ASA 8.3 e versioni successive: Esempio di autorizzazione Radius (ACS 5.x) per l'accesso VPN con ACL scaricabile con CLI e ASDM

Sommario

Introduzione

In questo documento viene descritto come configurare l'appliance di sicurezza per autenticare gli utenti per l'accesso alla rete. Poiché le autorizzazioni RADIUS possono essere attivate in modo implicito, in questo documento non viene fornita alcuna informazione sulla configurazione dell'autorizzazione RADIUS sull'accessorio di sicurezza. Vengono fornite informazioni sul modo in cui l'accessorio di protezione gestisce le informazioni dell'elenco degli accessi ricevute dai server RADIUS.

Èpossibile configurare un server RADIUS in modo che al momento dell'autenticazione venga scaricato un elenco degli accessi all'accessorio di protezione o un nome di elenco degli accessi.

L'utente è autorizzato a eseguire solo le operazioni consentite nell'elenco degli accessi specifico.

Gli elenchi degli accessi scaricabili sono il metodo più scalabile quando si utilizza Cisco Secure Access Control Server (ACS) per fornire gli elenchi degli accessi appropriati per ogni utente. Per ulteriori informazioni sulle funzionalità delle liste di accesso scaricabili e su Cisco Secure ACS, consultare il documento sulla configurazione di un server RADIUS per inviare liste di controllo degli accessi scaricabili e ACL IP scaricabili.

Per ulteriori informazioni, fare riferimento al documento ASA/PIX 8.x: Esempio di autorizzazione Radius (ACS) per l'accesso alla rete con ACL scaricabile con CLI e ASDM per la stessa configurazione sull'appliance Cisco ASA con versioni 8.2 e precedenti.

Prerequisiti

Requisiti

In questo documento si presume che le appliance ASA (Adaptive Security Appliance) siano completamente operative e configurate per consentire a Cisco Adaptive Security Device Manager (ASDM) o alla CLI di apportare modifiche alla configurazione.

Nota: per consentire la configurazione remota del dispositivo da parte di ASDM o Secure Shell (SSH), consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco ASA versione 8.3 e successive
- Cisco ASDM versione 6.3 e successive
- Cisco VPN Client versione 5.x e successive
- Cisco Secure ACS 5.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Èpossibile usare gli ACL IP scaricabili per creare set di definizioni di ACL che possono essere applicate a molti utenti o gruppi di utenti. Questi set di definizioni ACL sono chiamati contenuti ACL.

Gli ACL IP scaricabili funzionano nel modo seguente:

1. Quando ACS concede a un utente l'accesso alla rete, ACS determina se un ACL IP scaricabile è assegnato al profilo di autorizzazione nella sezione dei risultati.
2. Se ACS individua un ACL IP scaricabile assegnato al profilo di autorizzazione, invia un attributo (come parte della sessione utente, nel pacchetto RADIUS access-accept) che specifica l'ACL con nome e la versione dell'ACL con nome.
3. Se il client AAA risponde che la versione corrente dell'ACL non è presente nella cache, ossia l'ACL è nuovo o è stato modificato, ACS invia l'ACL (nuovo o aggiornato) al dispositivo.

Gli ACL IP scaricabili sono un'alternativa alla configurazione degli ACL nell'attributo RADIUS Cisco cisco-av-pair [26/9/1] di ciascun utente o gruppo di utenti. È possibile creare un ACL IP scaricabile una volta sola, assegnargli un nome e quindi assegnare l'ACL IP scaricabile a qualsiasi profilo di autorizzazione se si fa riferimento al nome. Questo metodo è più efficiente di quello utilizzato per configurare l'attributo RADIUS Cisco cisco-av-pair per il profilo di autorizzazione.

Quando si immettono le definizioni degli ACL nell'interfaccia Web di ACS, non usare parole chiave o nomi; per tutti gli altri aspetti, usare la sintassi dei comandi ACL standard e la semantica del client AAA a cui si intende applicare l'ACL IP scaricabile. Le definizioni ACL immesse in ACS comprendono uno o più comandi ACL. Ogni comando ACL deve essere su una riga separata.

Negli ACS, è possibile definire più ACL IP scaricabili e usarli in diversi profili di autorizzazione. In base alle condizioni specificate nelle regole di autorizzazione dei servizi di accesso, è possibile inviare profili di autorizzazione diversi contenenti ACL IP scaricabili a client AAA diversi.

Inoltre, è possibile modificare l'ordine dei contenuti dell'ACL in un ACL IP scaricabile. ACS esamina il contenuto degli ACL, a partire dalla parte superiore della tabella, e scarica il primo contenuto trovato. Quando si imposta l'ordine, è possibile garantire l'efficienza del sistema posizionando più in alto nell'elenco i contenuti degli ACL applicabili.

Per utilizzare un ACL IP scaricabile su un particolare client AAA, il client AAA deve rispettare le seguenti regole:

- Utilizza RADIUS per l'autenticazione
- Supporto di ACL IP scaricabili

Di seguito sono riportati alcuni esempi di dispositivi Cisco che supportano ACL IP scaricabili:

- ASA
- Dispositivi Cisco con IOS versione 12.3(8)T e successive

Questo è un esempio del formato da usare per immettere gli ACL ASA nella casella Definizioni ACL:

