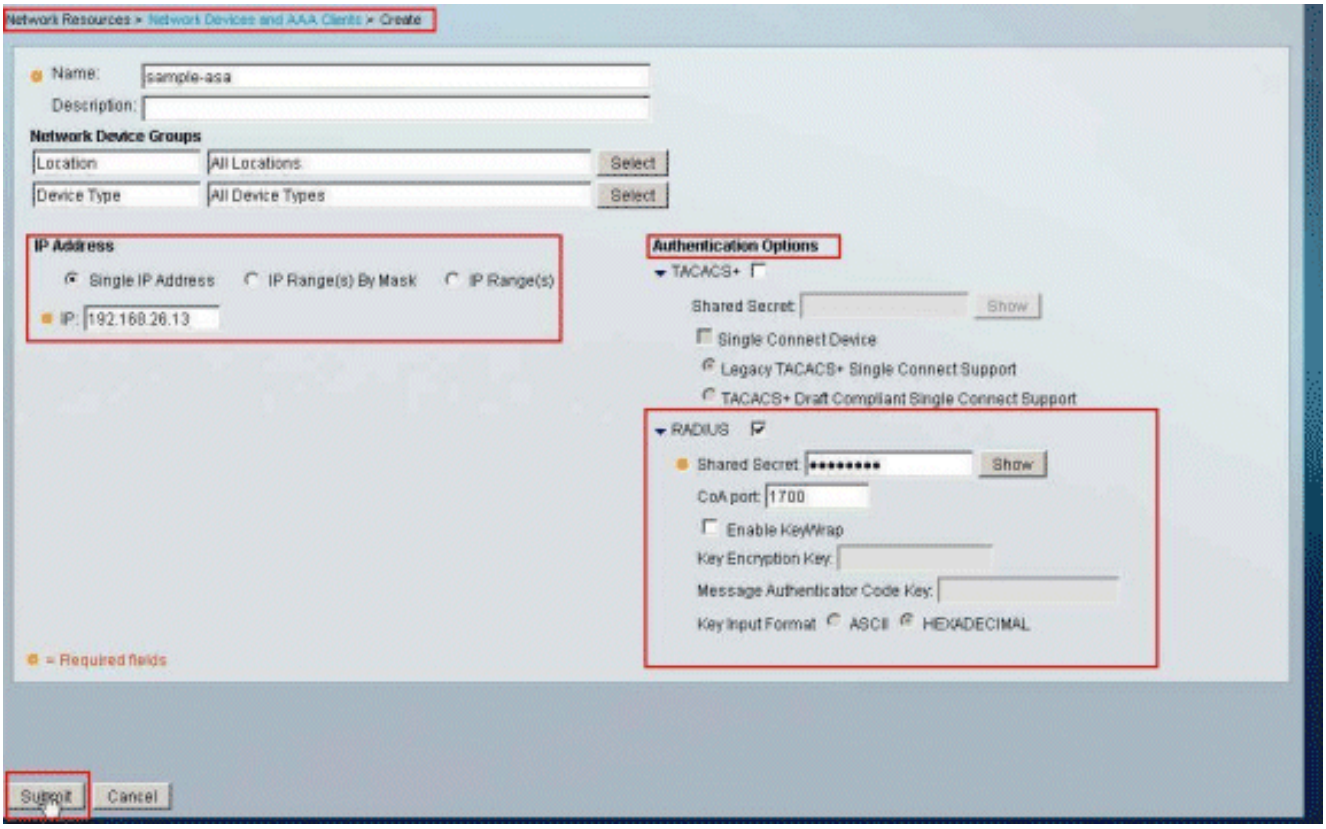
Dans cet exemple, l'utilisateur **Cisco d'**IPsec VPN authentifie avec succès, et le serveur de RADIUS envoie une liste d'accès téléchargeable aux dispositifs de sécurité. L'utilisateur « Cisco » peut accéder à seulement le serveur de 10.1.1.2 et refuse tout autre accès. Afin de vérifier l'ACL, voyez l'ACL téléchargeable pour la section d'utilisateur/groupe.

Terminez-vous ces étapes afin de configurer le client RADIUS dans un Cisco Secure ACS 5.x :

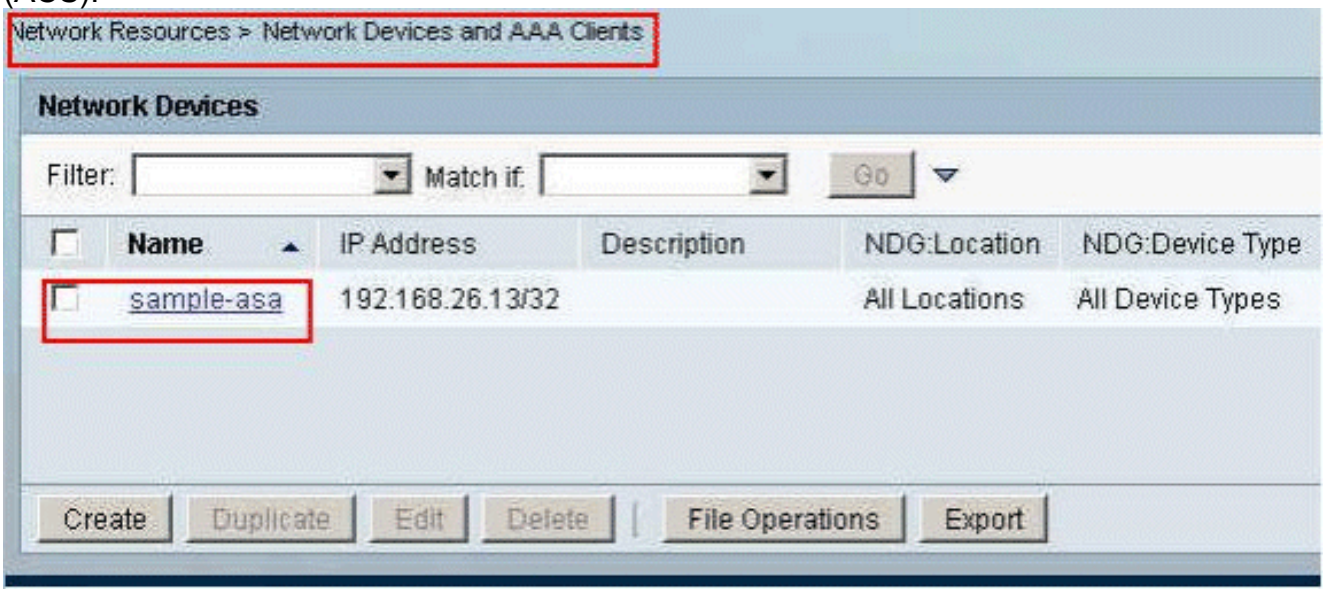
1. Choisissez les **ressources de réseau >** les **périphériques de réseau et les clients d'AAA**, et le clic **créent** afin d'ajouter une entrée pour l'ASA dans la base de données du serveur de RADIUS.



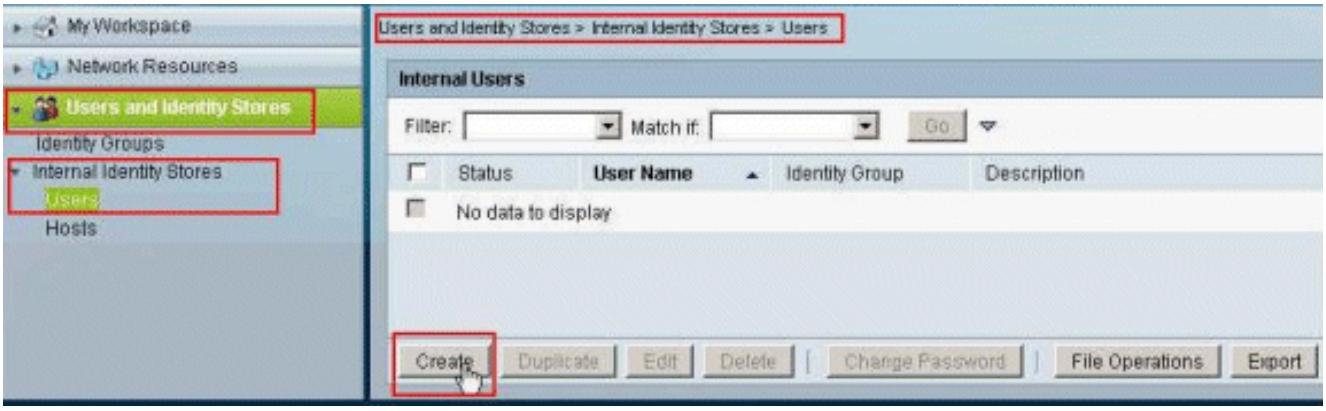
2. Écrivez le nom significatif a localement - pour l'ASA (échantillon-**asa**, dans cet exemple), puis entrez dans **192.168.26.13** dans le domaine d'adresse IP. Choisissez **RADIUS** dans la section Options d'authentification en vérifiant la case à cocher de **RADIUS** et écrivez **cisco123** pour le champ secret partagé. Cliquez sur **Submit**.



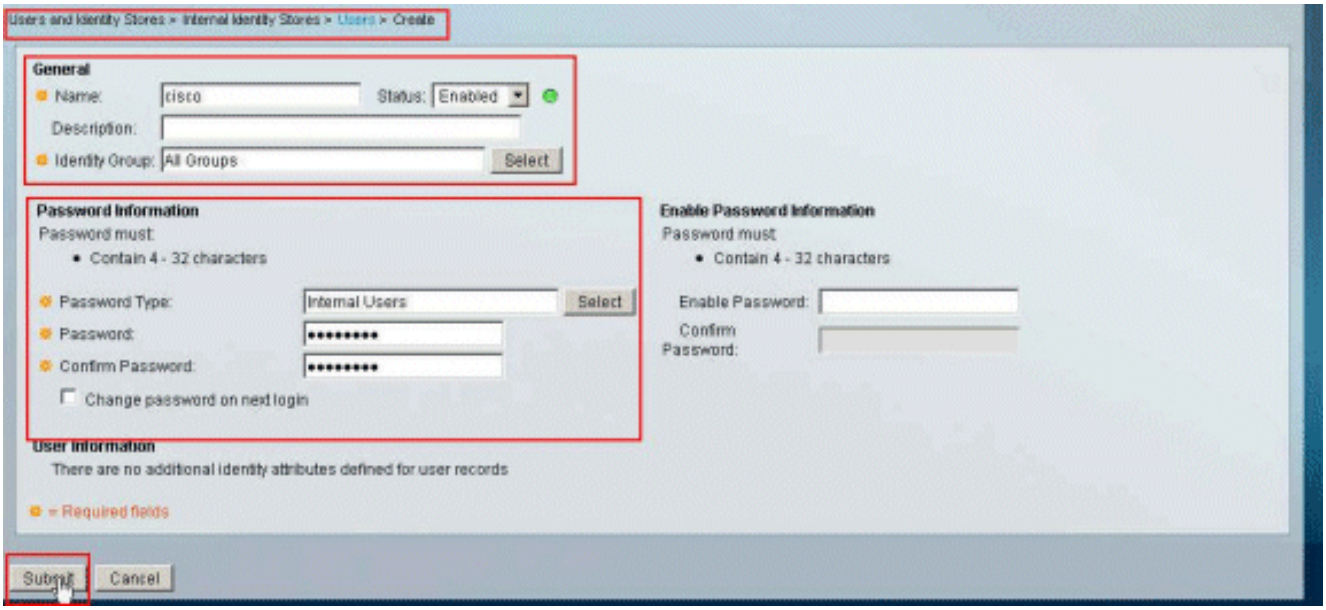
3. L'ASA est ajoutée avec succès à la base de données du serveur de RADIUS (ACS).



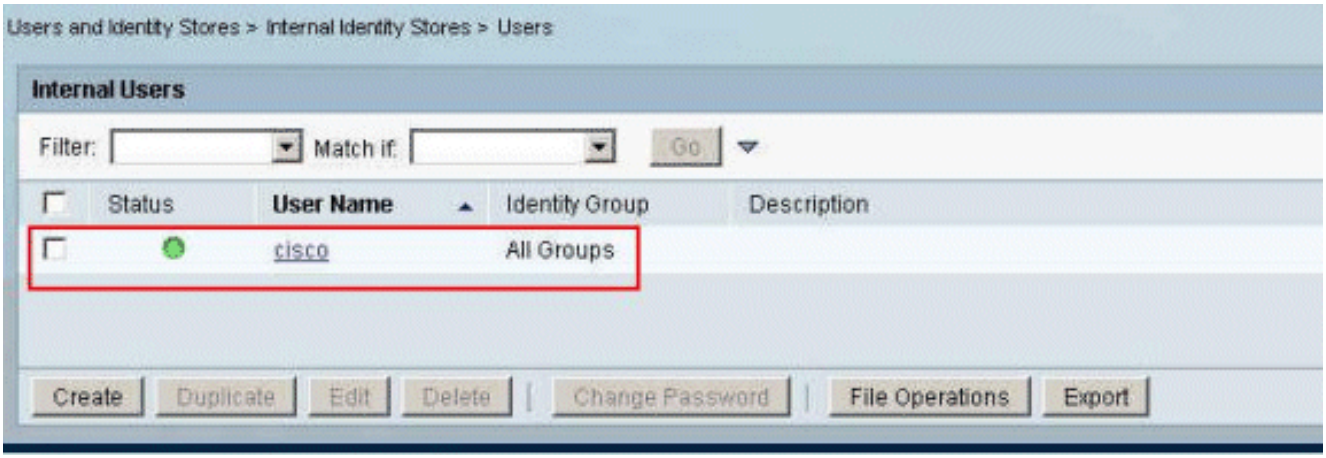
4. Choisissez les **utilisateurs et l'identité enregistre > identité interne enregistre >** des **utilisateurs**, et le clic **créent** afin de créer un utilisateur dans la base de données locale de l'ACS pour l'authentification
VPN.



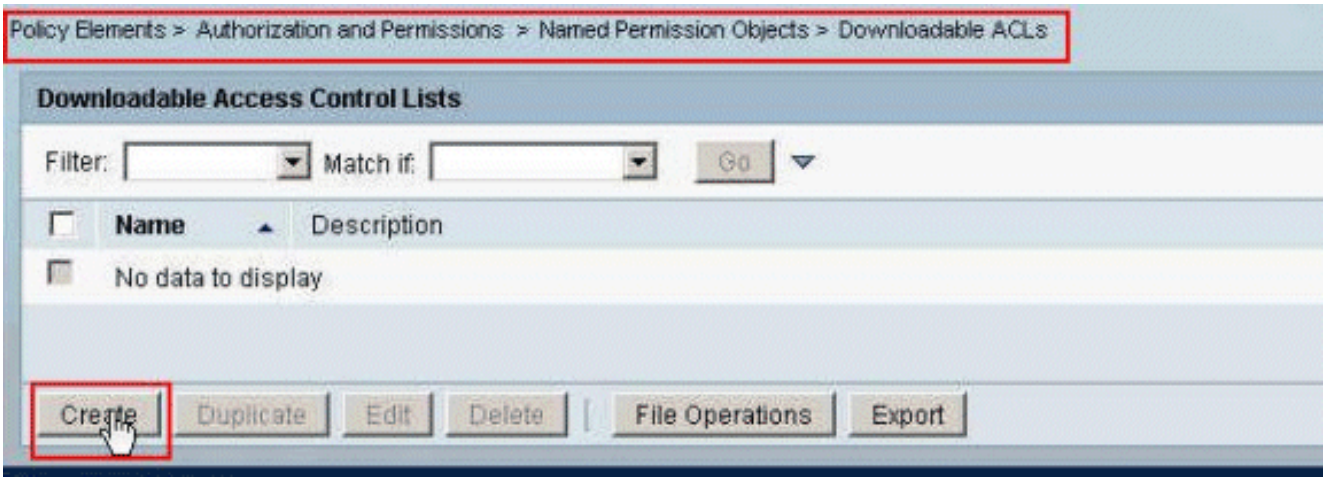
5. Écrivez le nom d'utilisateur **Cisco**. Sélectionnez le type de mot de passe comme **utilisateurs internes**, et entrez le mot de passe (**cisco123**, dans cet exemple). Confirmez le mot de passe, et cliquez sur Submit.



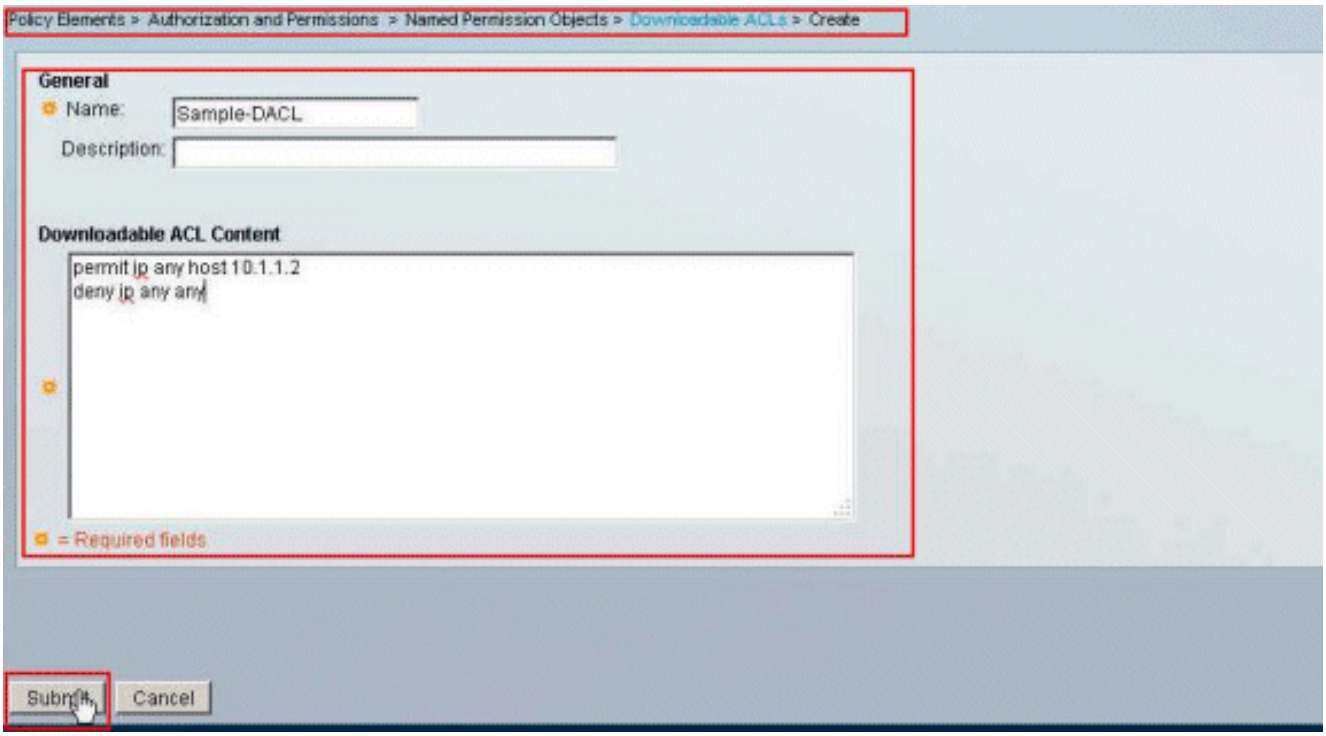
6. L'utilisateur **Cisco** est créé avec succès.



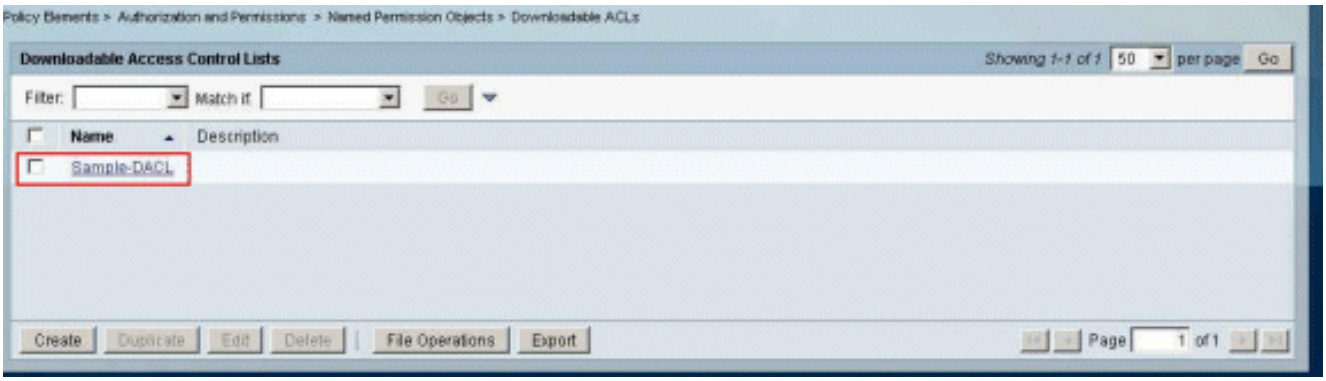
7. Afin de créer un ACL téléchargeable, choisir des **éléments de stratégie** > l'**autorisation et des autorisations** > **a nommé Permission Objects** > **ACLs téléchargeable**, et le clic **créent**.



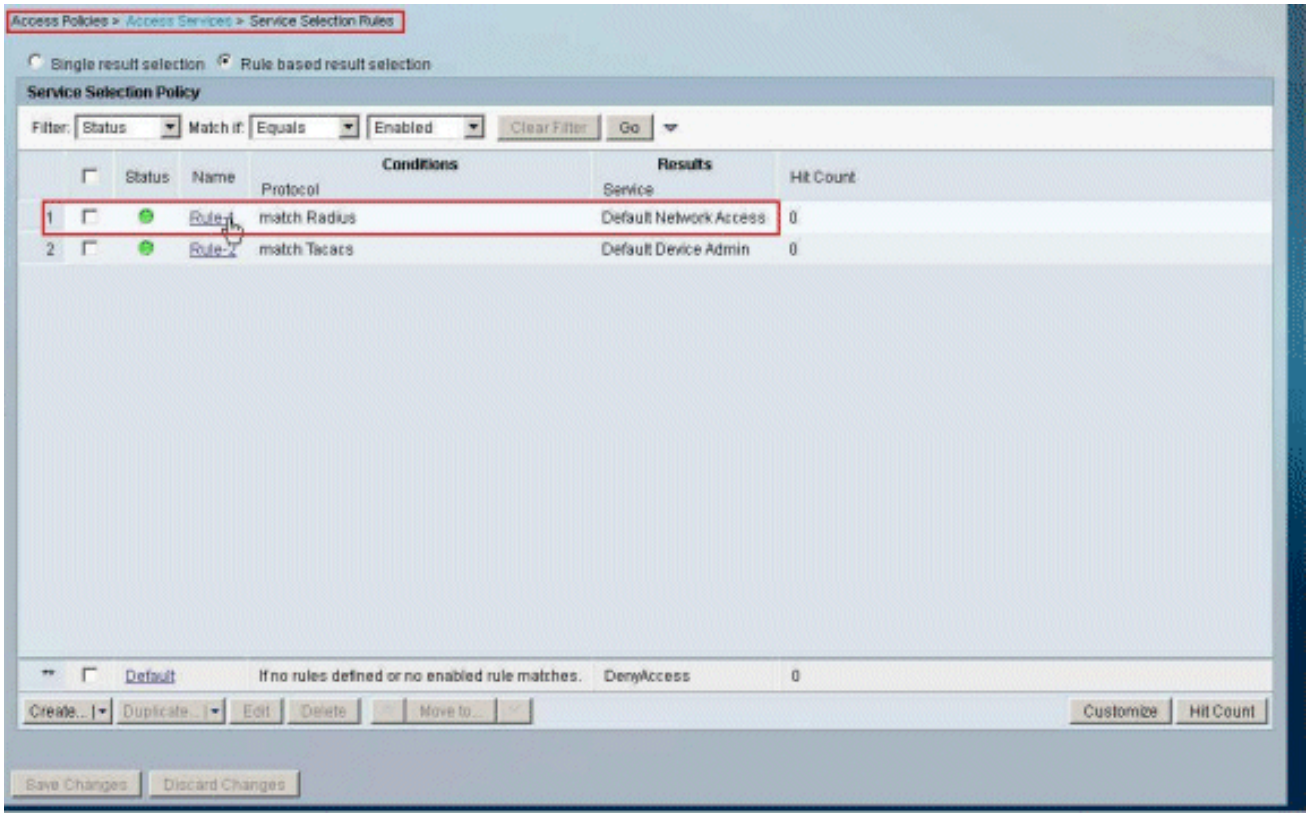
8. Fournissez le **nom** pour l'ACL téléchargeable, aussi bien que le **contenu d'ACL**. Cliquez sur **Submit**.



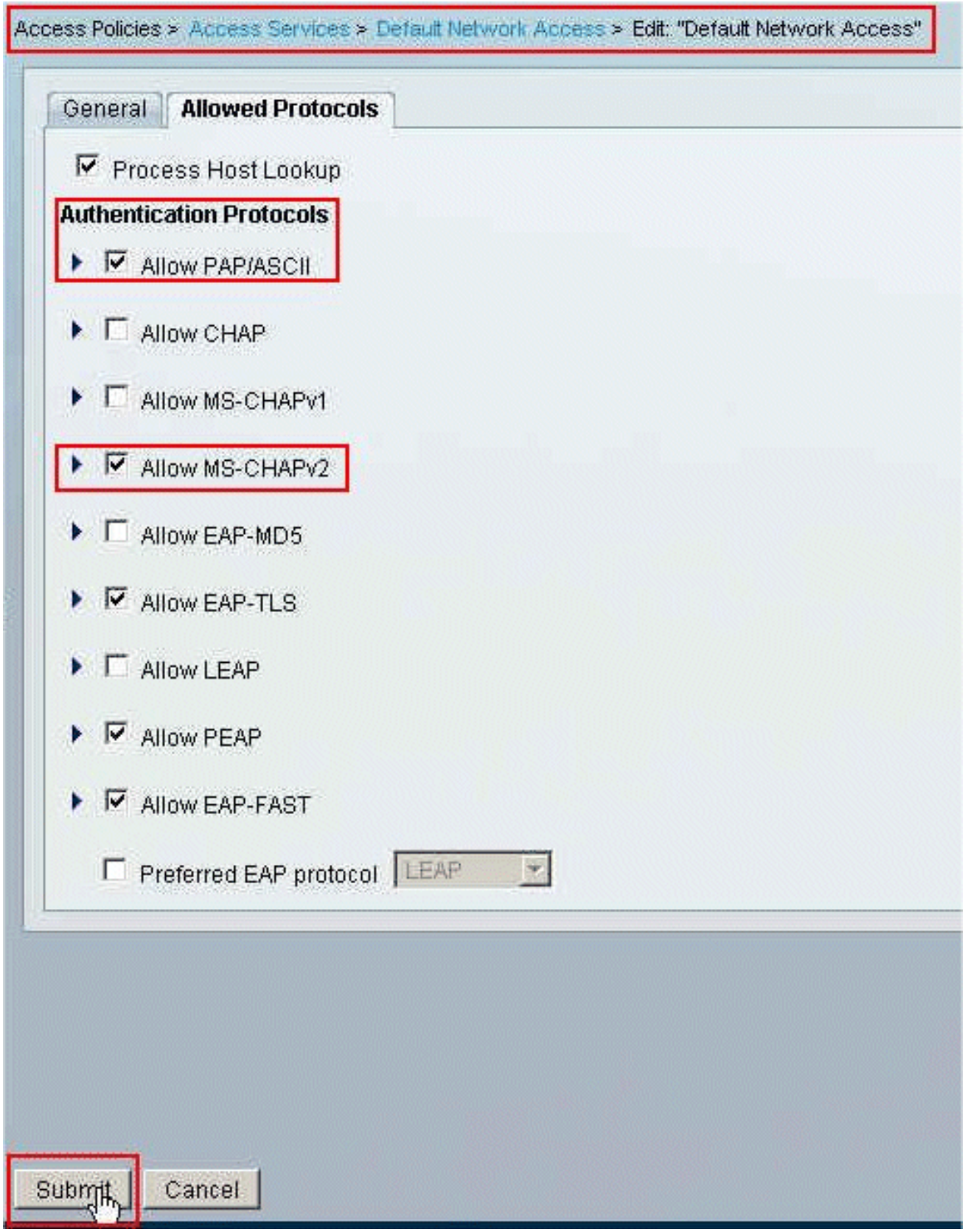
9. **L'échantillon-DACL** téléchargeable d'ACL est créé avec succès.



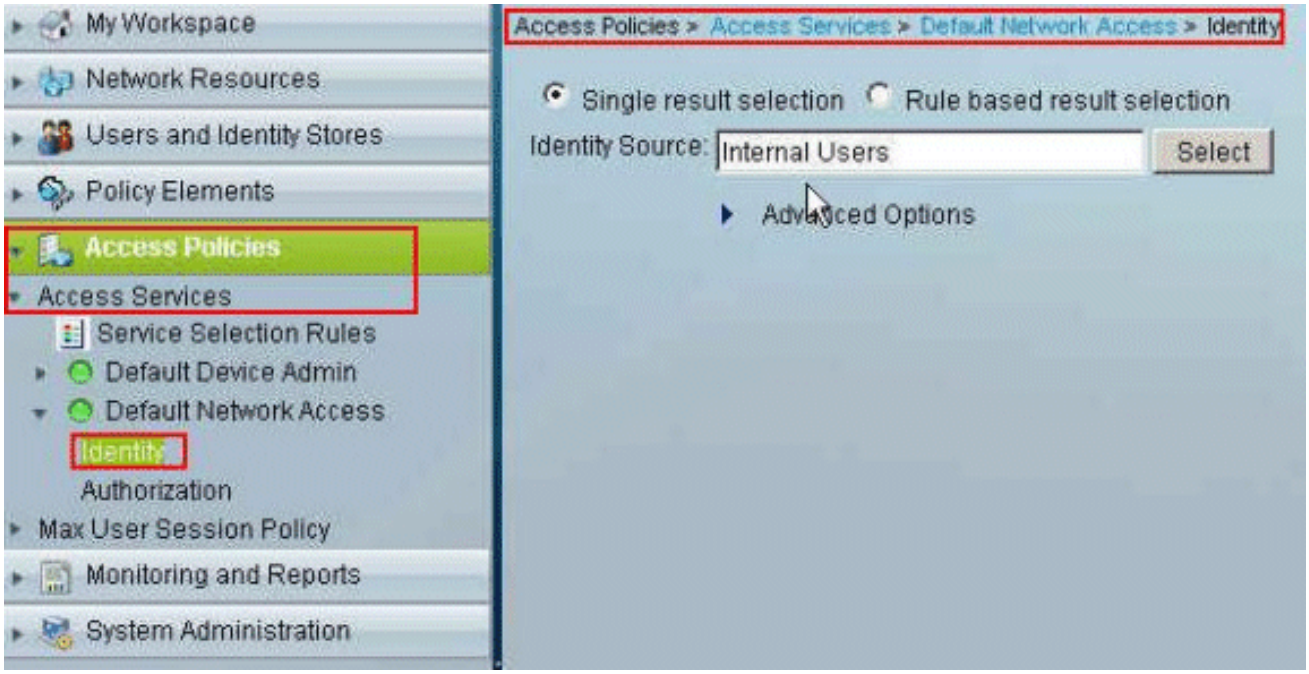
10. Afin de configurer les access-policy pour l'authentification VPN, choisissez les **stratégies d'Access >** les **services d'accès >** les **règles de sélection de service**, et déterminez quel service approvisionne au protocole RADIUS. Dans cet exemple, **ordonnez 1 les** correspondances **RADIUS**, et l'accès au réseau de par défaut approvisionnera à la demande
RADIUS.