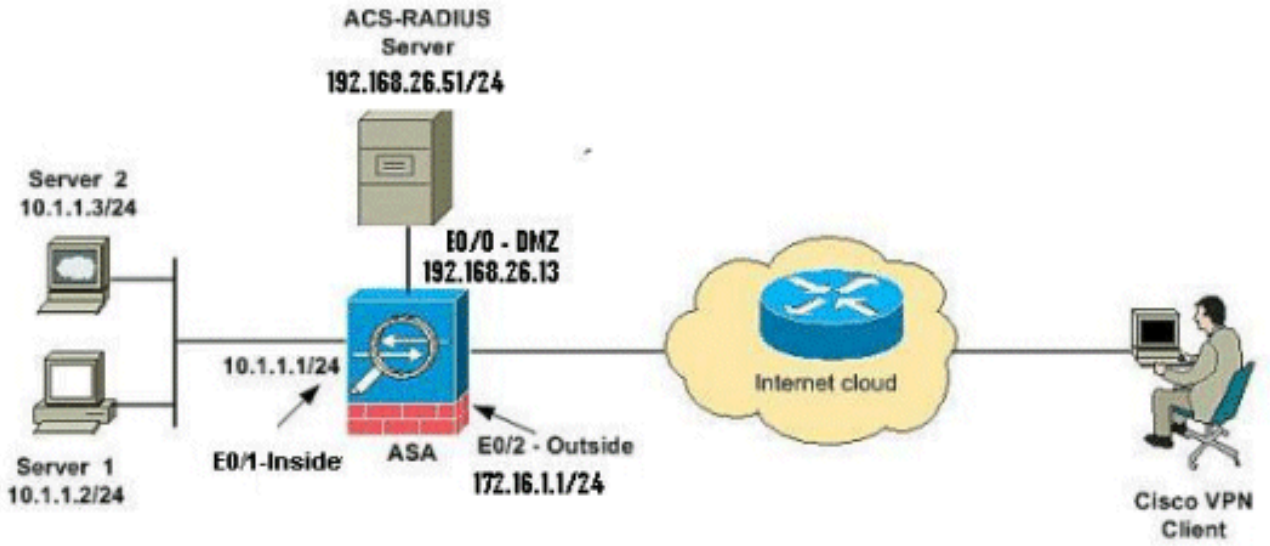
```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3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

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



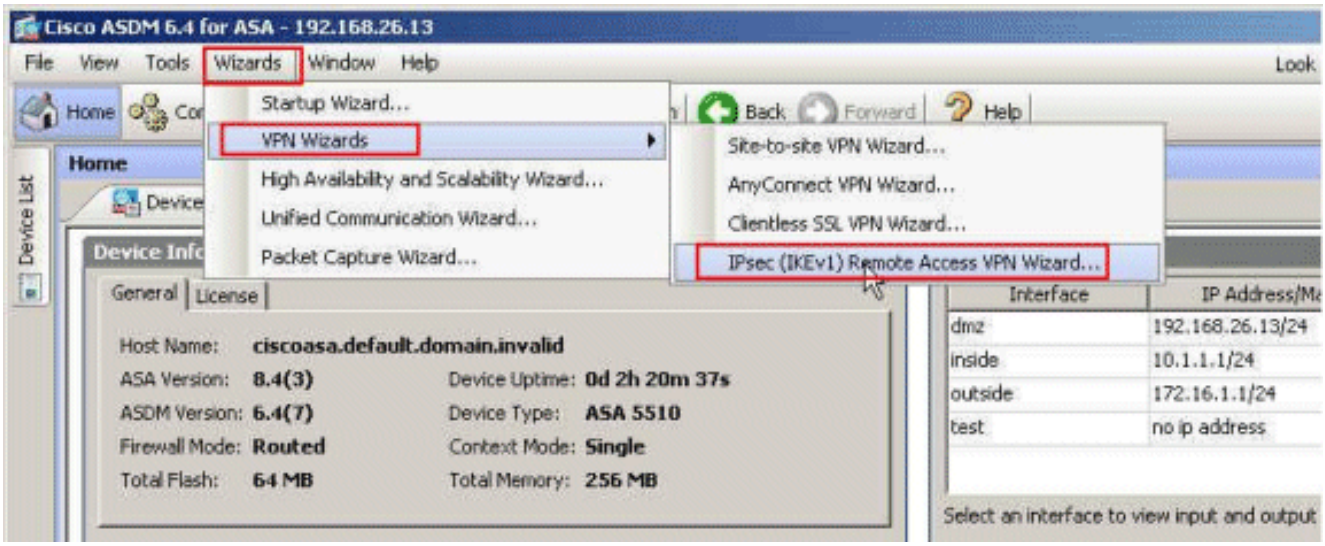
Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configura VPN di accesso remoto (IPsec)

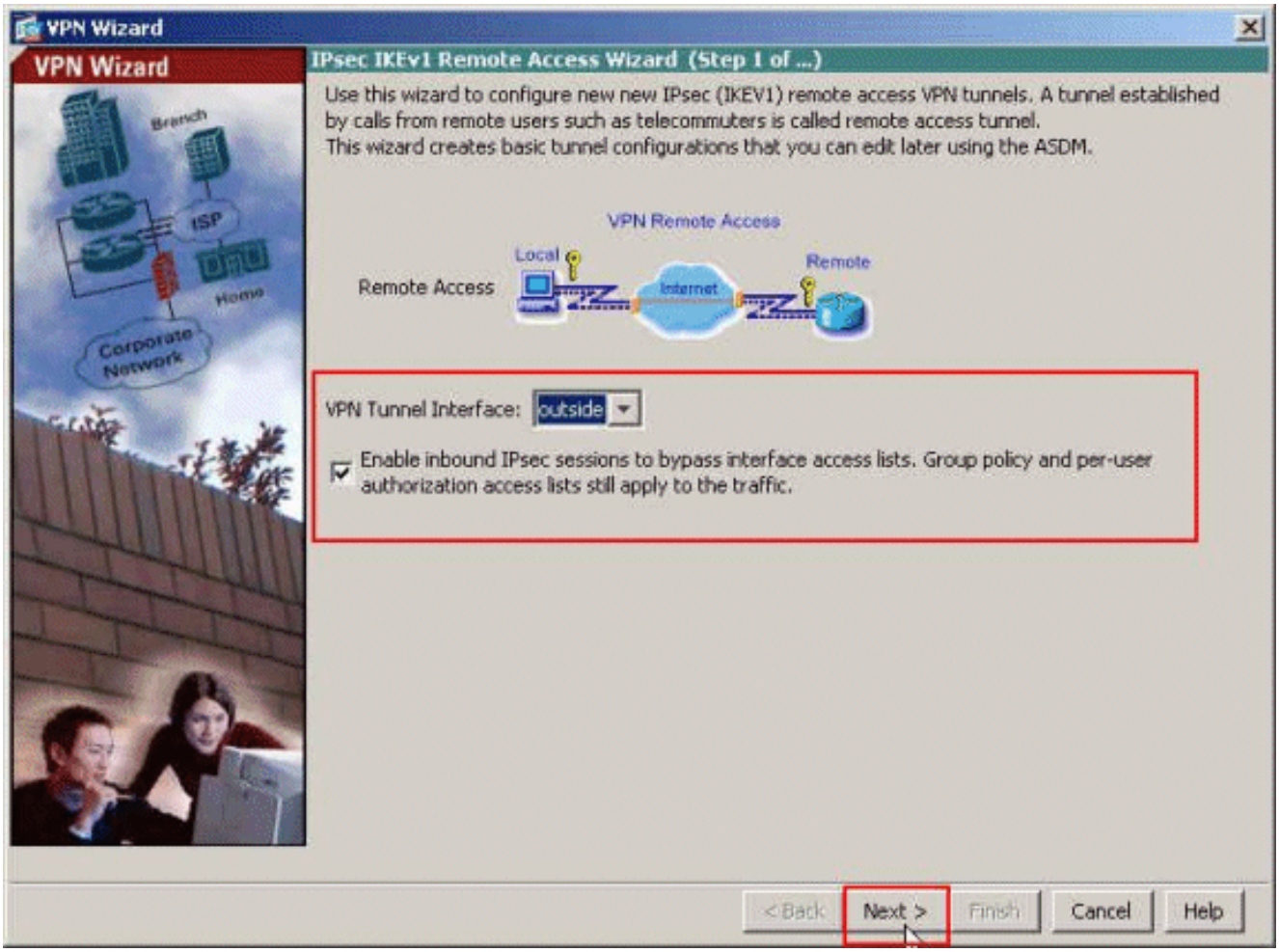
Procedura ASDM

Per configurare la VPN di accesso remoto, completare i seguenti passaggi:

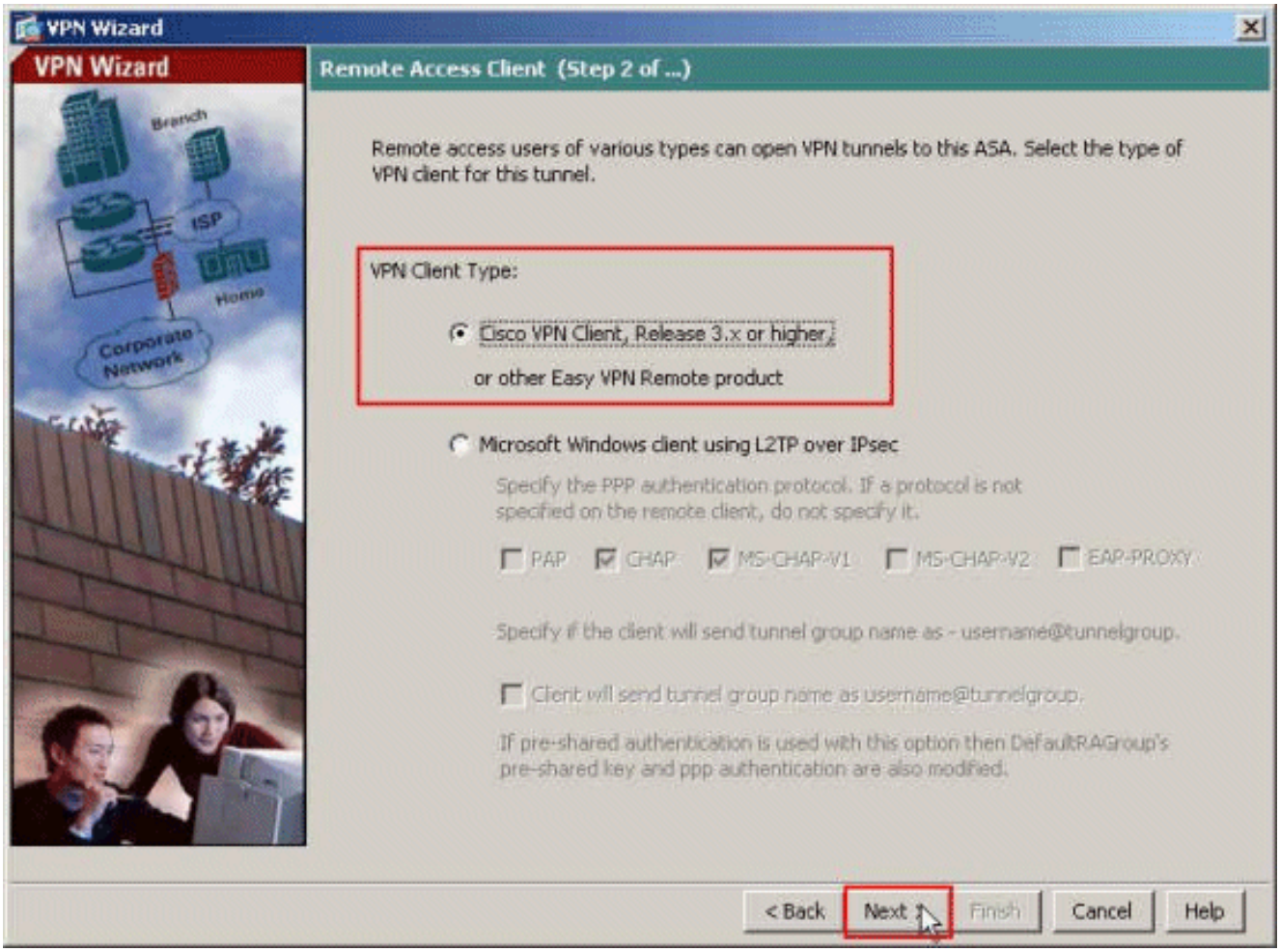
1. Selezionare **Procedure guidate > Procedure guidate VPN > Procedura guidata VPN ad accesso remoto IPsec(IKEv1)** dalla finestra Home.



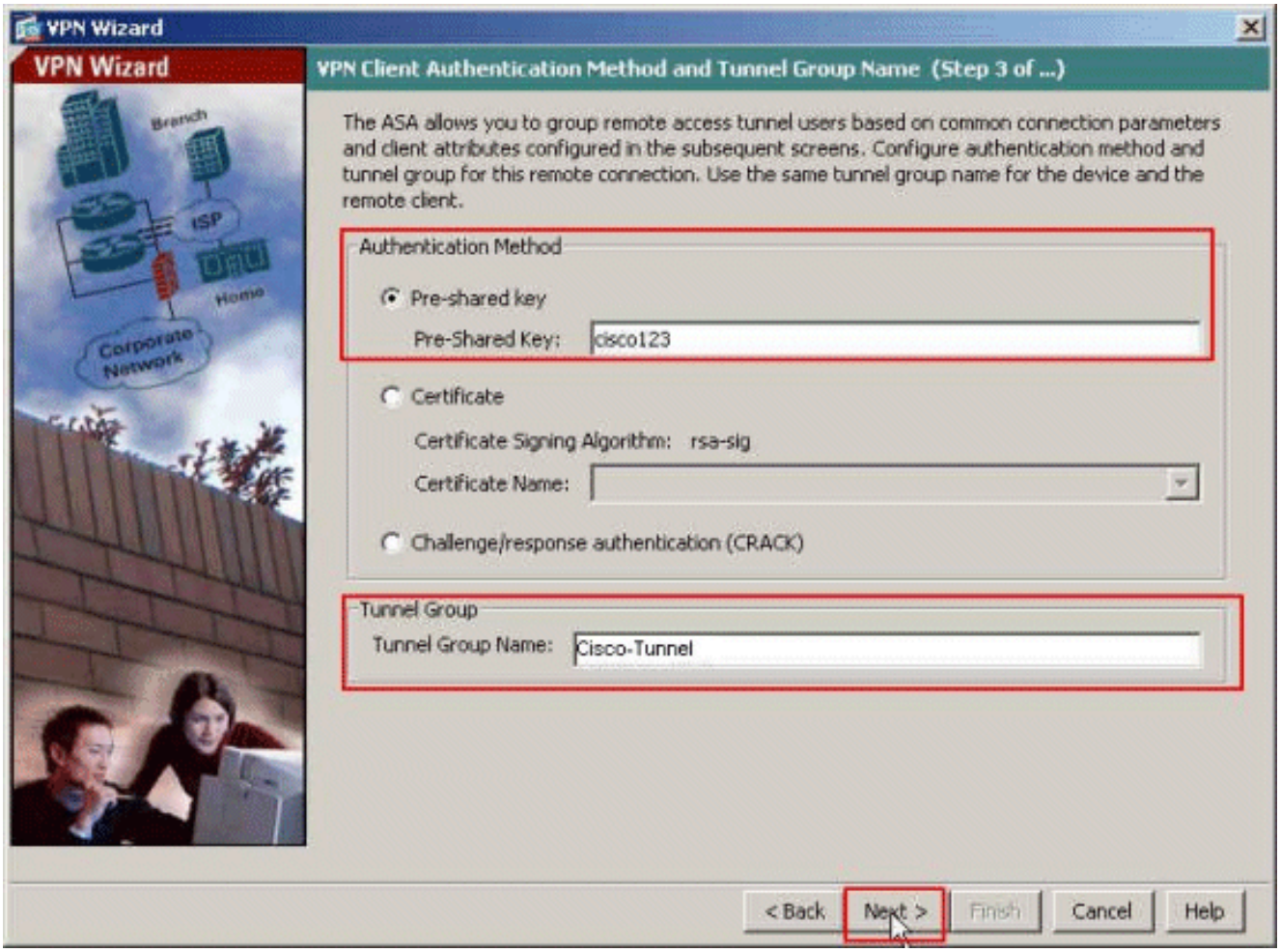
2. Selezionare **VPN Tunnel Interface** come richiesto (**Outside**, in questo esempio) e verificare anche che la casella di controllo accanto a **Abilita sessioni IPsec in entrata per ignorare gli elenchi degli accessi all'interfaccia** sia selezionata.



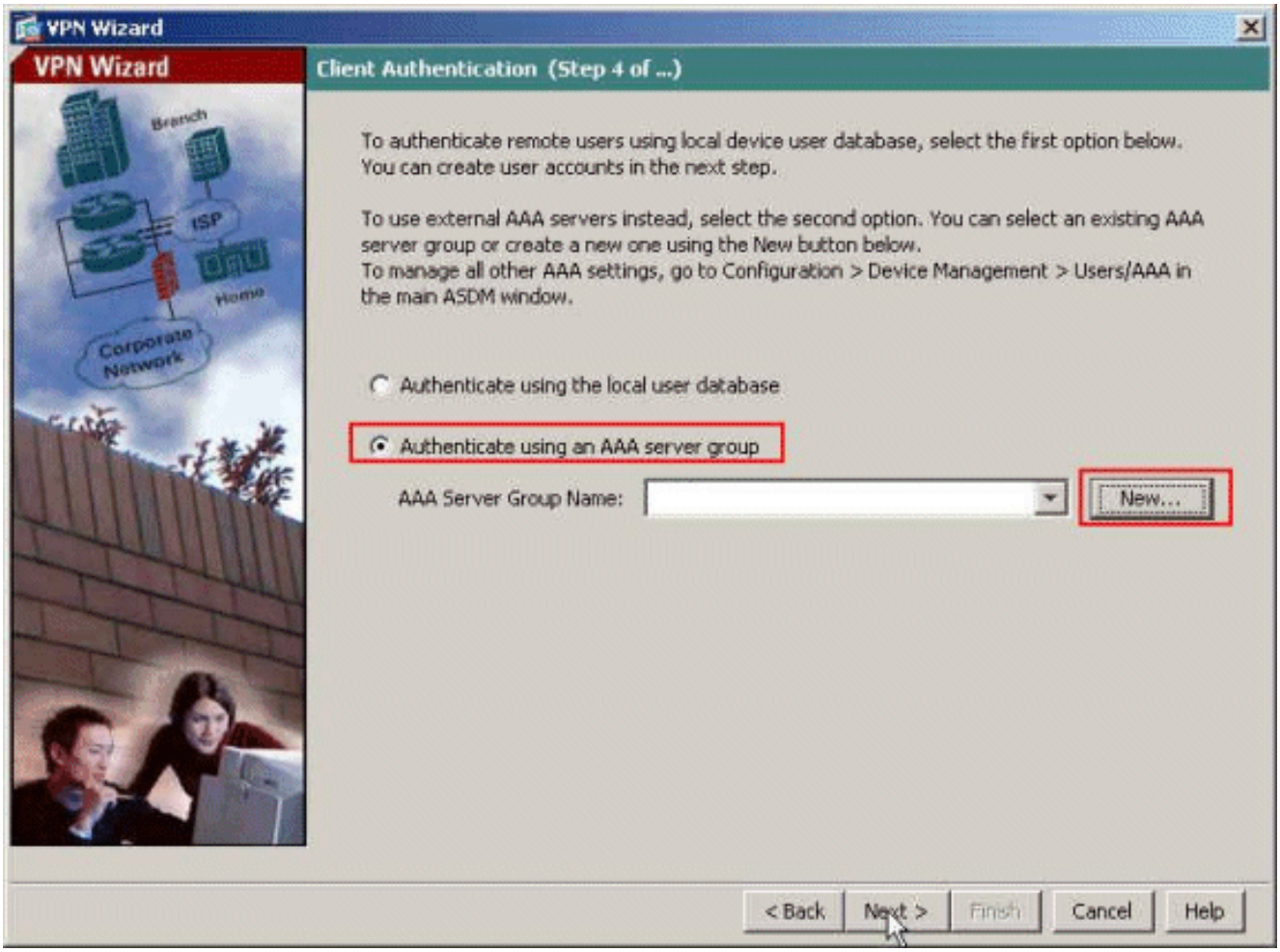
3. Scegliere il tipo di client VPN come **Cisco VPN Client, versione 3.x o successive**. Fare clic su **Next**
(Avanti).



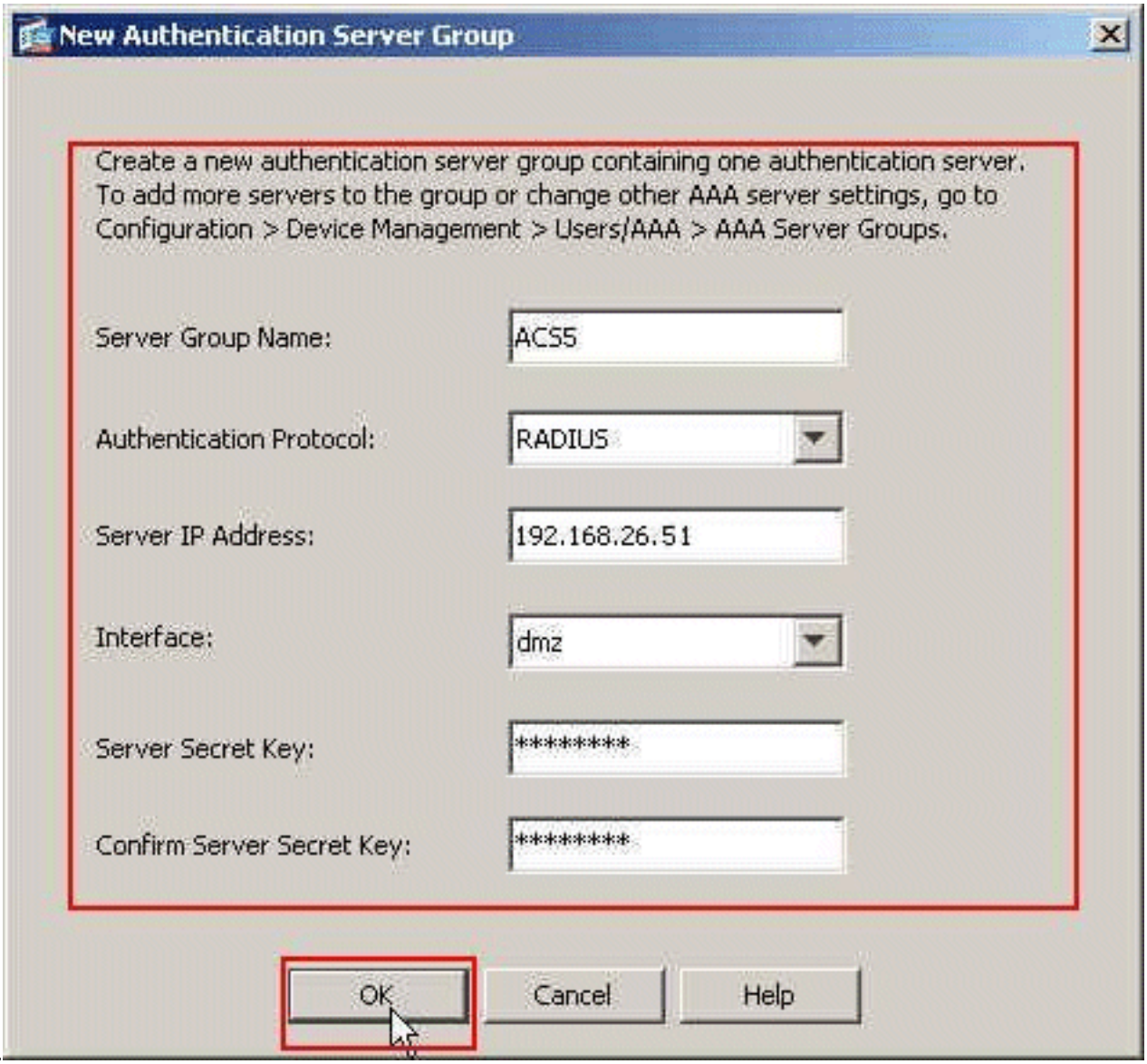
4. Scegliere il **Metodo di autenticazione** e fornire le informazioni di autenticazione. Il metodo di autenticazione utilizzato è la **chiave già condivisa**. Inoltre, fornire un nome di **gruppo di tunnel** nello spazio fornito. La **chiave precondivisa** utilizzata è **cisco123**, il nome del gruppo di tunnel è **Cisco-Tunnel**. Fare clic su **Next**
(Avanti).



5. Specificare se si desidera che gli utenti remoti vengano autenticati nel database degli utenti locale o in un gruppo di server AAA esterno. In questo caso, si sceglie **Autentica utilizzando un gruppo di server AAA**. Per creare un nuovo nome di gruppo di server AAA, fare clic su **New** (Nuovo) accanto al campo AAA Server Group Name (Nome gruppo server AAA).

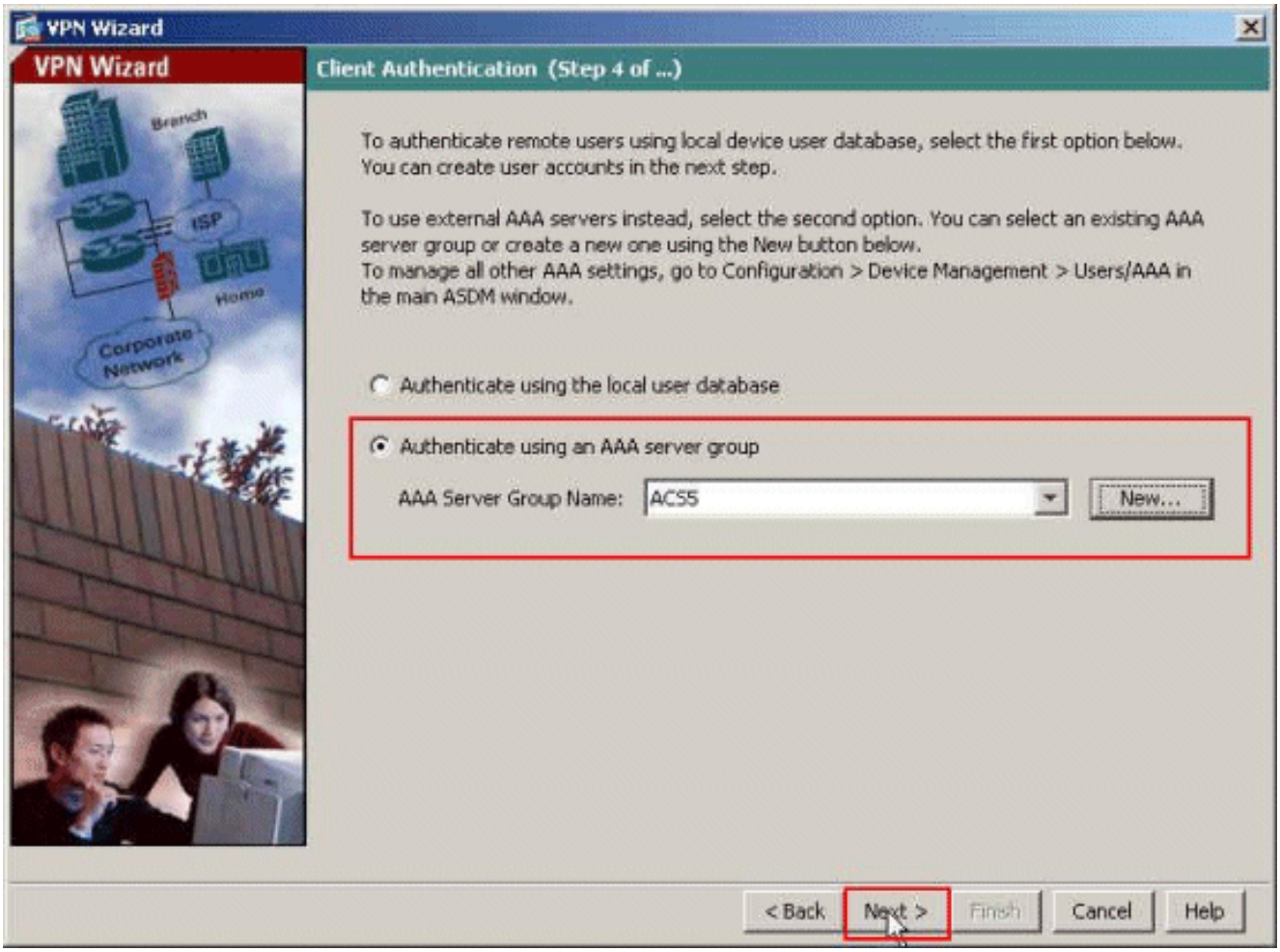


6. Specificare il nome del gruppo di server, il protocollo di autenticazione, l'indirizzo IP del server, il nome dell'interfaccia e la chiave privata del server negli spazi corrispondenti e fare clic su

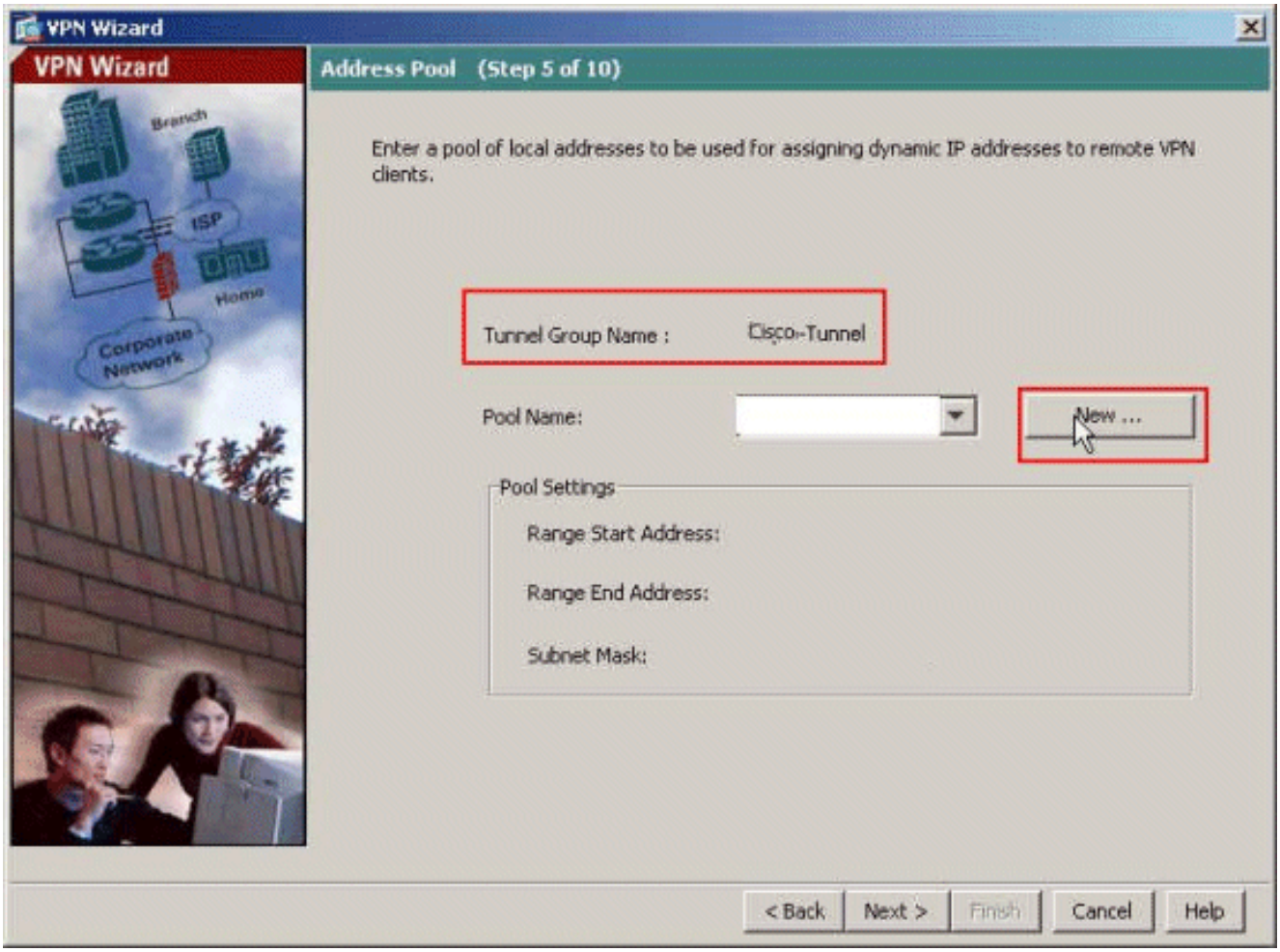


OK.

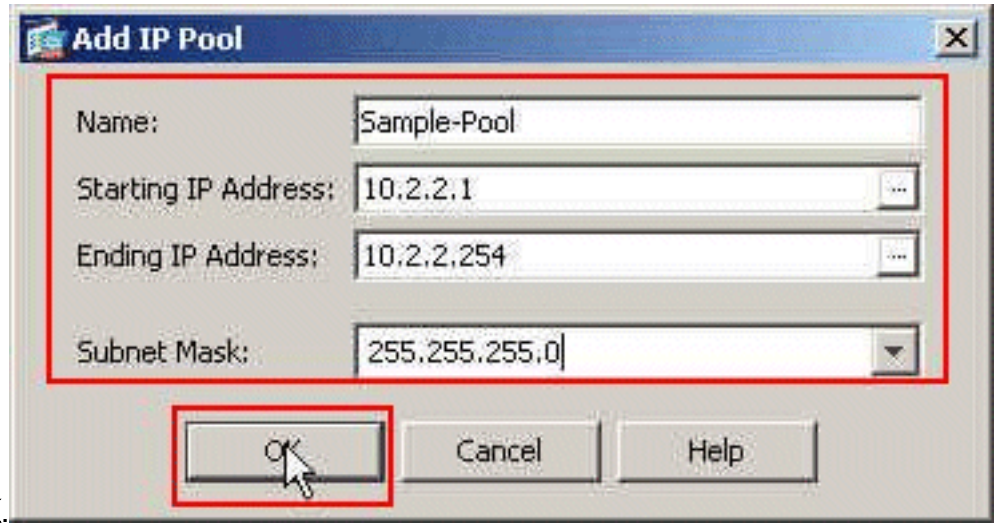
7. Fare clic su **Next** (Avanti).



8. Definire un pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti quando si connettono. Per creare un nuovo pool di indirizzi locali, fare clic su **New** (Nuovo).

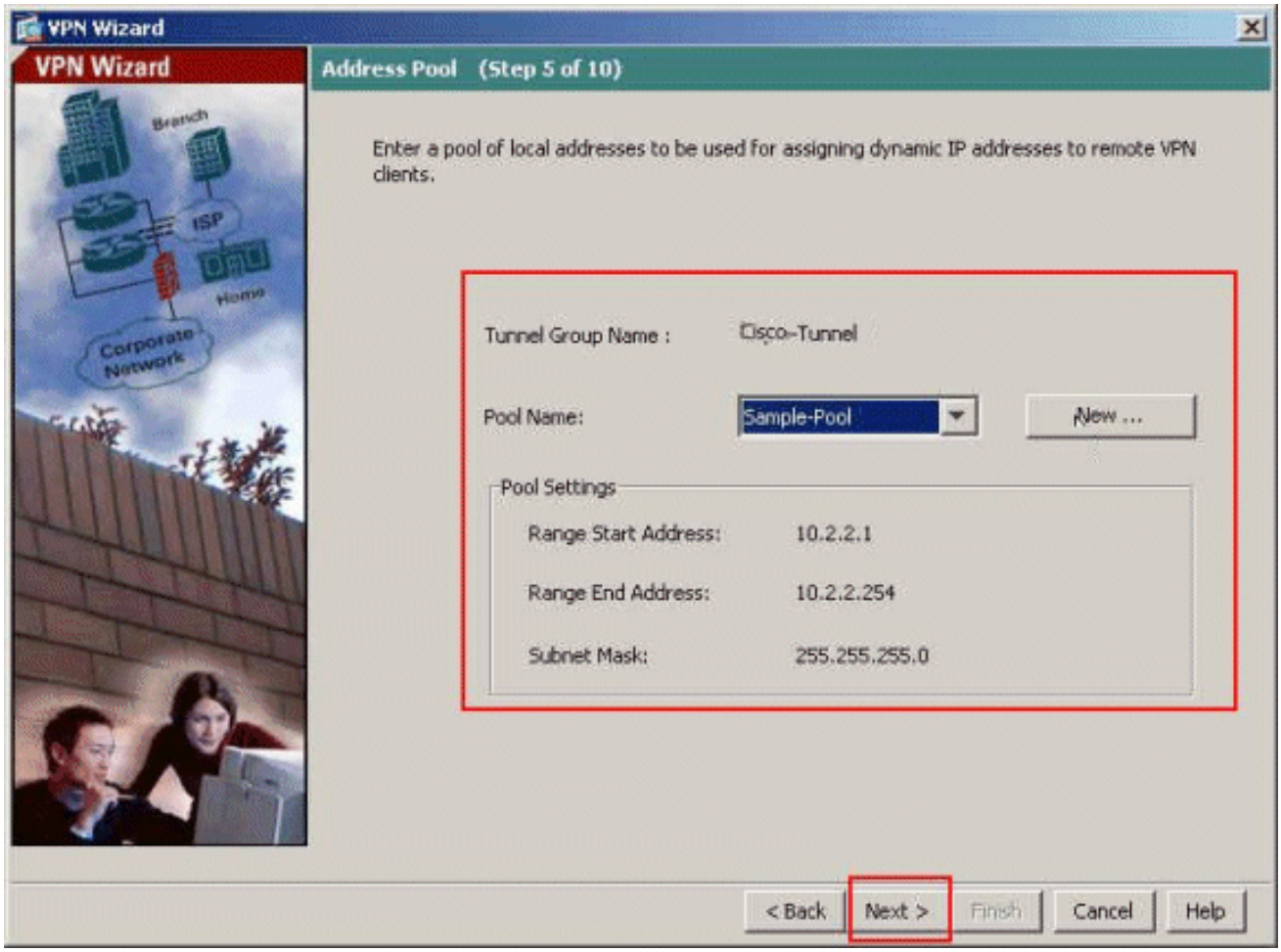


9. Nella finestra Aggiungi pool IP, fornire il nome del pool, l'indirizzo IP iniziale, l'indirizzo IP finale e la subnet mask. Fare clic su

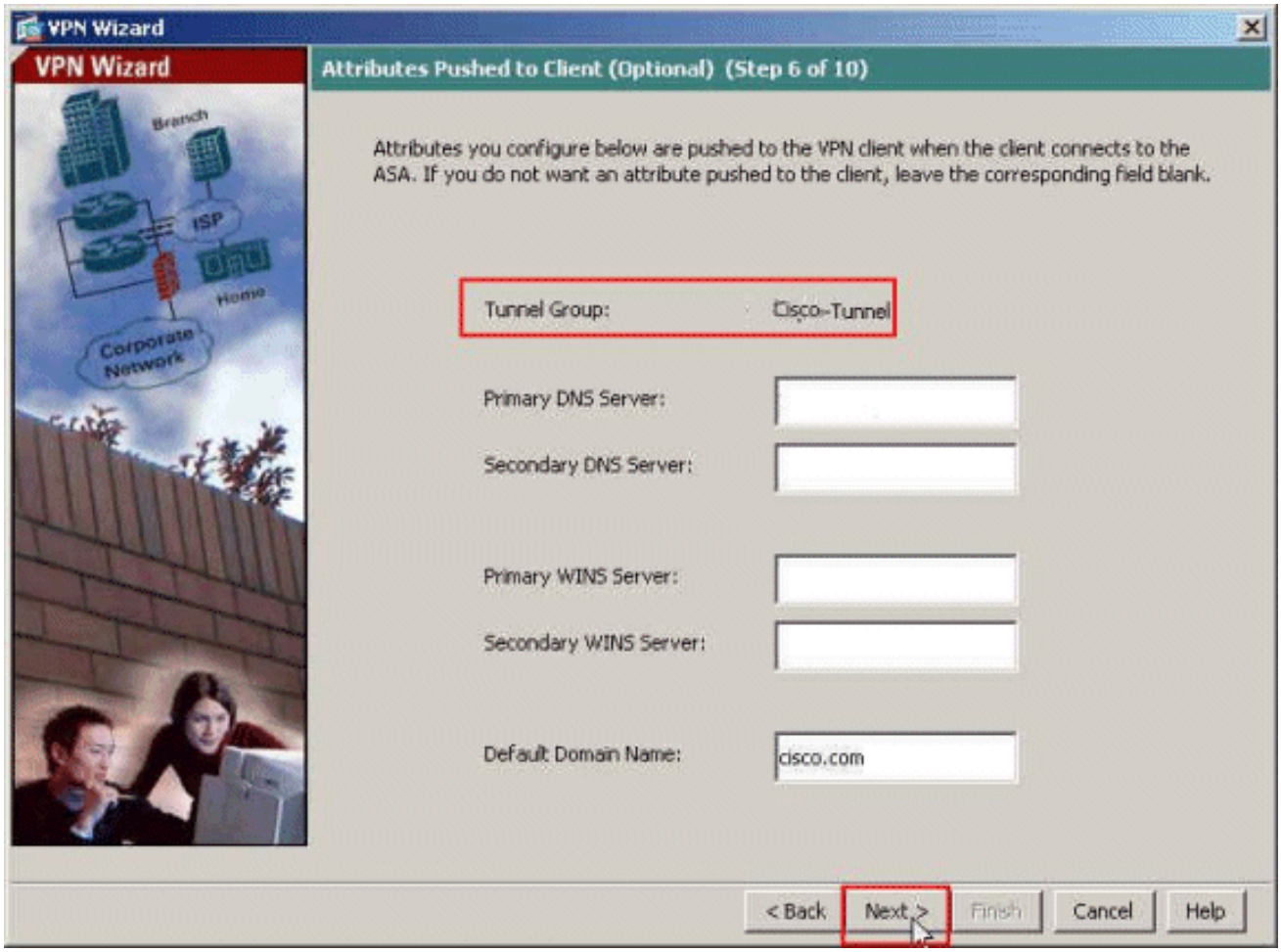


OK.

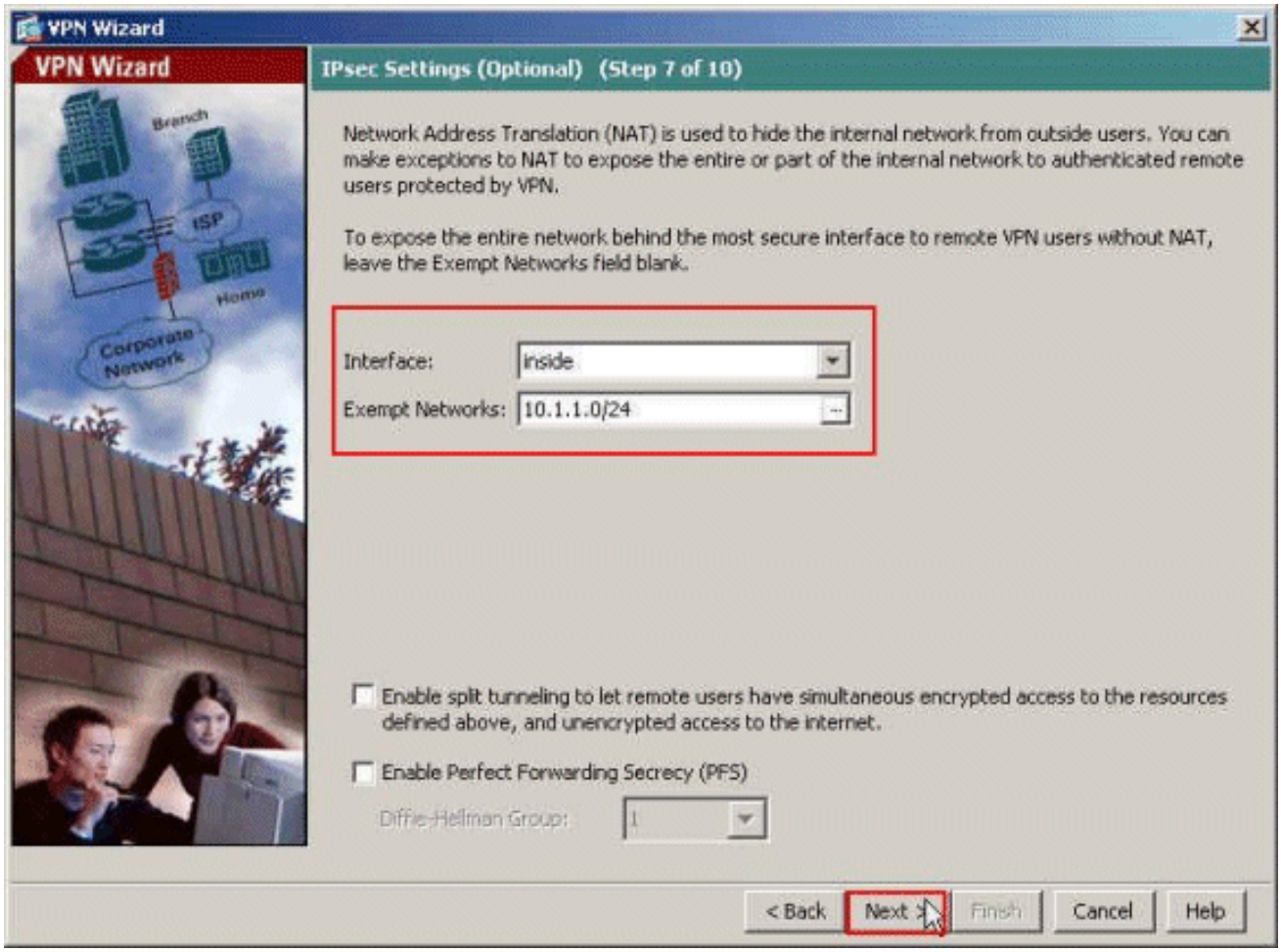
10. Selezionare il nome del pool dall'elenco a discesa e fare clic su **Avanti**. Il nome del pool per questo esempio è **Sample-Pool**, creato nel passaggio 9.



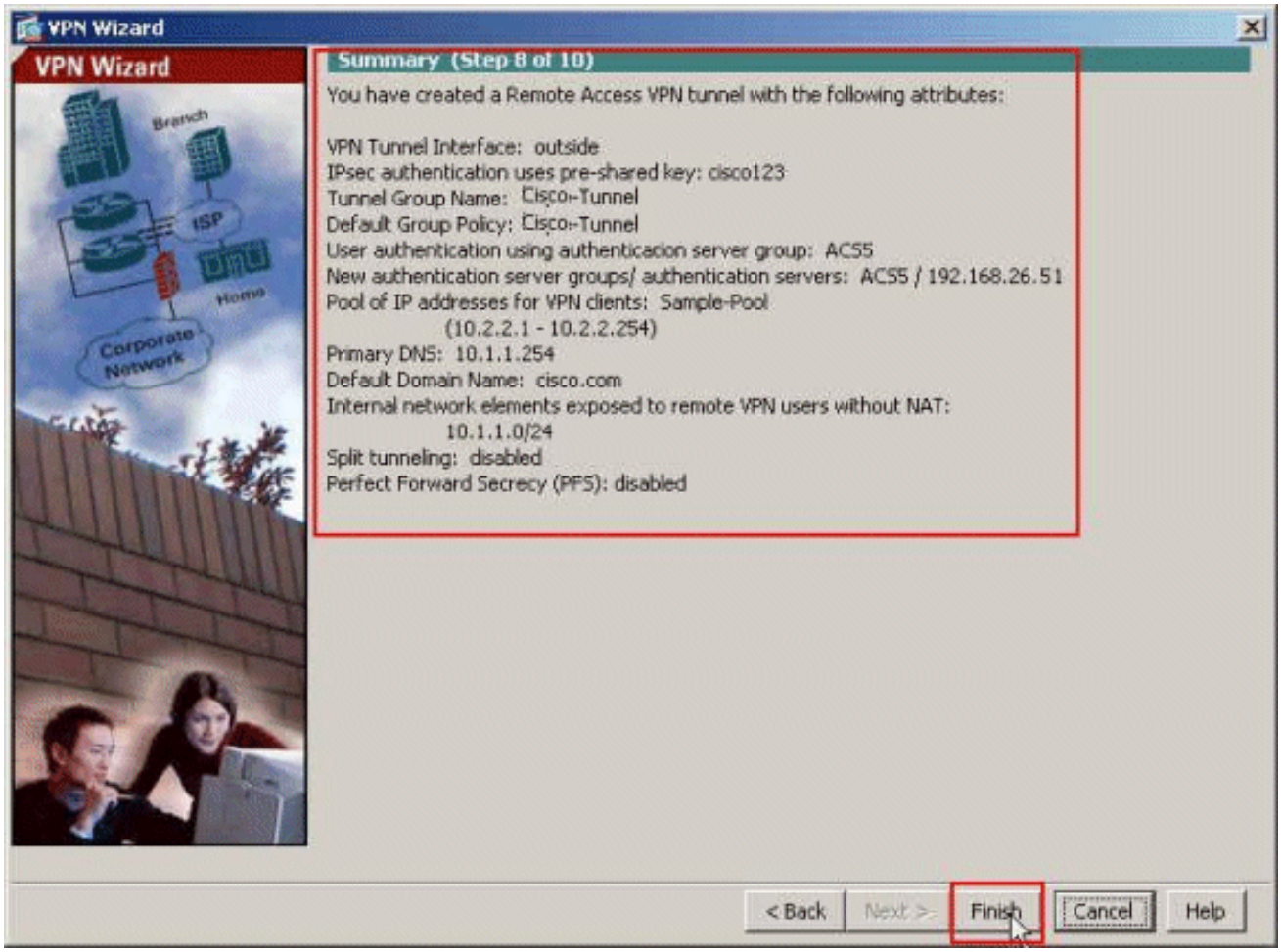
11. *Facoltativo:* Specificare le informazioni sui server DNS e WINS e un nome di dominio predefinito da inserire nei client VPN
remoti.



12. Specificare gli eventuali host interni o reti da esporre agli utenti VPN remoti. Fare clic su **Avanti** dopo aver fornito il nome dell'interfaccia e le reti a cui applicare l'esenzione nel campo Reti esenti.Se si lascia vuoto questo elenco, gli utenti VPN remoti possono accedere all'intera rete interna dell'appliance ASA.In questa finestra è anche possibile abilitare il tunneling suddiviso. Il tunneling ripartito cripta il traffico diretto alle risorse definite in precedenza in questa procedura e fornisce l'accesso non crittografato a Internet in senso lato evitando il tunneling del traffico. Se il tunneling suddiviso *non* è abilitato, tutto il traffico proveniente dagli utenti VPN remoti viene tunneling verso l'appliance ASA. In base alla configurazione, questa operazione può richiedere un uso intensivo della larghezza di banda e del
processore.



13. Questa finestra mostra un riepilogo delle azioni intraprese. Se la configurazione è soddisfacente, fare clic su **Fine**.



Configurazione dell'ASA con CLI

Questa è la configurazione CLI:

Esecuzione della configurazione sul dispositivo 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#
```

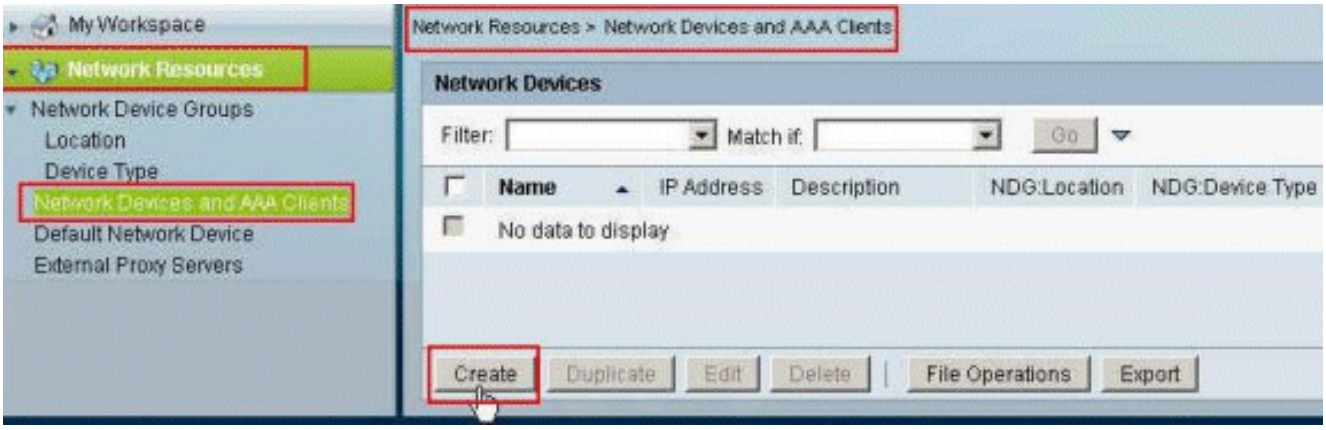
Configurazione di ACS per ACL scaricabili per un singolo utente

Èpossibile configurare elenchi degli accessi scaricabili in Cisco Secure ACS 5.x come oggetti con autorizzazioni denominate e quindi assegnarli a un profilo di autorizzazione che verrà scelto nella sezione dei risultati della regola in Access-Service.

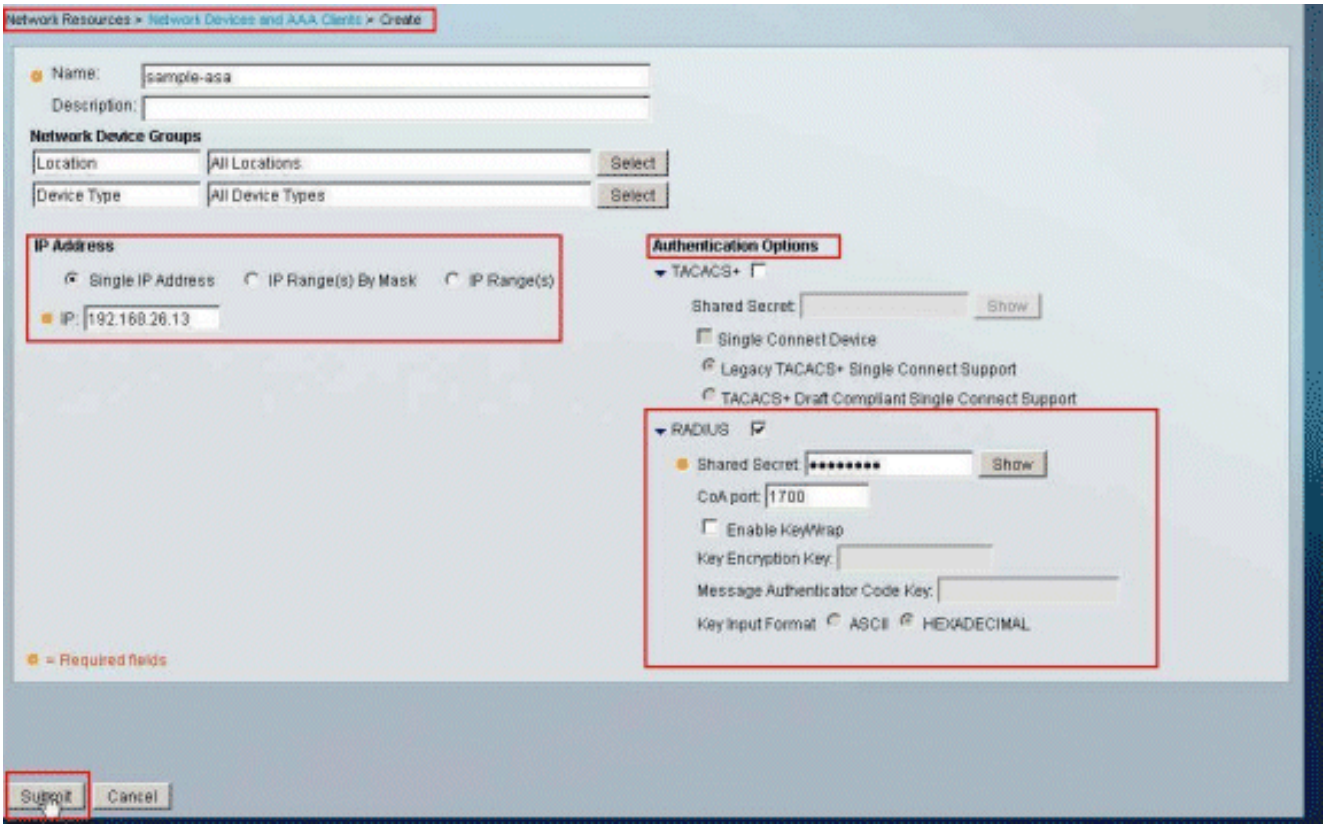
Nell'esempio, l'utente VPN IPsec **cisco** viene autenticato correttamente e il server RADIUS invia un elenco degli accessi scaricabili all'appliance di sicurezza. L'utente "cisco" può accedere solo al server 10.1.1.2 e nega tutti gli altri tipi di accesso. Per verificare l'ACL, consultare la sezione ACL scaricabili per utente/gruppo.

Completare questa procedura per configurare il client RADIUS in un Cisco Secure ACS 5.x:

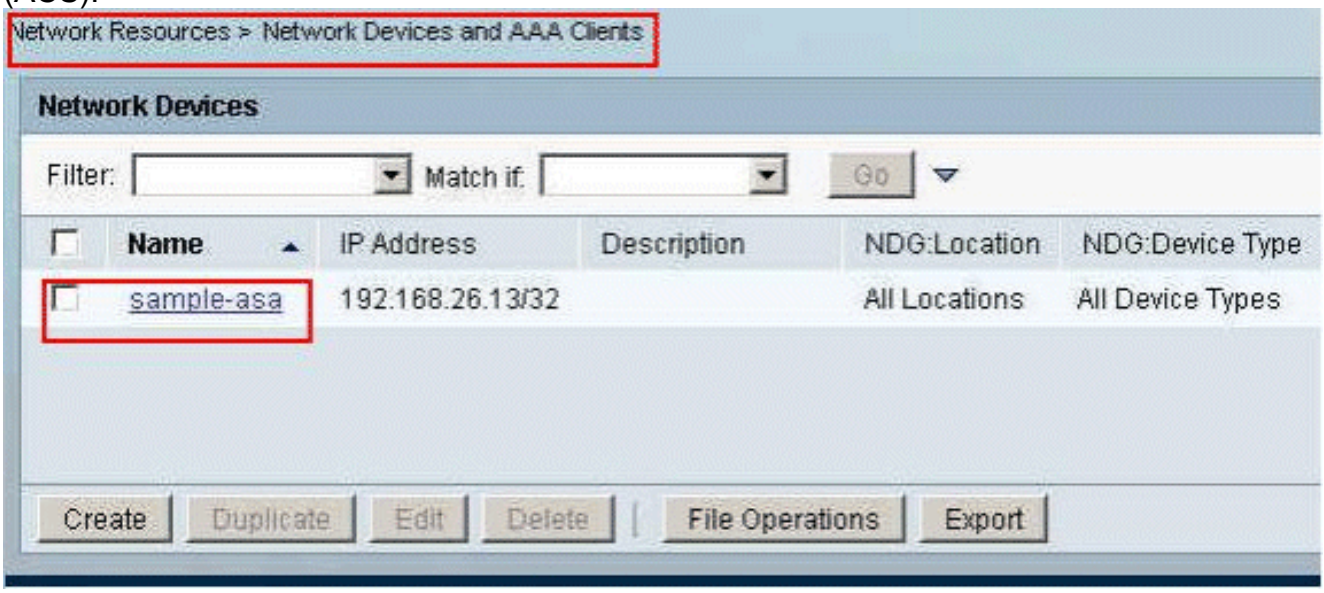
1. Scegliere **Risorse di rete > Dispositivi di rete e client AAA**, quindi fare clic su **Crea** per aggiungere una voce per l'appliance ASA nel database del server RADIUS.



2. Immettere un nome localmente significativo per l'ASA (**sample-asa**, in questo esempio), quindi immettere **192.168.26.13** nel campo dell'indirizzo IP. Selezionare la casella di controllo **RADIUS** nella sezione Authentication Options (Opzioni di autenticazione) e immettere **cisco123** come campo Shared Secret. Fare clic su **Invia**.

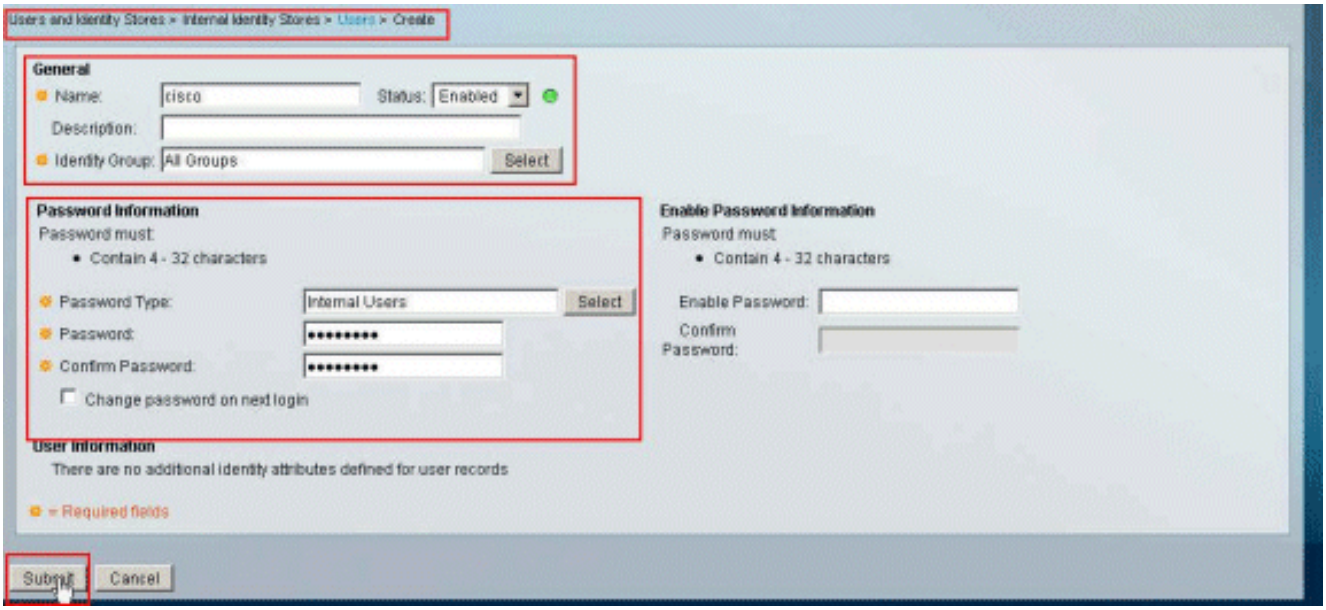


3. L'appliance ASA viene aggiunta correttamente al database del server RADIUS (ACS).

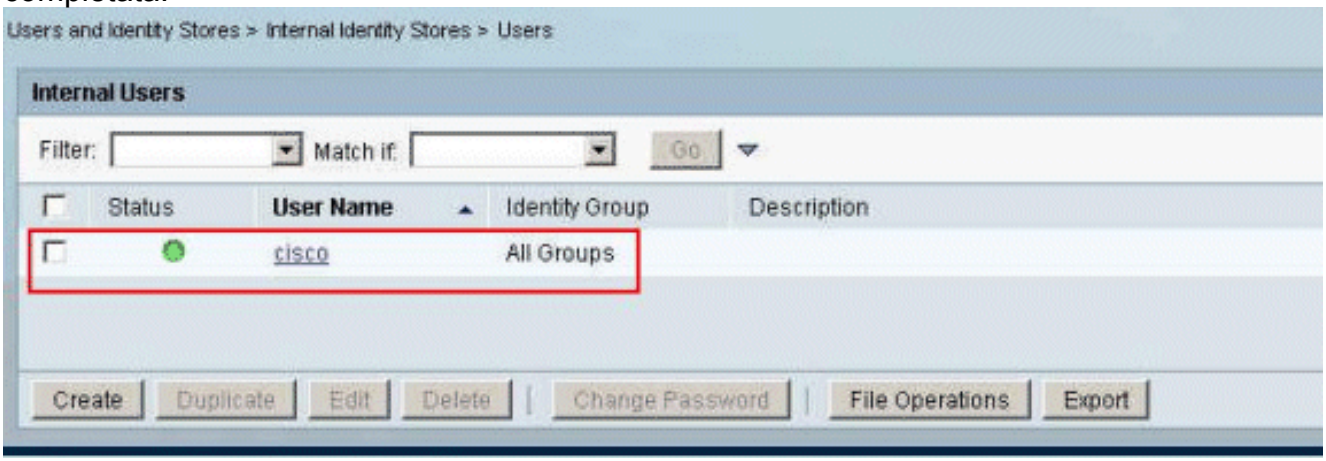


4. Scegliere **Utenti e archivi identità > Archivi identità interni > Utenti**, quindi fare clic su **Crea** per creare un utente nel database locale del server ACS per l'autenticazione VPN.