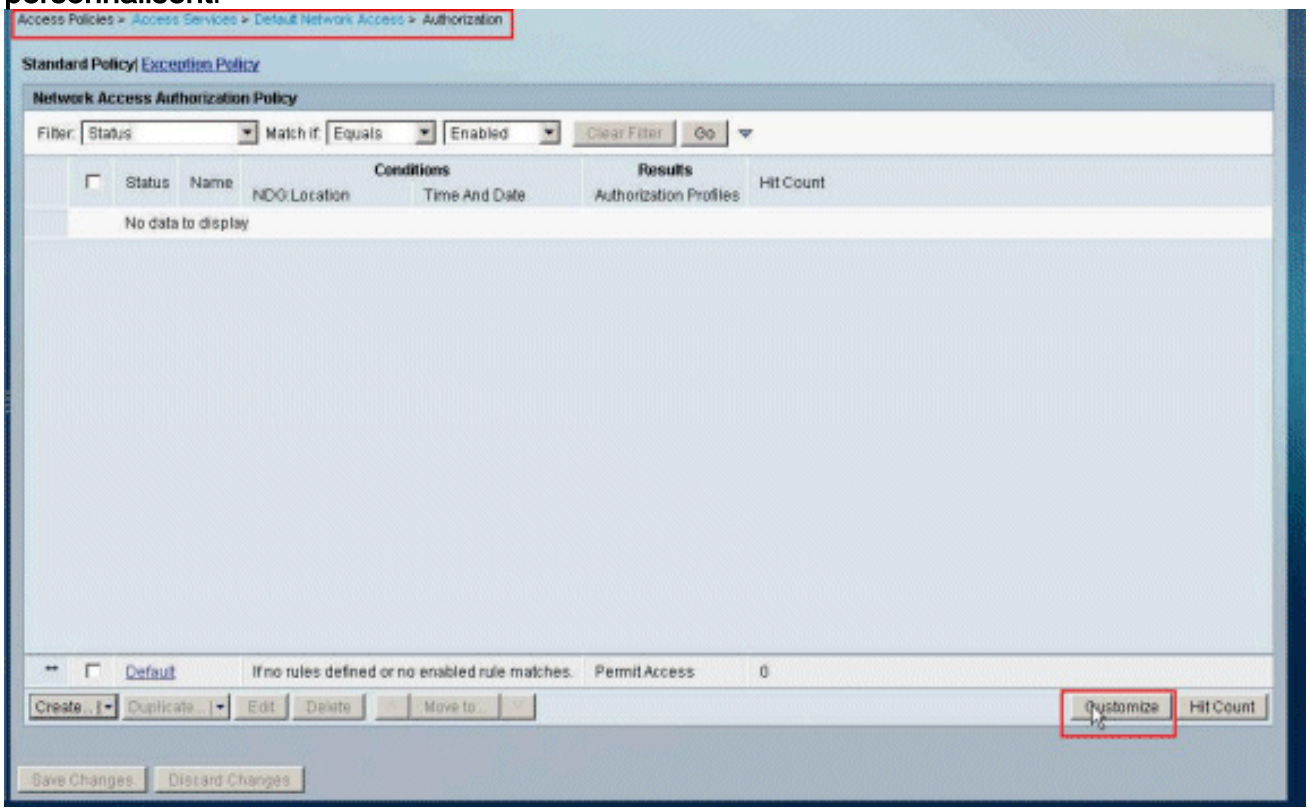
11. Choisissez le **service d'accès** déterminé de l'étape 10. Dans cet exemple, l'**accès au réseau par défaut** est utilisé. Choisissez l'onglet **permis de protocoles**, et assurez-vous que **permettez PAP/ASCII** et **permettez MS-CHAPv2** sont sélectionnés. Cliquez sur **Submit**.



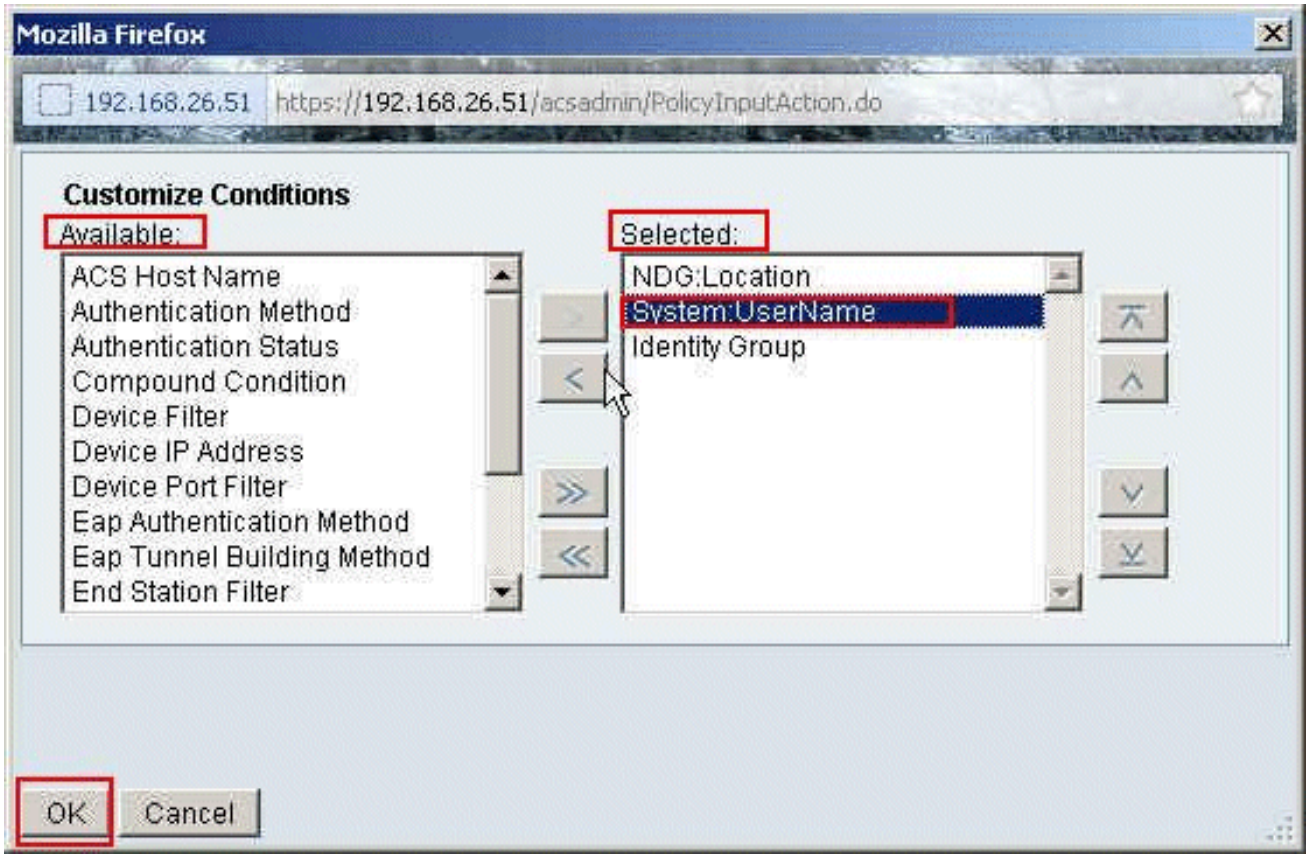
12. Cliquez sur en fonction la **section d'identité des services d'accès**, et assurez-vous que des **utilisateurs internes** est sélectionnés comme source d'identité. Dans cet exemple, nous avons pris l'accès au réseau par
défaut.



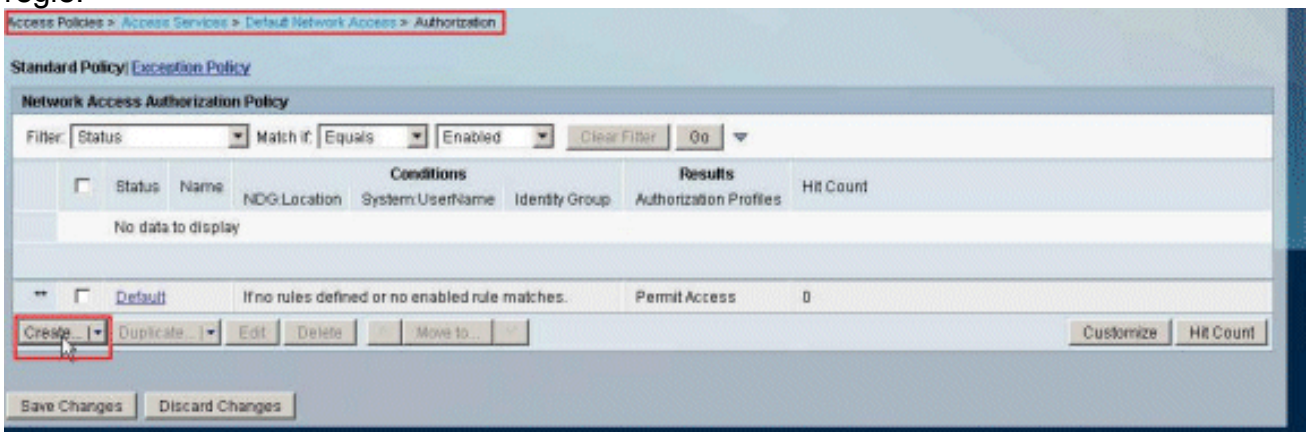
13. Choisissez les **stratégies d'Access** > les **services d'accès** > l'**accès au réseau** > l'**autorisation de par défaut**, et le clic **personnalisent**.



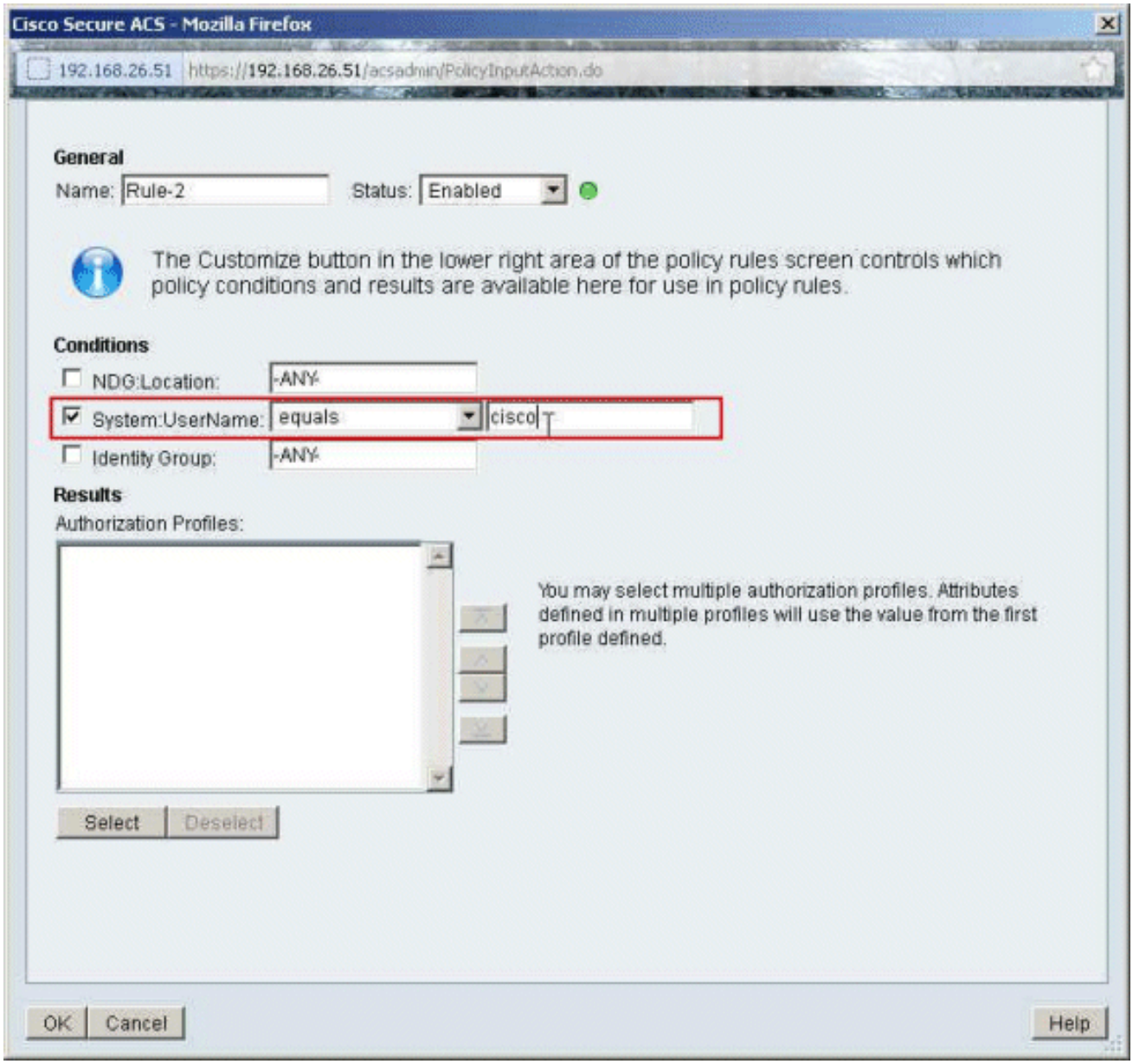
14. **Système de** mouvement : **Le nom d'utilisateur de la** colonne **disponible à la** colonne **sélectionnée**, et cliquent sur OK.



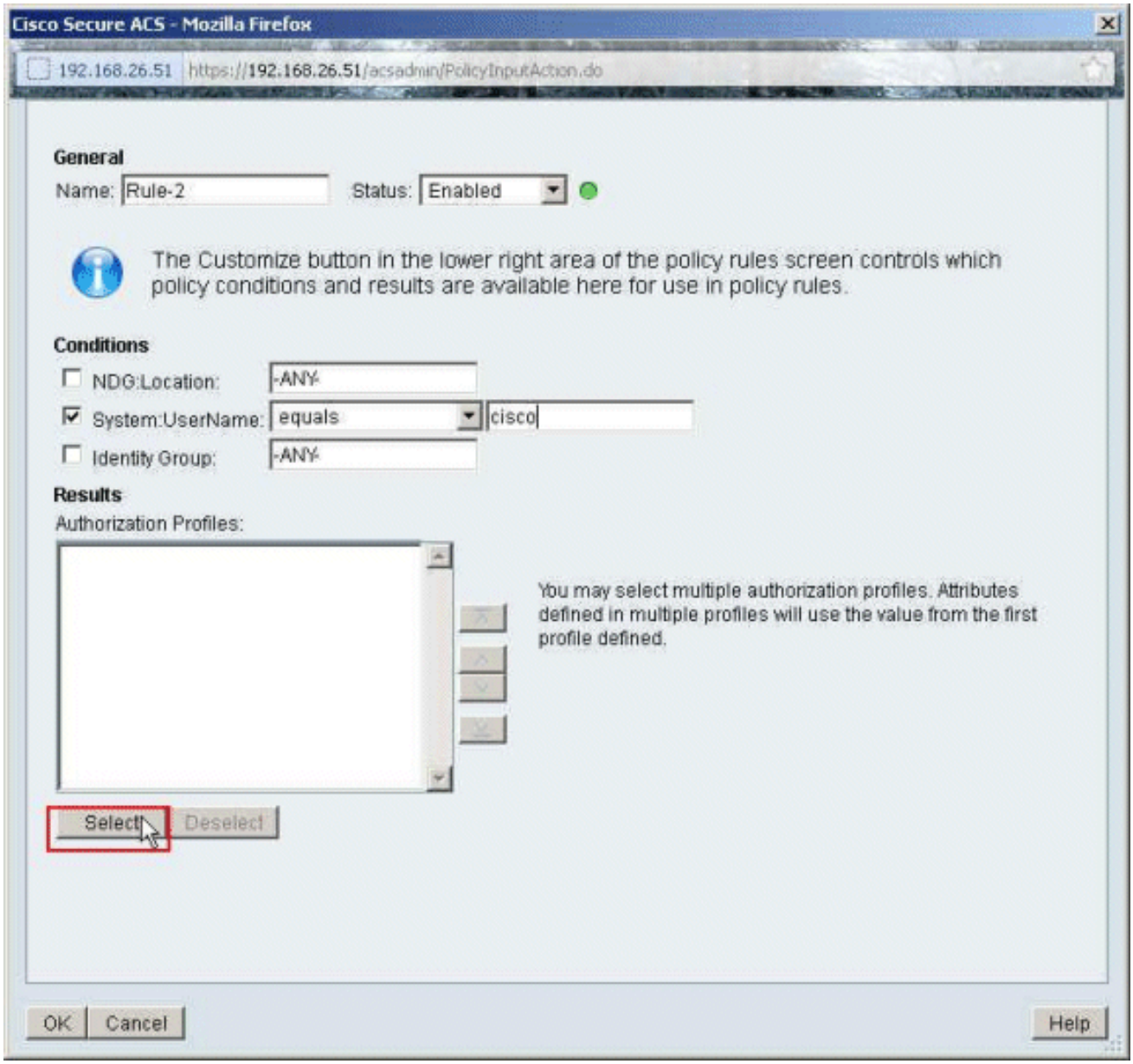
15. Le clic **créent** afin de créer une nouvelle règle.



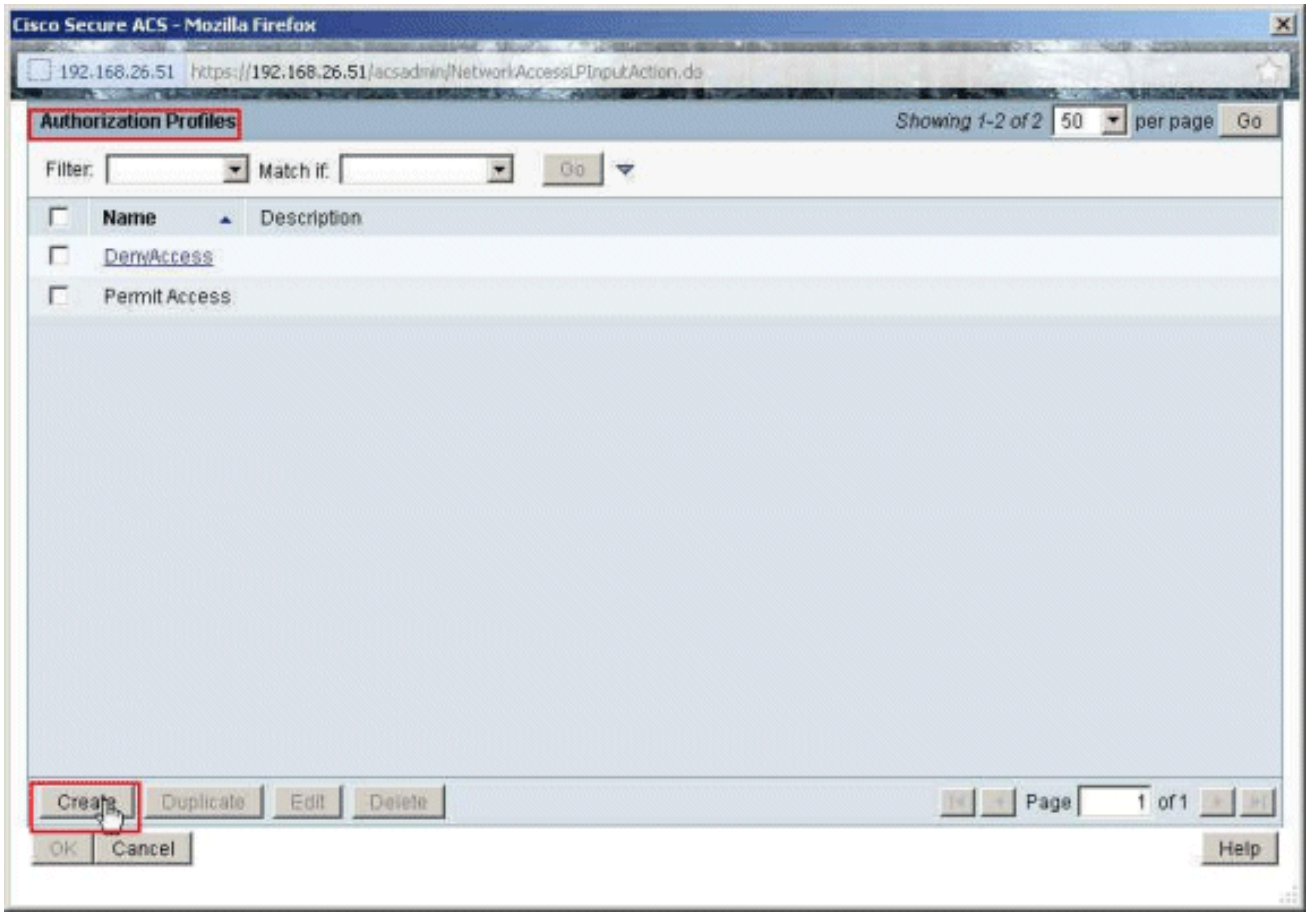
16. Assurez-vous que la case à cocher à côté du **système : Le nom d'utilisateur** est sélectionné, choisit des **égaux de la** liste déroulante, et écrit le nom d'utilisateur **Cisco**.



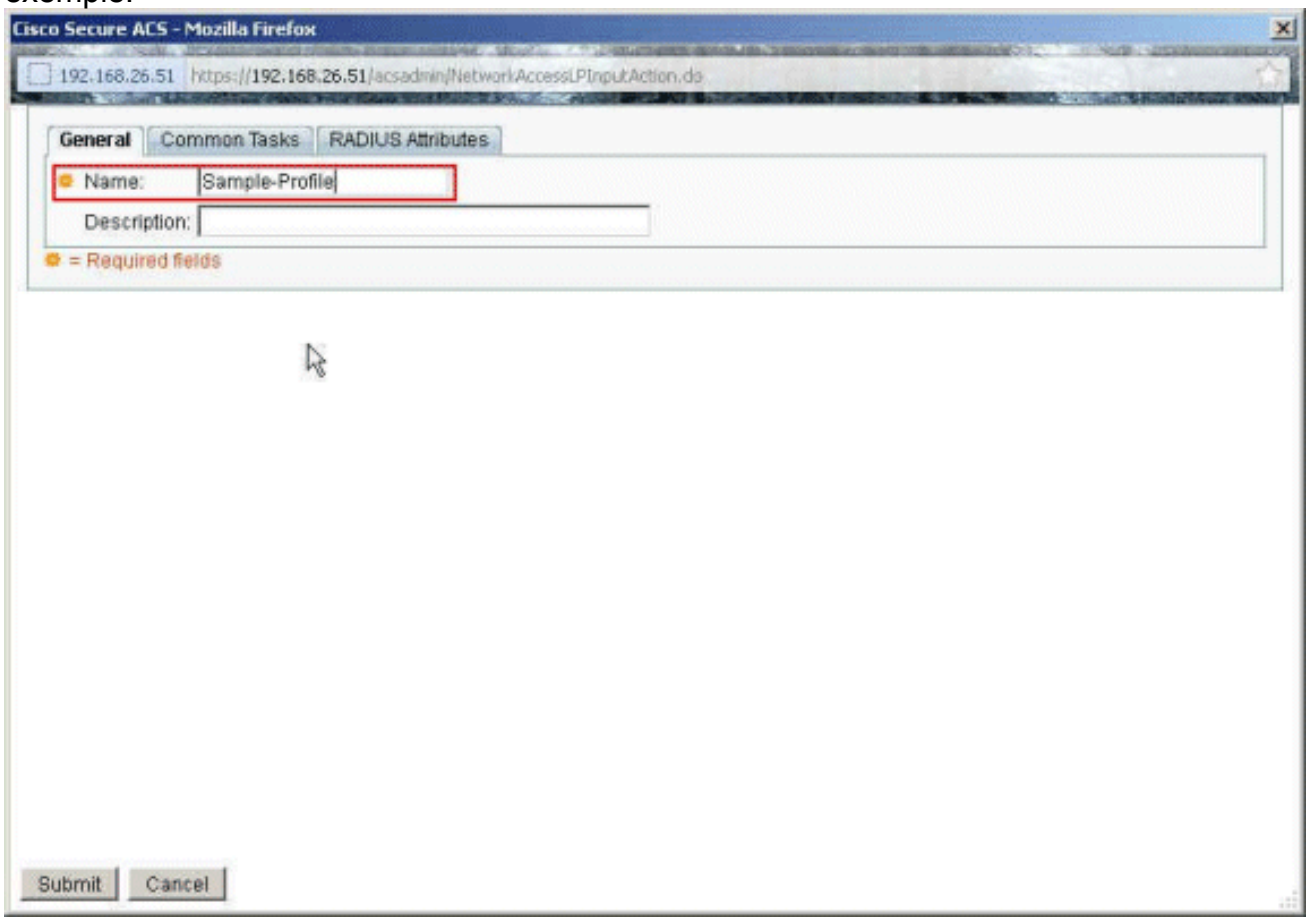
17. Clic **choisi**.



18. Le clic **créent** afin de créer un nouveau profil d'autorisation.

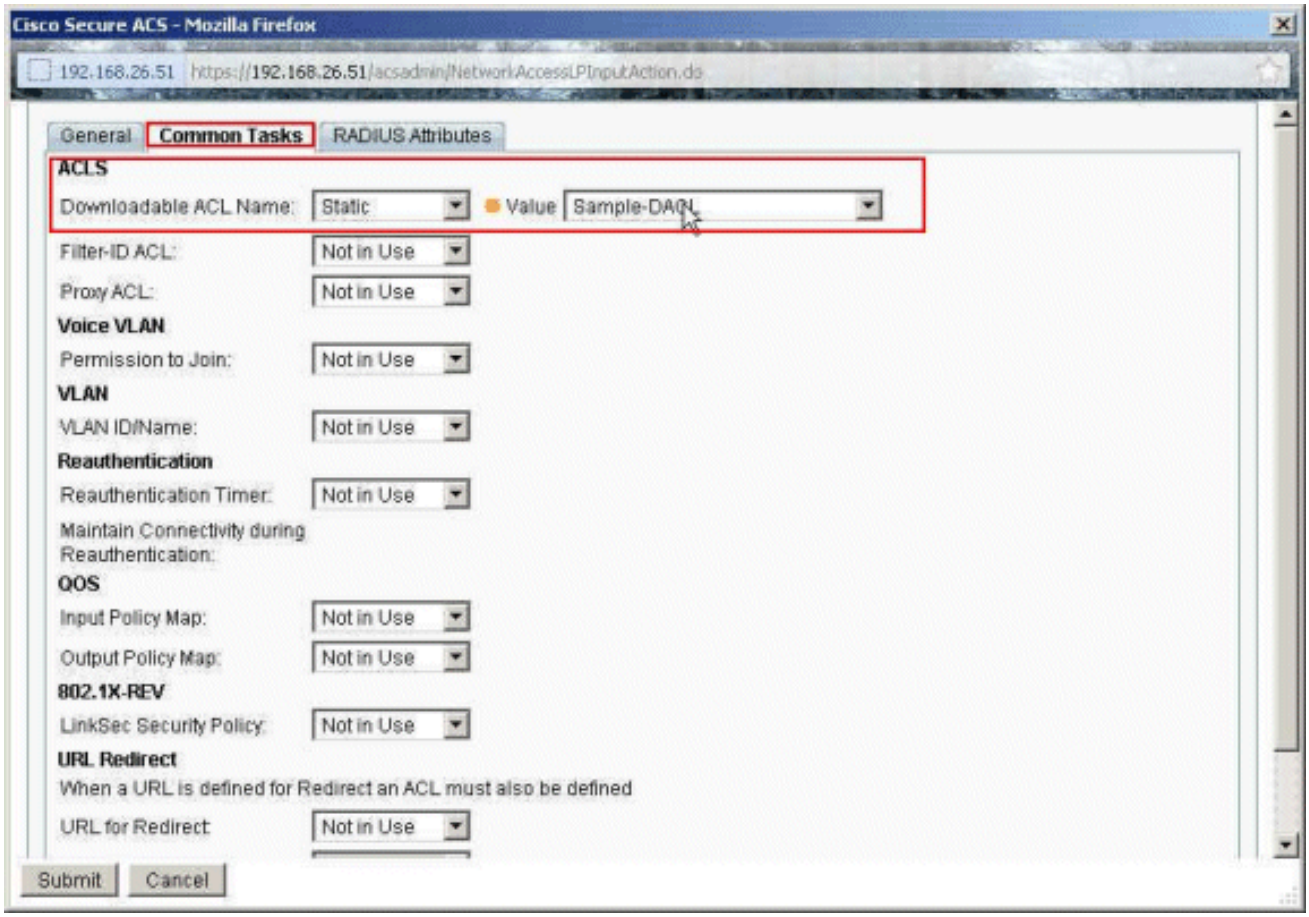


19. Fournissez un nom pour le **profil d'autorisation**. **L'exemple de profil** est utilisé dans cet exemple.

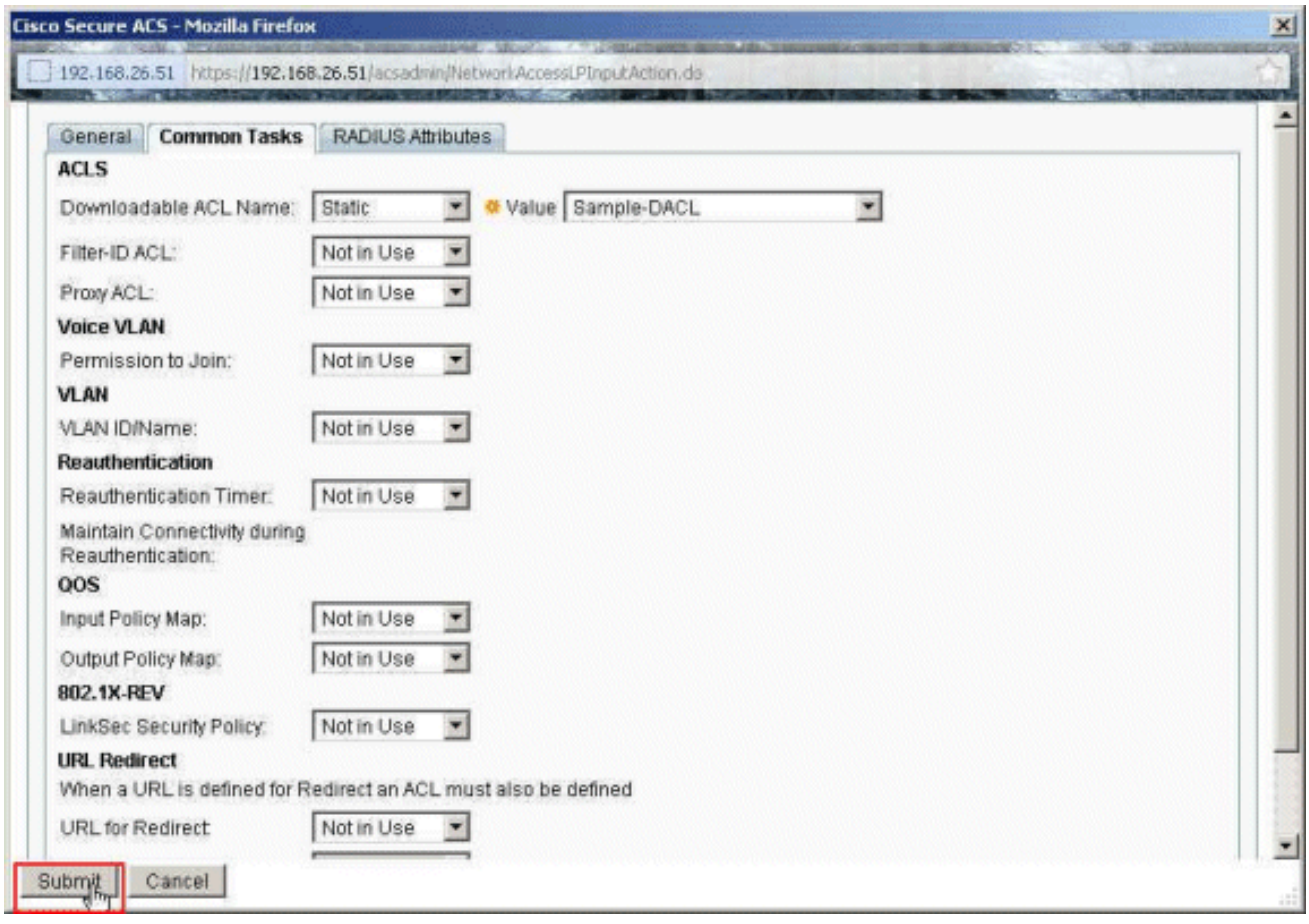


20. Choisissez l'onglet de **fonctionnalités usuelles**, et la **charge statique** choisie de la liste déroulante pour le **nom téléchargeable d'ACL**. Choisissez le **DACL** de création récente **(l'échantillon - DACL) de la** liste déroulante de

valeur.

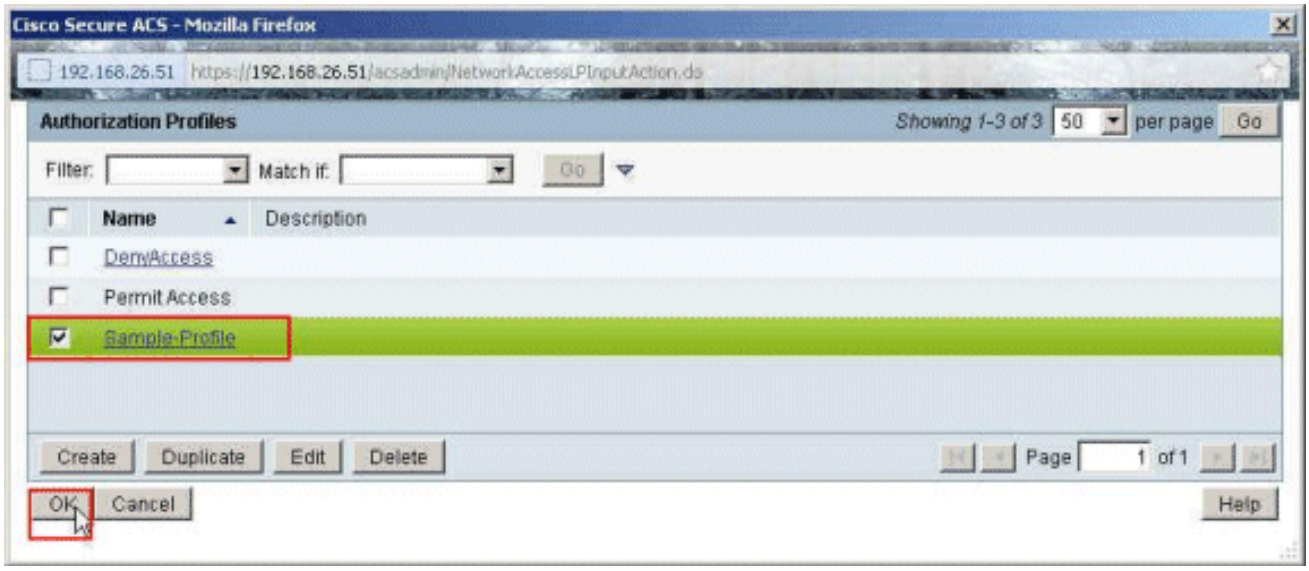


21. Cliquez sur **Submit**.

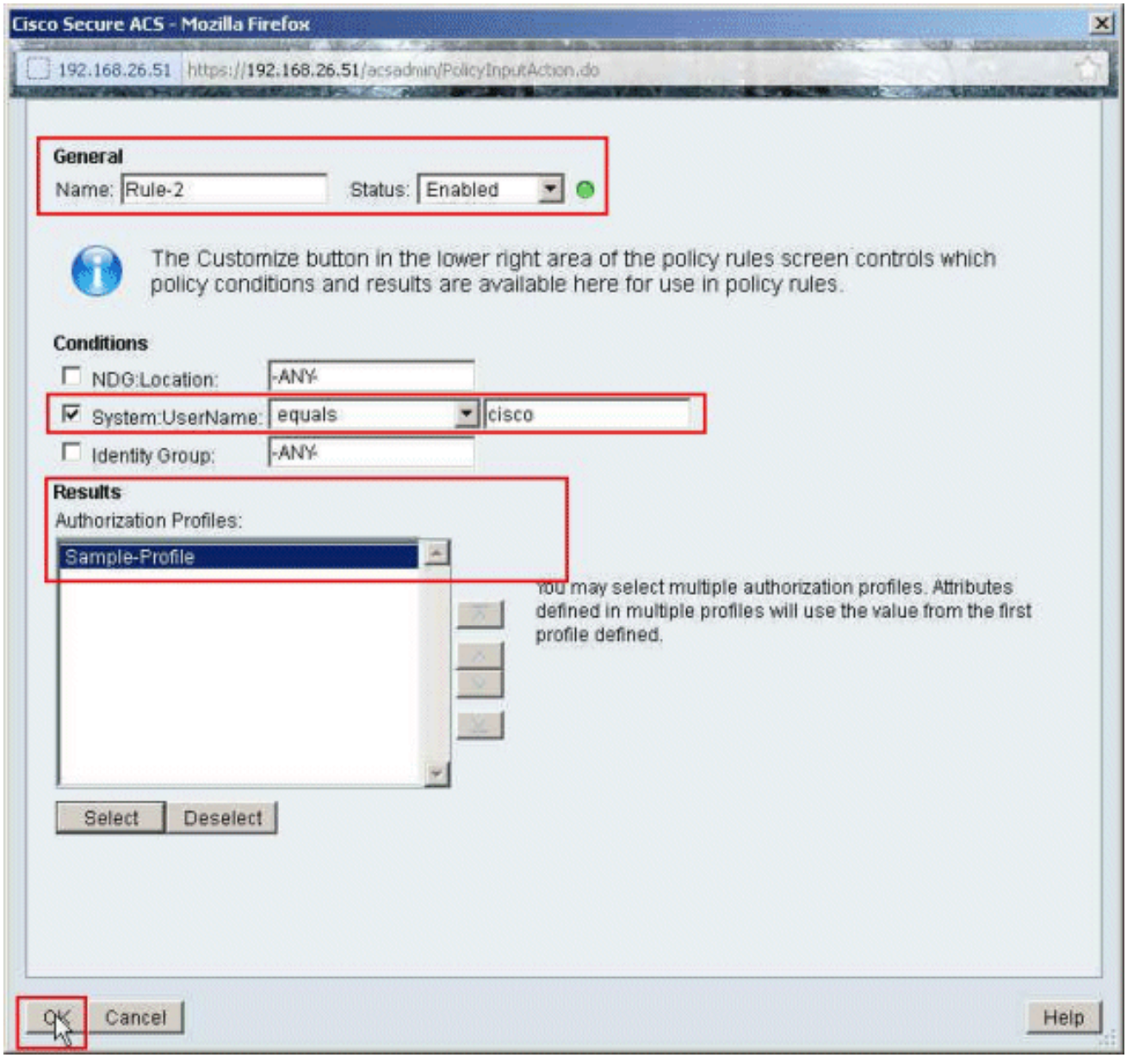


22. Assurez-vous que la case à cocher à côté de l'**exemple de profil** (le profil de création récente d'autorisation) est vérifiée, et cliquez sur

OK.

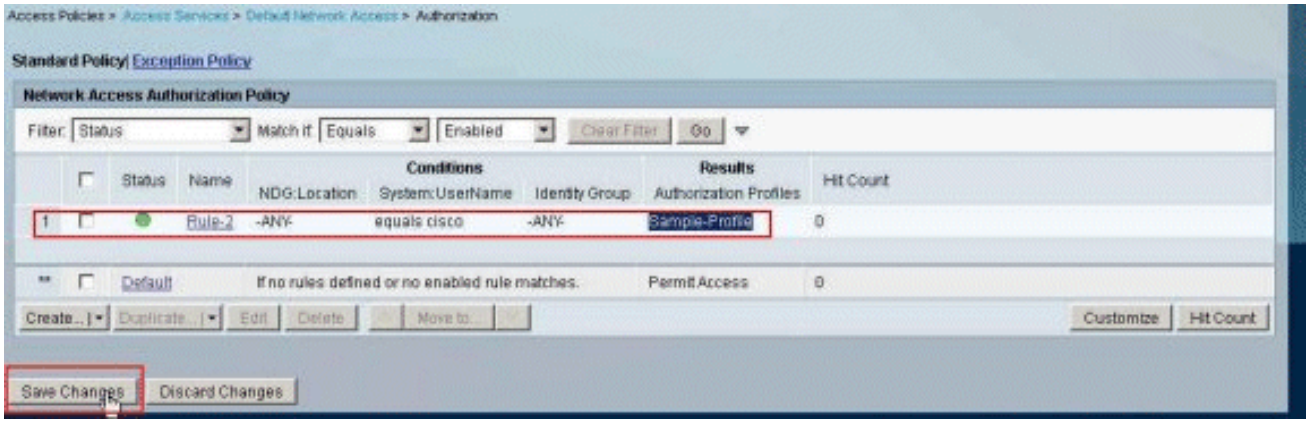


23. Une fois que vous avez vérifié que l'**exemple de profil** de création récente est sélectionné dans les **profils d'autorisation** mettez en place, cliquez sur
OK.



24. Vérifiez que la nouvelle règle (**Rule-2**) est créée avec le système : Le nom d'utilisateur **égale des** états et l'**exemple de profil de Cisco** comme résultat. **Modifications de**

sauvegarde de clic. La règle 2 est créée avec succès.



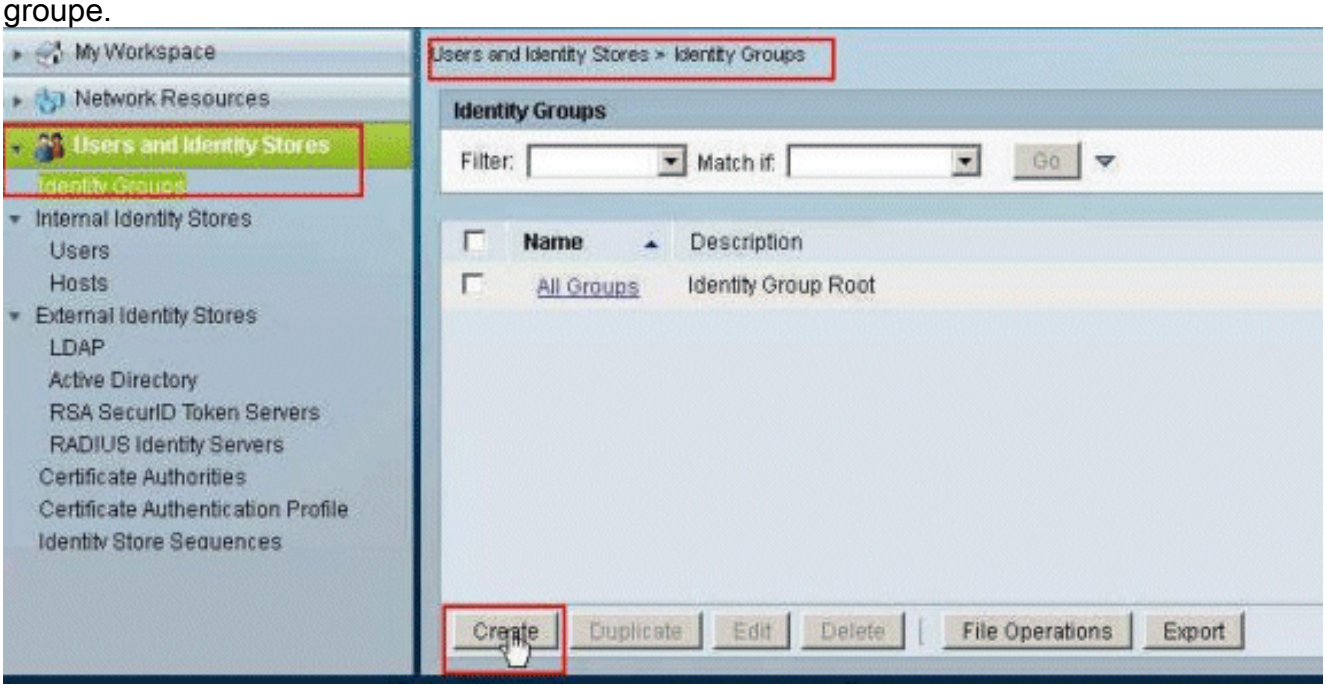
Configurez ACS pour l'ACL téléchargeable pour le groupe

Étapes complètes 1 à 12 du configurer ACS pour l'ACL téléchargeable pour l'utilisateur individuel et exécutent ces étapes afin de configurer l'ACL téléchargeable pour le groupe dans un Cisco Secure ACS.

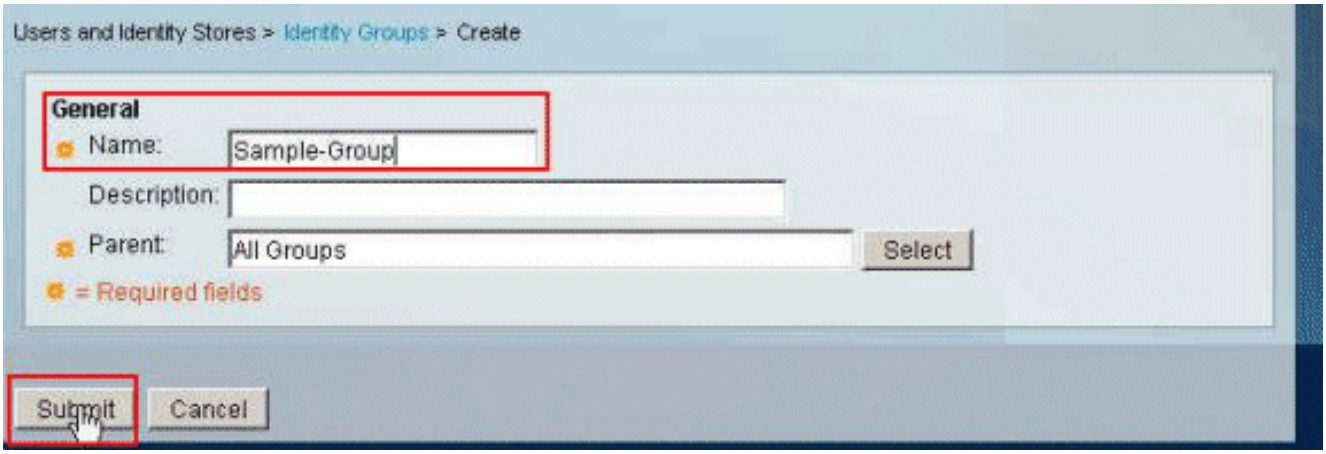
Dans cet exemple, l'utilisateur « Cisco » d'IPsec VPN appartient au l'Échantillon-**groupe**.

L'utilisateur **Cisco d'Échantillon-groupe** authentifie avec succès, et le serveur de RADIUS envoie une liste d'accès téléchargeable aux dispositifs de sécurité. L'utilisateur « Cisco » peut accéder à seulement le serveur de 10.1.1.2 et refuse tout autre accès. Afin de vérifier l'ACL, référez-vous à l'ACL téléchargeable pour la section d'utilisateur/groupe.

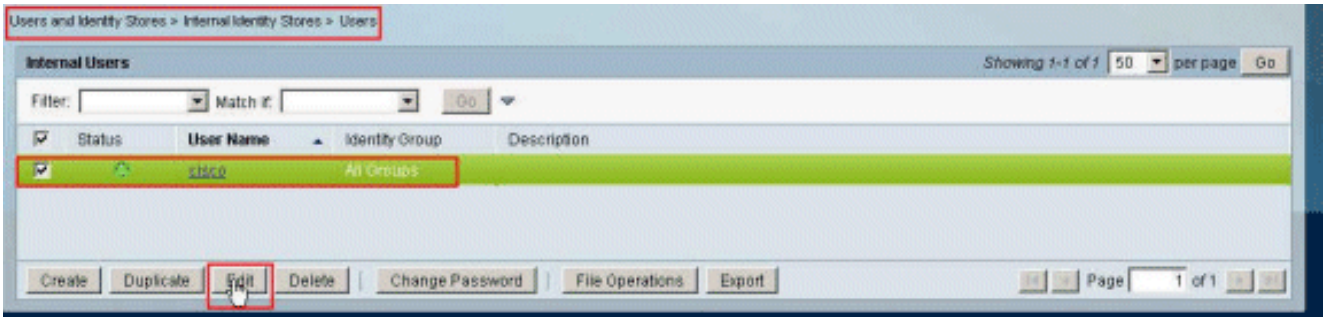
1. Dans la barre de navigation, les **utilisateurs et l'identité de** clic **enregistre** > des **groupes d'identité**, et le clic **créent** afin de créer un nouveau groupe.



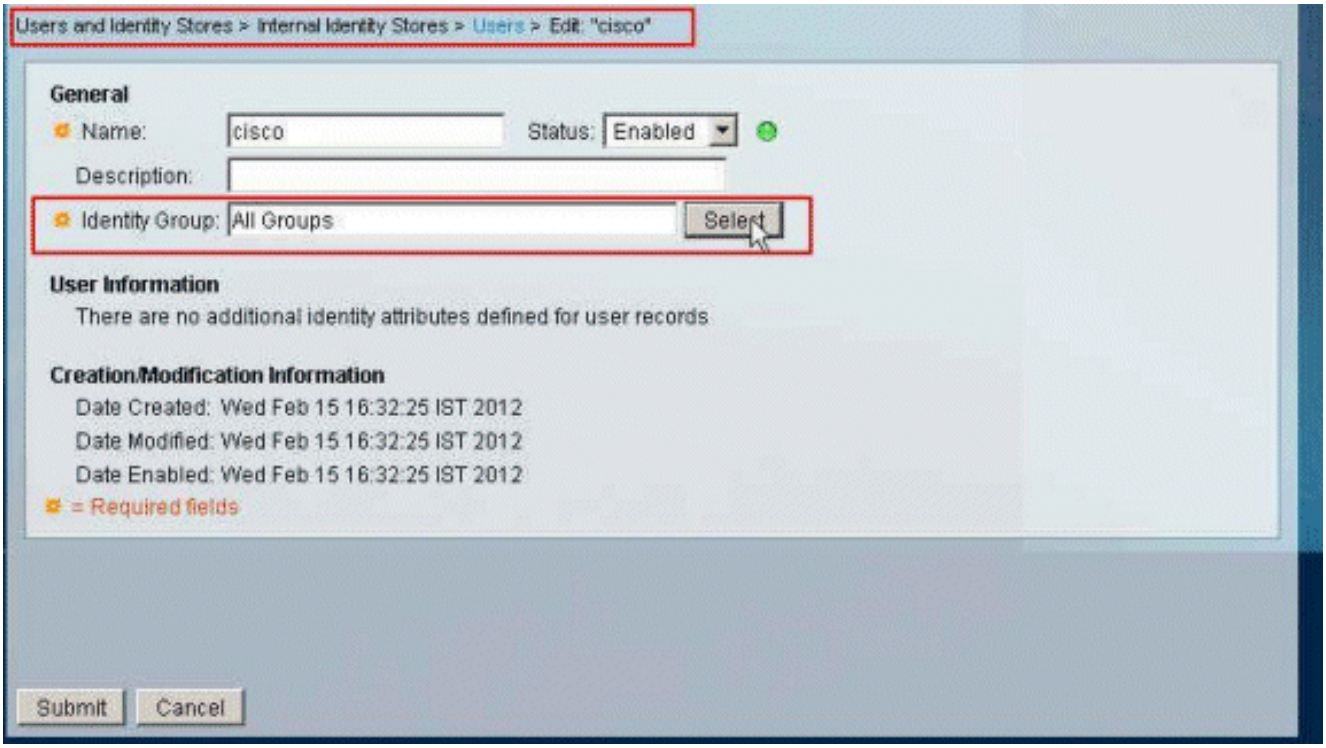
2. Fournissez un nom de groupe (Échantillon-**groupe**), et cliquez sur Submit.



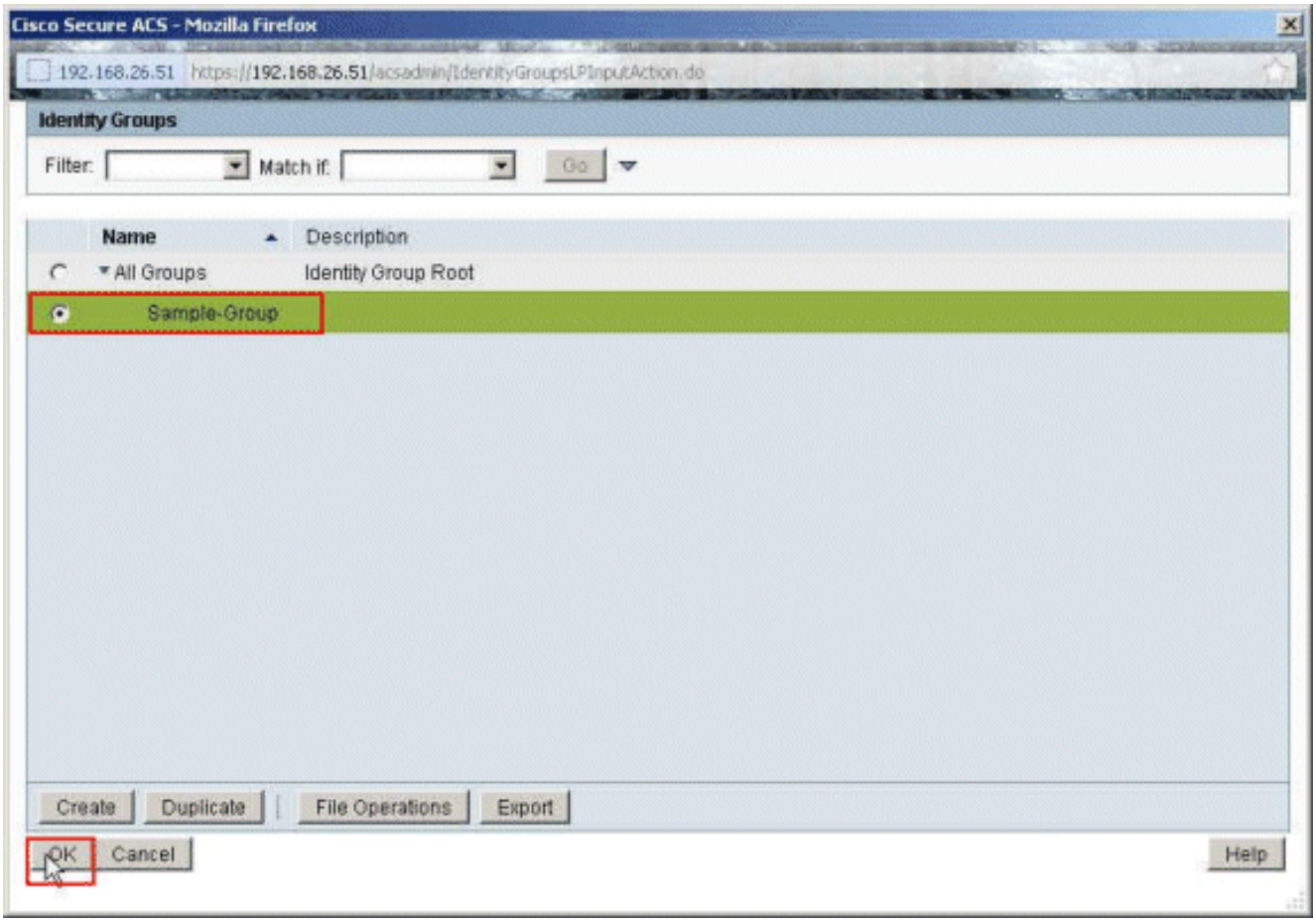
3. Choisissez les **mémoires d'identité de l'utilisateur > identité interne enregistre >** des **utilisateurs**, et sélectionne l'utilisateur **Cisco**. Cliquez sur Edit afin de changer l'adhésion à des associations de cet utilisateur.



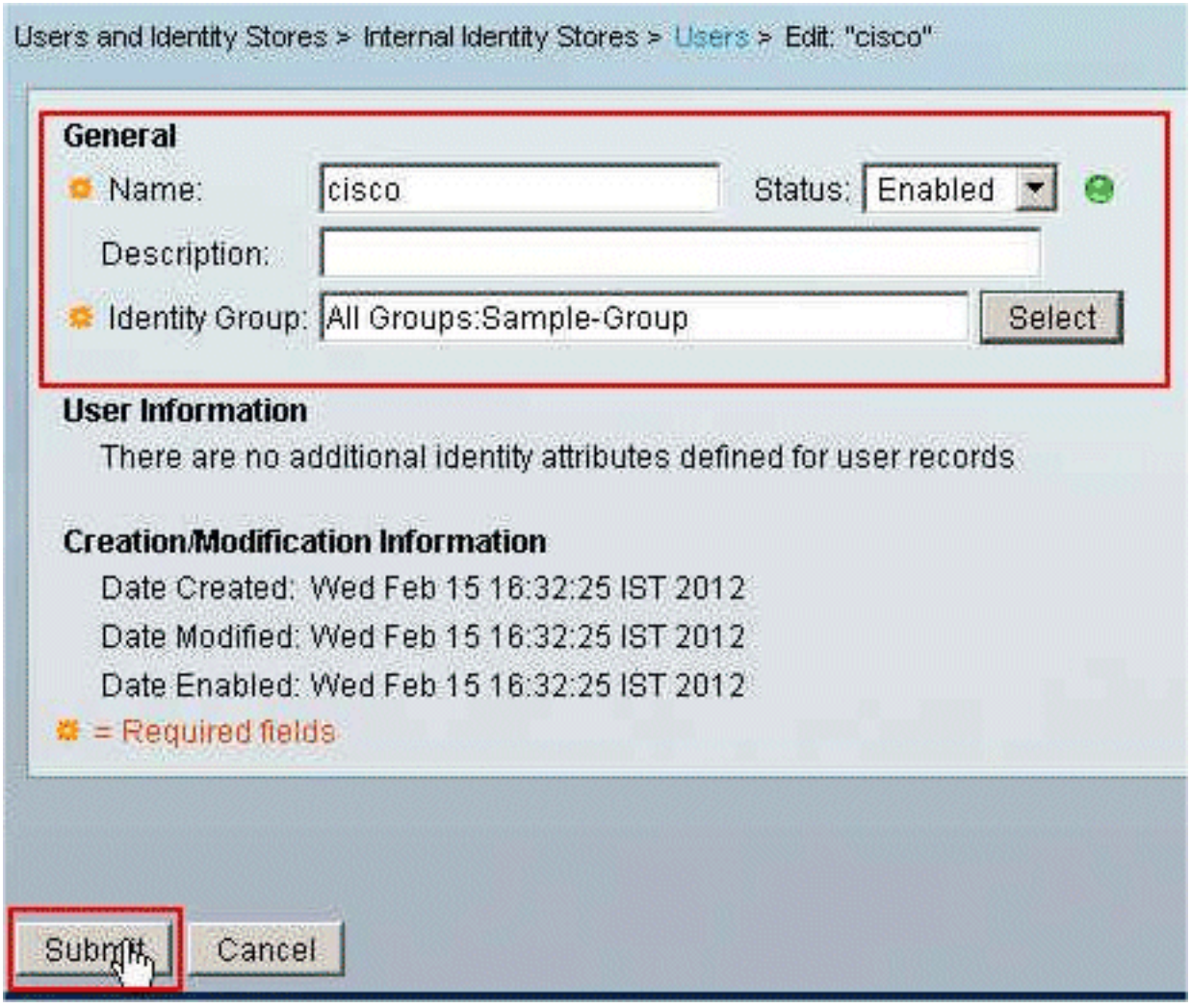
4. Clic **choisi** à côté du groupe d'identité.