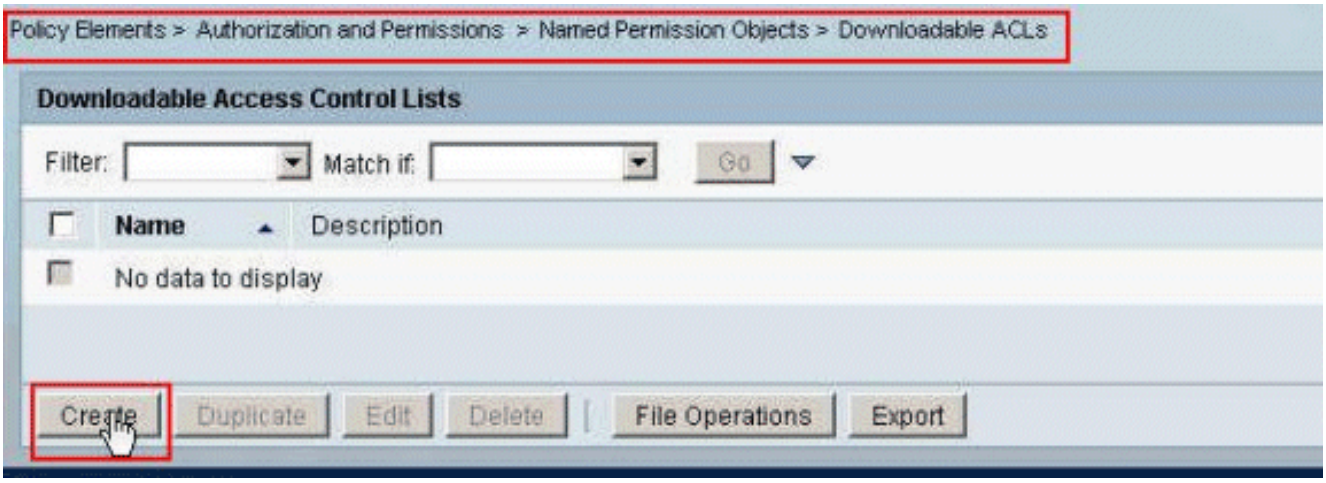
5. Immettere il nome utente **cisco**. Selezionare il tipo di password **Internal Users** (Utenti interni), quindi immettere la password (**cisco123**, in questo esempio). Confermare la password e fare clic su
Invia.



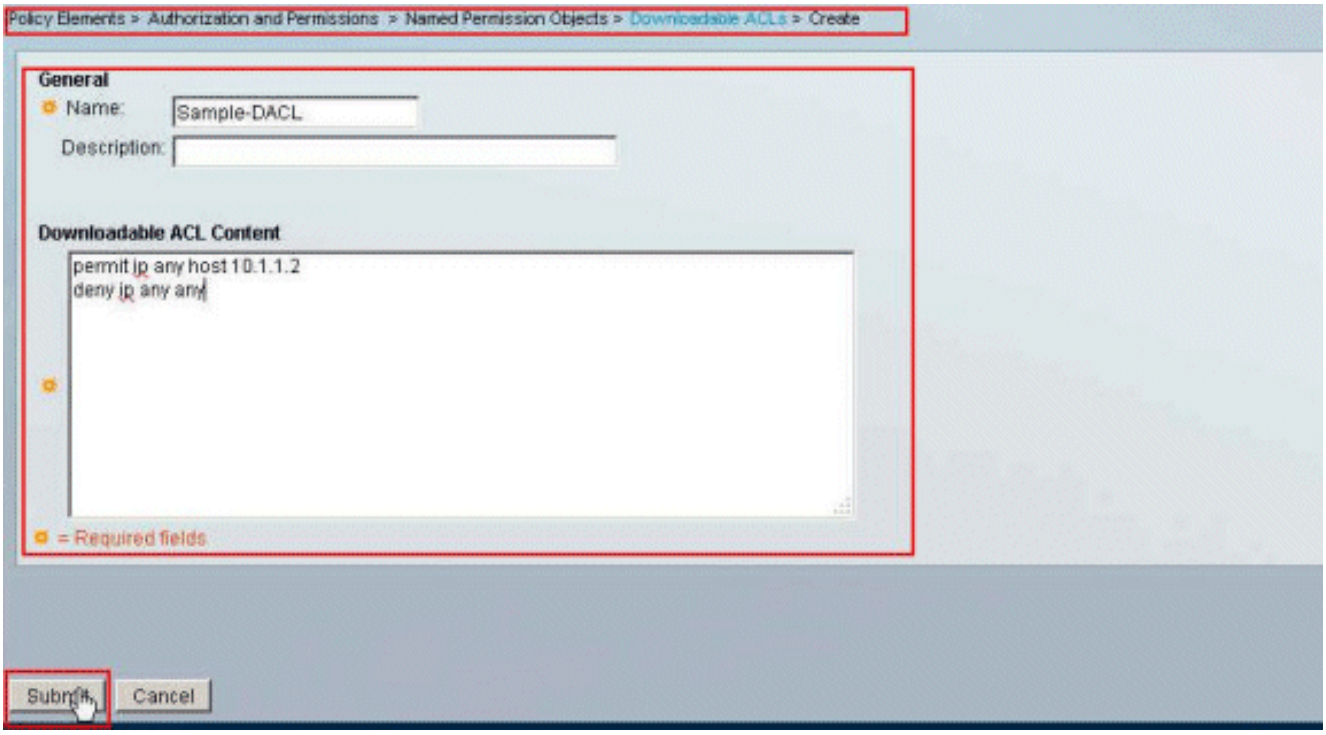
6. Creazione dell'utente **cisco**
completata.



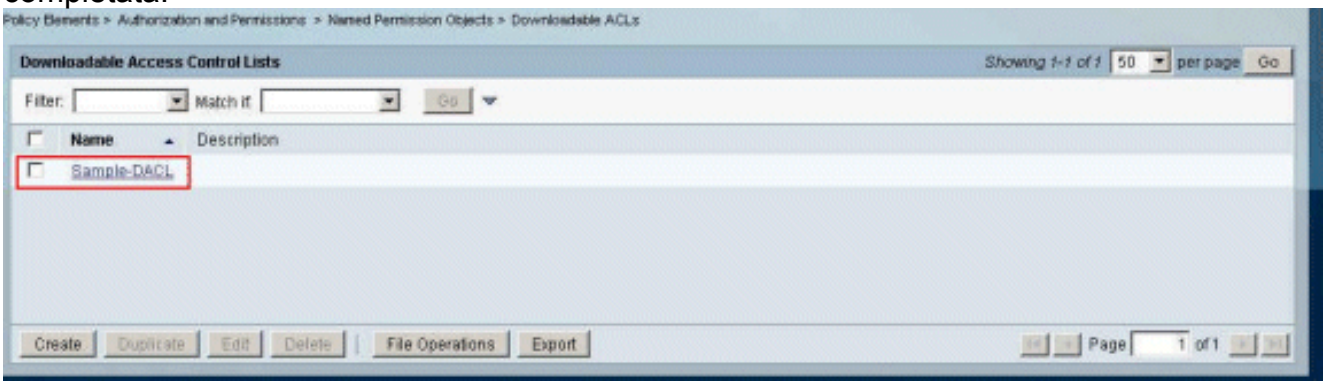
7. Per creare un ACL scaricabile, scegliere Elementi dei criteri **> Autorizzazioni e autorizzazioni > Oggetti autorizzazioni con nome > ACL scaricabili**, quindi fare clic su
Crea.



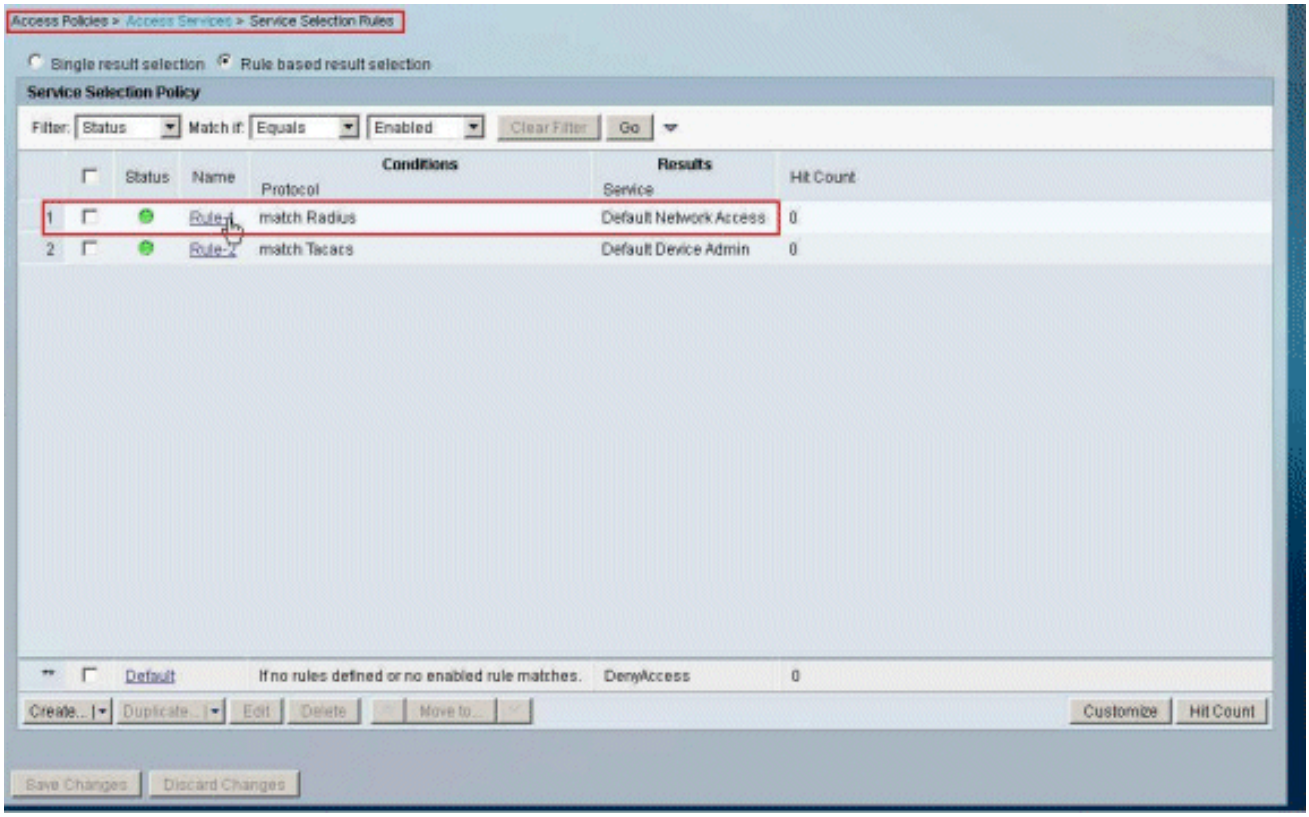
8. Specificare il **nome** dell'ACL scaricabile e il **contenuto** dell'**ACL**. Fare clic su
Invia.



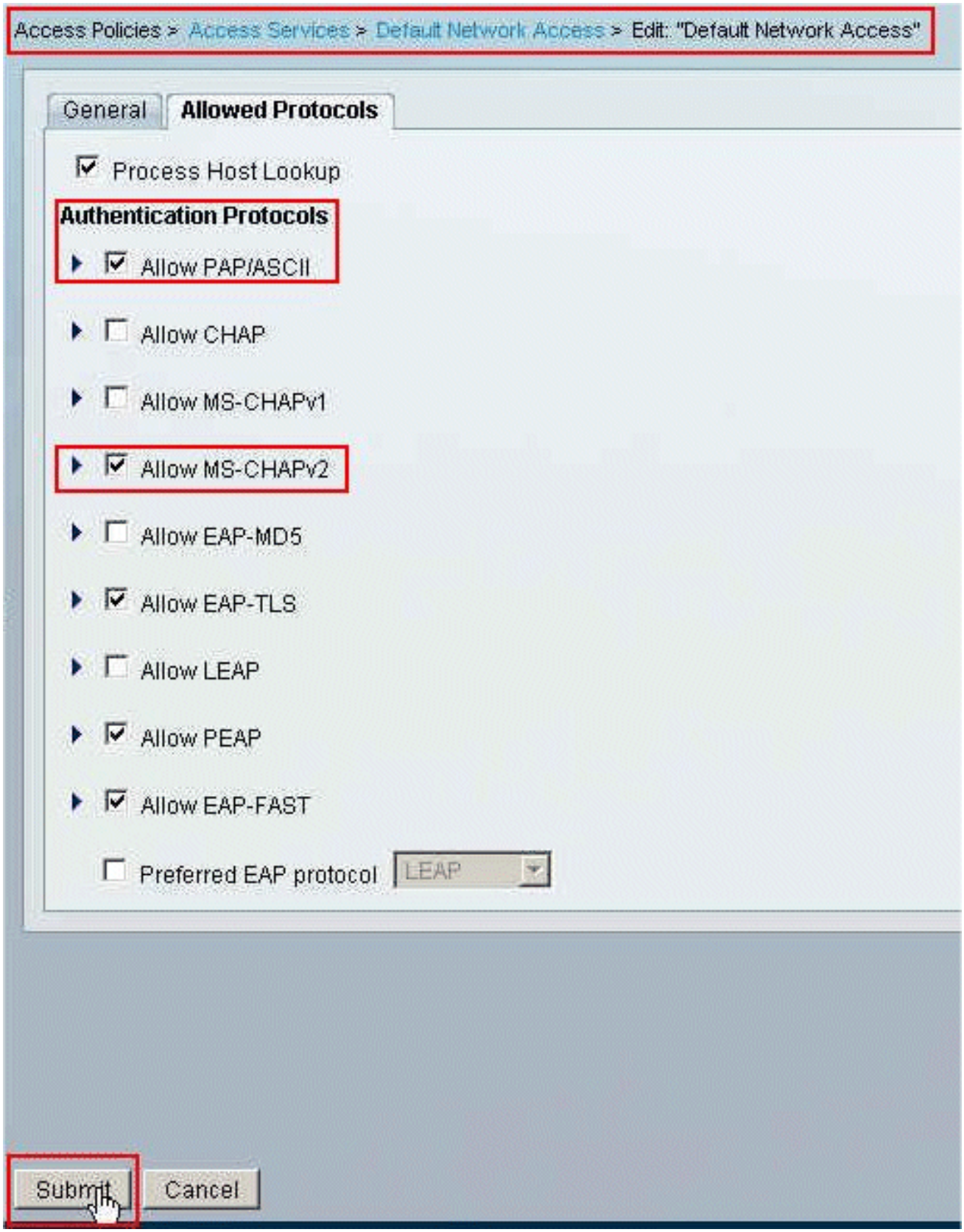
9. Creazione dell'ACL scaricabile **Sample-DACL** completata.



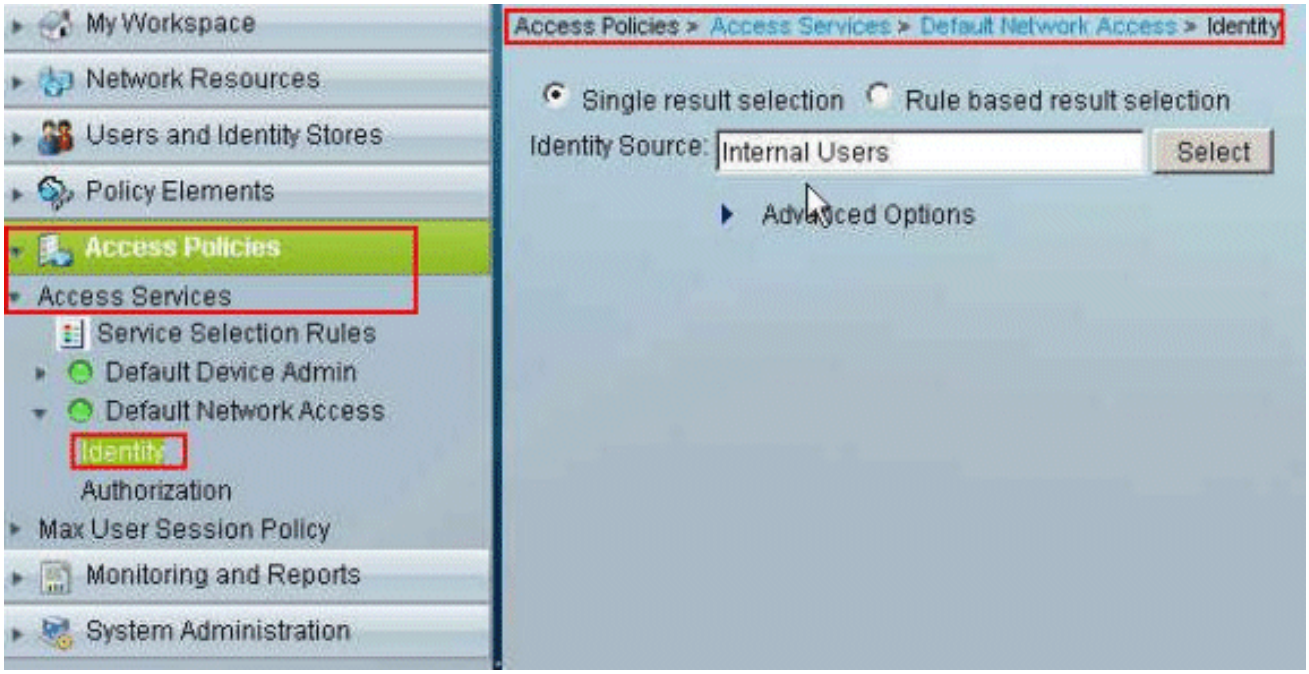
10. Per configurare i criteri di accesso per l'autenticazione VPN, scegliere **Criteri di accesso > Servizi di accesso > Regole di selezione dei servizi** e determinare il servizio che gestisce il protocollo RADIUS. Nell'esempio, la **regola 1** corrisponde a **RADIUS** e Accesso alla rete predefinito soddisferà la richiesta RADIUS.



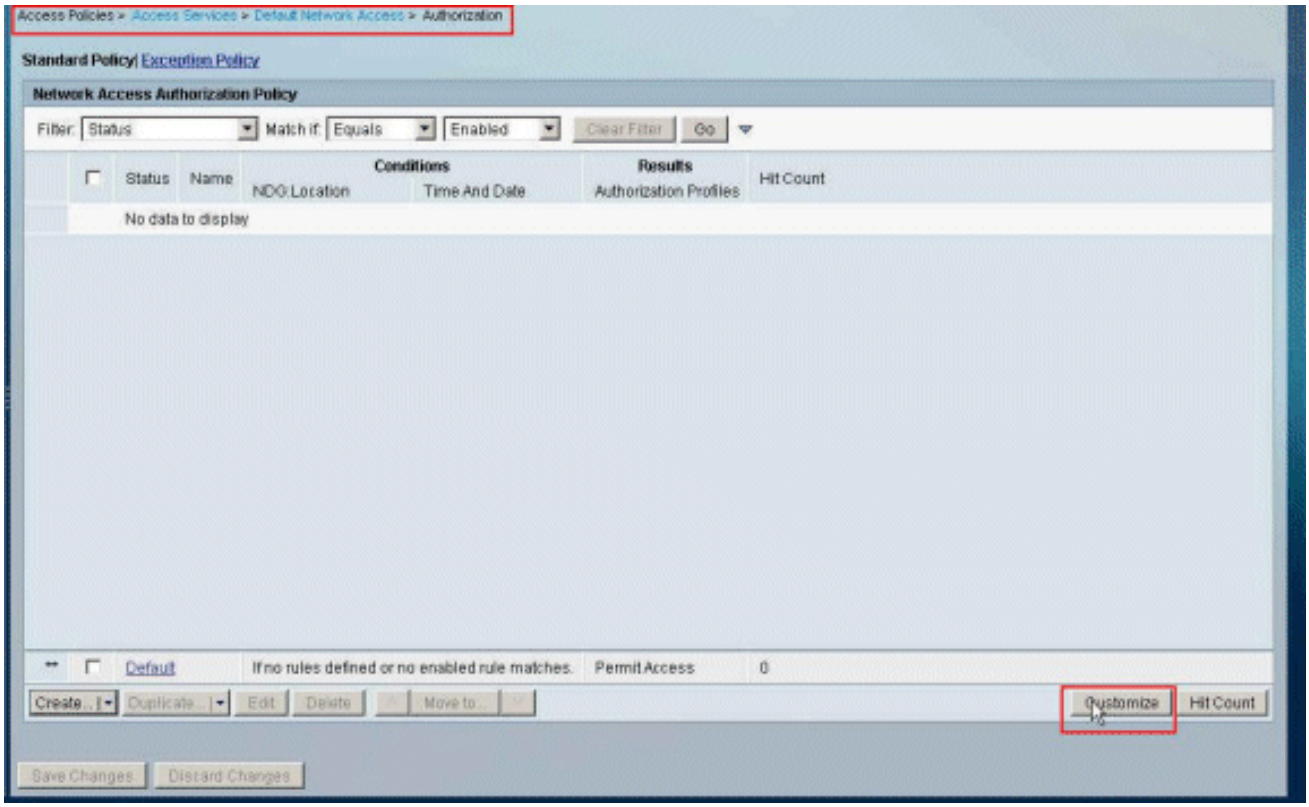
11. Scegliere il **servizio Access** determinato dal passo 10. In questo esempio viene utilizzato **Accesso di rete predefinito**. Scegliere la scheda **Protocolli consentiti** e verificare che **Consenti PAP/ASCII** e **Consenti MS-CHAPv2** siano selezionati. Fare clic su **Invia**.