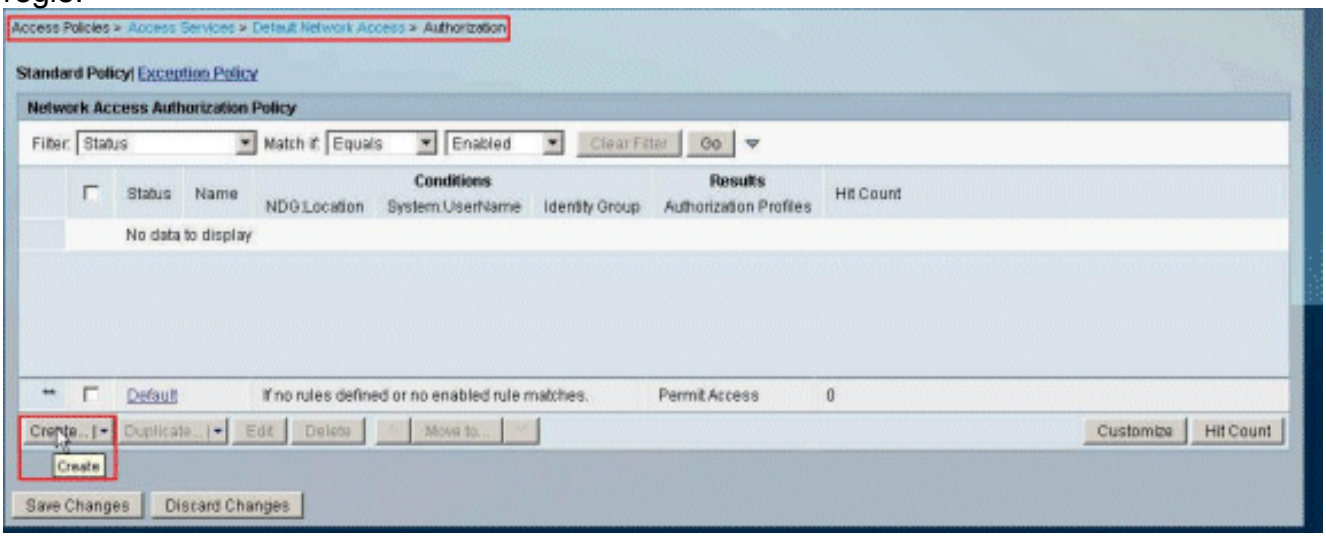
5. Sélectionnez le groupe de création récente (c'est-à-dire, Échantillon-**groupe**), et cliquez sur OK.



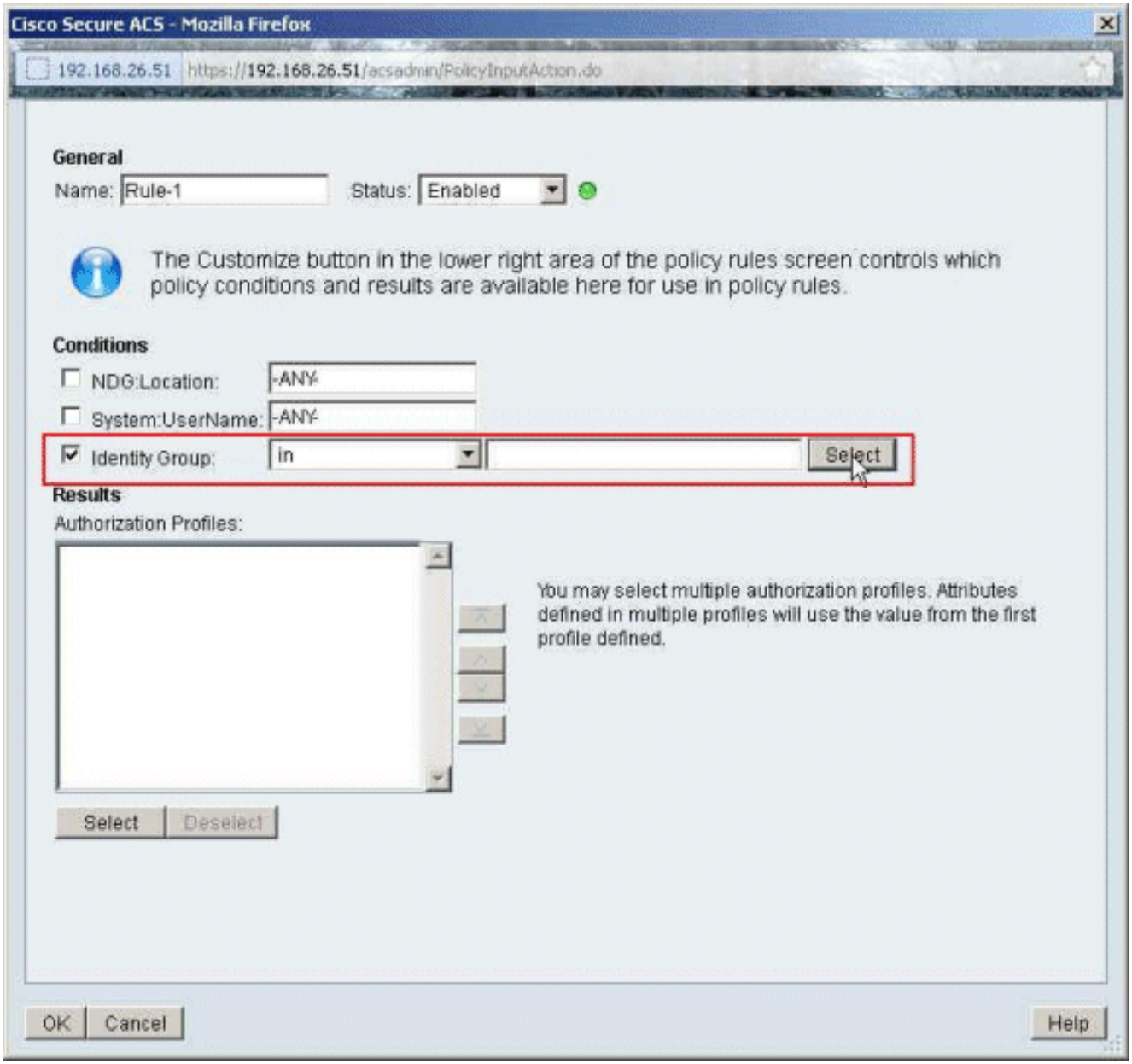
6. Cliquez sur **Submit**.



7. Choisissez les **stratégies d'Access** > les **services d'accès** > l'**accès au réseau** > l'**autorisation de par défaut**, et le clic **créent** afin de créer une nouvelle règle.

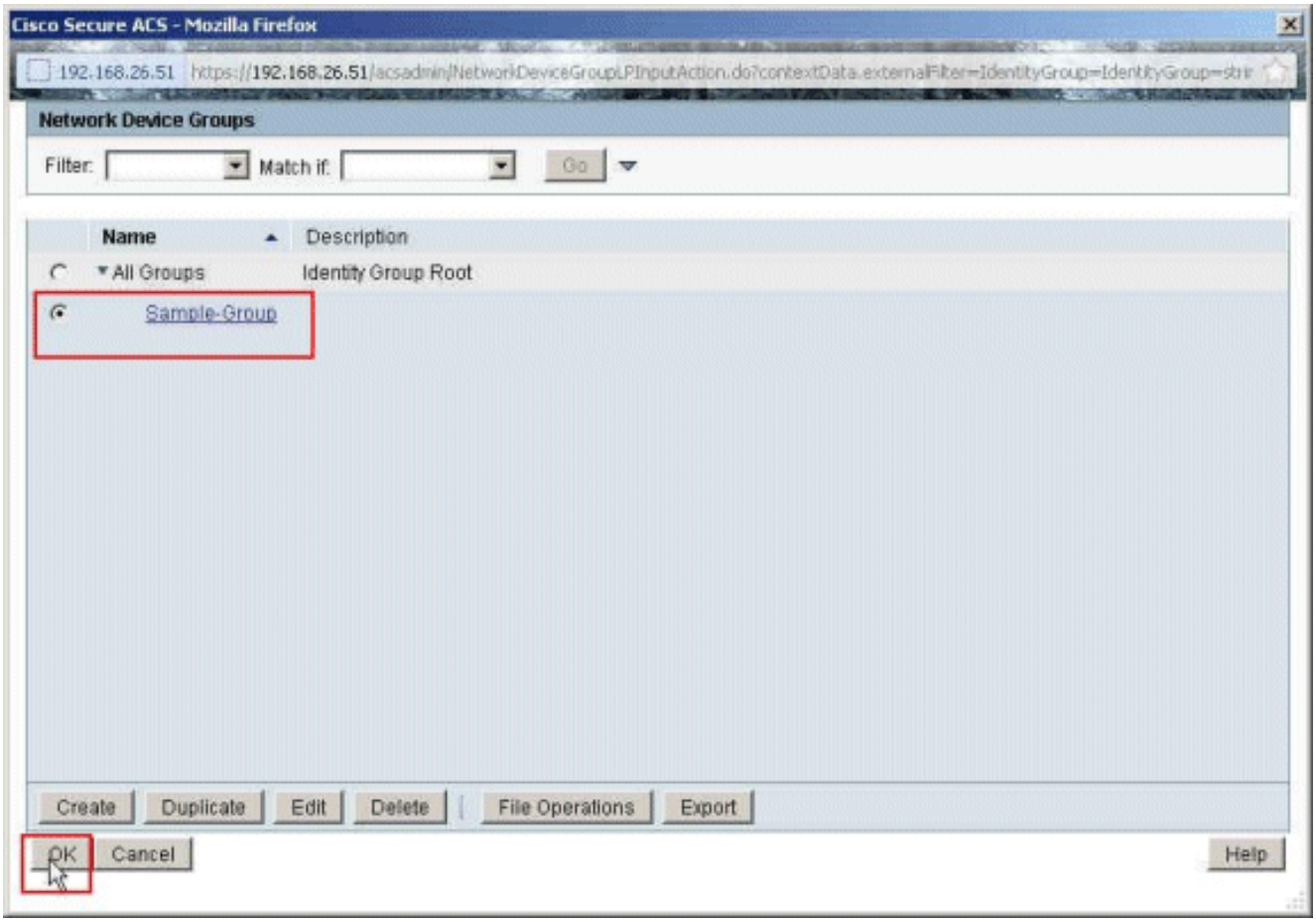


8. Assurez-vous que la case à cocher à côté du **groupe d'identité** est vérifiée, et cliquez sur **choisi**.

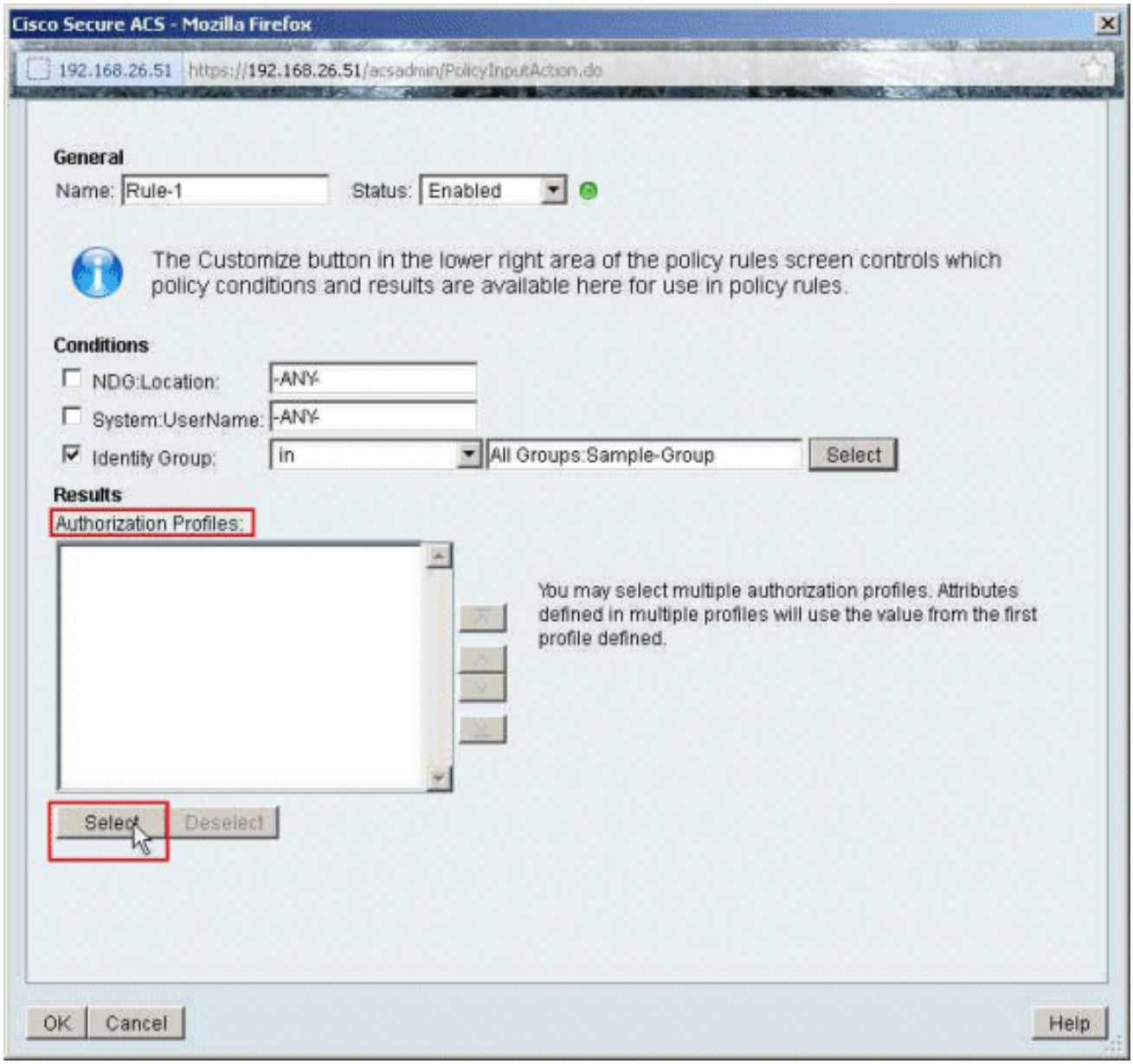


9. Choisissez l'Échantillon-**groupe**, et cliquez sur

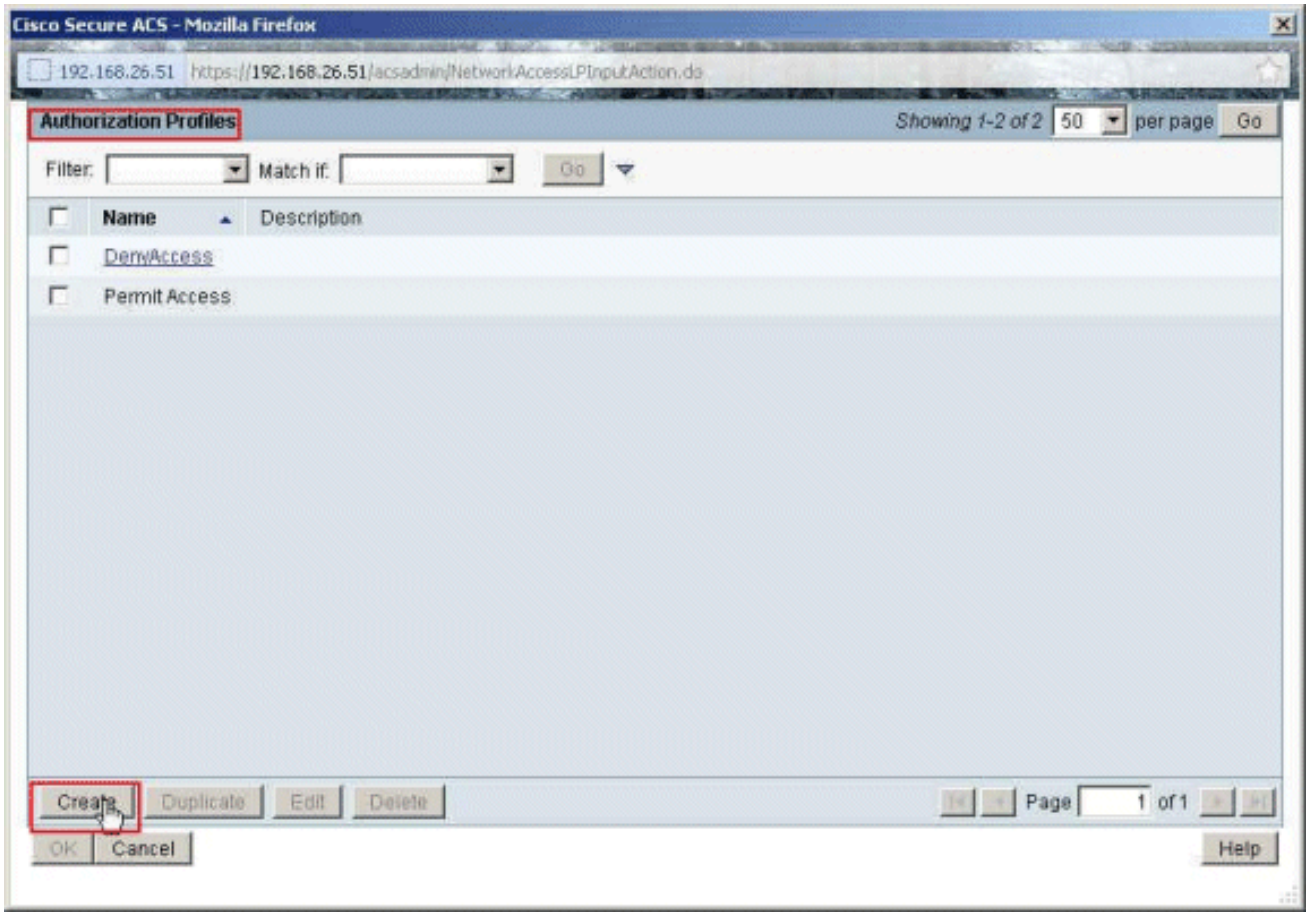
OK.



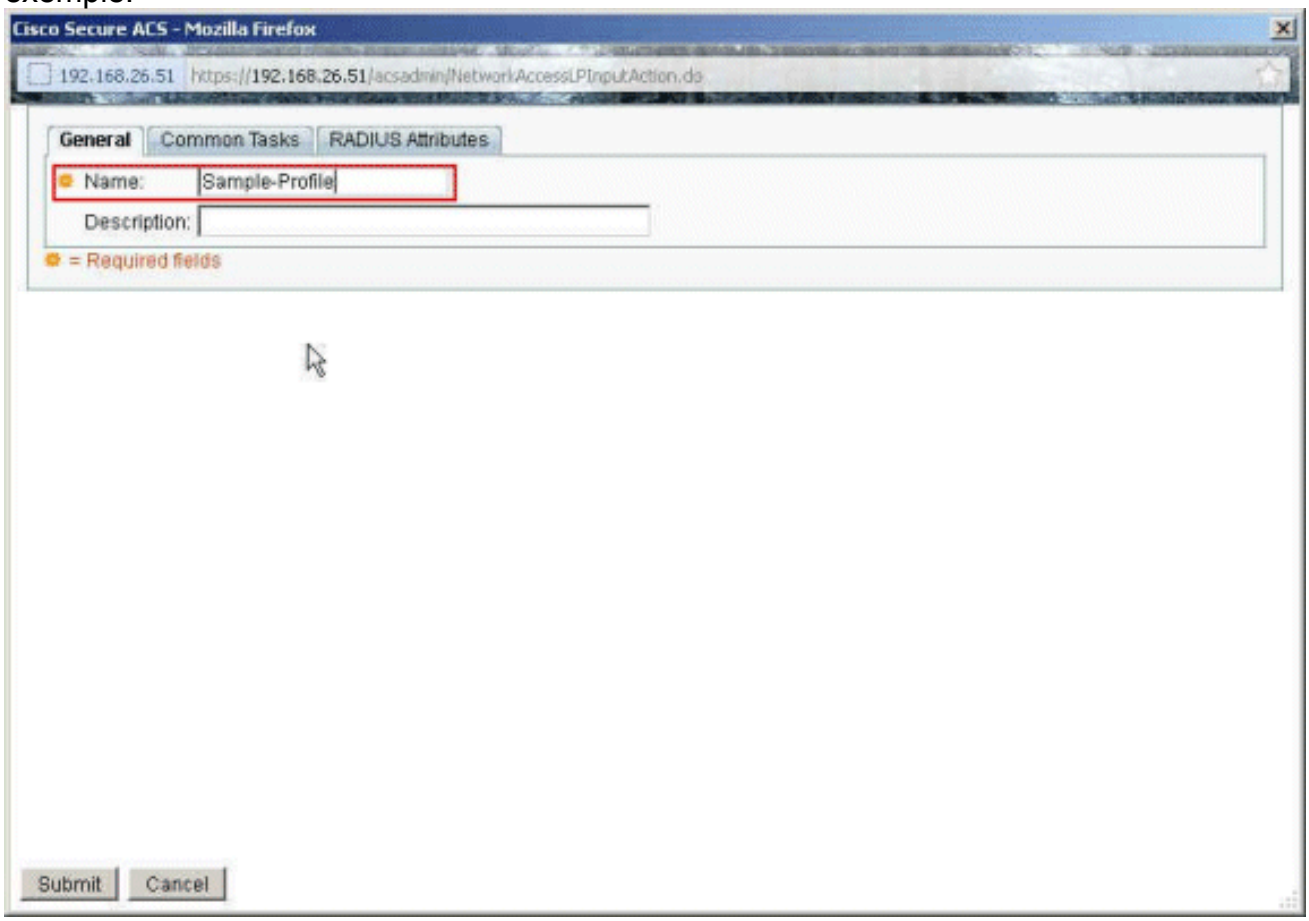
10. Clic **choisi**, dans la section de profils d'autorisation.



11. Le clic **créent** afin de créer un nouveau profil d'autorisation.

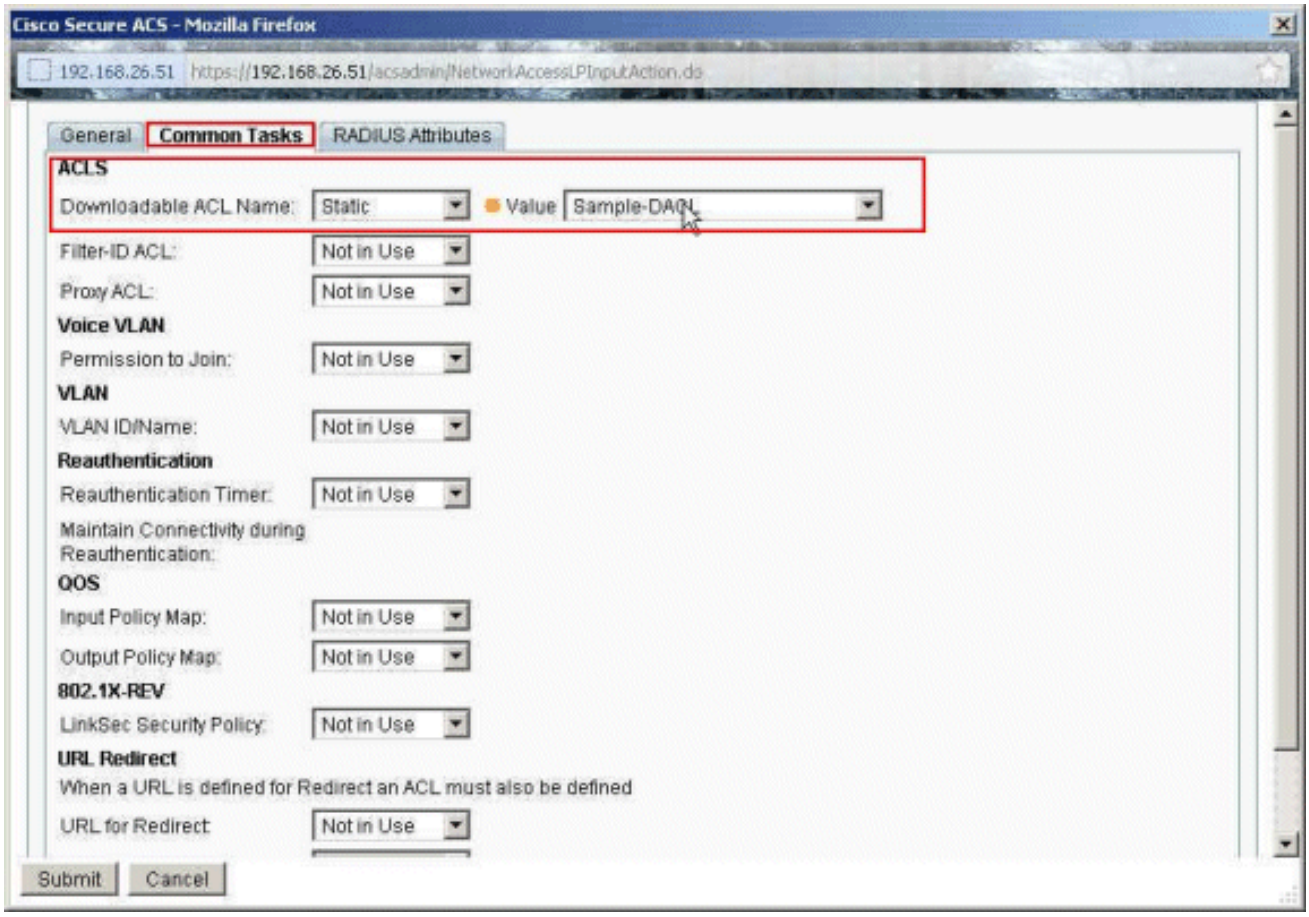


12. Fournissez un nom pour le **profil d'autorisation**. **L'exemple de profil** est le nom utilisé dans cet
exemple.

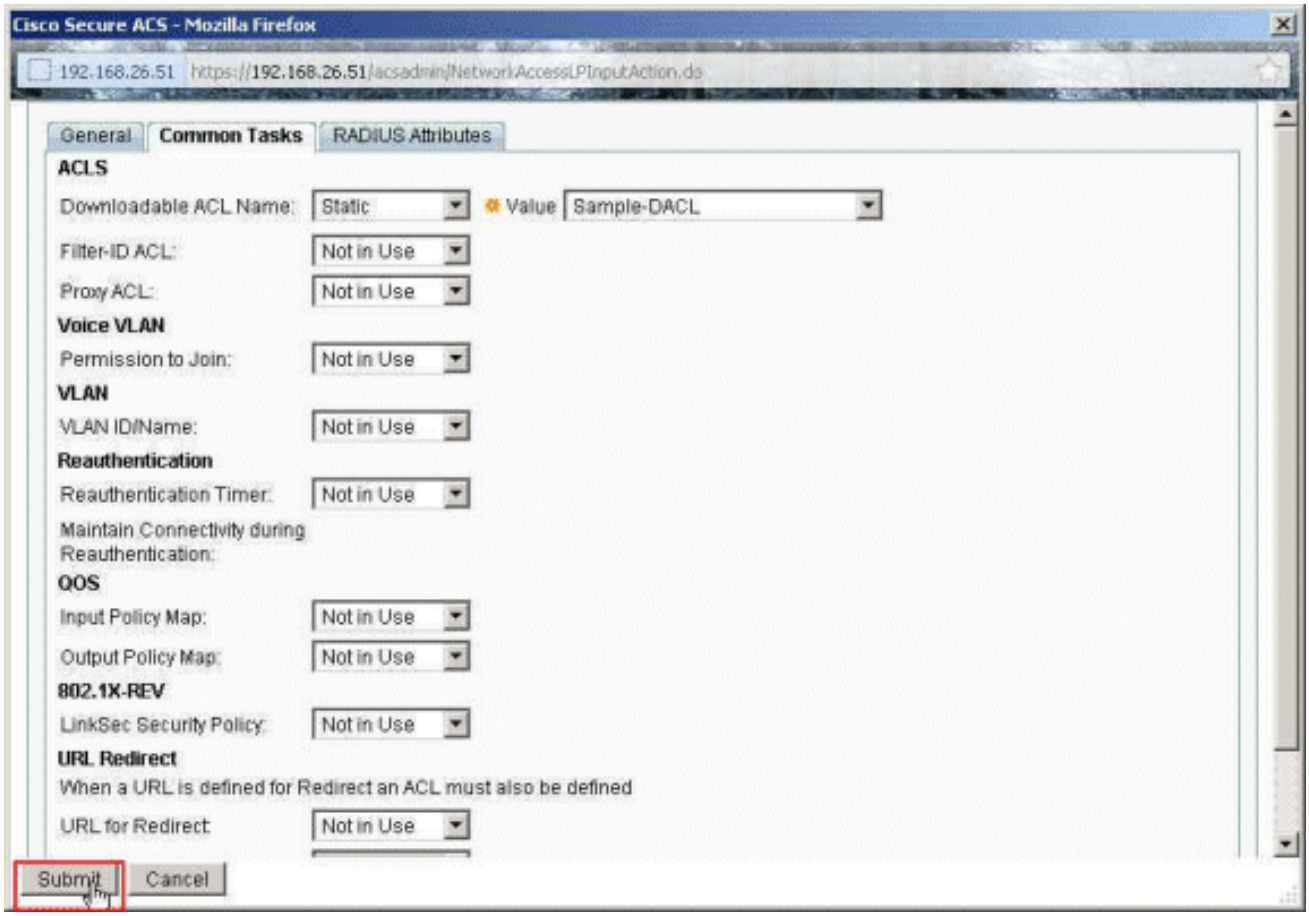


13. Choisissez l'onglet de **fonctionnalités usuelles**, et la **charge statique** choisie de la liste déroulante pour le **nom téléchargeable d'ACL**. Choisissez le **DACL** de création récente

(l'échantillon - DACL) de la liste déroulante de valeur.

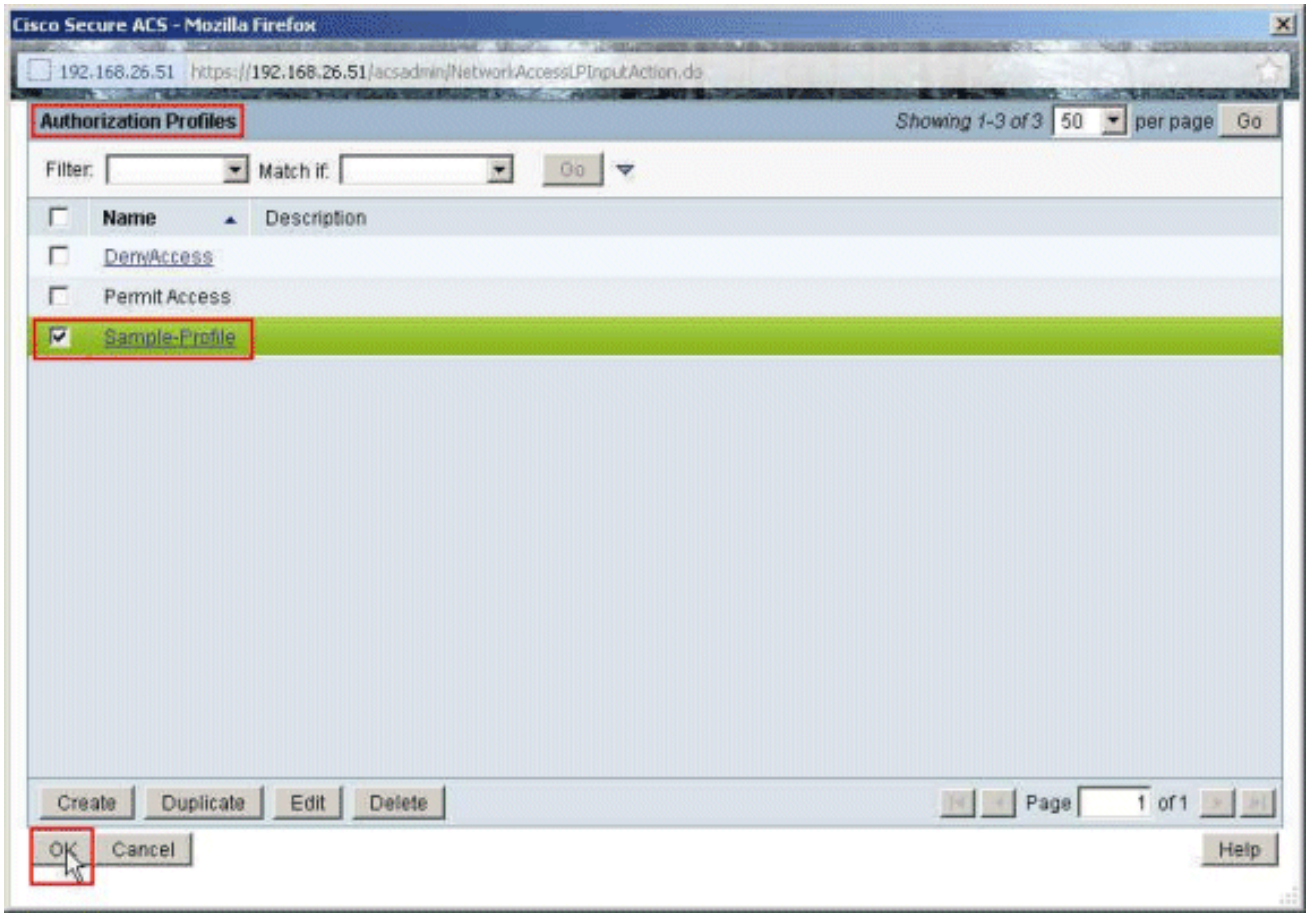


14. Cliquez sur **Submit**.

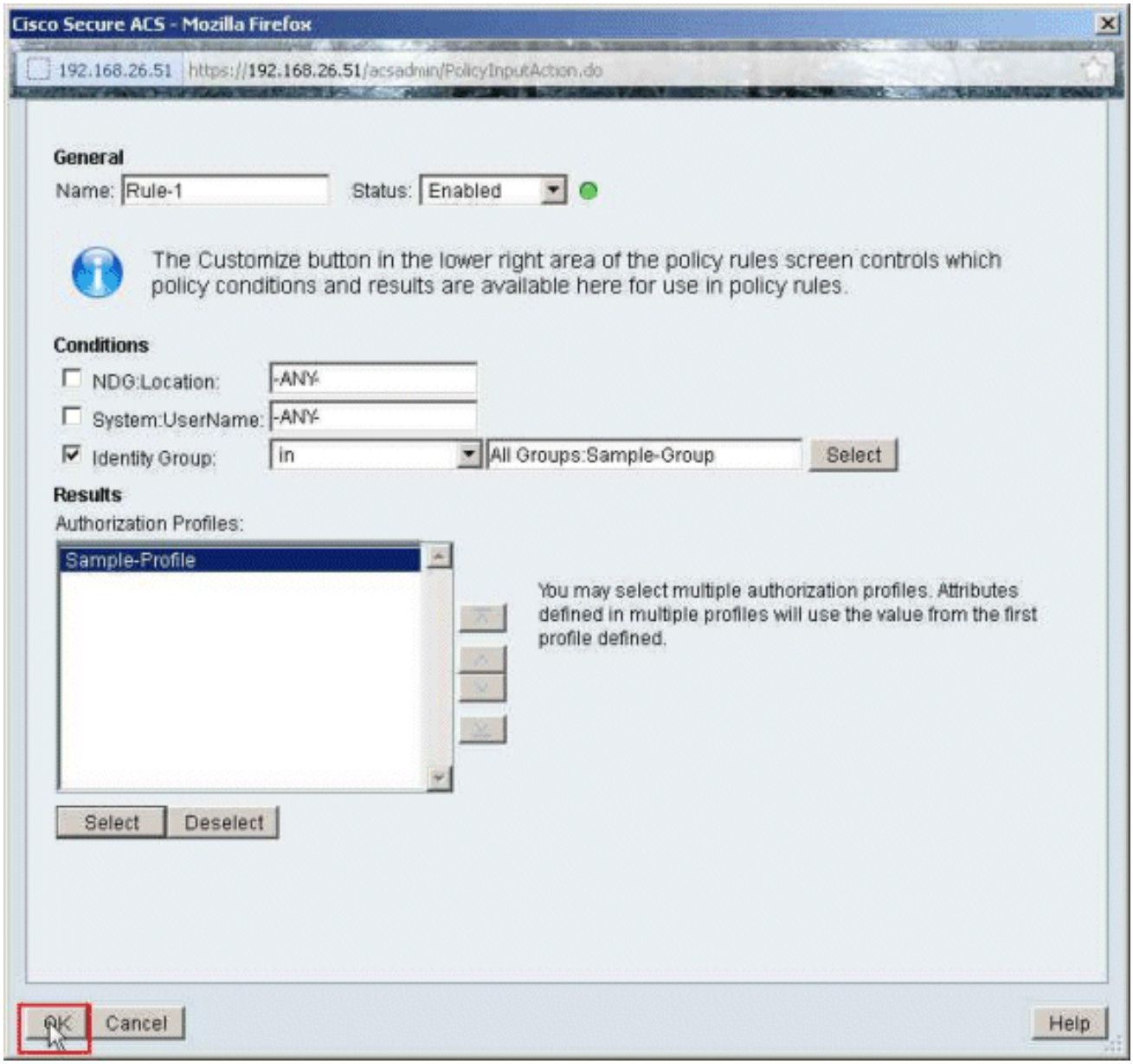


15. Choisissez l'**exemple de profil de** profil d'autorisation créé plus tôt, et cliquez sur

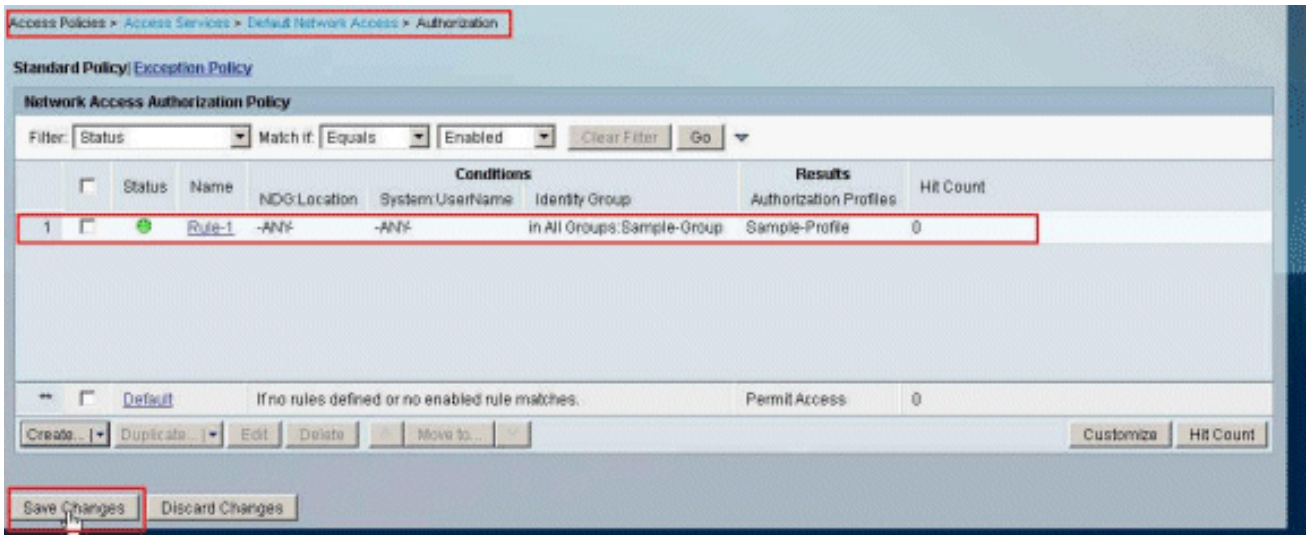
OK.



16. Cliquez sur
OK.



17. Vérifiez que **Rule-1** est créé avec l'Échantillon-**groupe de** groupe d'identité comme condition et l'**exemple de profil** comme résultat. **Modifications de sauvegarde de** clic.



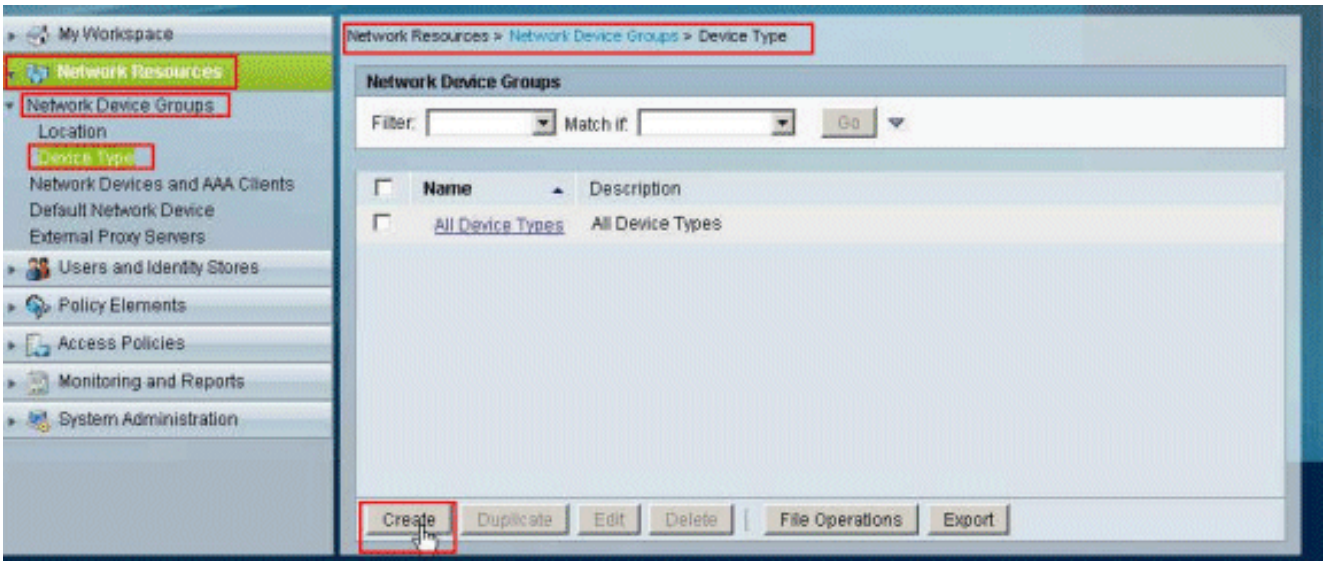
Configurez ACS pour l'ACL téléchargeable pour un groupe de périphériques réseau

Étapes complètes 1 à 12 du configurer ACS pour l'ACL téléchargeable pour l'utilisateur individuel

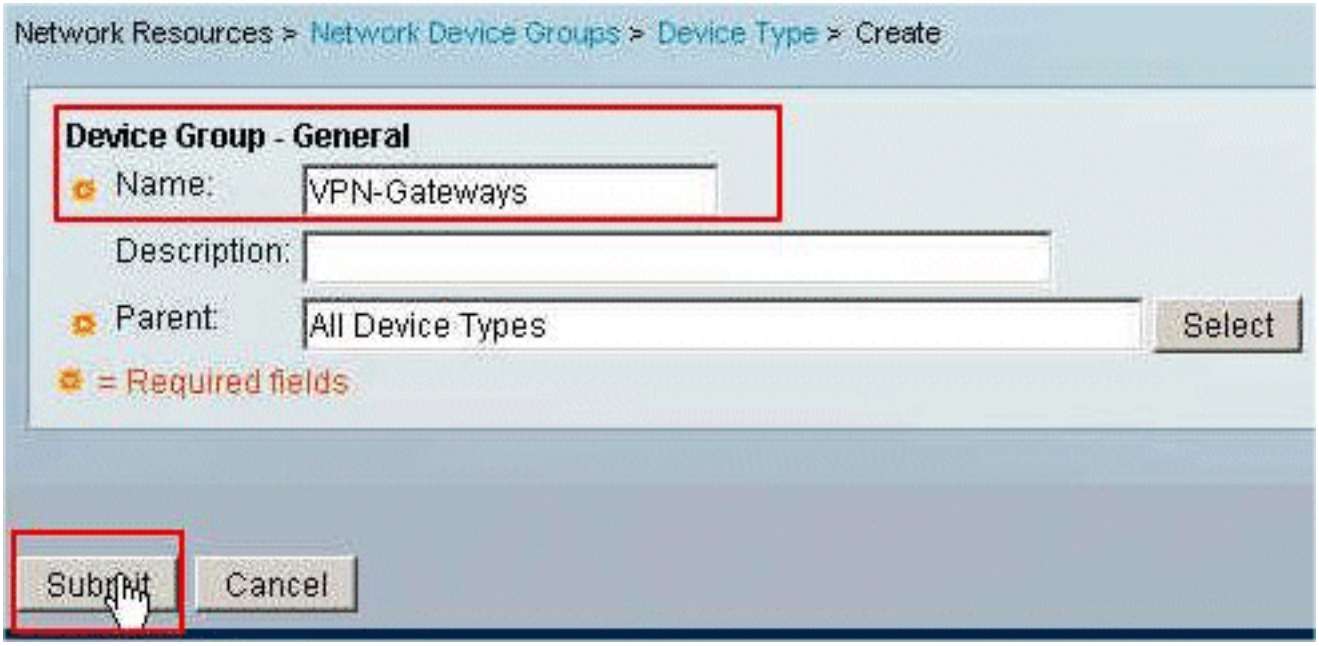
et exécutent ces étapes afin de configurer l'ACL téléchargeable pour un groupe de périphériques réseau dans un Cisco Secure ACS.

Dans cet exemple, le client RADIUS (ASA) appartient au groupe de périphériques réseau que la demande d'authentification VPN-Gateways.The VPN provenant l'ASA pour l'utilisateur « Cisco » authentifie avec succès, et le serveur de RADIUS envoie une liste d'accès téléchargeable aux dispositifs de sécurité. L'utilisateur « Cisco » peut accéder à seulement le serveur de 10.1.1.2 et refuse tout autre accès. Afin de vérifier l'ACL, référez-vous à l'ACL téléchargeable pour la section d'utilisateur/groupe.

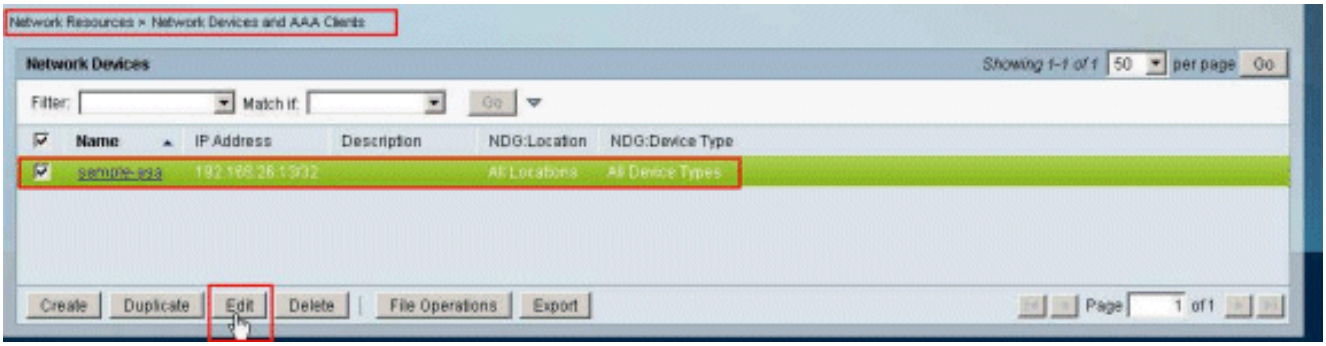
1. Choisissez les **ressources de réseau** > les **groupes de périphériques réseau** > le **type de périphérique**, et le clic **créent** afin de créer un nouveau groupe de périphériques réseau.



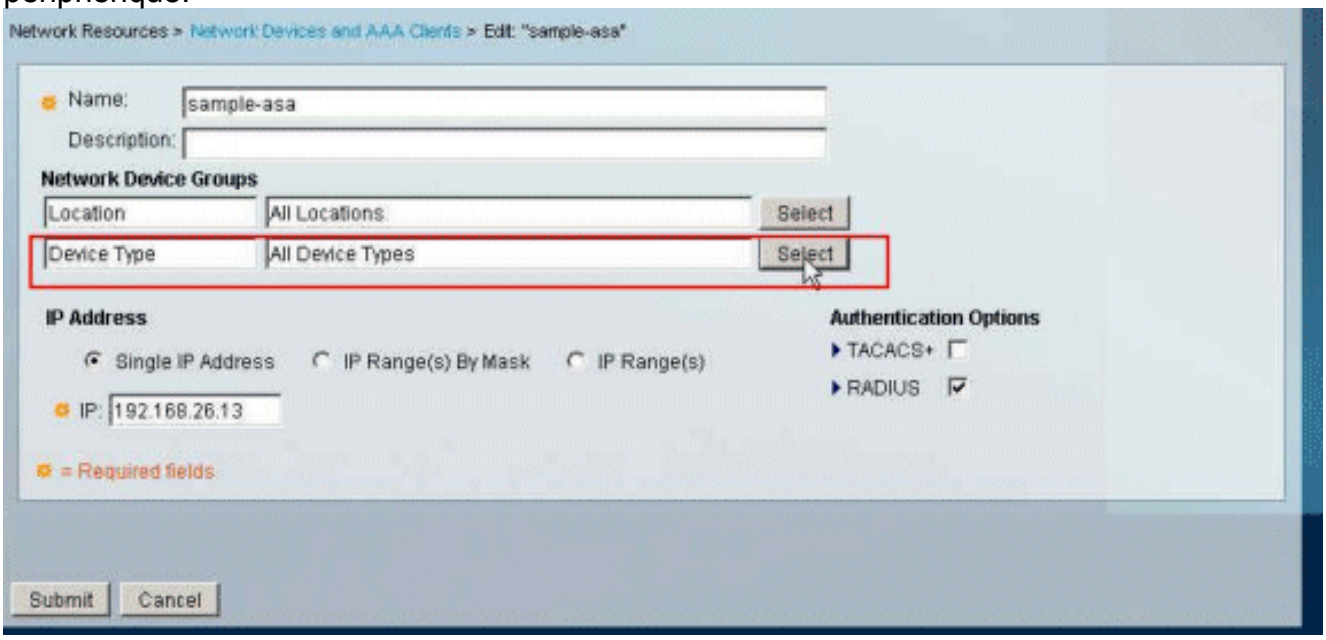
2. Fournissez un nom de **groupe de périphériques réseau** (**passerelles VPN** dans cet exemple), et cliquez sur
Submit.



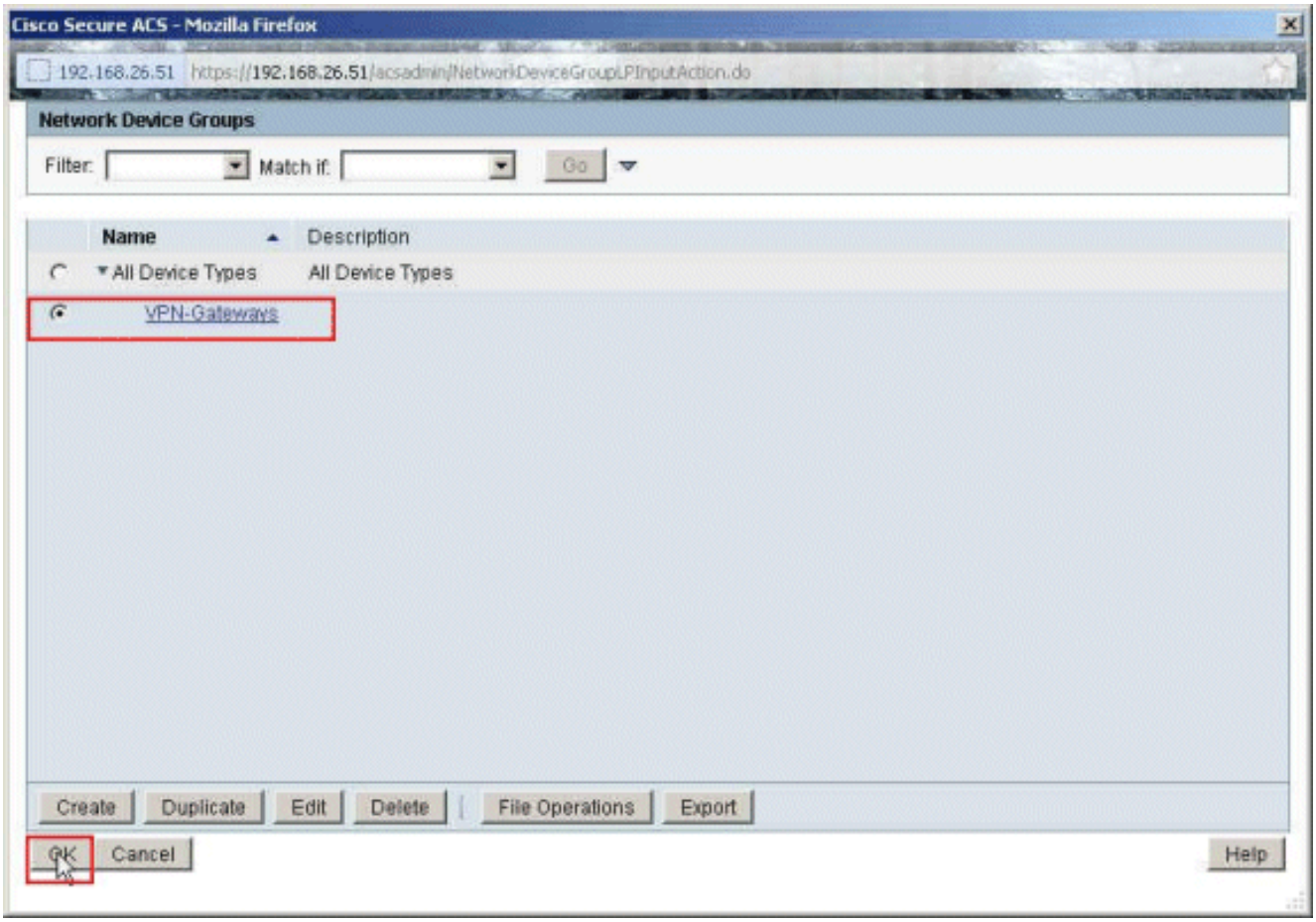
3. Choisissez les **ressources de réseau** > les **périphériques de réseau et les clients d'AAA**, et sélectionnez le **client RADIUS échantillon-asa** créé plus tôt. Cliquez sur Edit afin de changer l'adhésion de **groupe de périphériques réseau de** ce client RADIUS
(asa).



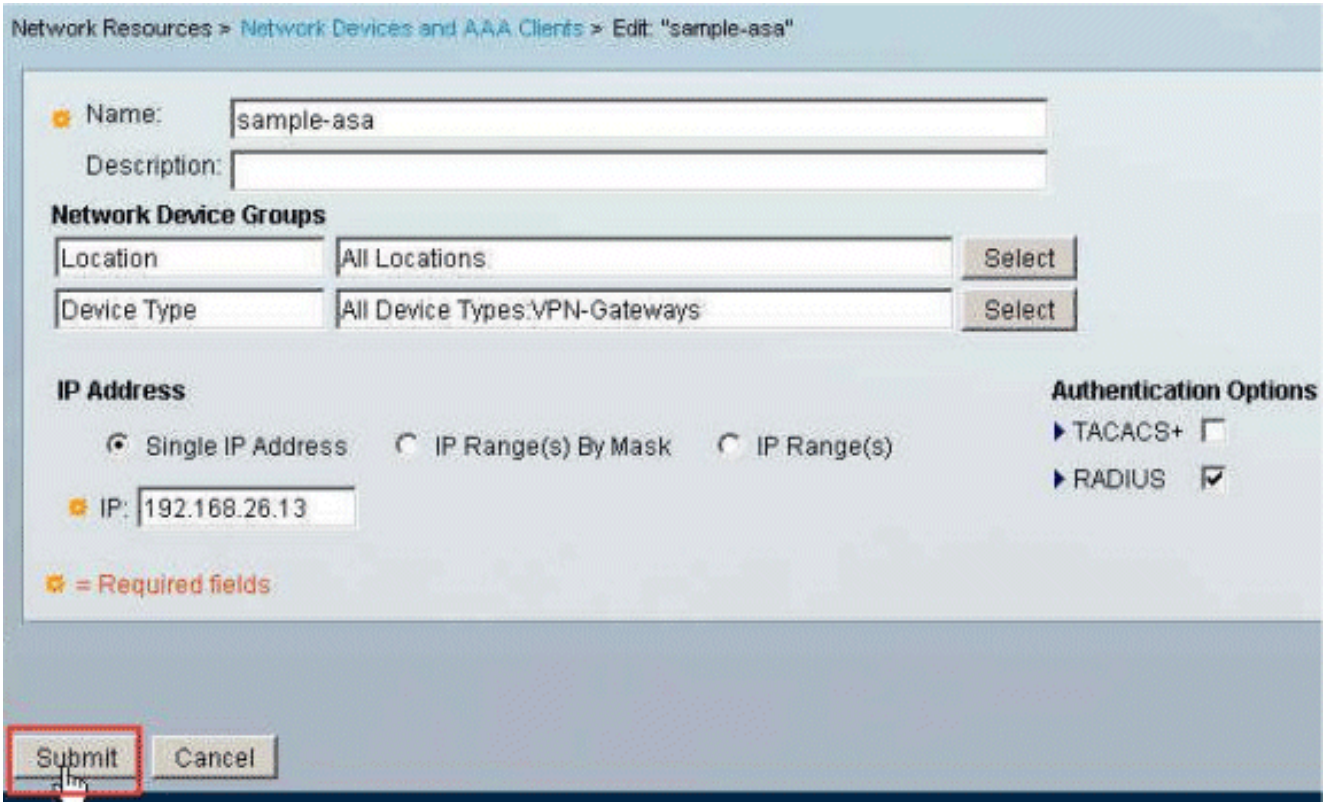
4. Clic **choisi** à côté du type de périphérique.



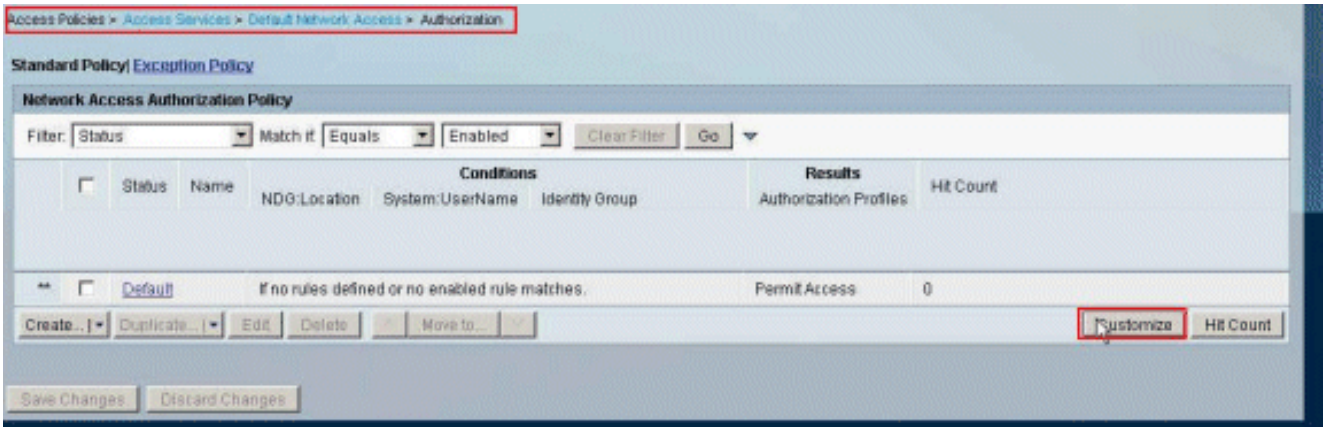
5. Sélectionnez le groupe de périphériques réseau de création récente (qui est des **passerelles VPN**), et cliquez sur OK.



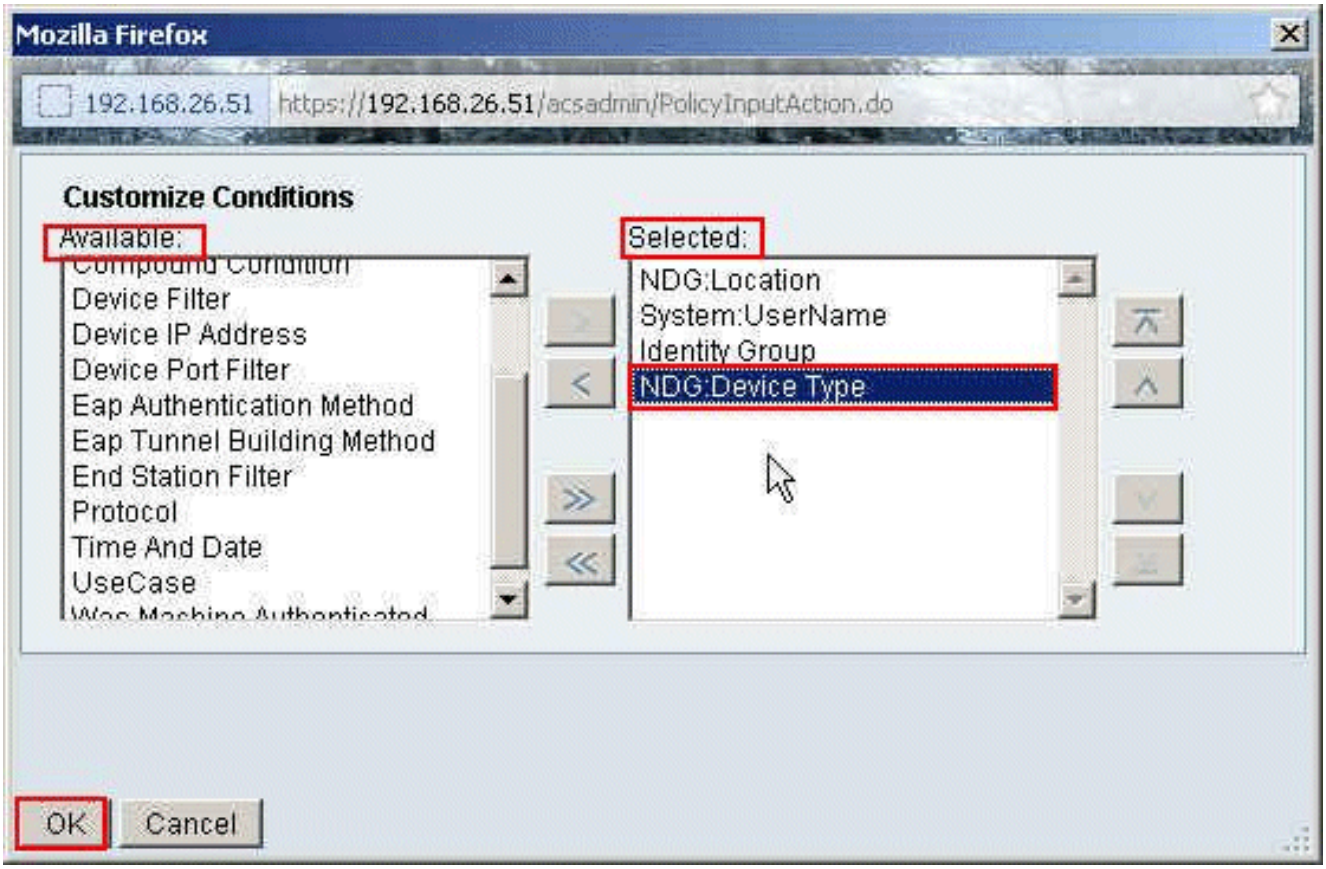
6. Cliquez sur **Submit**.