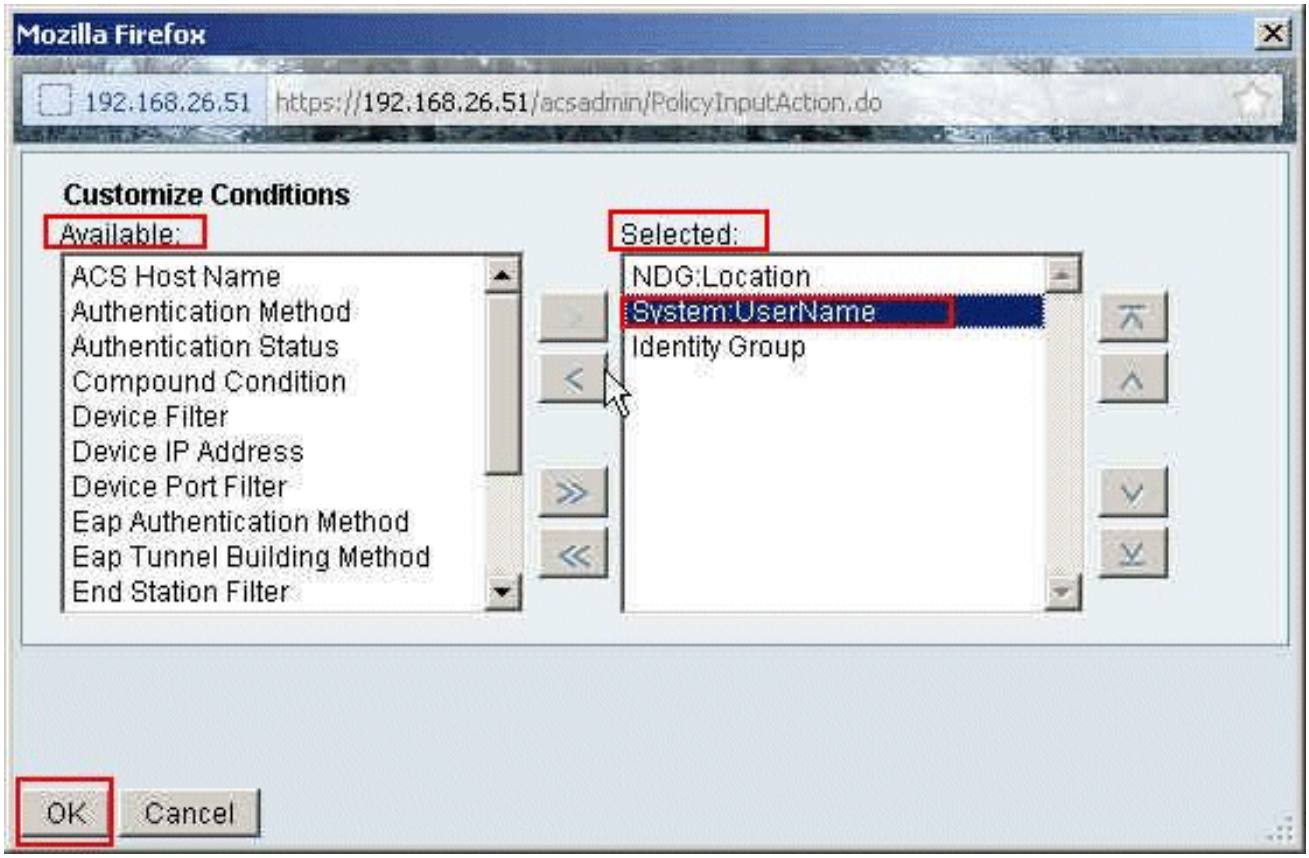
12. Fare clic sulla **sezione Identità** di **Access Services** e verificare che **Internal Users** sia selezionato come Origine identità. Nell'esempio, è stato utilizzato l'accesso alla rete predefinito.



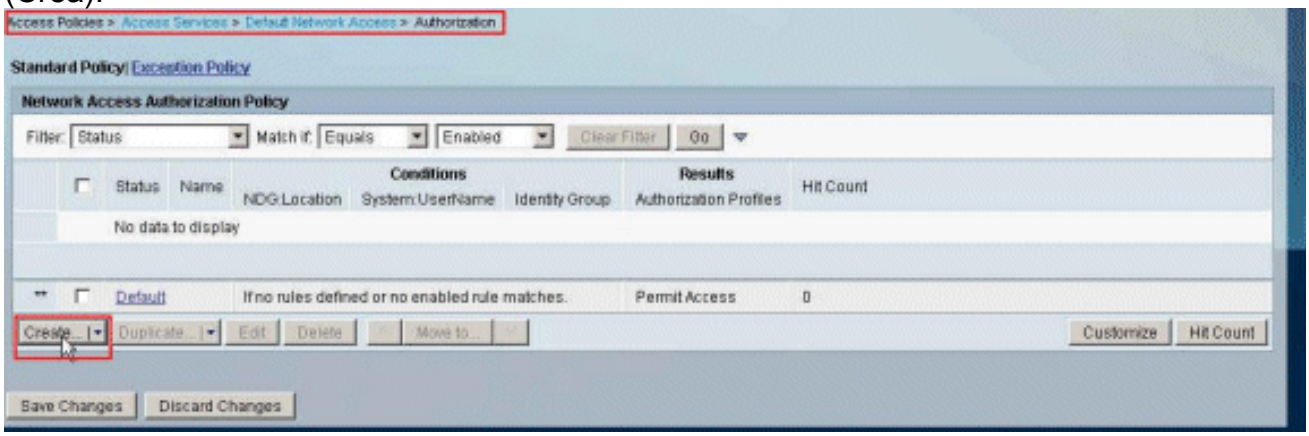
13. Scegliere Criteri di accesso > **Servizi di accesso** > **Accesso di rete predefinito** > **Autorizzazione**, quindi fare clic su **Personalizza**.



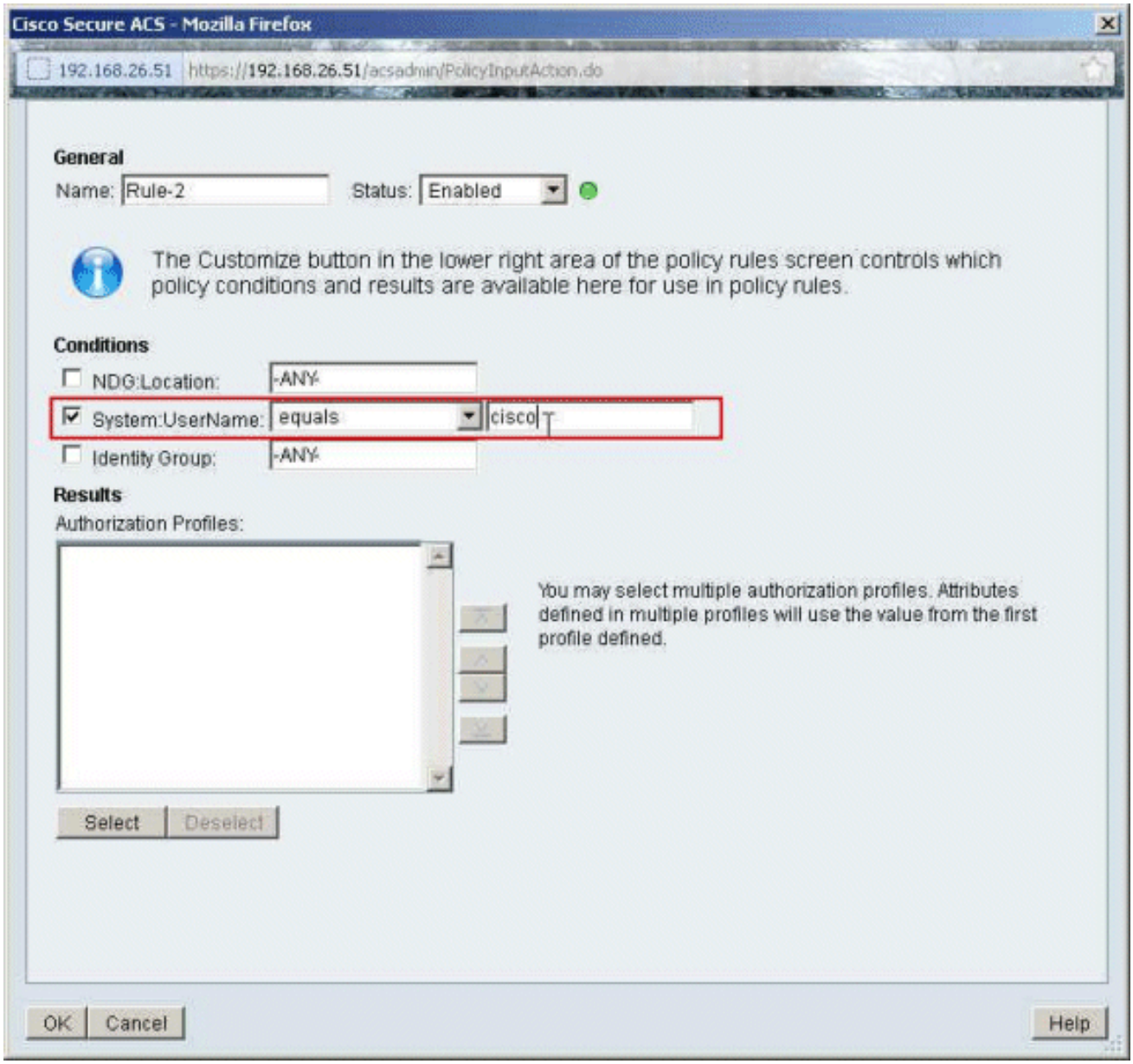
14. Spostare **System:UserName** dalla colonna **Available** alla colonna **Selected** e fare clic su **OK**.



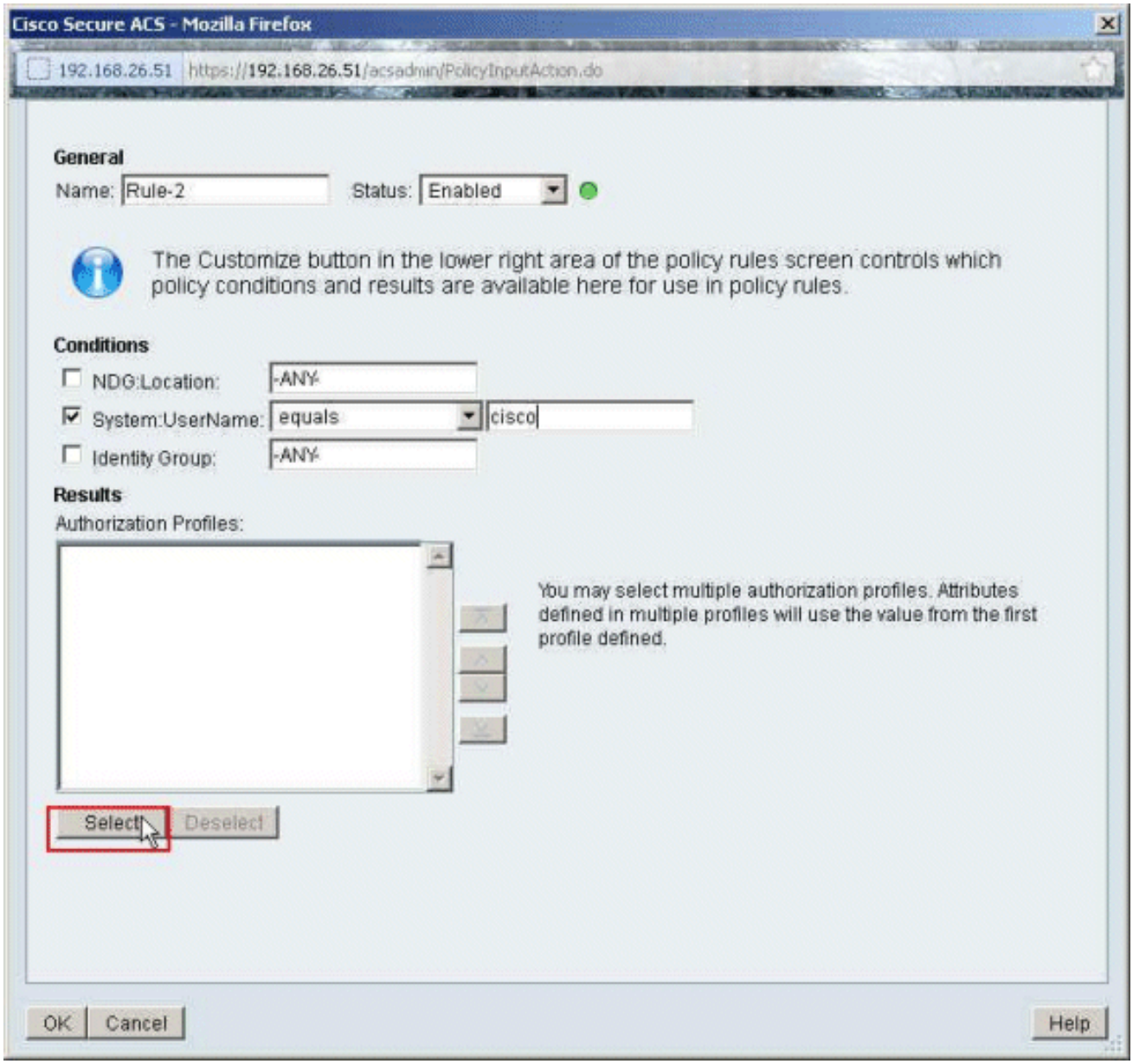
15. Per creare una nuova regola, fare clic su **Create** (Crea).



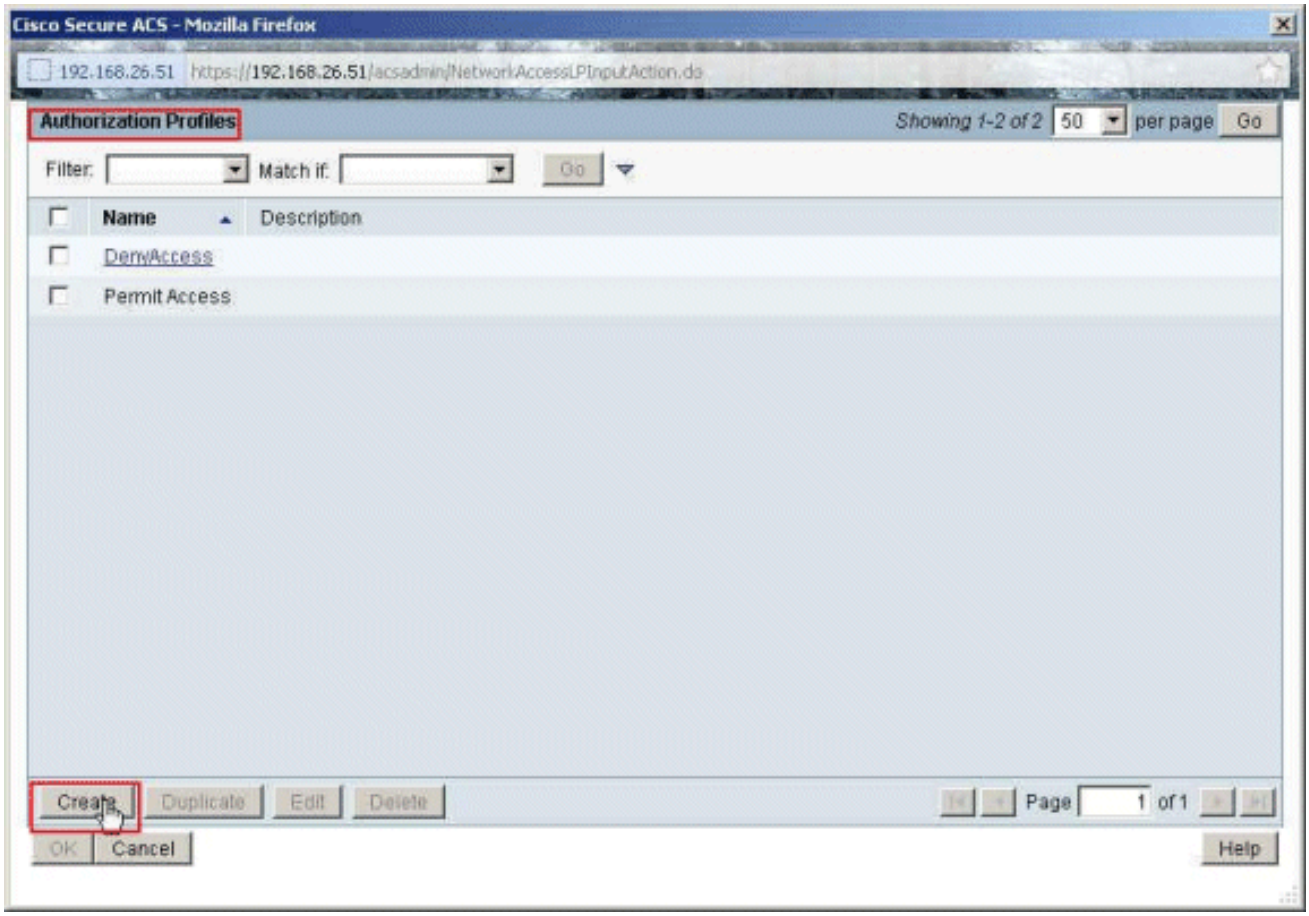
16. Verificare che la casella di controllo accanto a **System:UserName** sia selezionata, scegliere **uguale** dall'elenco a discesa e immettere il nome utente **cisco**.



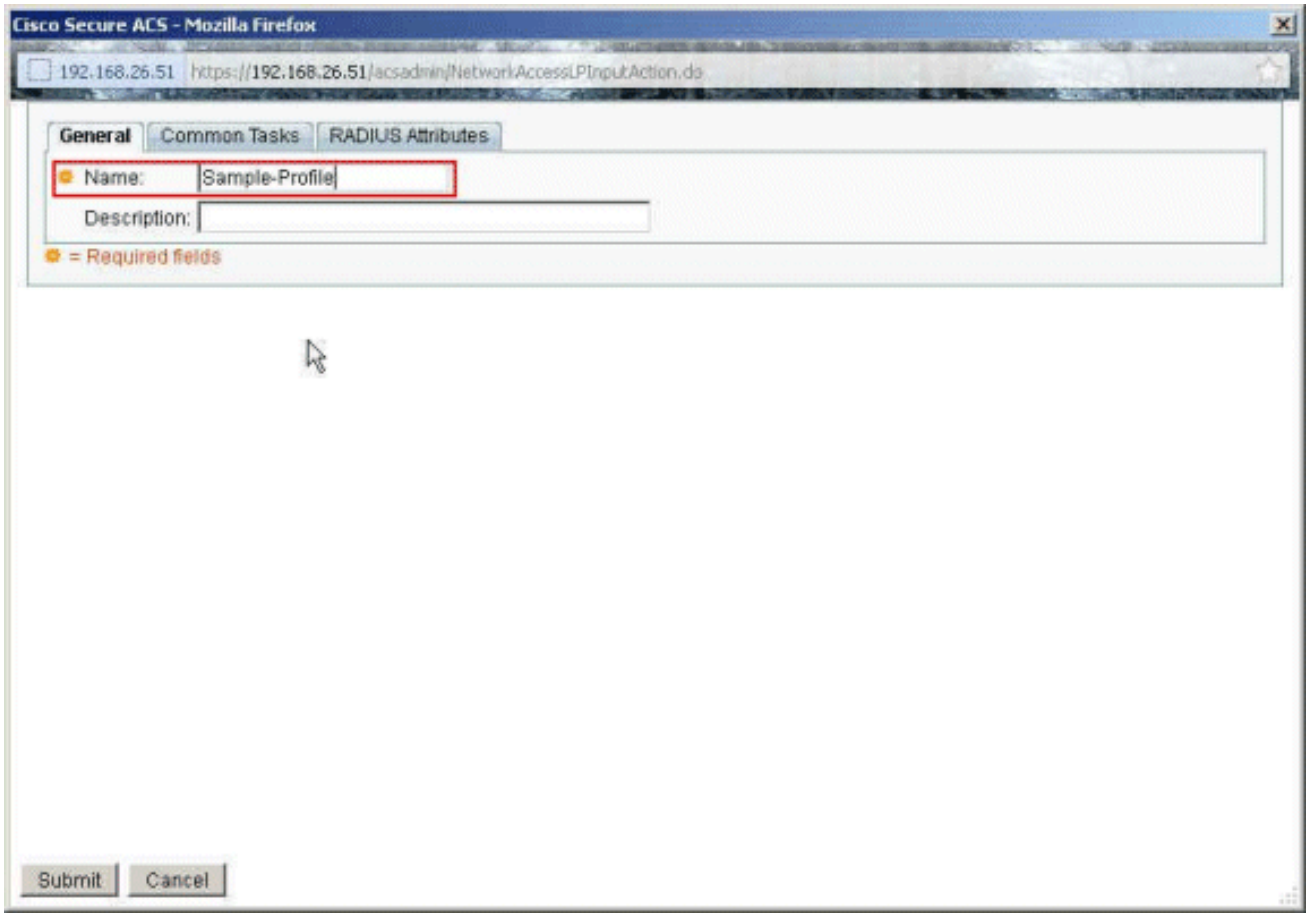
17. Fare clic su **Seleziona**.