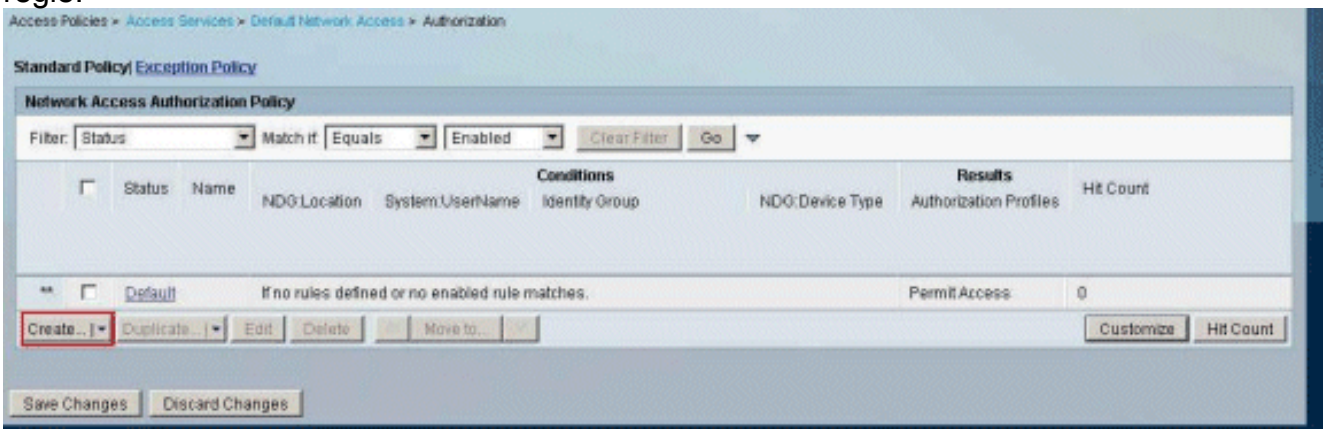
7. Choisissez les **stratégies d'Access** > les **services d'accès** > l'**accès au réseau** > l'**autorisation de par défaut**, et le clic **personnalisent**.



8. Mouvement **NDG : Le type de périphérique de la** section **disponible à la** section **sélectionnée**, et cliquent sur
OK.

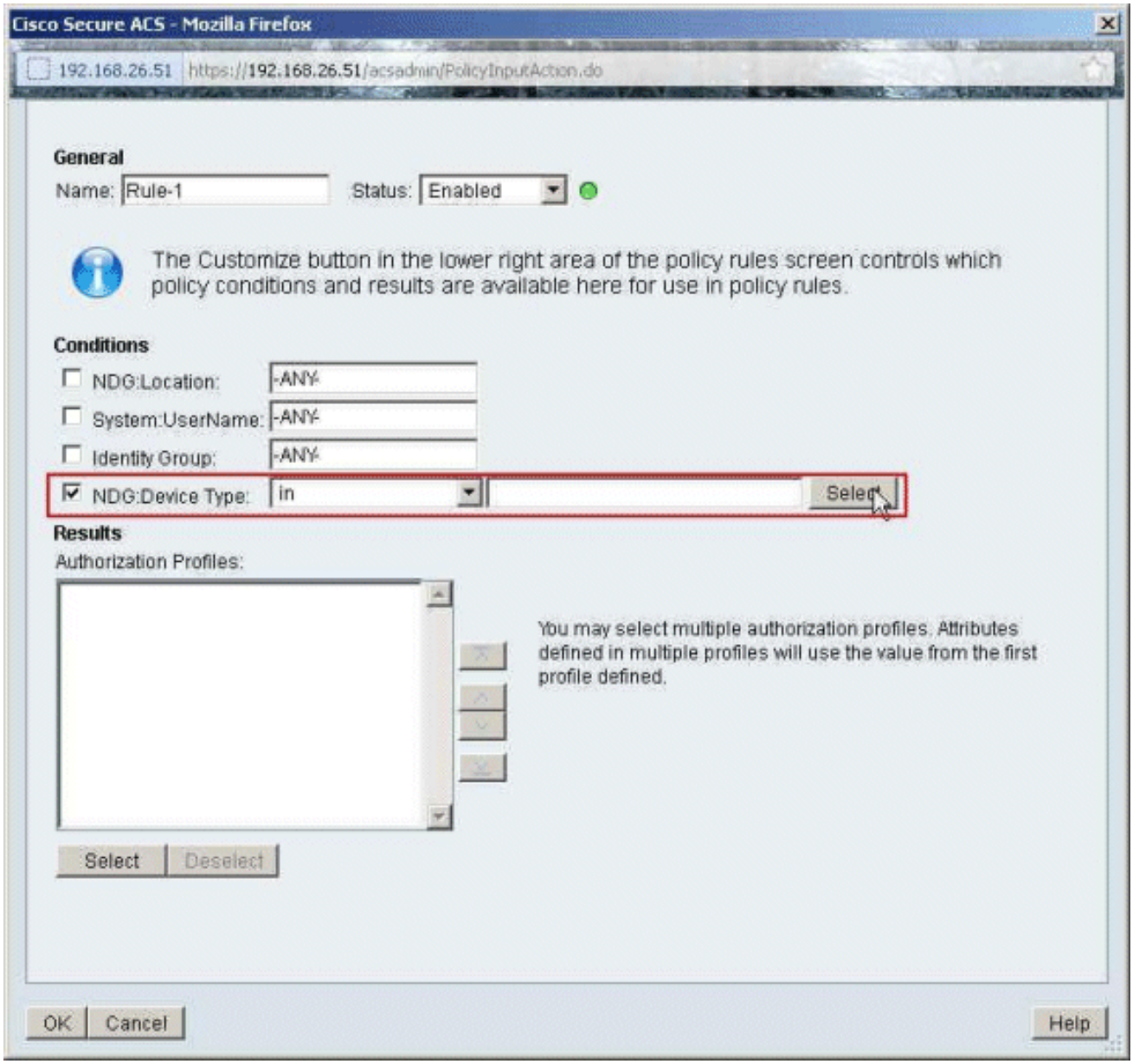


9. Le clic **créent** afin de créer une nouvelle
règle.

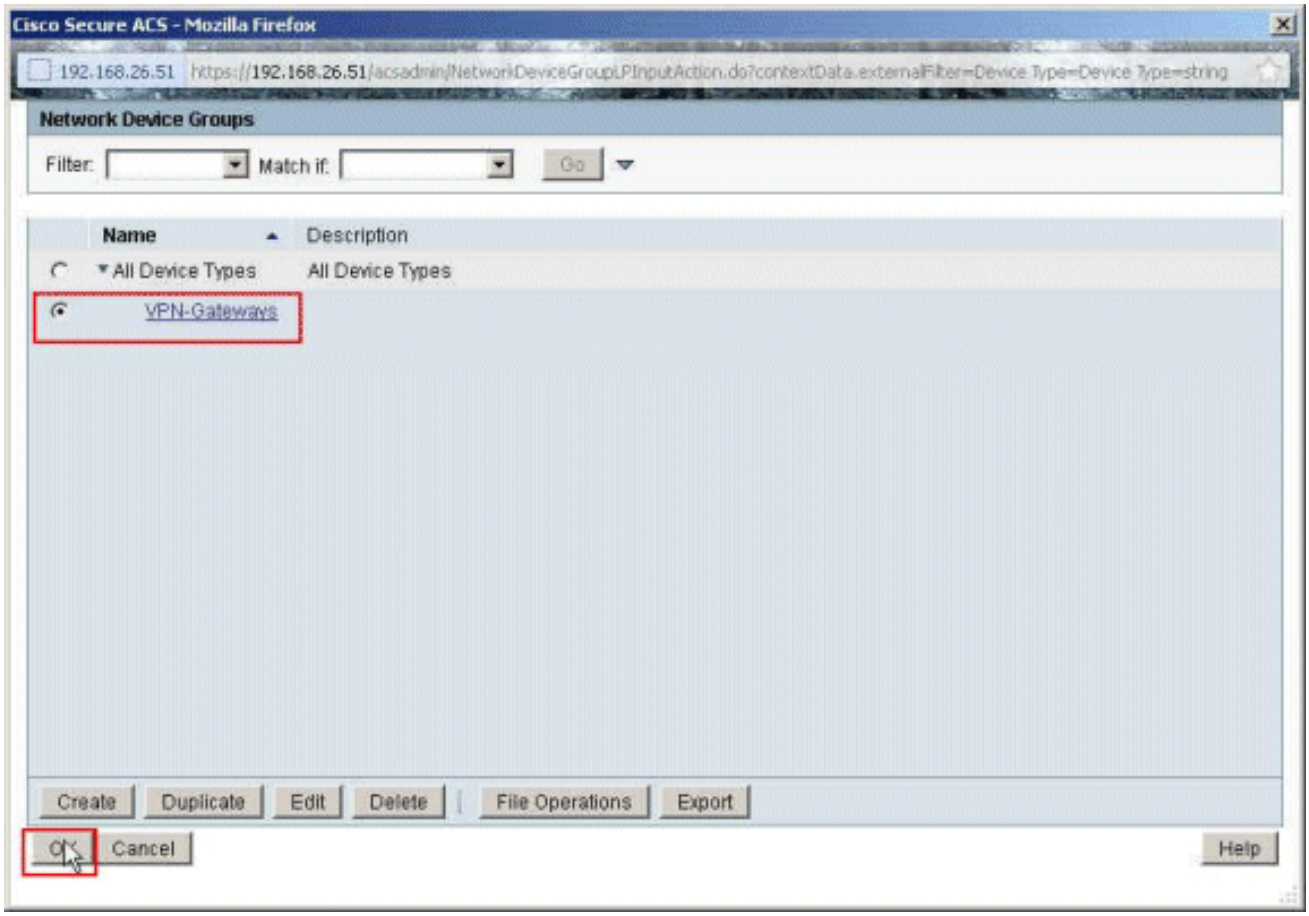


10. Assurez-vous que la case à cocher à côté de **NDG : Le type de périphérique** est sélectionné et choisit **dedans de la** liste déroulante. Clic

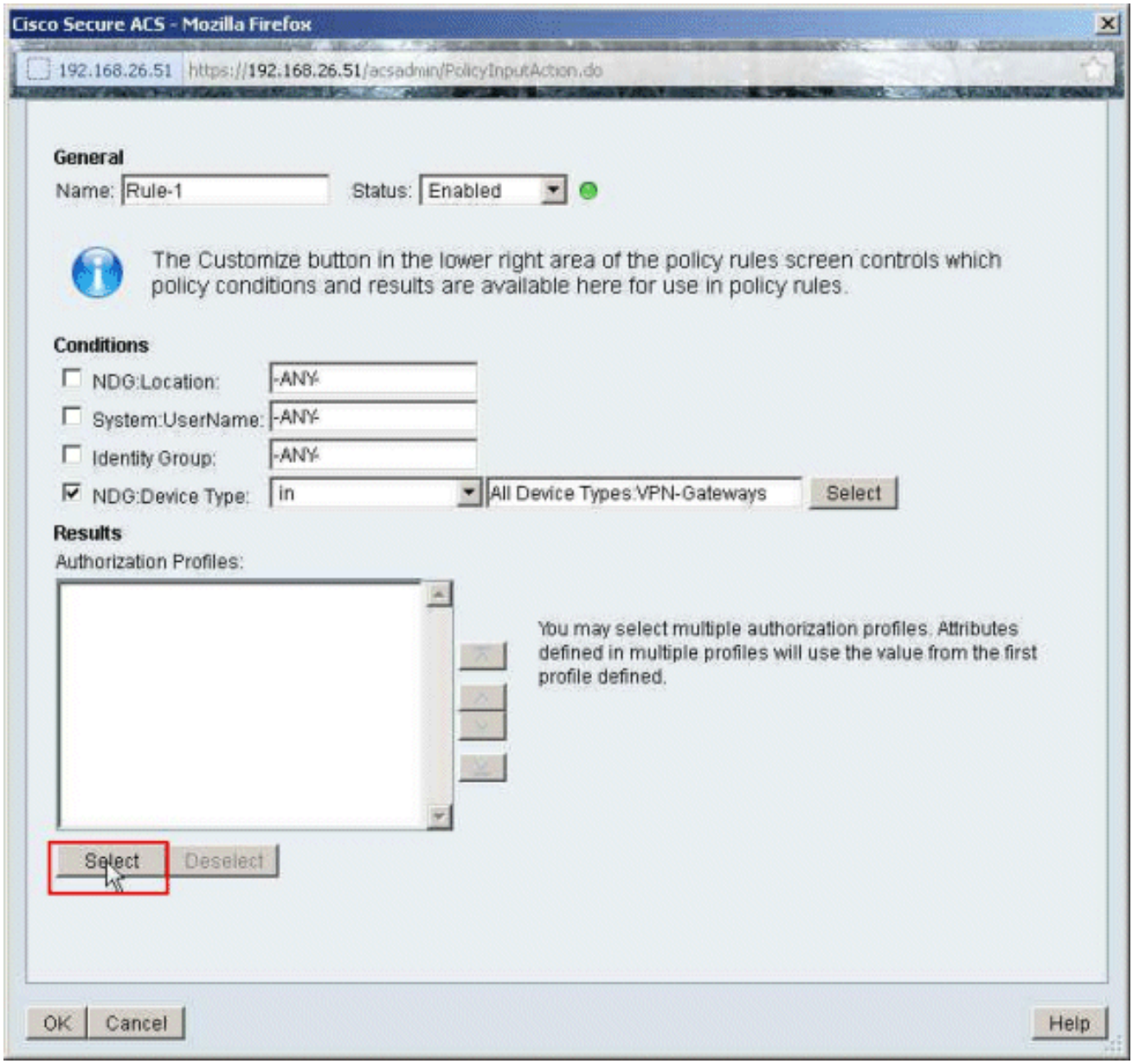
choisi.



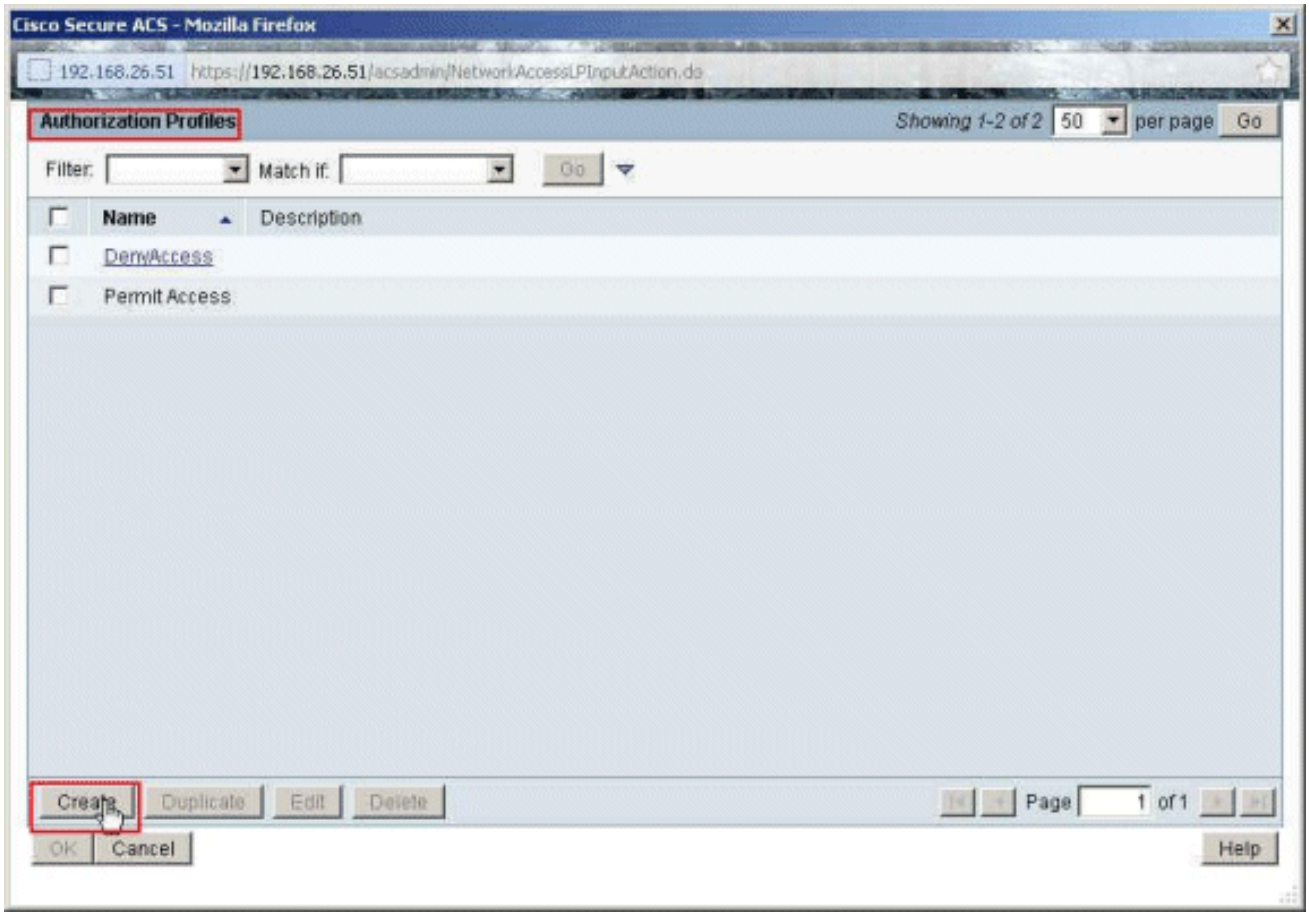
11. Choisissez les **passerelles VPN de** groupe de périphériques réseau créées plus tôt, et cliquez sur
OK.



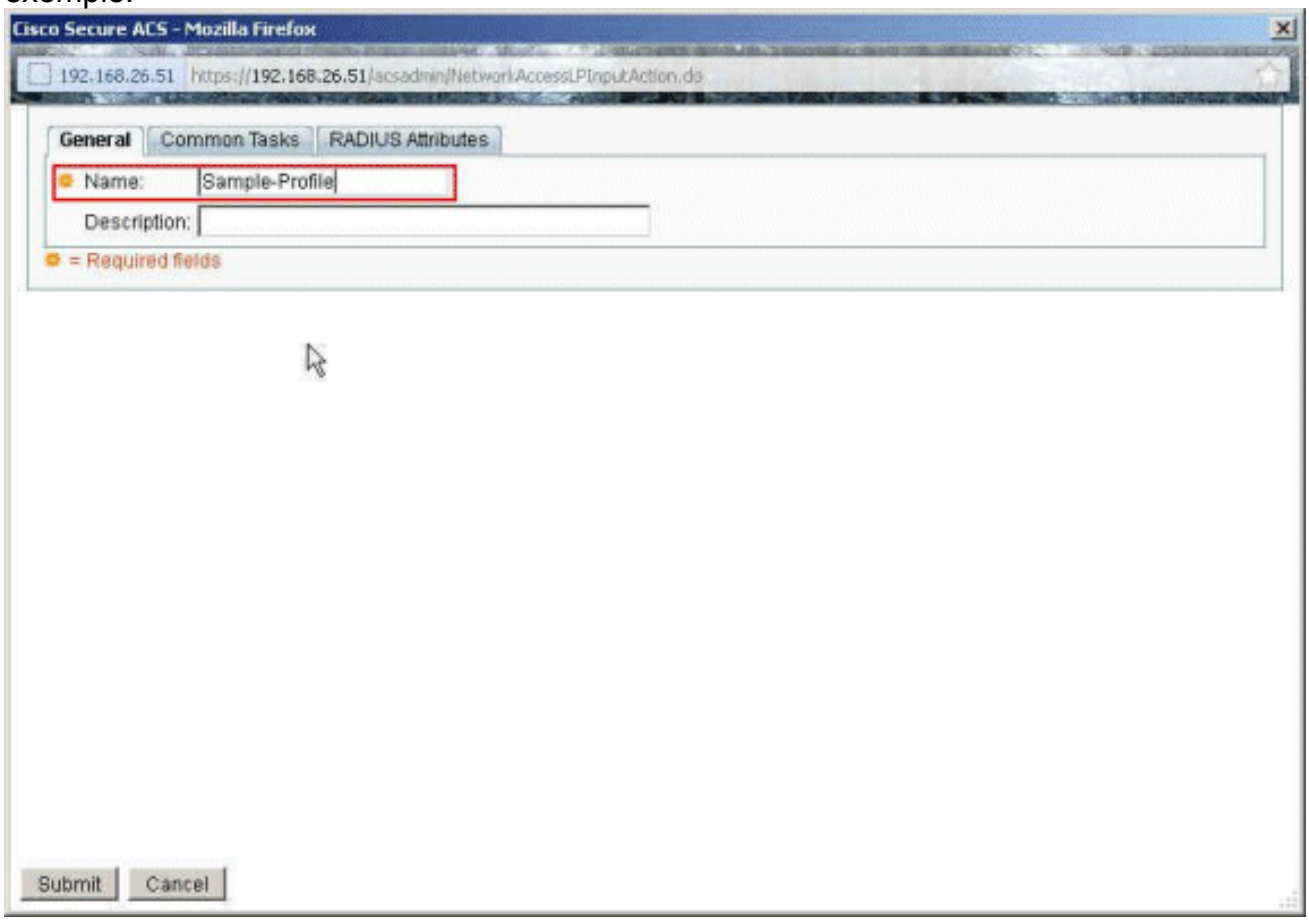
12. Clic **choisi**.



13. Le clic **créent** afin de créer un nouveau profil d'autorisation.

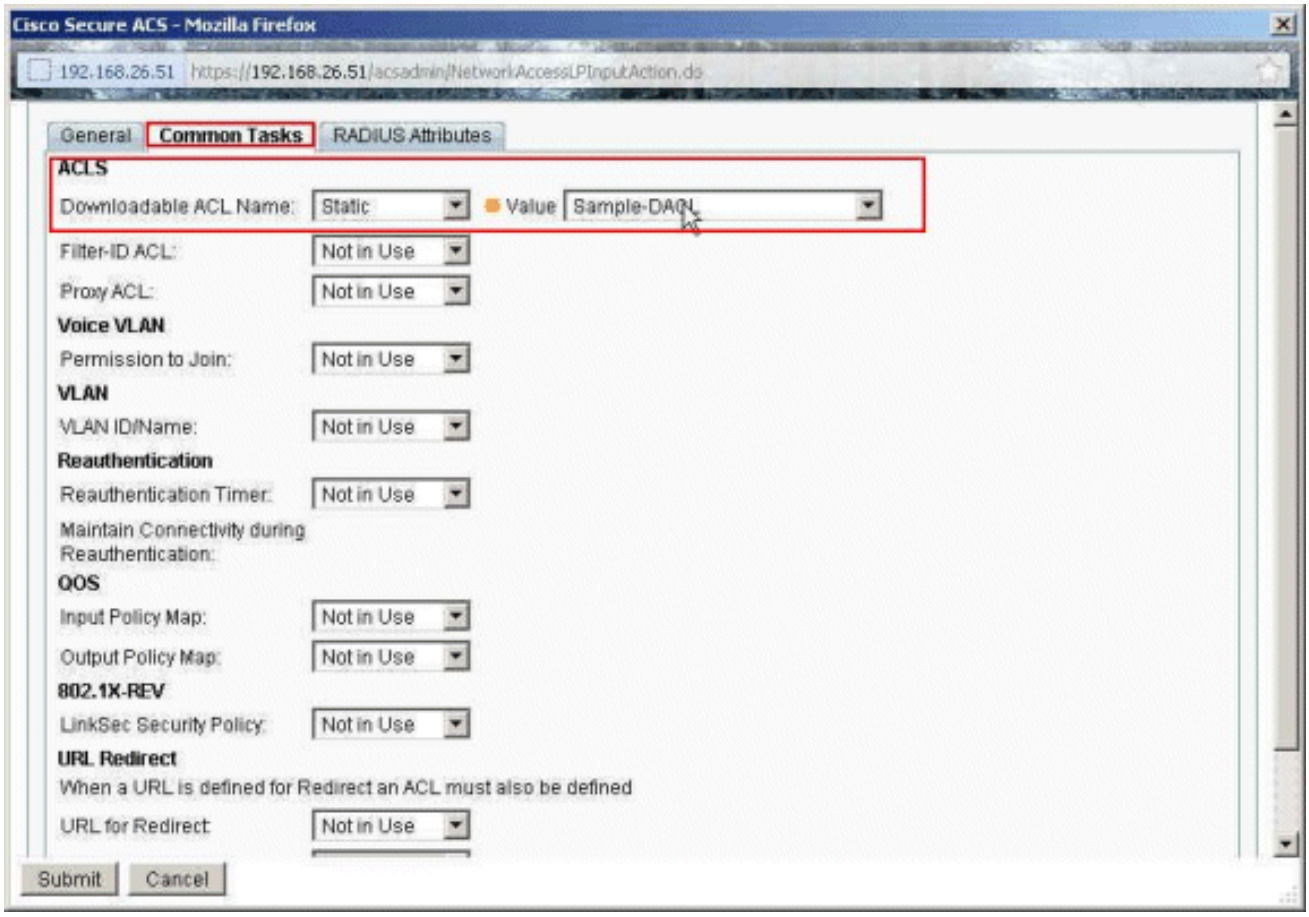


14. Fournissez un nom pour le **profil d'autorisation**. **L'exemple de profil** est le nom utilisé dans cet
exemple.

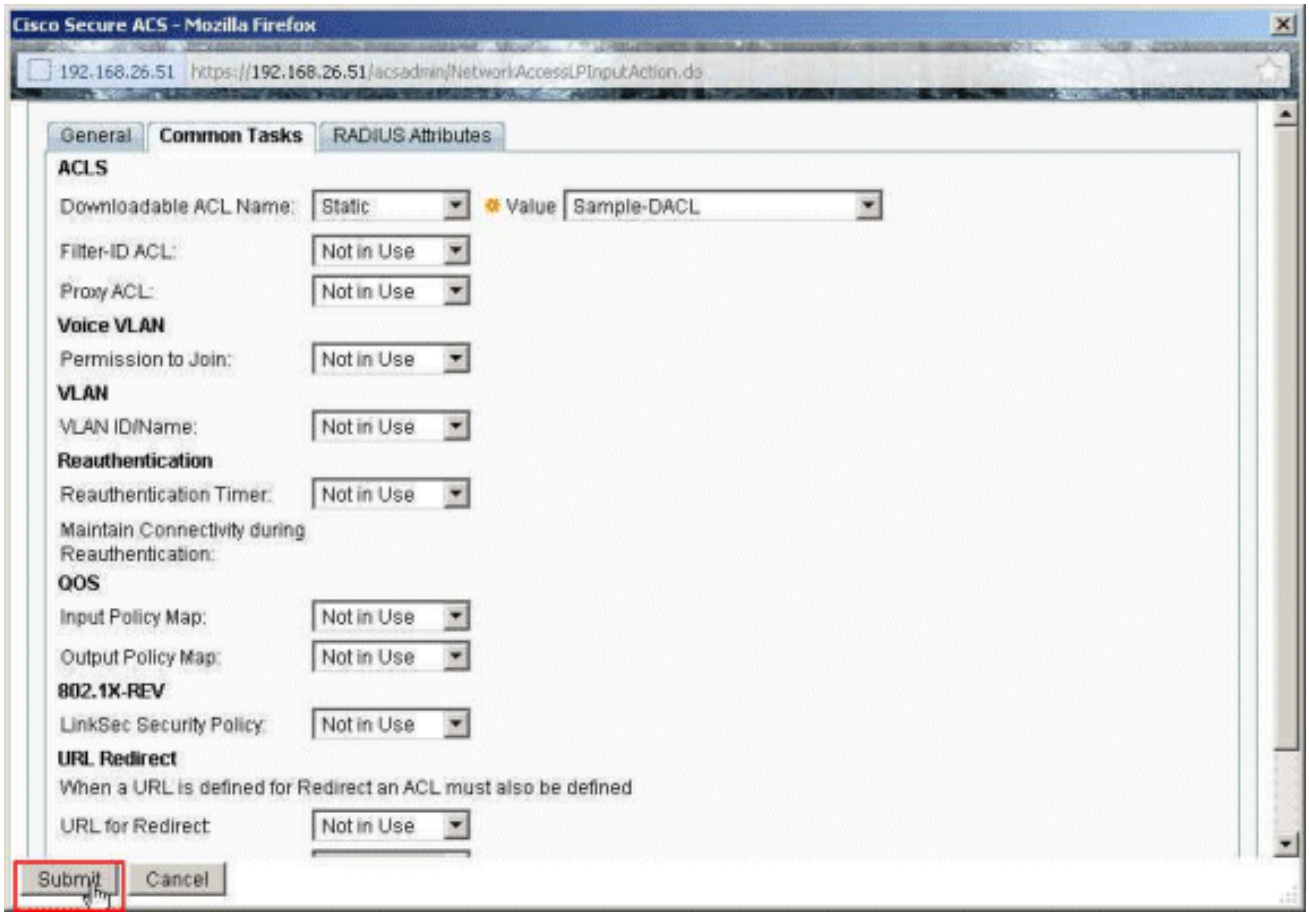


15. Choisissez l'onglet de **fonctionnalités usuelles**, et la **charge statique** choisie de la liste déroulante pour le nom téléchargeable d'ACL. Choisissez le **DACL** de création récente

(échantillon-DACL) de la liste déroulante de valeur.