18. Per creare un nuovo profilo di autorizzazione, fare clic su **Crea**.

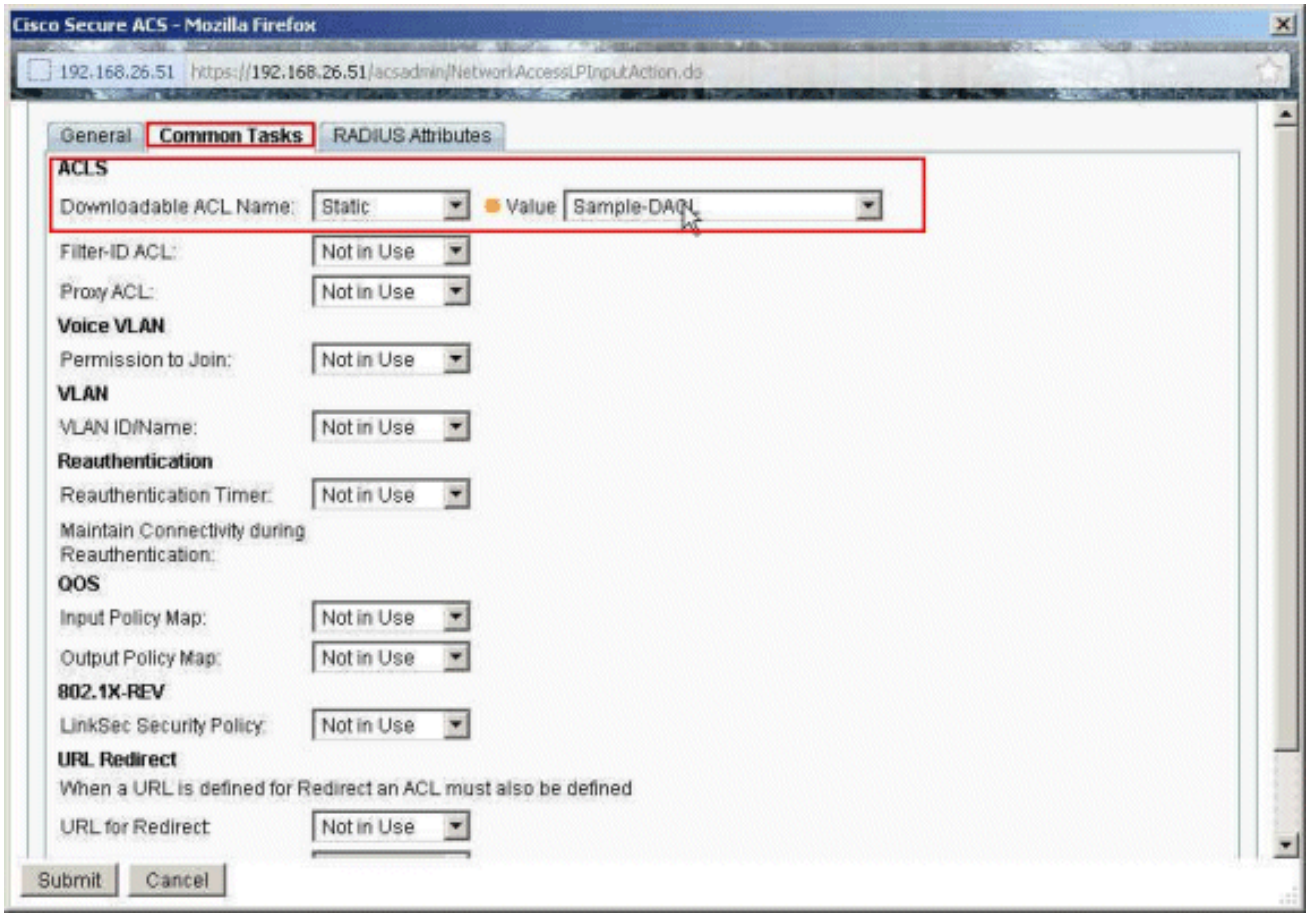


19. Specificare un nome per il **profilo di autorizzazione**. Nell'esempio viene utilizzato **Sample-Profile**.

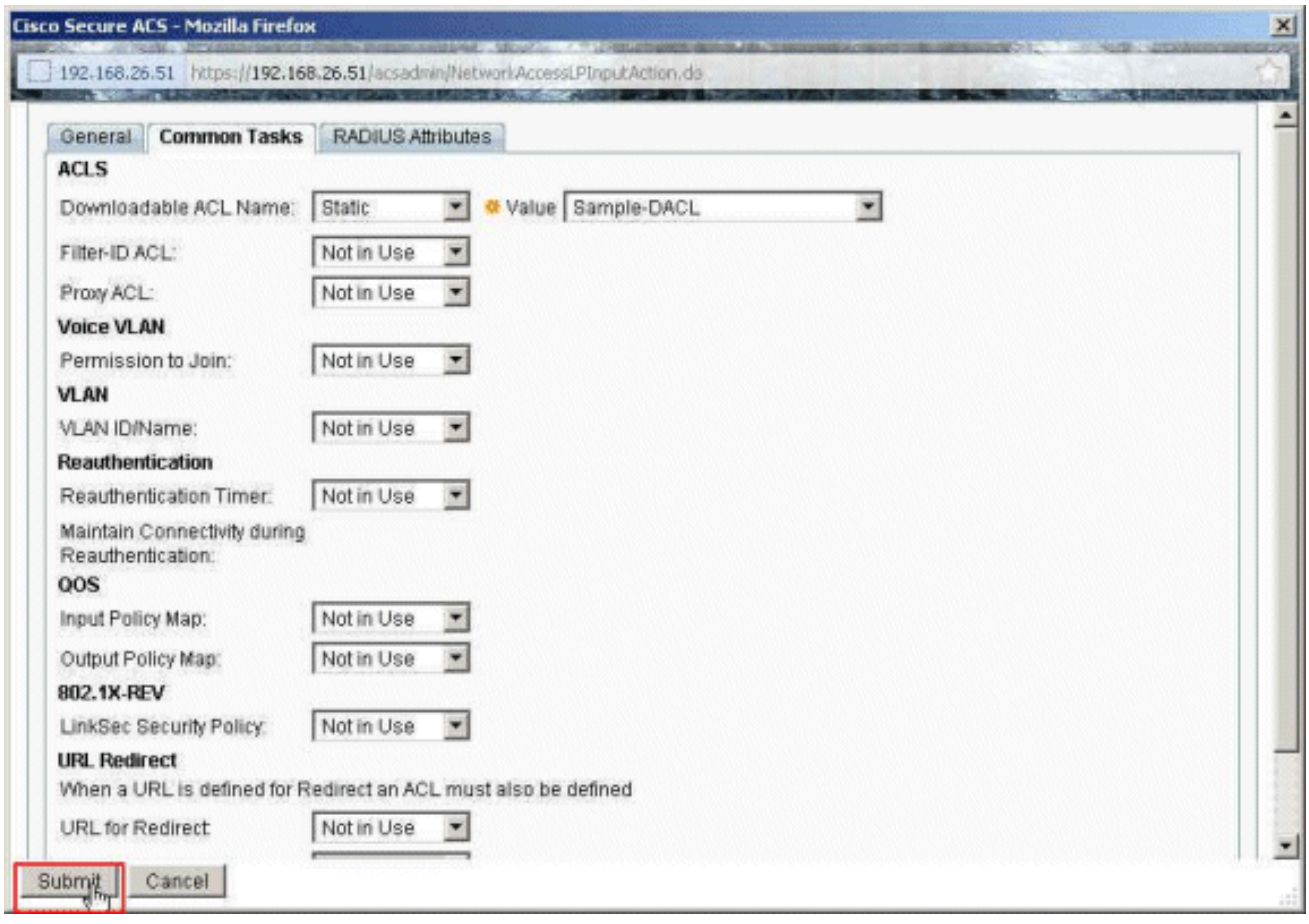


20. Scegliere la scheda **Common Tasks** e selezionare **Static** (Statica) dall'elenco a discesa per il valore **Downloadable ACL Name** (Nome ACL scaricabile). Scegliere il nuovo **DACL (Sample -DACL)** creato dall'elenco a discesa dei

valori.

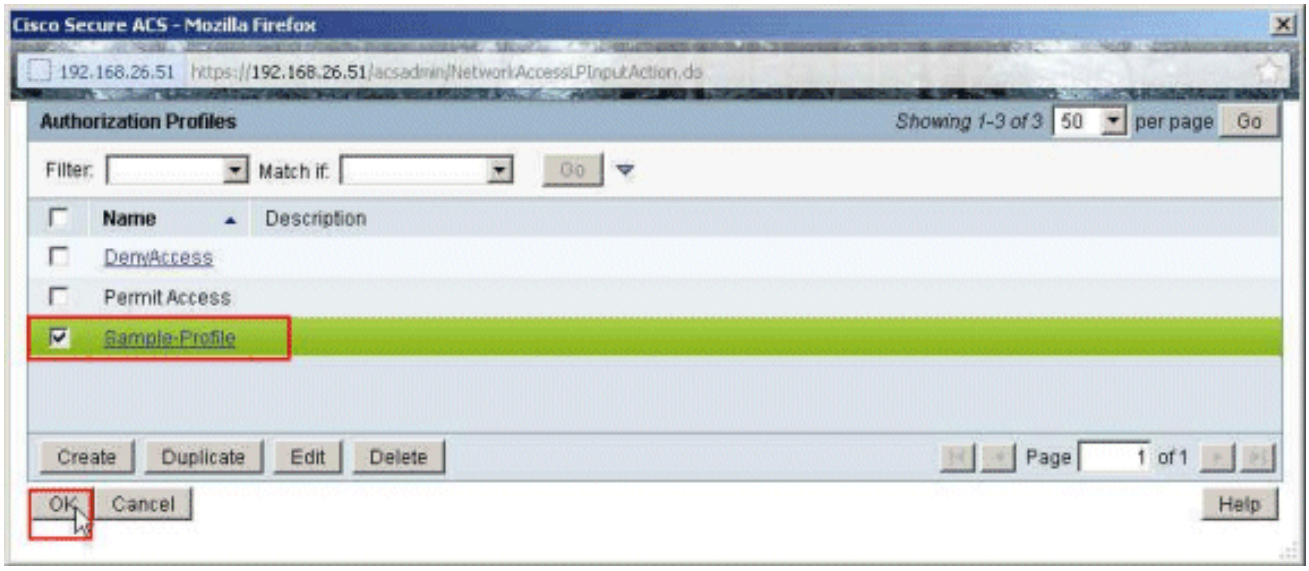


21. Fare clic su **Invia**.

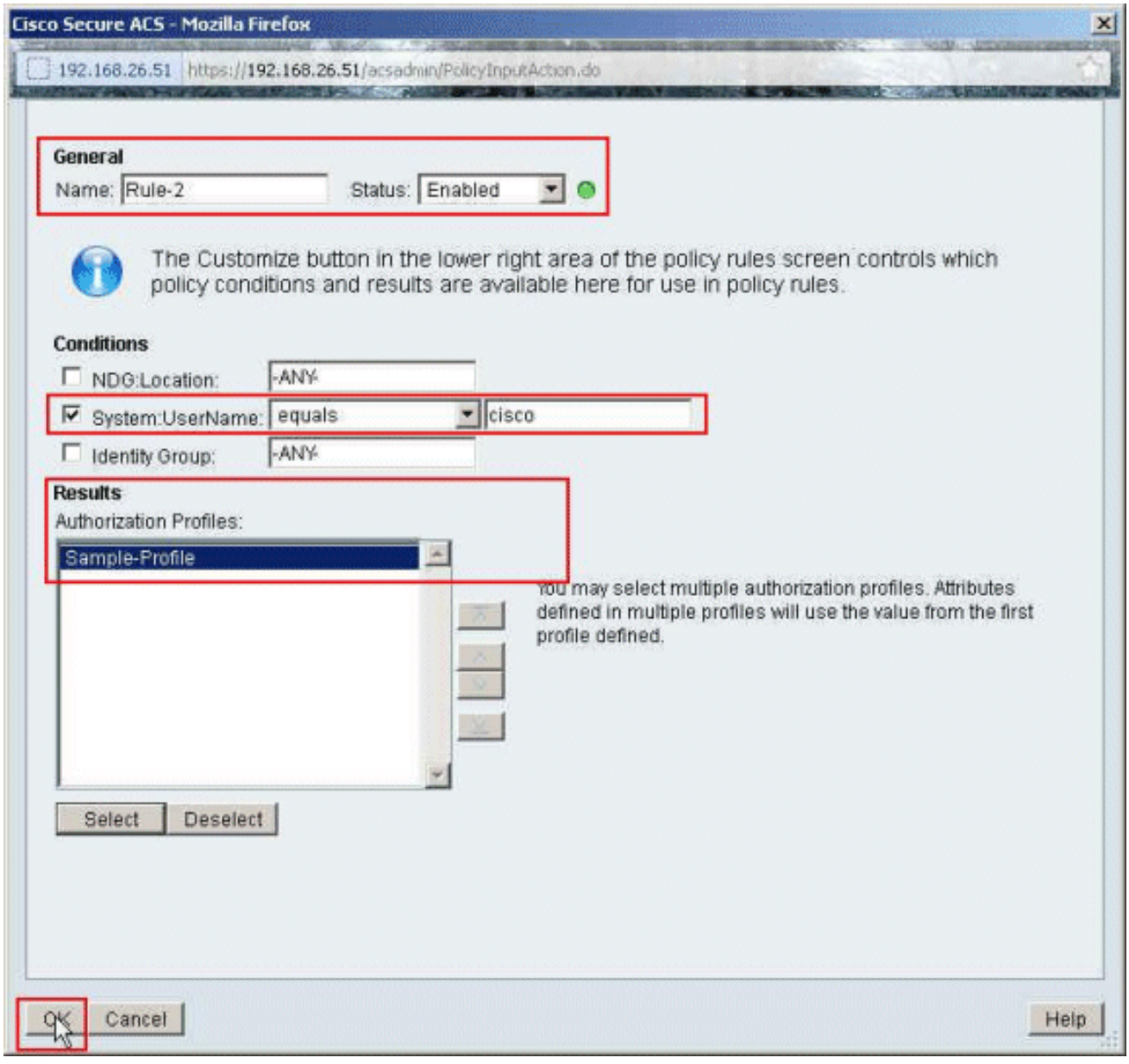


22. Verificare che la casella di controllo accanto a **Sample-Profile** (Profilo di autorizzazione appena creato) sia selezionata e fare clic su

OK.

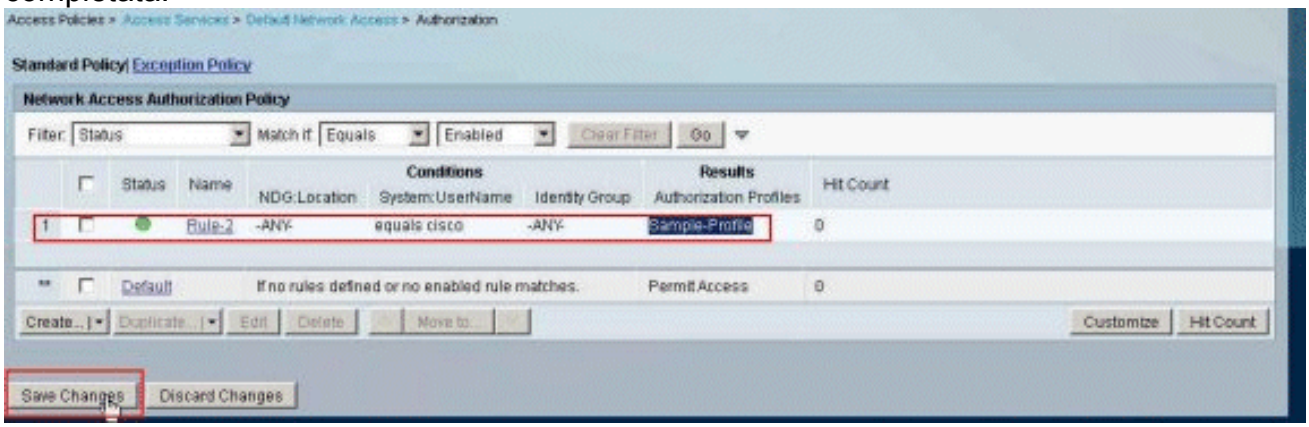


23. Dopo aver verificato che il nuovo **Profilo campione** sia selezionato nel campo **Profili di autorizzazione**, fare clic su
OK.



24. Verificare che la nuova regola (**Regola-2**) sia stata creata con System:UserName **uguale** alle condizioni **cisco** e **Sample-Profile** come risultato. Fare clic su **Salva modifiche**.

Creazione della regola 2 completata.



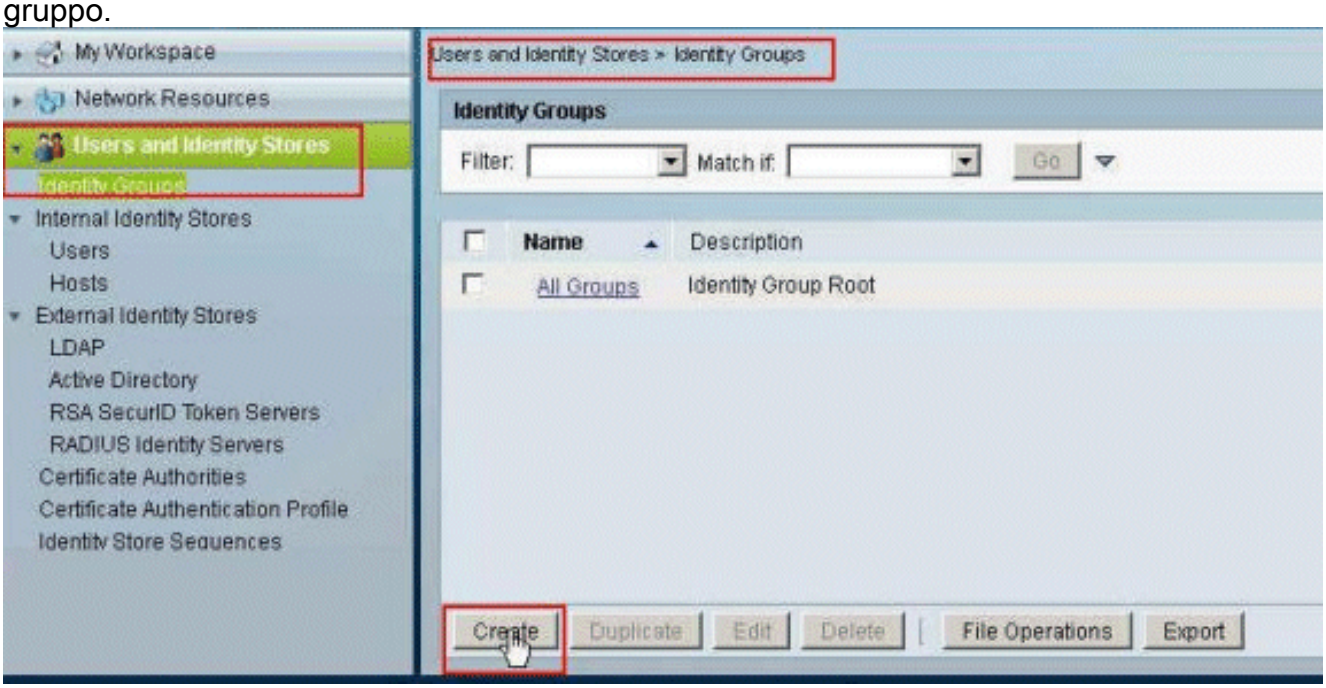
Configurazione di ACS per ACL scaricabili per gruppo

Completare i punti da 1 a 12 di Configure ACS for Downloadable ACL for Individual User (Configura ACL scaricabili per un singolo utente) ed eseguire questa procedura per configurare un ACL scaricabile per un gruppo in un ACS Cisco Secure.

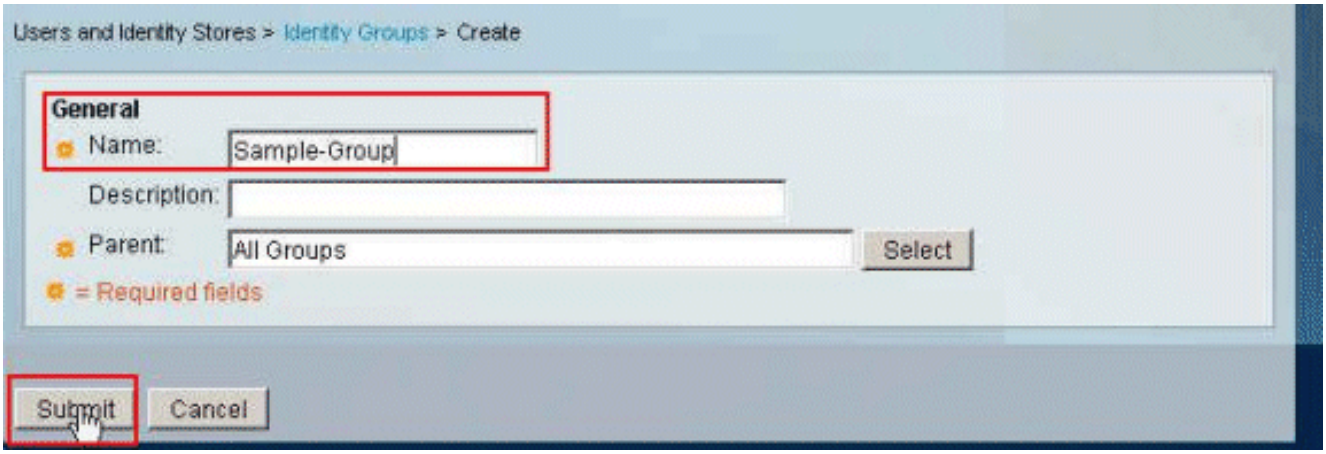
Nell'esempio, l'utente VPN IPsec "cisco" appartiene al **gruppo di esempio**.

L'utente **Sample-Group** cisco esegue l'autenticazione e il server RADIUS invia un elenco degli accessi scaricabile all'appliance di sicurezza. L'utente "cisco" può accedere solo al server 10.1.1.2 e nega tutti gli altri tipi di accesso. Per verificare l'ACL, consultare la sezione ACL scaricabili per utente/gruppo.

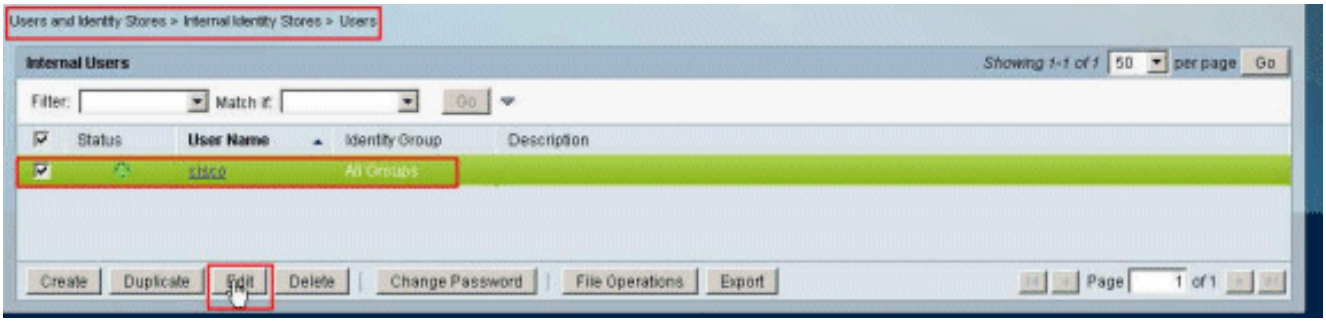
1. Nella barra di navigazione, fare clic su **Utenti e archivi identità** > **Gruppi di identità**, quindi fare clic su **Crea** per creare un nuovo gruppo.



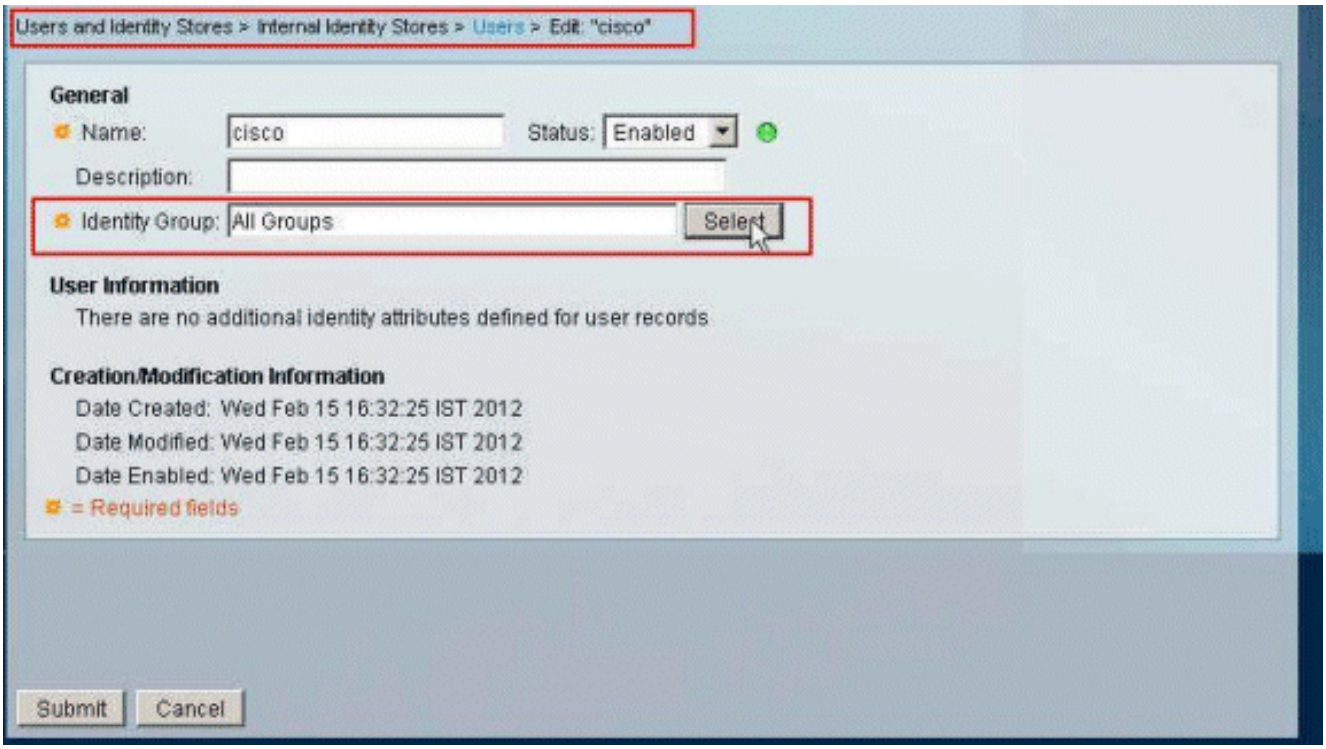
2. Fornire un nome di gruppo (**Sample-Group**) e fare clic su **Invia**.



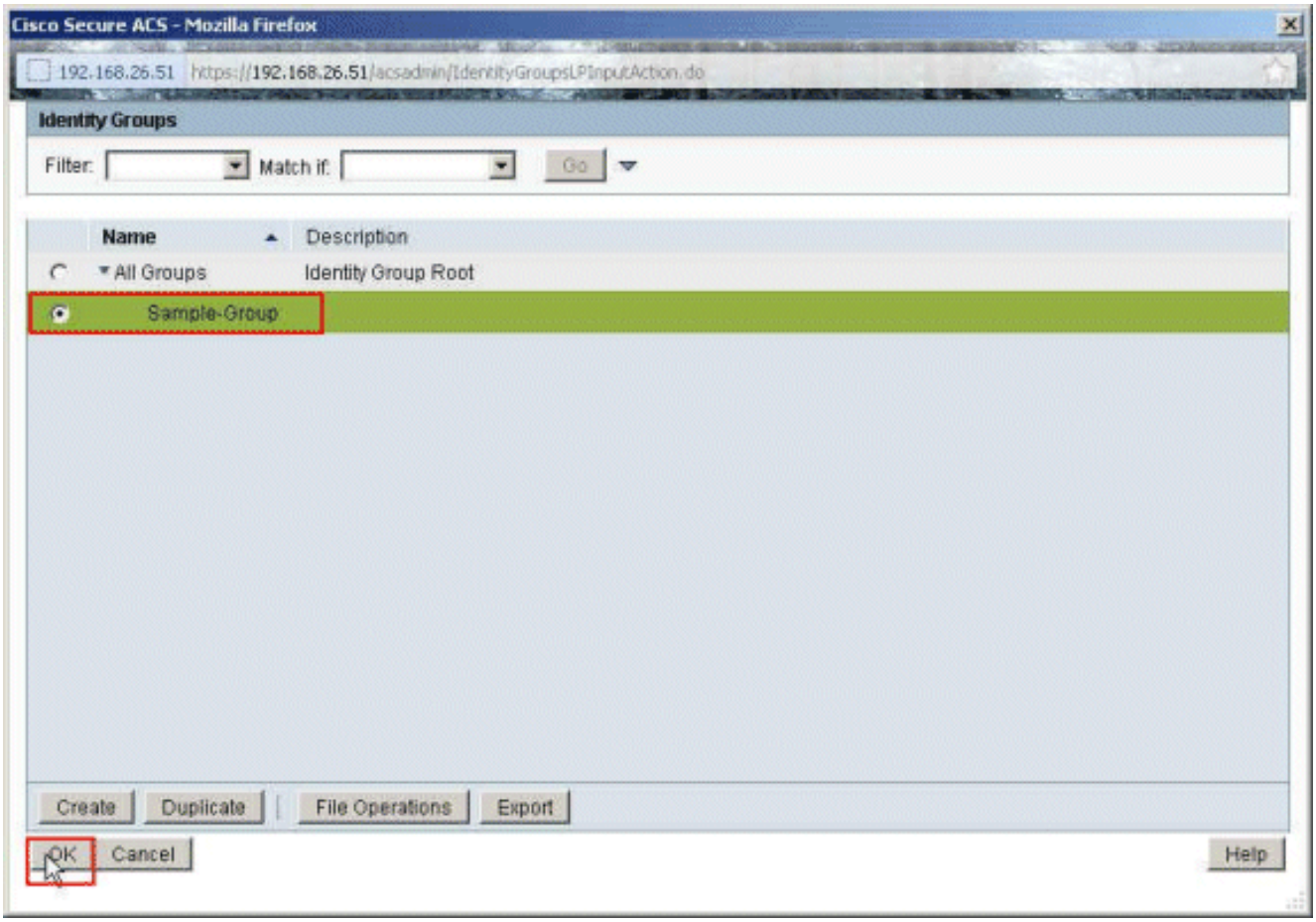
3. Scegliere **Archivi identità utente > Archivi identità interni > Utenti**, quindi selezionare l'utente **cisco**. Per modificare l'appartenenza ai gruppi di questo utente, fare clic su **Modifica**.



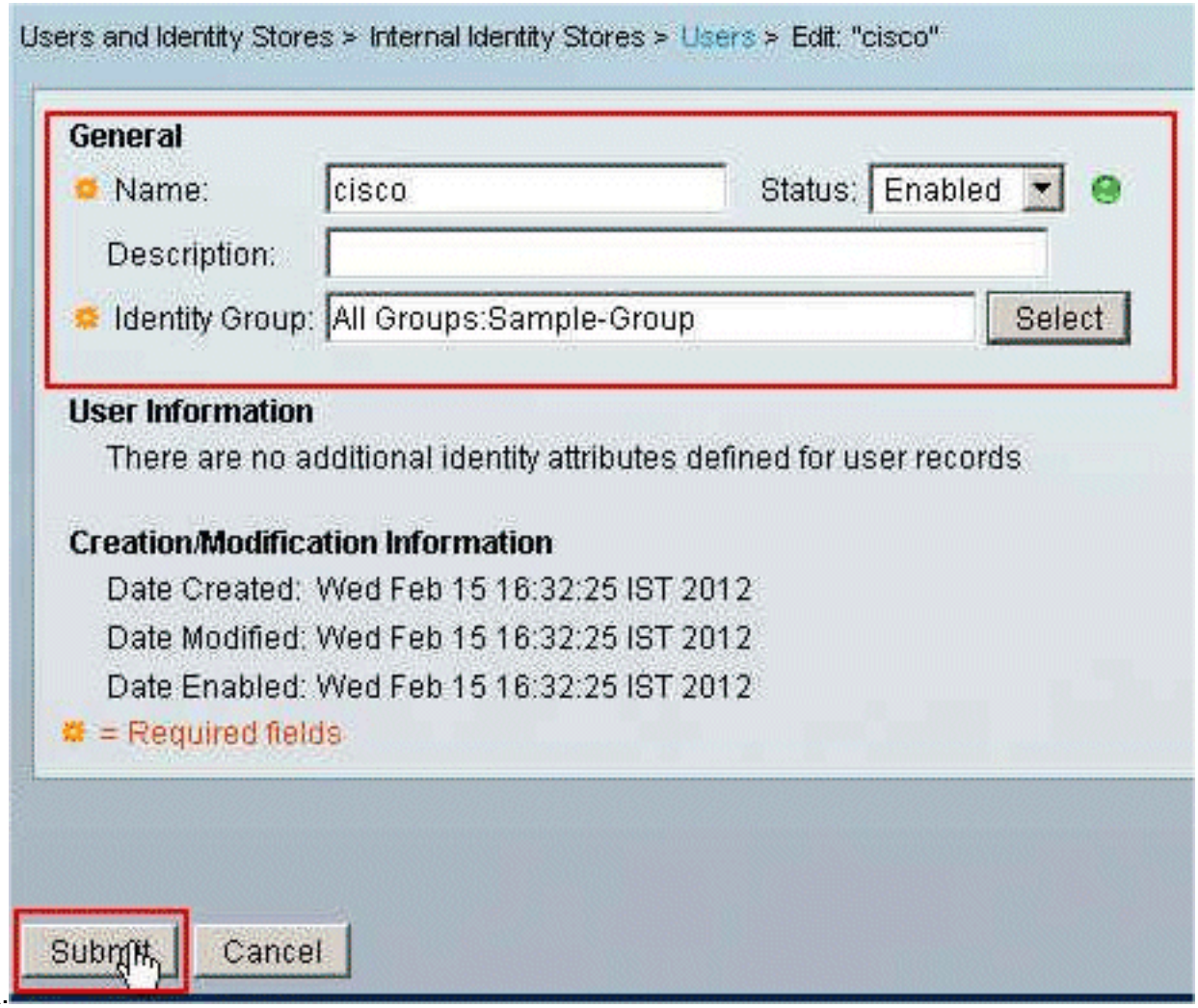
4. Fare clic su **Seleziona** accanto al gruppo di identità.



5. Selezionate il gruppo appena creato (ovvero **Sample-Group**) e fate clic su **OK**.



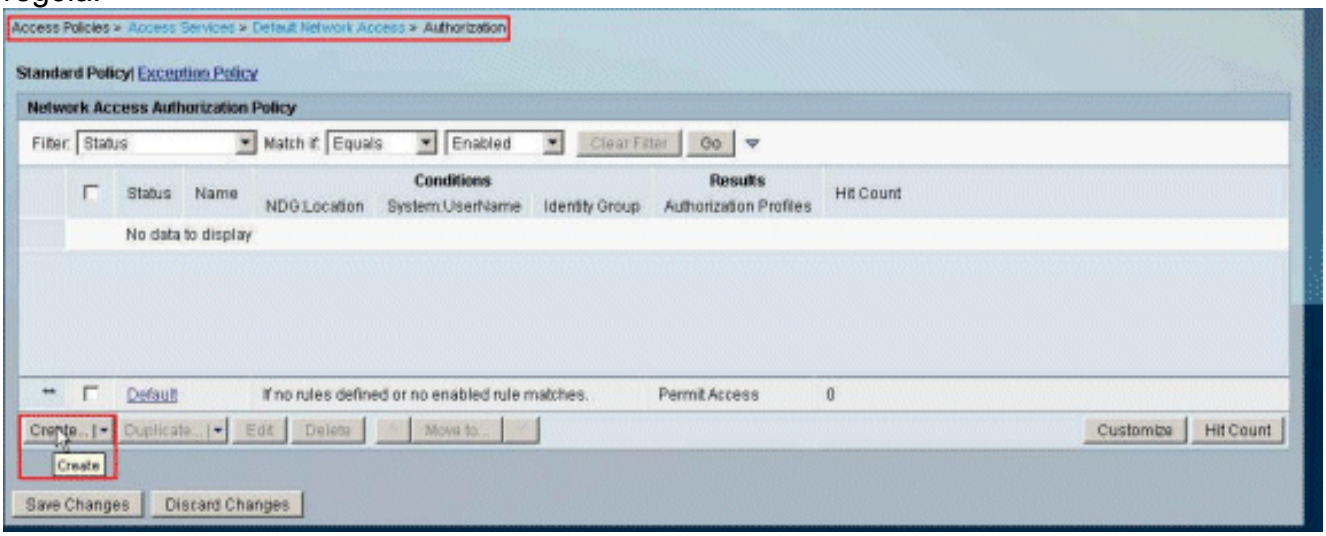
6. Fare clic su



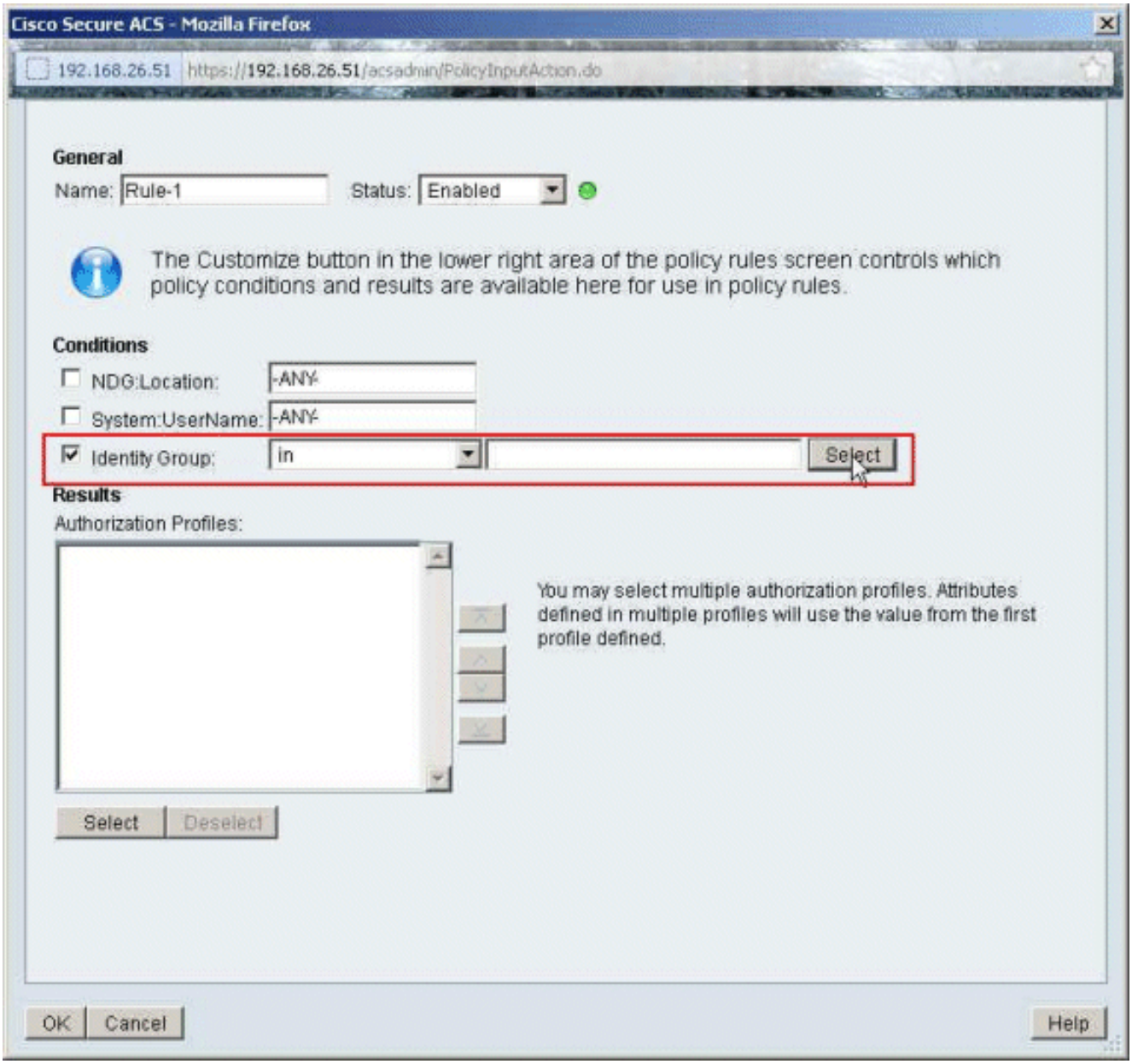
Invia.

7. Scegliere Criteri di accesso > **Servizi di accesso > Accesso di rete predefinito >**

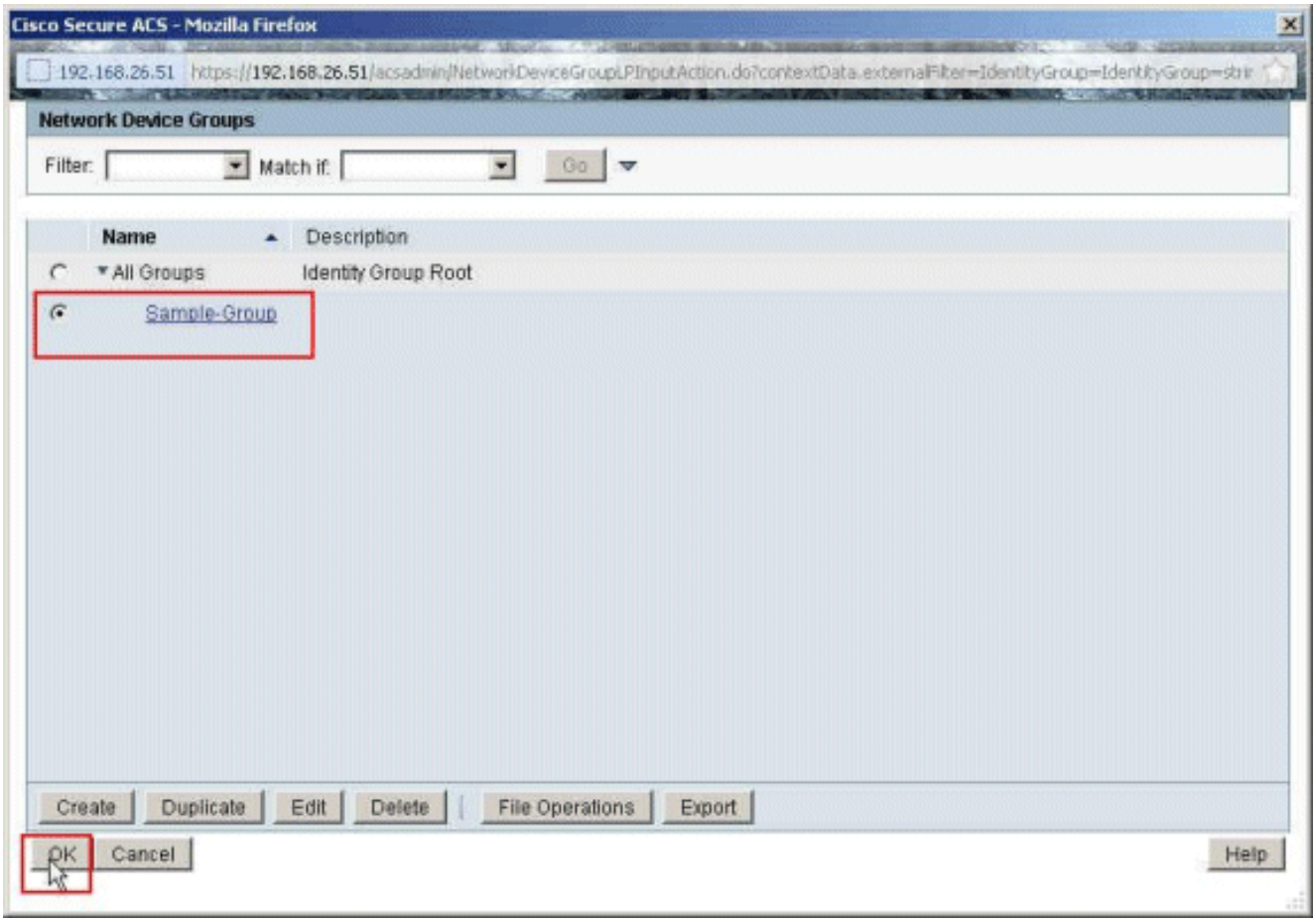
Autorizzazione, quindi fare clic su **Crea** per creare una nuova regola.