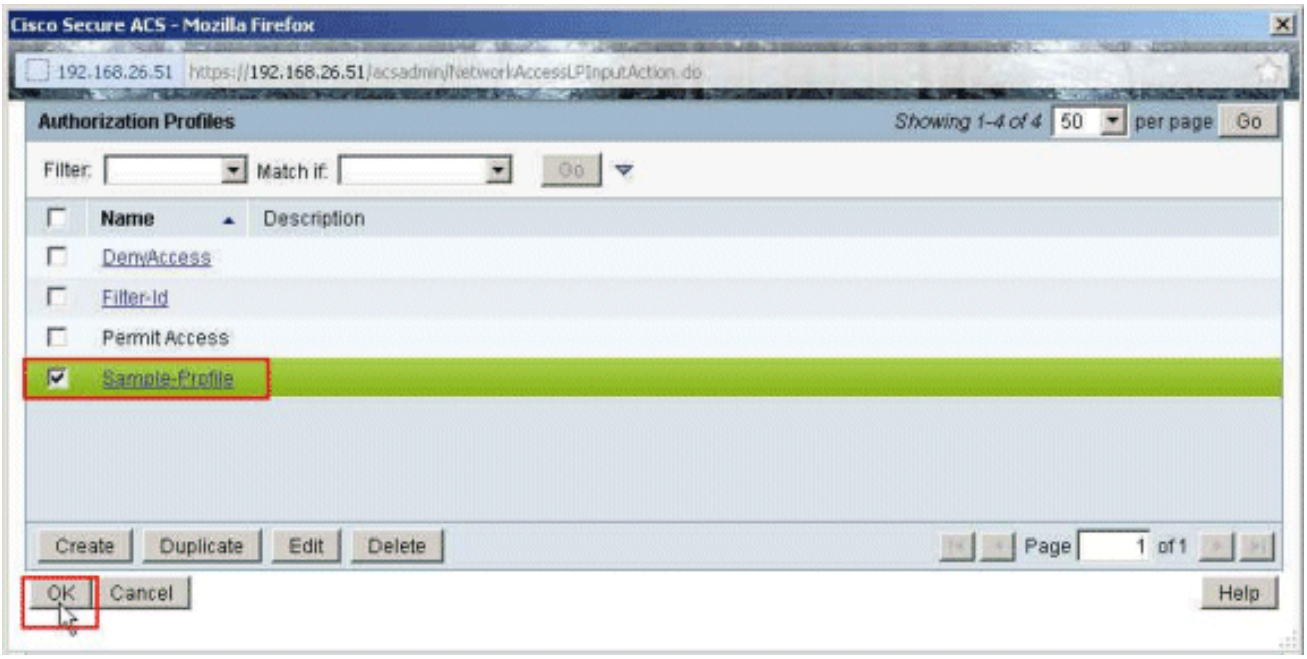


16. Cliquez sur **Submit**.

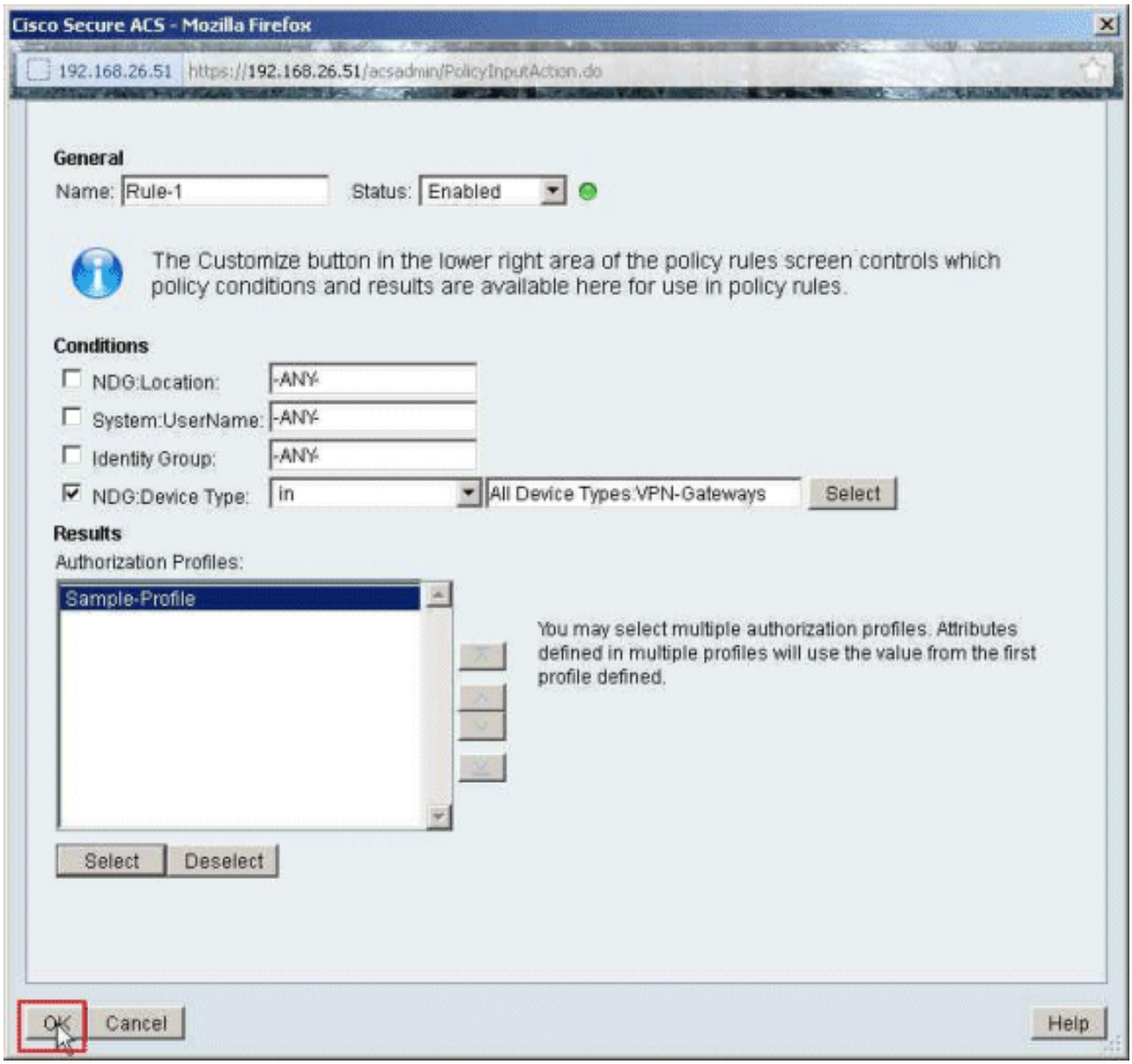


17. **L'exemple de profil** choisi créé plus tôt, et cliquent sur

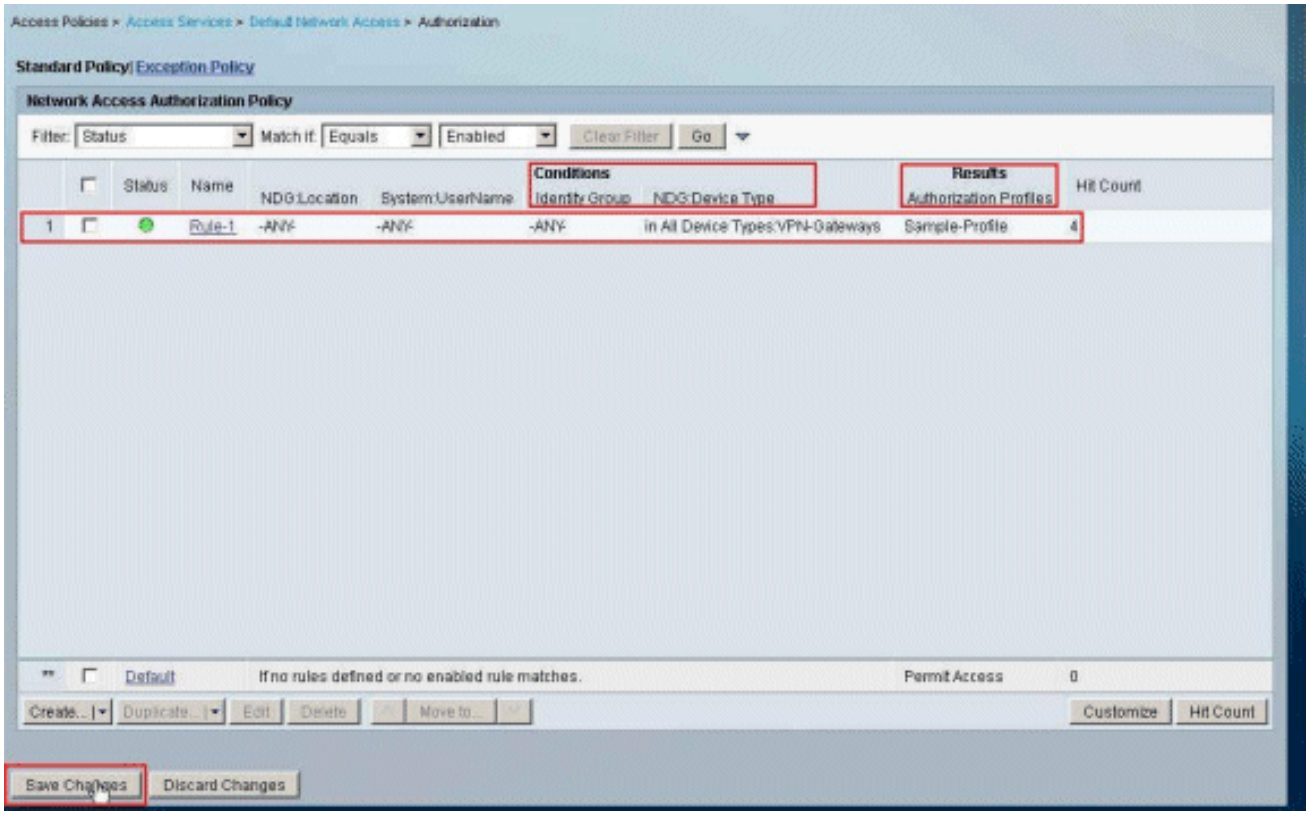
OK.



18. Cliquez sur
OK.



19. Vérifiez que **Rule-1** est créé avec des **passerelles VPN** comme NDG : Type de périphérique comme condition, et **exemple de profil** comme résultat. **Modifications de sauvegarde de** clic.



Configurez les configurations IETF RADIUS pour un groupe d'utilisateurs

Afin de télécharger un nom pour une liste d'accès que vous avez déjà créée sur les dispositifs de sécurité du serveur de RADIUS quand un utilisateur authentifie, configurez l'attribut de filtre-id IETF RADIUS (attribut numéro 11) :

```
filter-id=acl_name
```

L'usercisco d'Échantillon-groupe authentifie avec succès, et le serveur de RADIUS télécharge un nom d'ACL (nouveau) pour une liste d'accès que vous avez déjà créée sur les dispositifs de sécurité. L'utilisateur « Cisco » peut accéder à tous les périphériques qui sont à l'intérieur du réseau de l'ASA **excepté le** serveur de 10.1.1.2. Afin de vérifier l'ACL, voyez la section d'ACL de Filtre-id.

Selon l'exemple, l'ACL nommé **nouveau** est configuré pour filtrer dans l'ASA :

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

Ces paramètres apparaissent seulement quand ce sont vrais. Vous avez configuré :

- Client d'AAA pour utiliser un des protocoles RADIUS en configuration réseau
- Un profil d'autorisation avec le Filtre-id de RADIUS (IETF) est sélectionné sous la section de

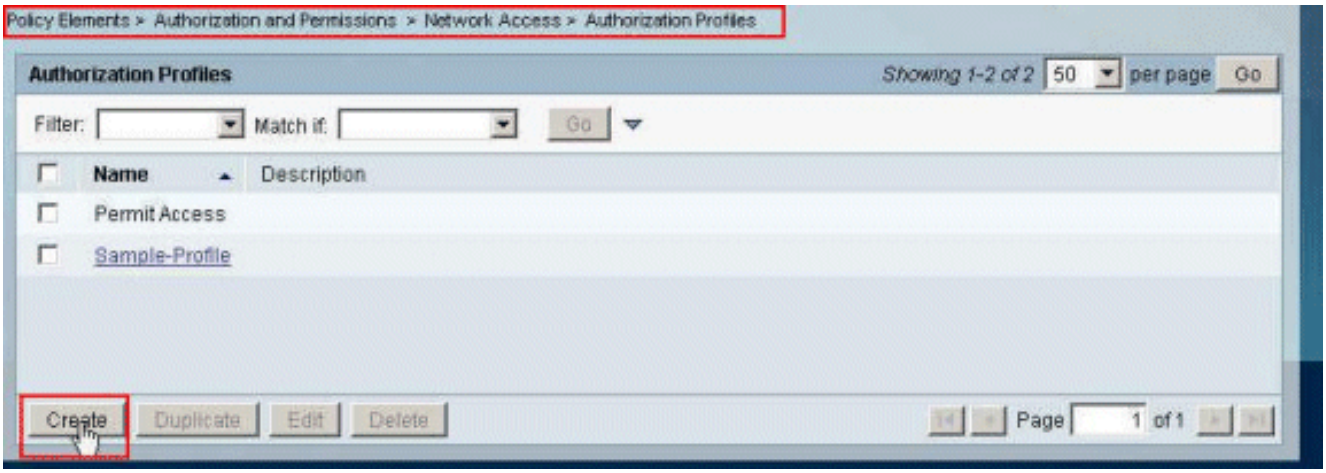
résultat de la règle au service d'accès.

Des attributs RADIUS sont envoyés comme profil pour chaque utilisateur d'ACS au client de demande d'AAA.

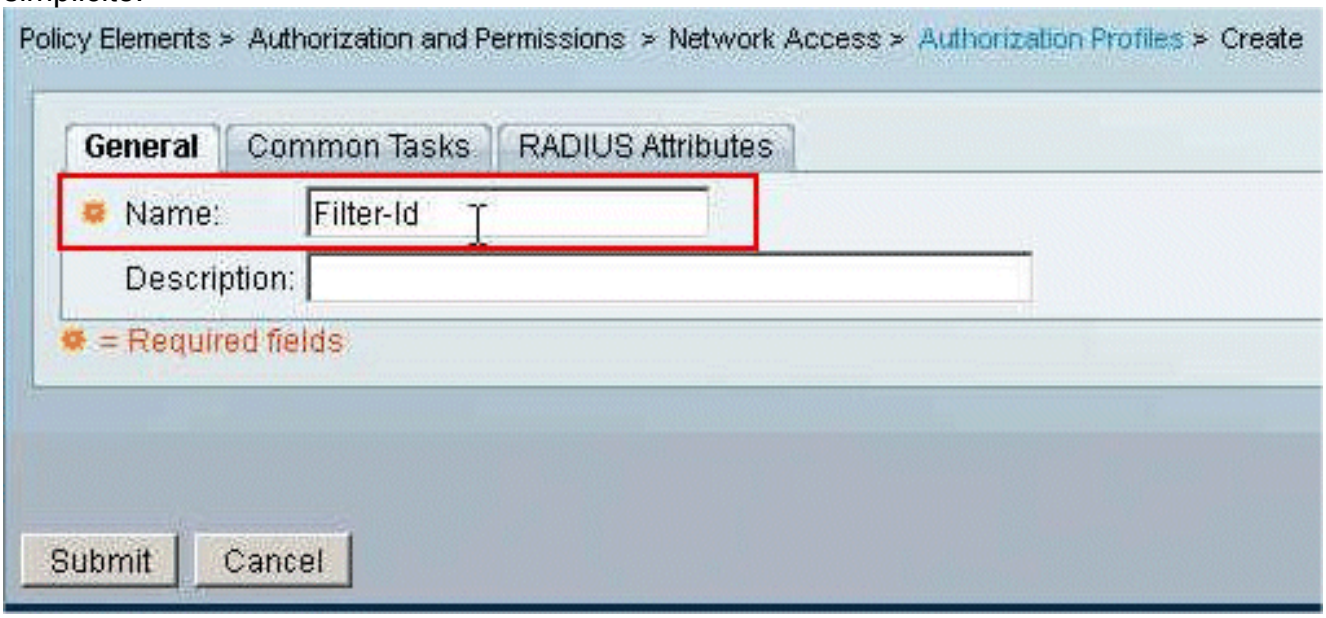
Étapes complètes 1 à 6 et à 10 à 12 du configurer ACS pour l'ACL téléchargeable pour l'utilisateur individuel, suivi des étapes 1 à 6 du configurer ACS pour l'ACL téléchargeable pour le groupe, et exécutent ces étapes dans cette section afin de configurer le Filtre-id dans le Cisco Secure ACS.

Afin de configurer des configurations d'**attribut RADIUS IETF** pour s'appliquer comme dans le profil d'autorisation, exécutez ces étapes :

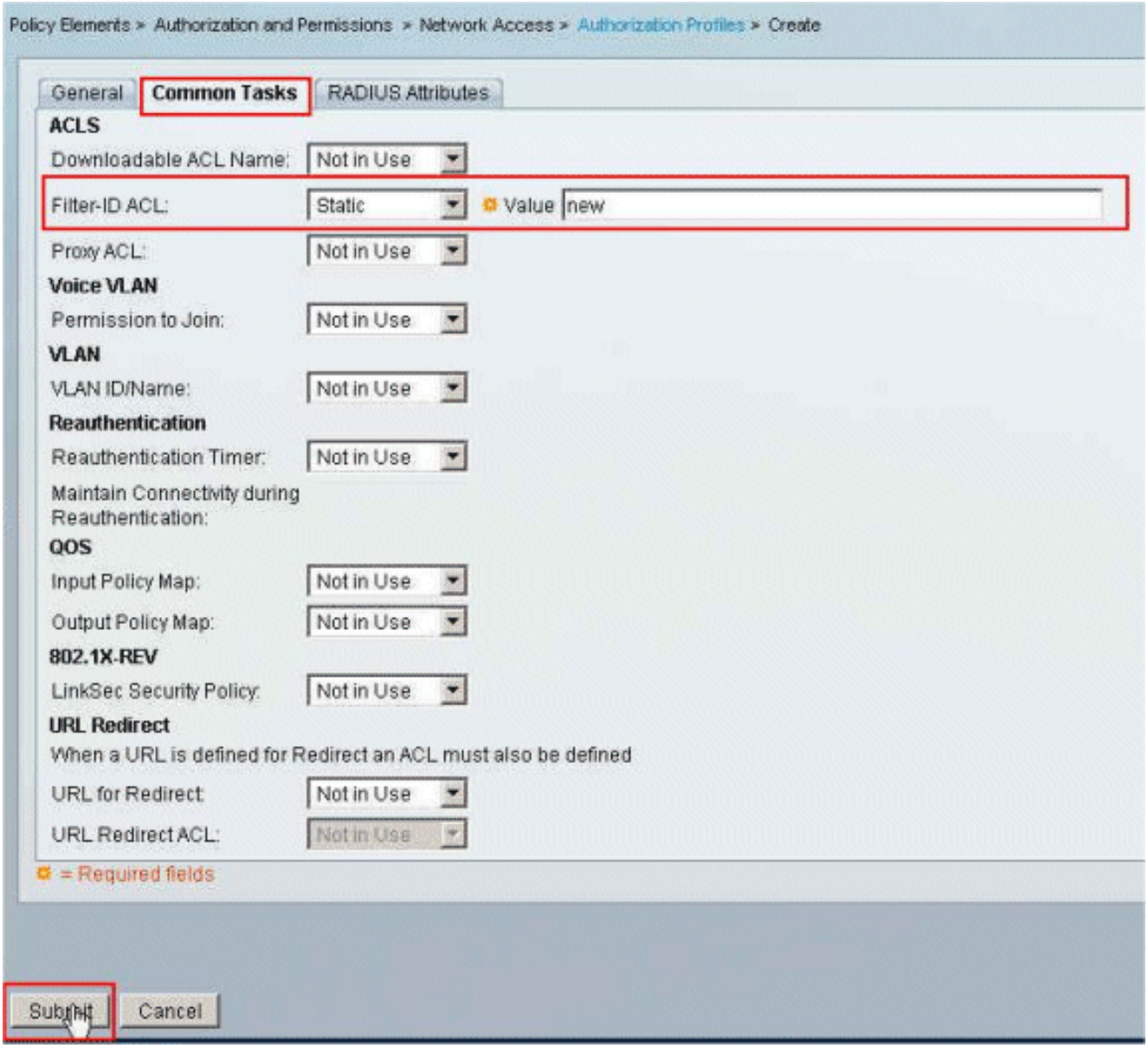
1. Choisissez les **éléments de stratégie** > l'**autorisation et les autorisations** > les **profils d'accès au réseau** > d'**autorisation**, et le clic **créent** afin de créer un nouveau profil d'autorisation.



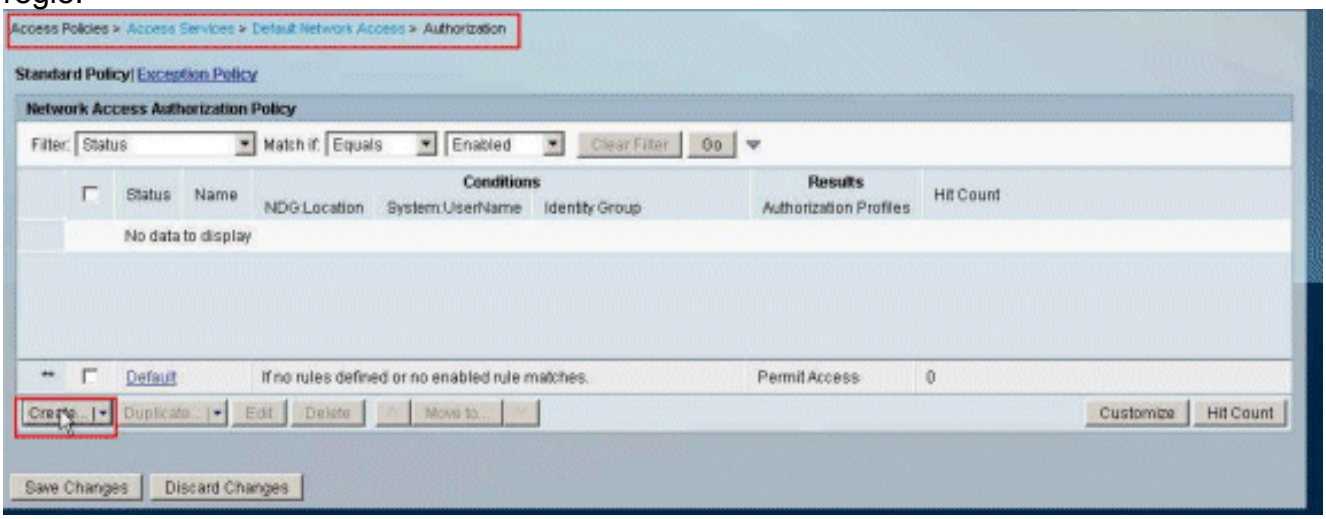
2. Fournissez un nom pour le **profil d'autorisation**. **Le Filtre-id** est le nom de profil d'autorisation choisi dans cet exemple pour la simplicité.



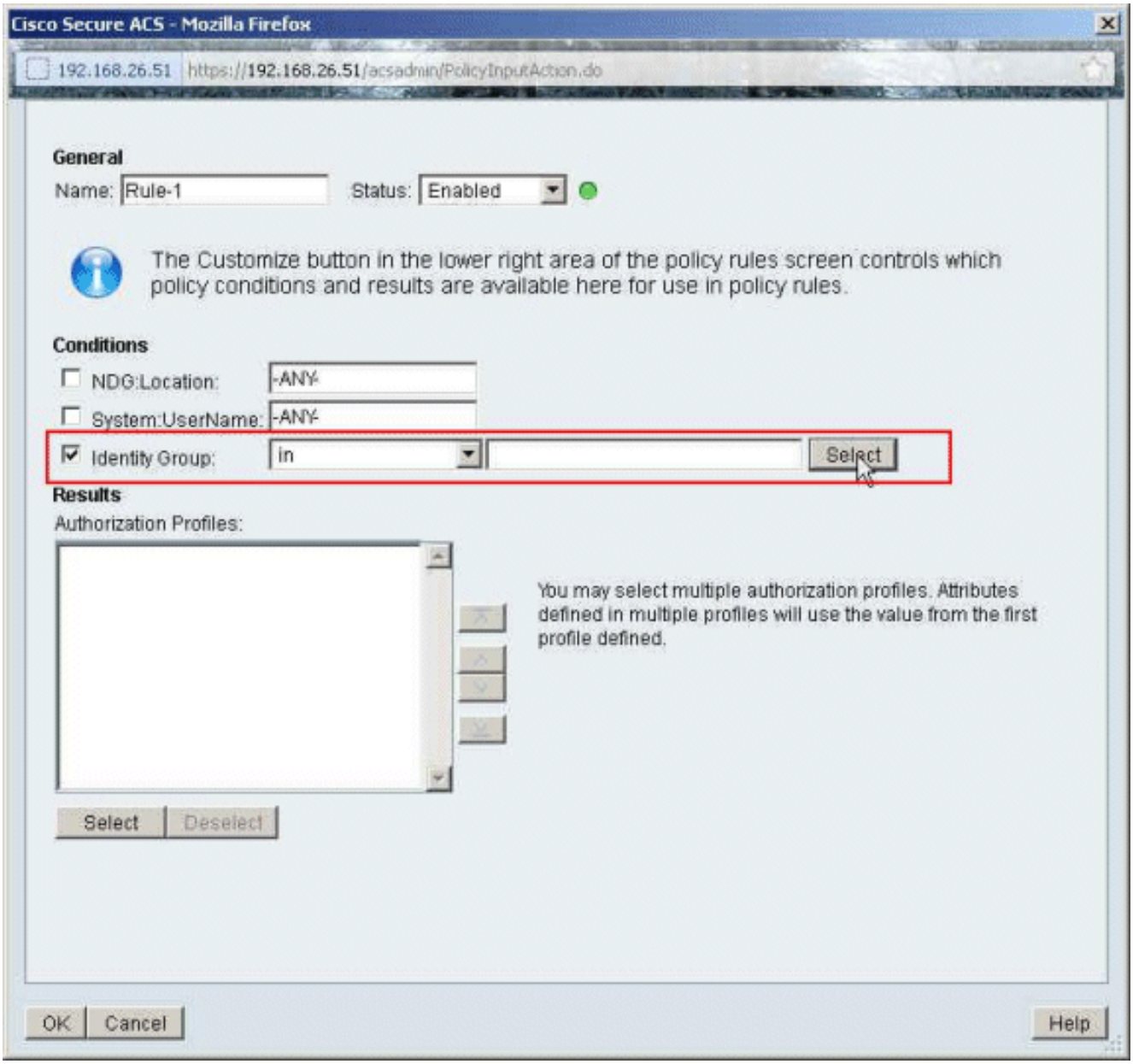
3. Cliquez sur l'onglet de **fonctionnalités usuelles**, et choisissez la **charge statique de la** liste déroulante pour l'**ACL de Filtre-ID**. Écrivez le nom de liste d'accès comme **nouveau** dans le domaine de valeur, et cliquez sur Submit.



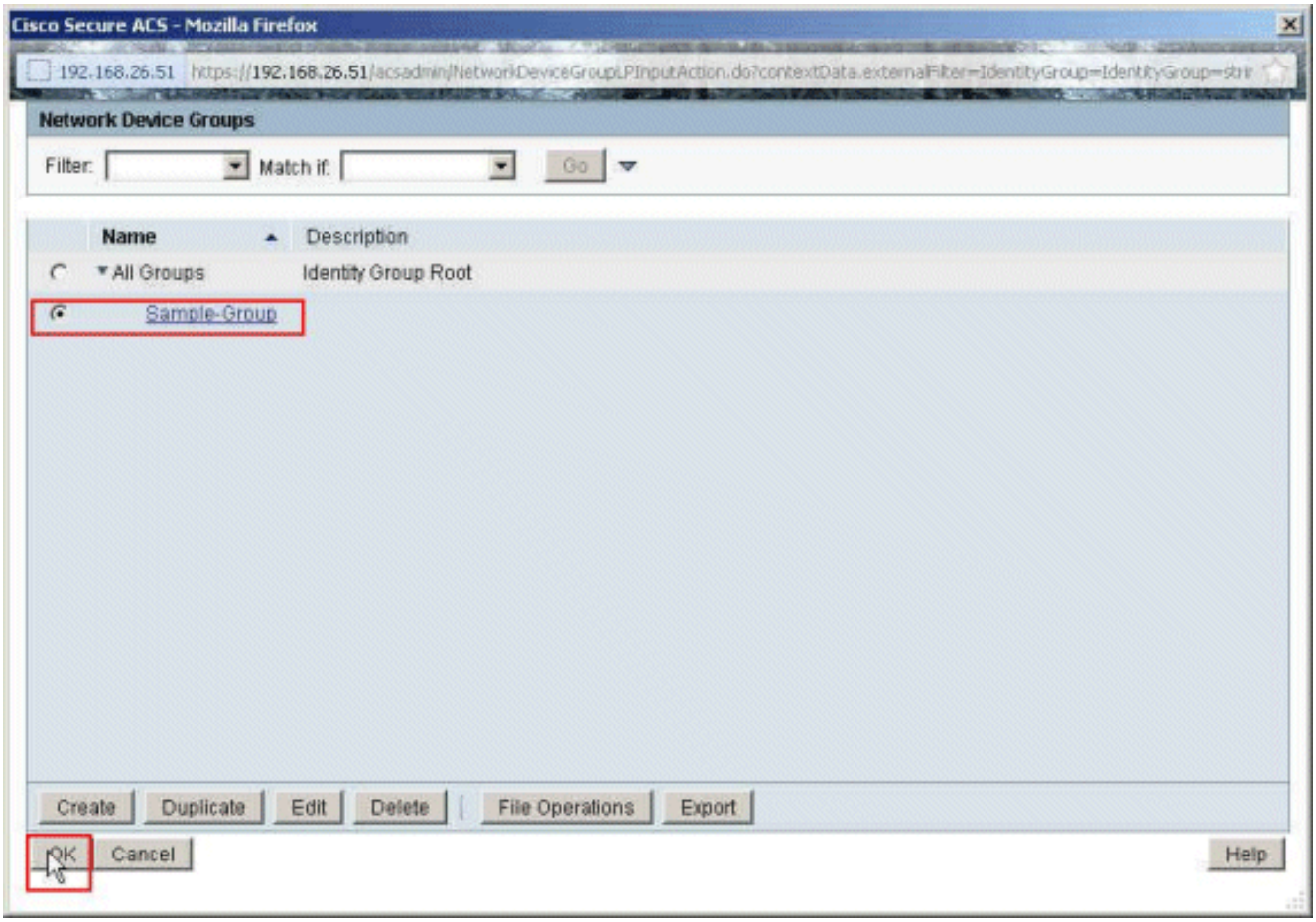
4. Choisissez les **stratégies d'Access** > les **services d'accès** > l'**accès au réseau** > l'**autorisation de par défaut**, et le clic **créent** afin de créer une nouvelle règle.