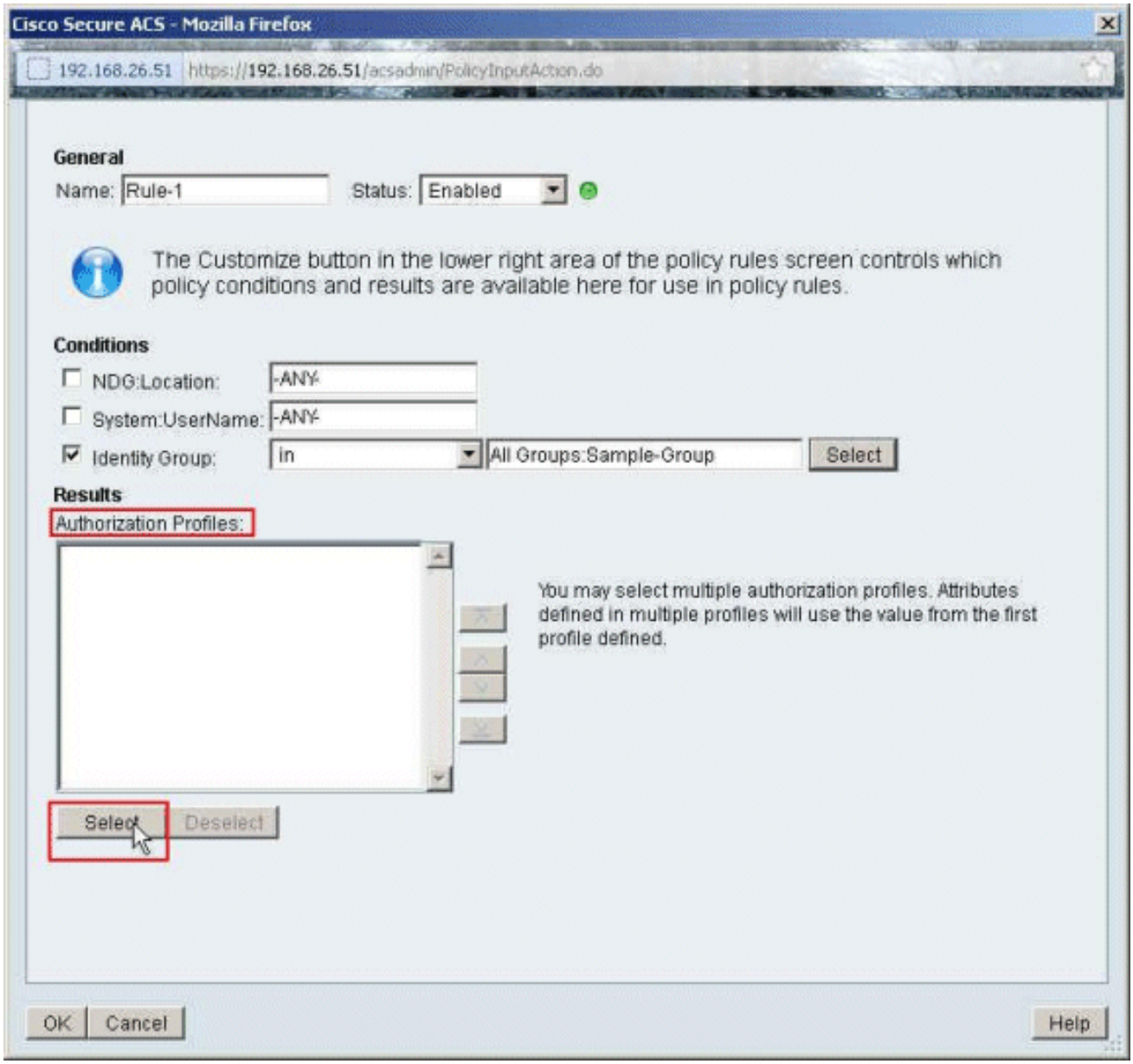
8. Verificare che la casella di controllo accanto a **Gruppo di identità** sia selezionata e fare clic su **Seleziona**.



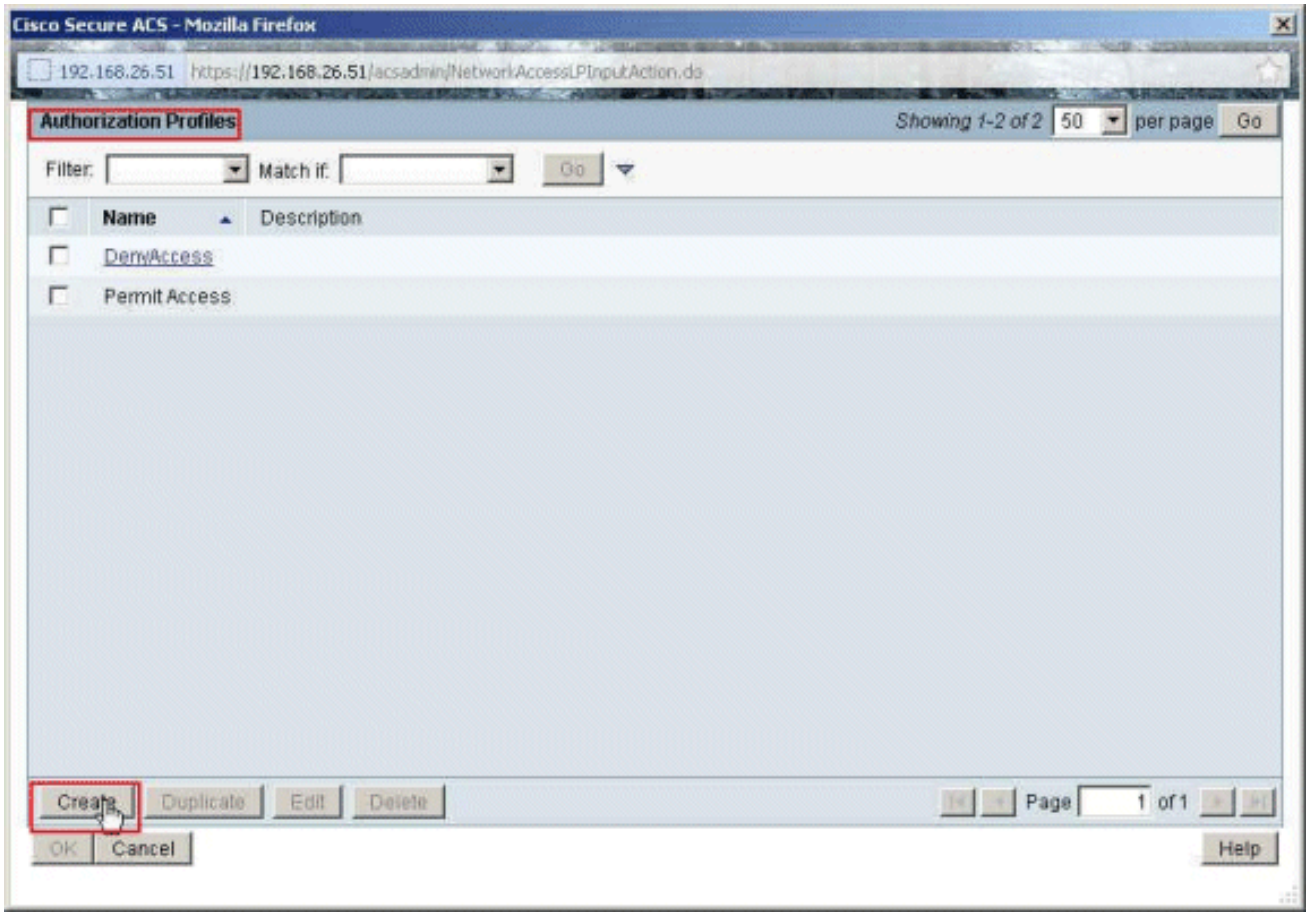
9. Selezionate **Sample-Group**, quindi fate clic su **OK**.



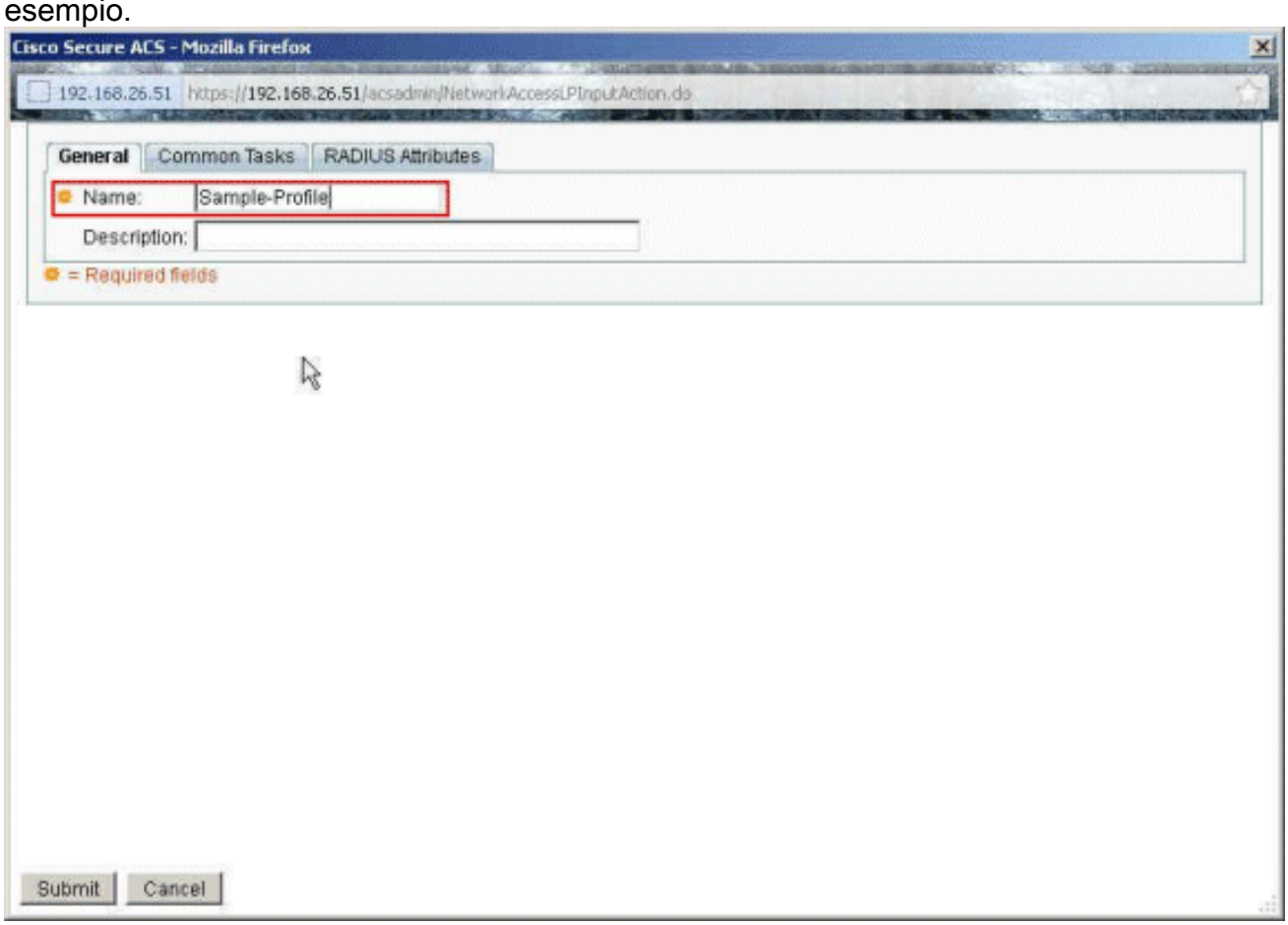
10. Fare clic su **Seleziona** nella sezione Profili di autorizzazione.



11. Per creare un nuovo profilo di autorizzazione, fare clic su **Crea**.

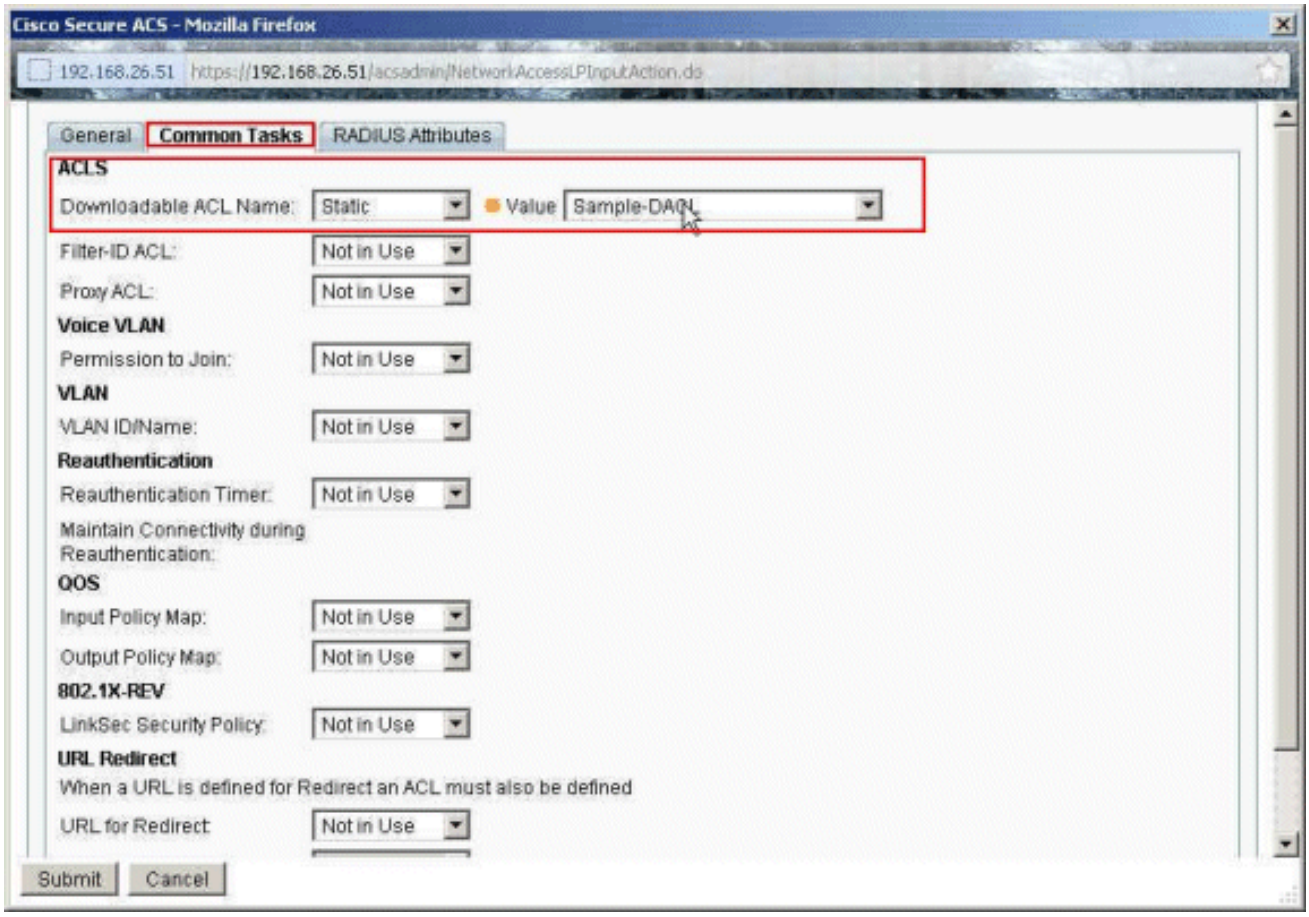


12. Specificare un nome per il **profilo di autorizzazione**. **Sample-Profile** è il nome utilizzato in questo
esempio.

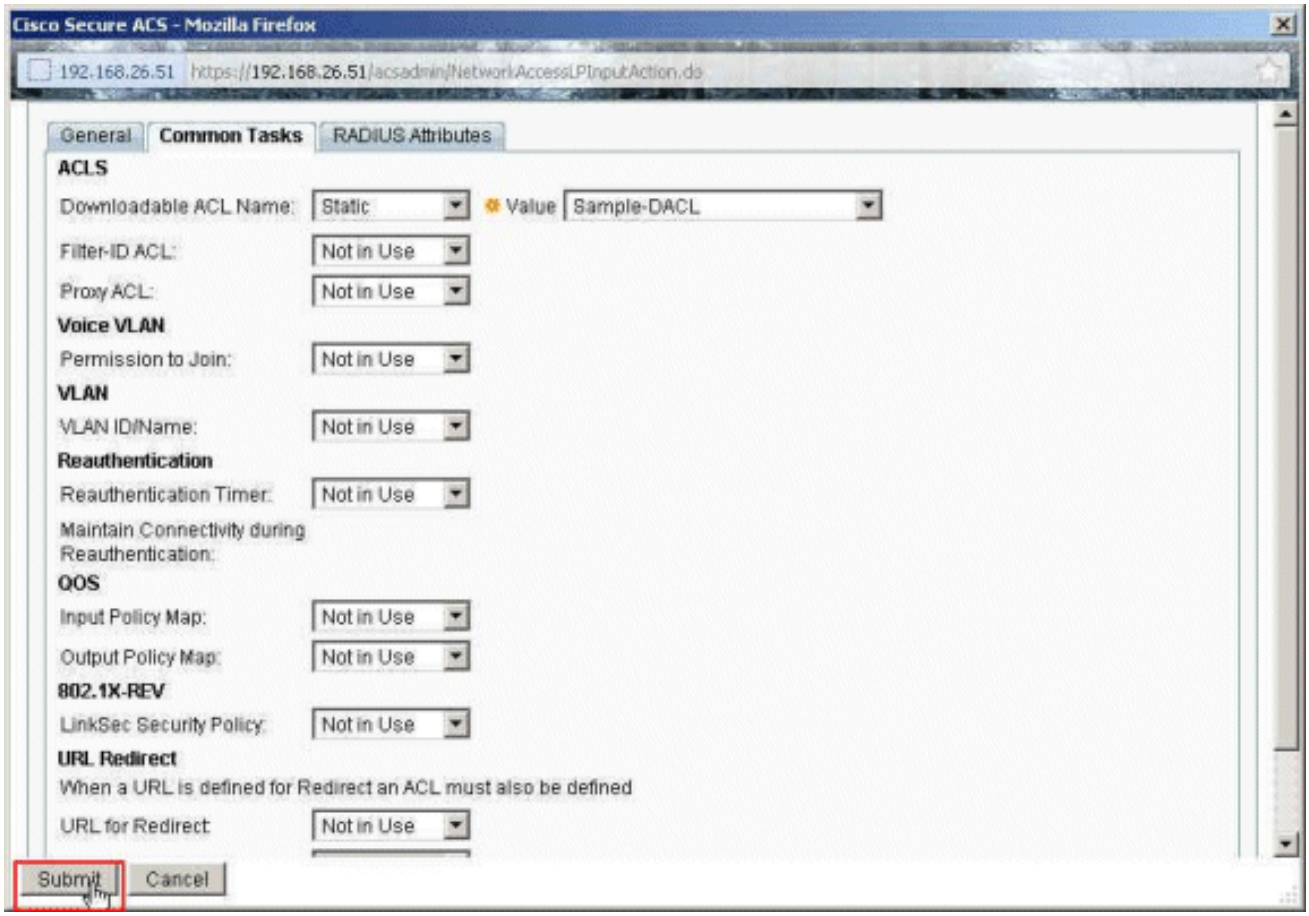


13. Scegliere la scheda **Common Tasks** e selezionare **Static** (Statica) dall'elenco a discesa per il valore **Downloadable ACL Name** (Nome ACL scaricabile). Scegliere il nuovo **DACL**

(Sample -DACL) creato dall'elenco a discesa Valore.

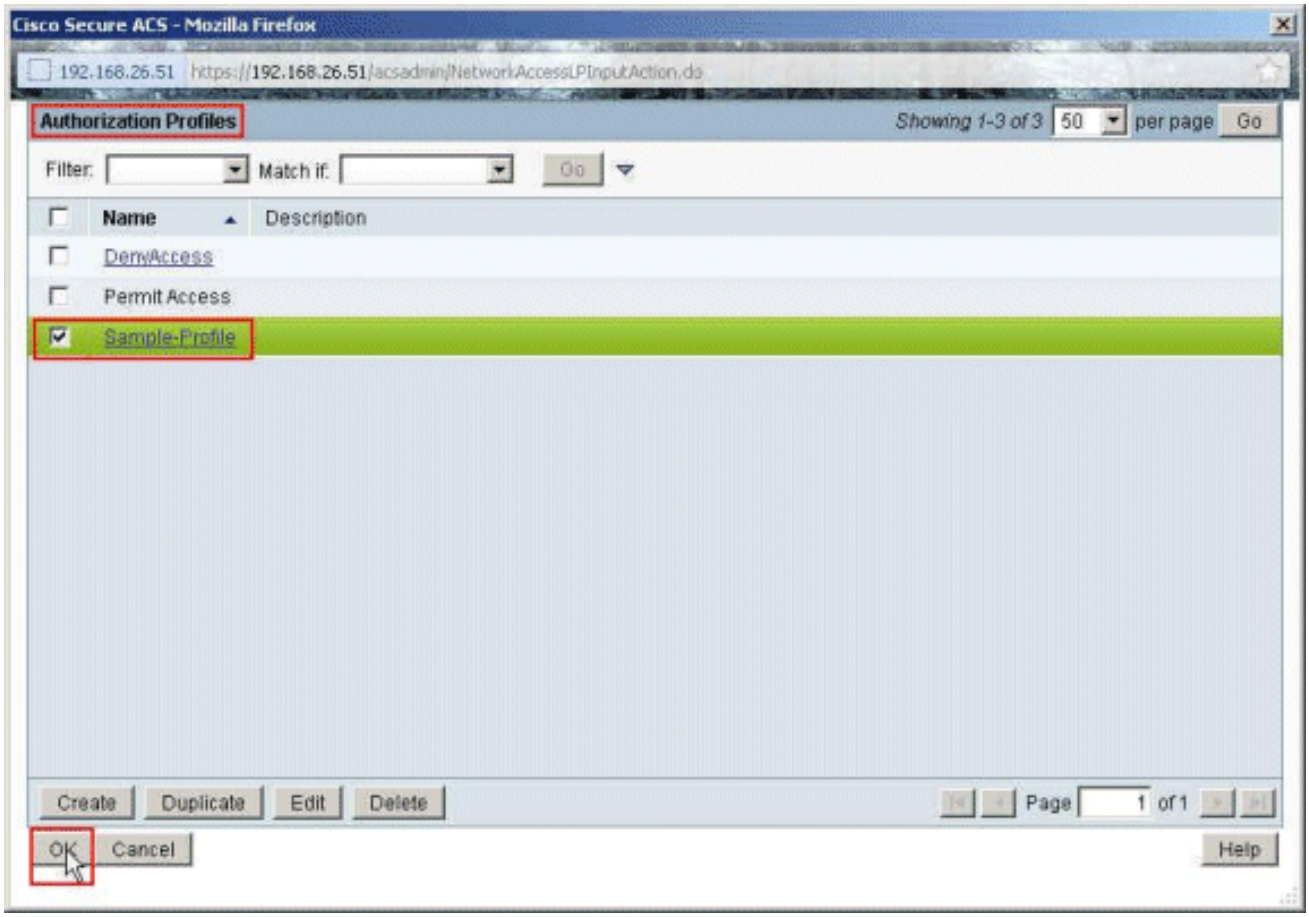


14. Fare clic su **Invia**.