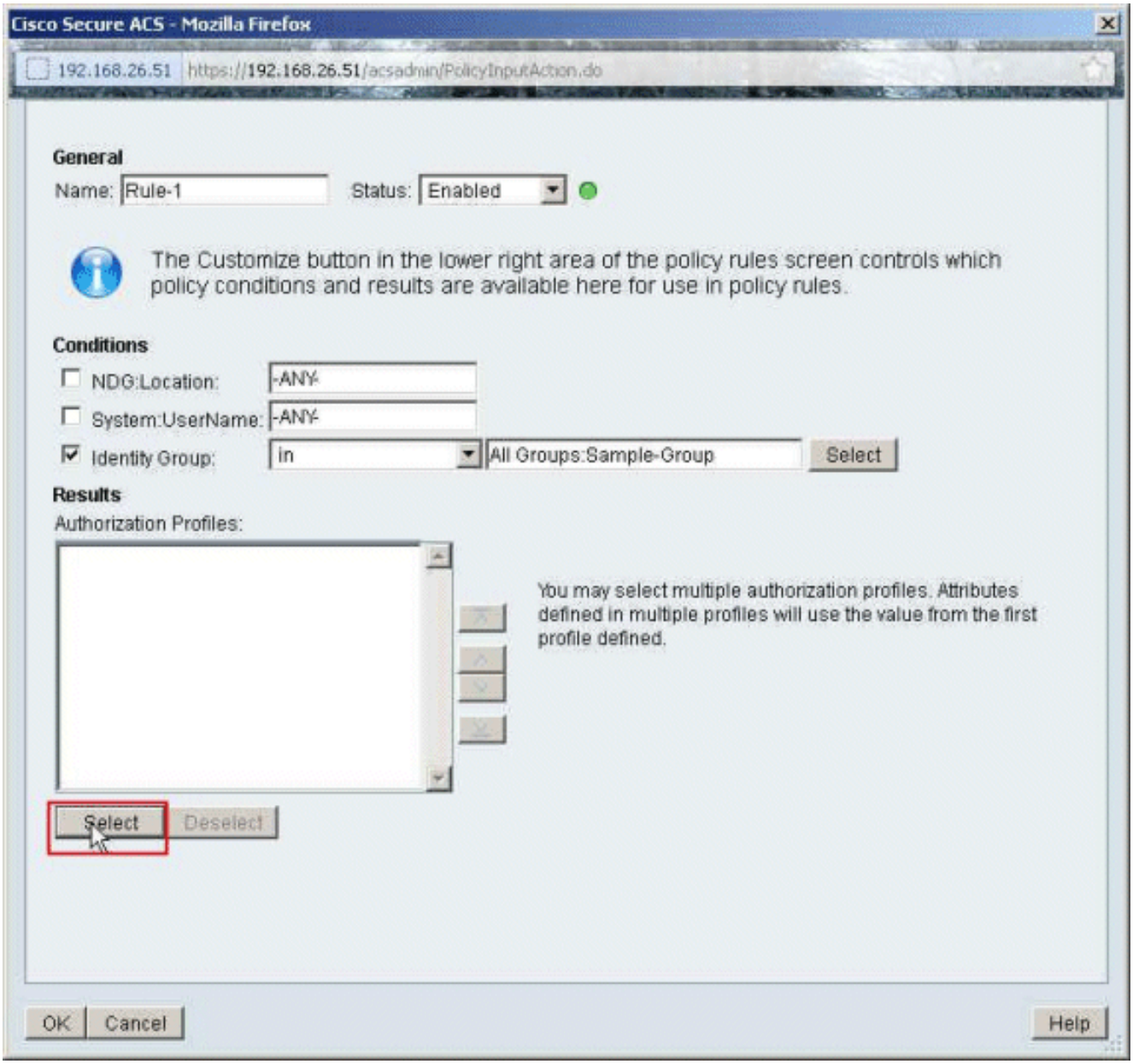
5. Assurez-vous que la case à cocher à côté du **groupe d'identité** est vérifiée, et cliquez sur **choisi**.



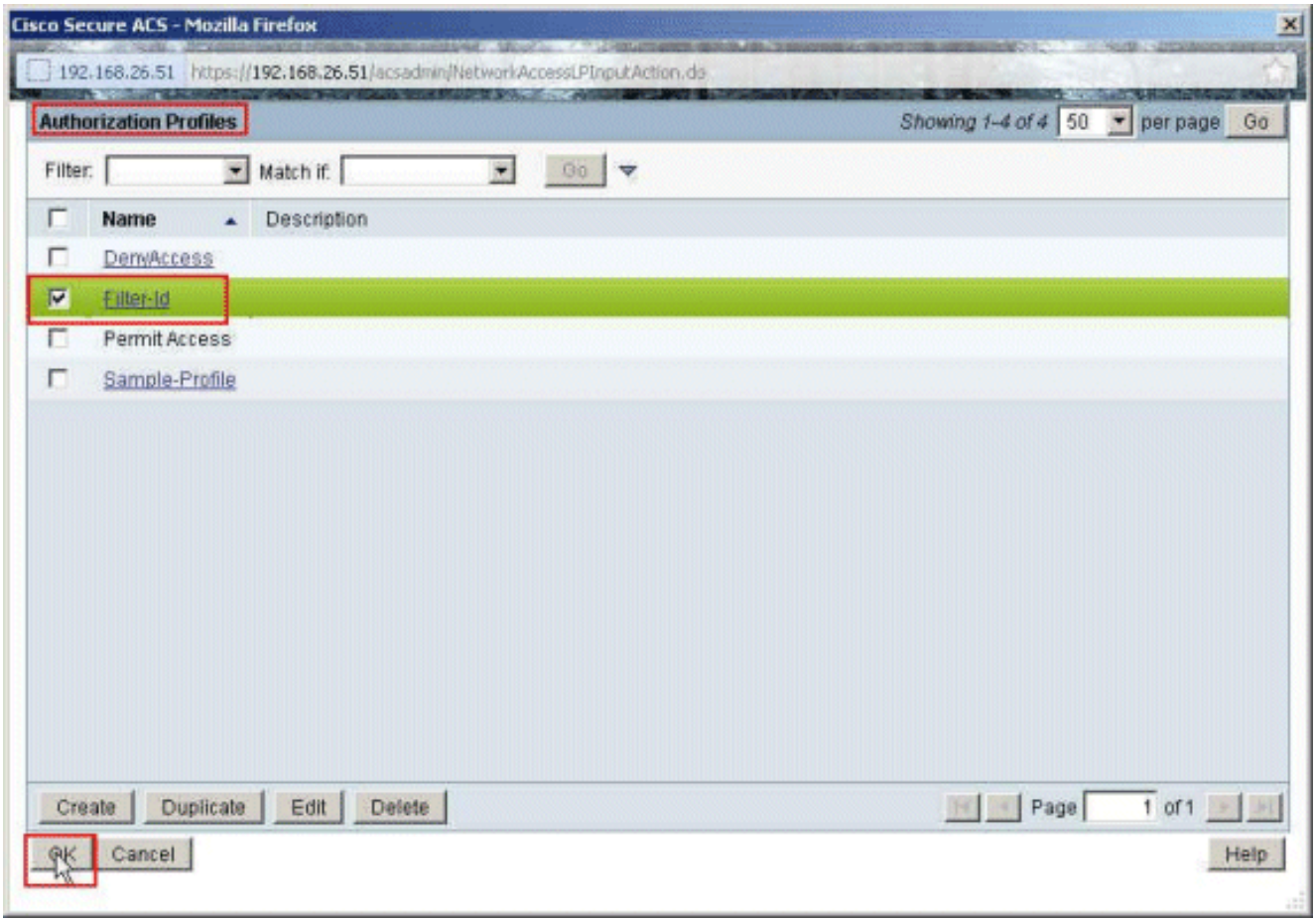
6. Choisissez l'Échantillon-**groupe**, et cliquez sur OK.



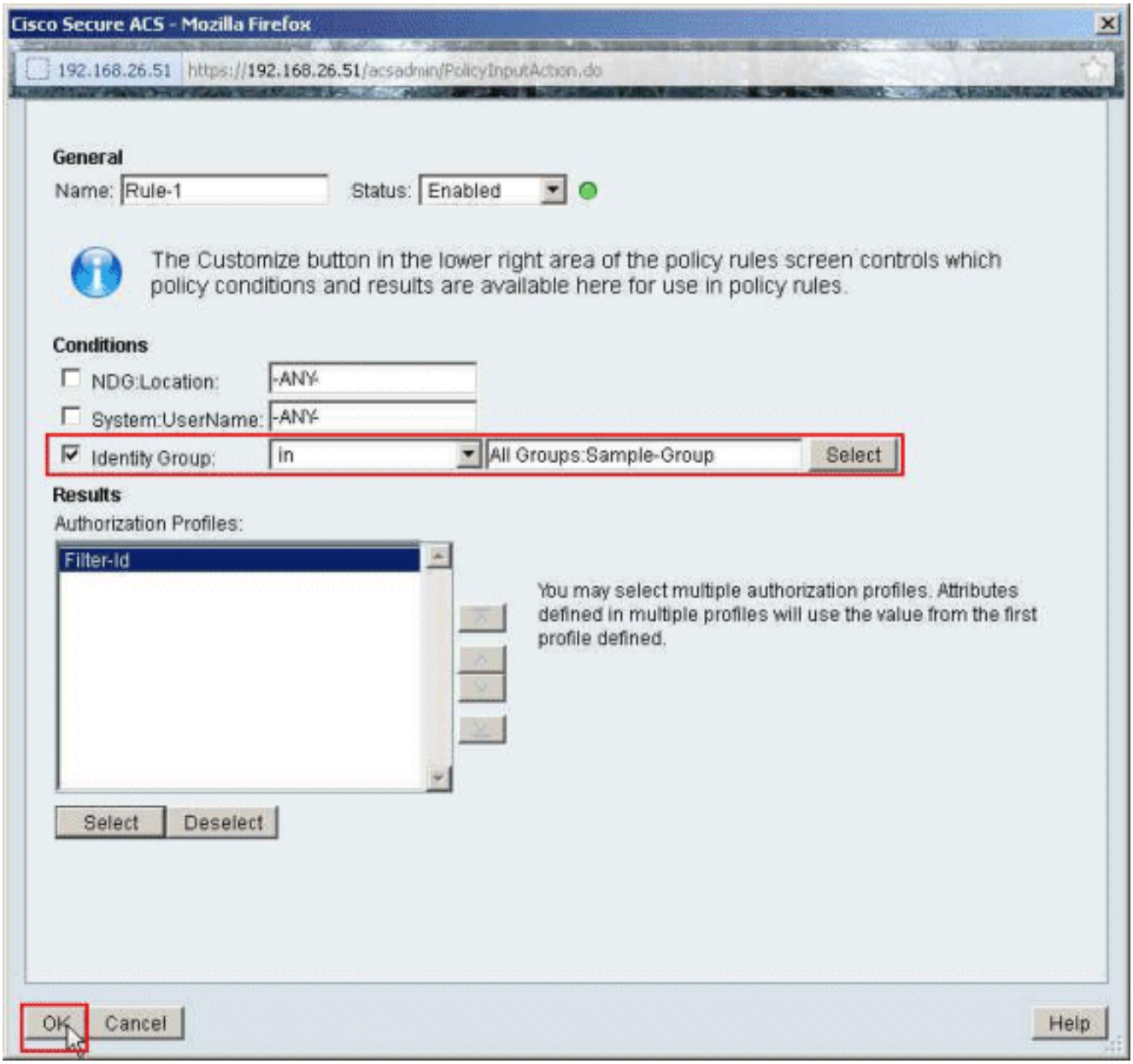
7. Clic **choisi** dans la section de profils d'autorisation.



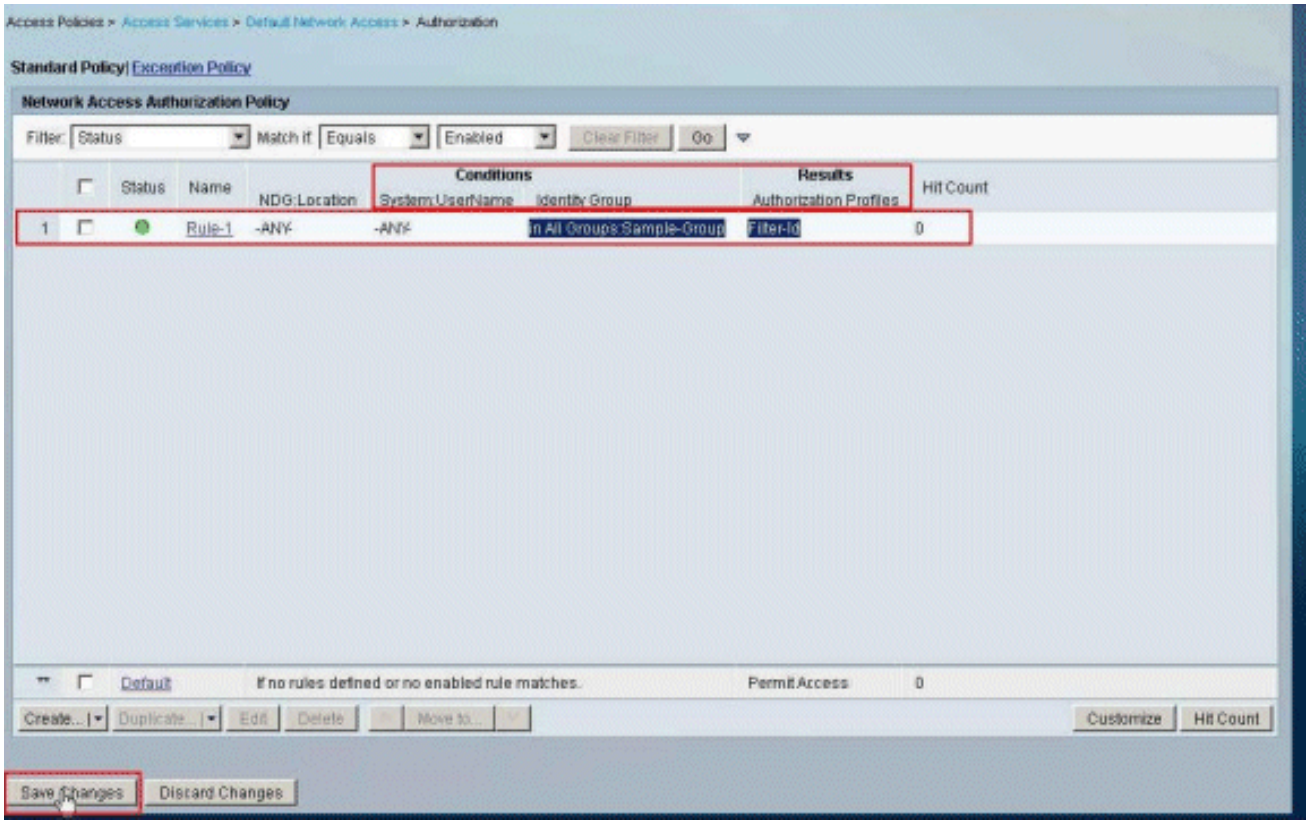
8. Choisissez le Filtre-**id de** profil d'autorisation créé plus tôt, et cliquez sur OK.



9. Cliquez sur **OK**.



10. Vérifiez que **Rule-1** est créé avec l'Échantillon-**groupe de** groupe d'identité comme condition et le Filtre-**id** comme résultat. **Modifications de sauvegarde de**
clic.

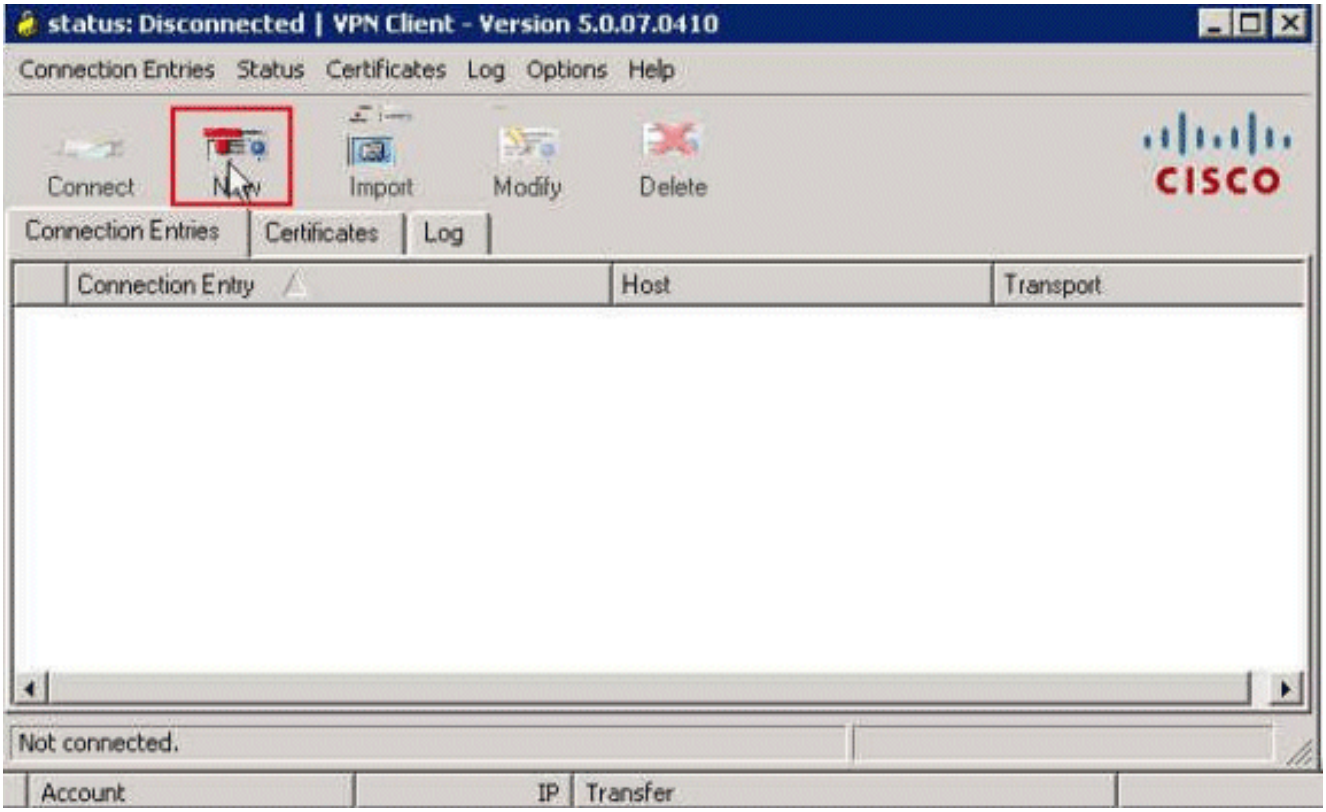


Configuration de Client VPN Cisco

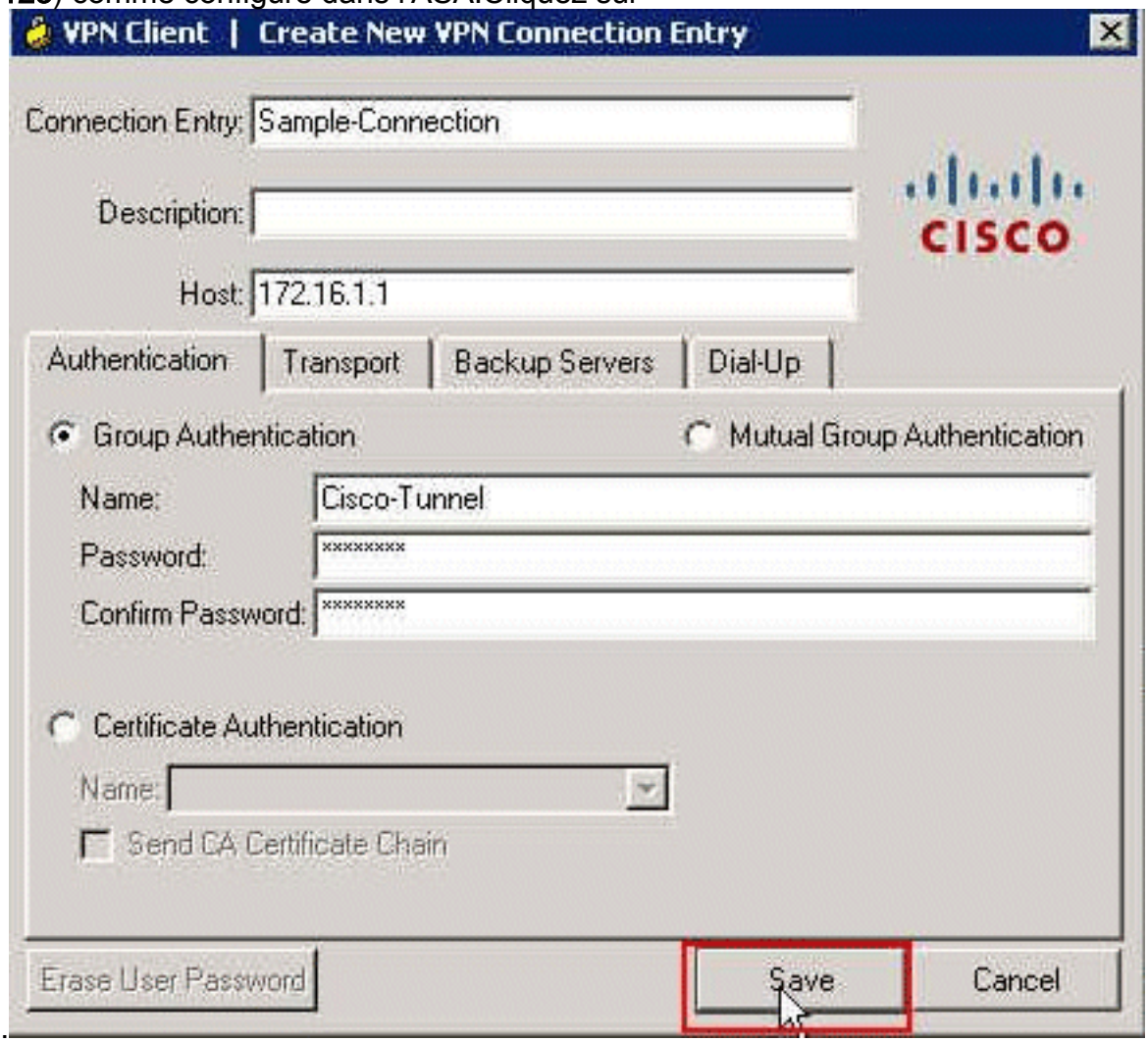
Connectez à Cisco ASA au Client VPN Cisco afin de vérifier que l'ASA est avec succès configurée.

Procédez comme suit :

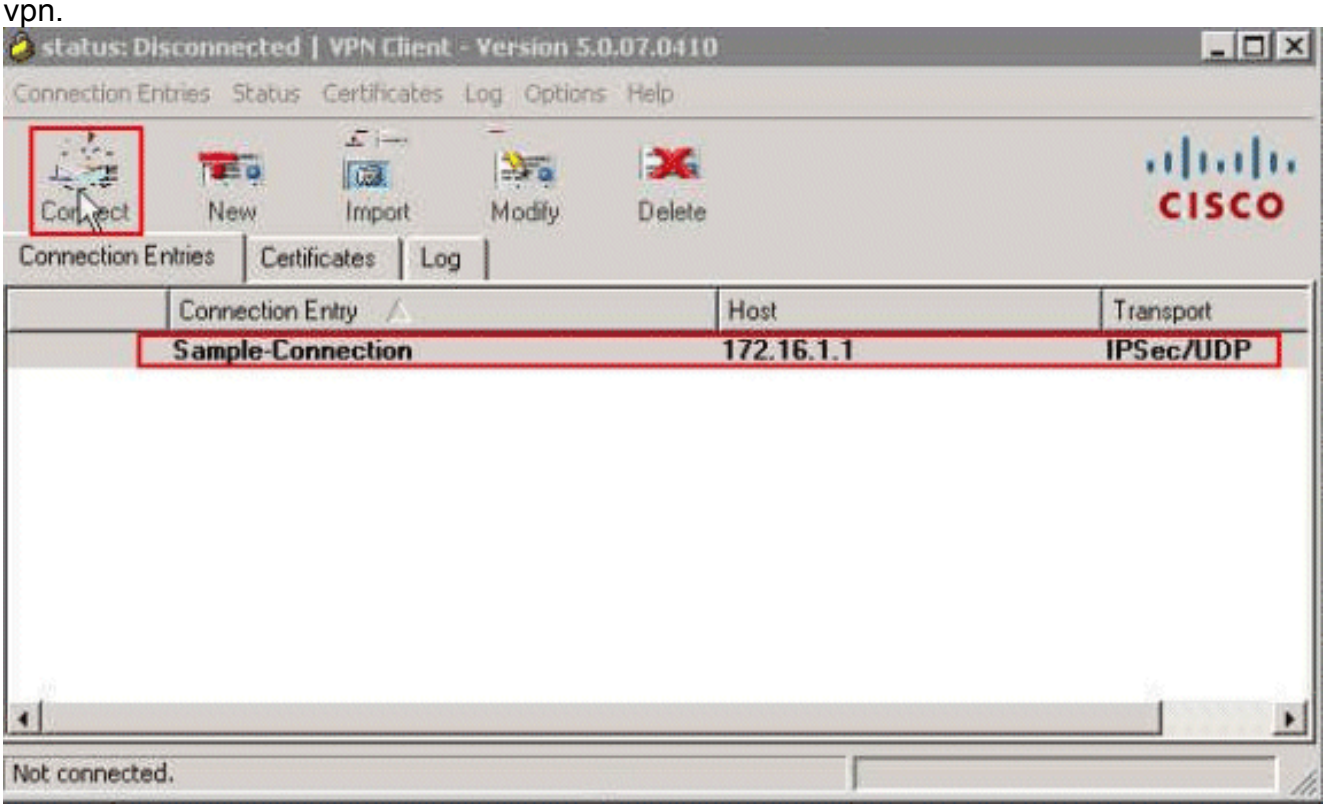
1. Choisissez le **début** > les **programmes** > le **client vpn de Cisco Systems** > le **client vpn**.
2. Cliquez sur New afin de lancer la nouvelle fenêtre d'entrée de connexion VPN de création.



3. Complétez les détails de votre nouvelle connexion :Entrez le nom de l'entrée de connexion avec une description.Écrivez l'**adresse IP extérieure de l'ASA** dans la case d'hôte.Entrez le nom de groupe de tunnel VPN (Cisco-**tunnel**) et le mot de passe (clé pré-partagée - **cisco123**) comme configuré dans l'ASA.Cliquez sur **Save**.

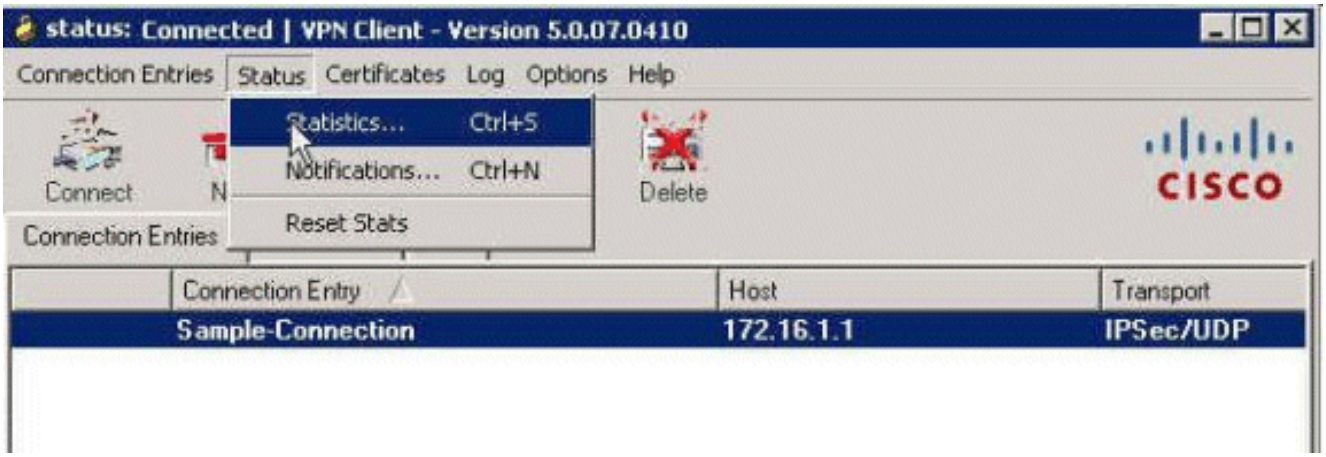


4. Cliquez sur la connexion que vous voulez utiliser, et le clic **se connectent de la** fenêtre principale de client
vpn.



5. Une fois incité, entrez le nom d'utilisateur **Cisco** et le mot de passe **cisco123** comme configuré dans l'ASA pour l'authentification, et cliquez sur OK afin de se connecter au réseau distant.

6. Une fois que la connexion est avec succès établie, choisissez les **statistiques du** menu d'état afin de vérifier les détails du
tunnel.



Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Affichez les cryptos commandes

- **show crypto isakmp sa** - Affiche toutes les associations de sécurité en cours d'IKE (SAS) à un pair.

```
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** - Affiche les configurations utilisées par le courant 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
```

ACL téléchargeable pour l'utilisateur/groupe

Vérifiez l'ACL téléchargeable pour l'utilisateur Cisco. ACLs sont téléchargés du 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
```

ACL de Filtre-id

Le Filtre-id [011] s'est appliqué pour le groupe - l'Échantillon-groupe, et les utilisateurs du groupe sont filtrés selon l'ACL (nouveau) défini dans l'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
```

Dépanner

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration. L'exemple de sortie Debug est également affiché.

Remarque: Pour plus d'informations sur l'Accès à distance IPsec VPN de dépannage, référez-vous à la plupart des solutions communes de dépannage VPN d'IPsec L2L et d'Accès à distance.

Suppression des associations de sécurité

Quand vous dépannez, veillez à effacer SAS existante après que vous apportiez une modification. En mode privilégiée du PIX, utilisez les commandes suivantes :

- **effacez [crypto] ipsec SA** - Supprime l'IPsec actif SAS. Le mot clé crypto est facultatif.
- **effacez [crypto] ISAKMP SA** - Supprime l'IKE actif SAS. Le mot clé crypto est facultatif.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec 7** - Affiche les négociations IPSecs du Phase 2.
- **debug crypto isakmp 7** - Affiche les négociations ISAKMP du Phase 1.

Informations connexes

- Page d'assistance des appliances de sécurité adaptables de la gamme Cisco ASA 5500
- Références de commandes de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Cisco Adaptive Security Device Manager
- Page de support de la négociation IPSec/des protocoles IKE
- Cisco VPN Client Support Page
- Système de contrôle d'accès sécurisé (ACS) de Cisco
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems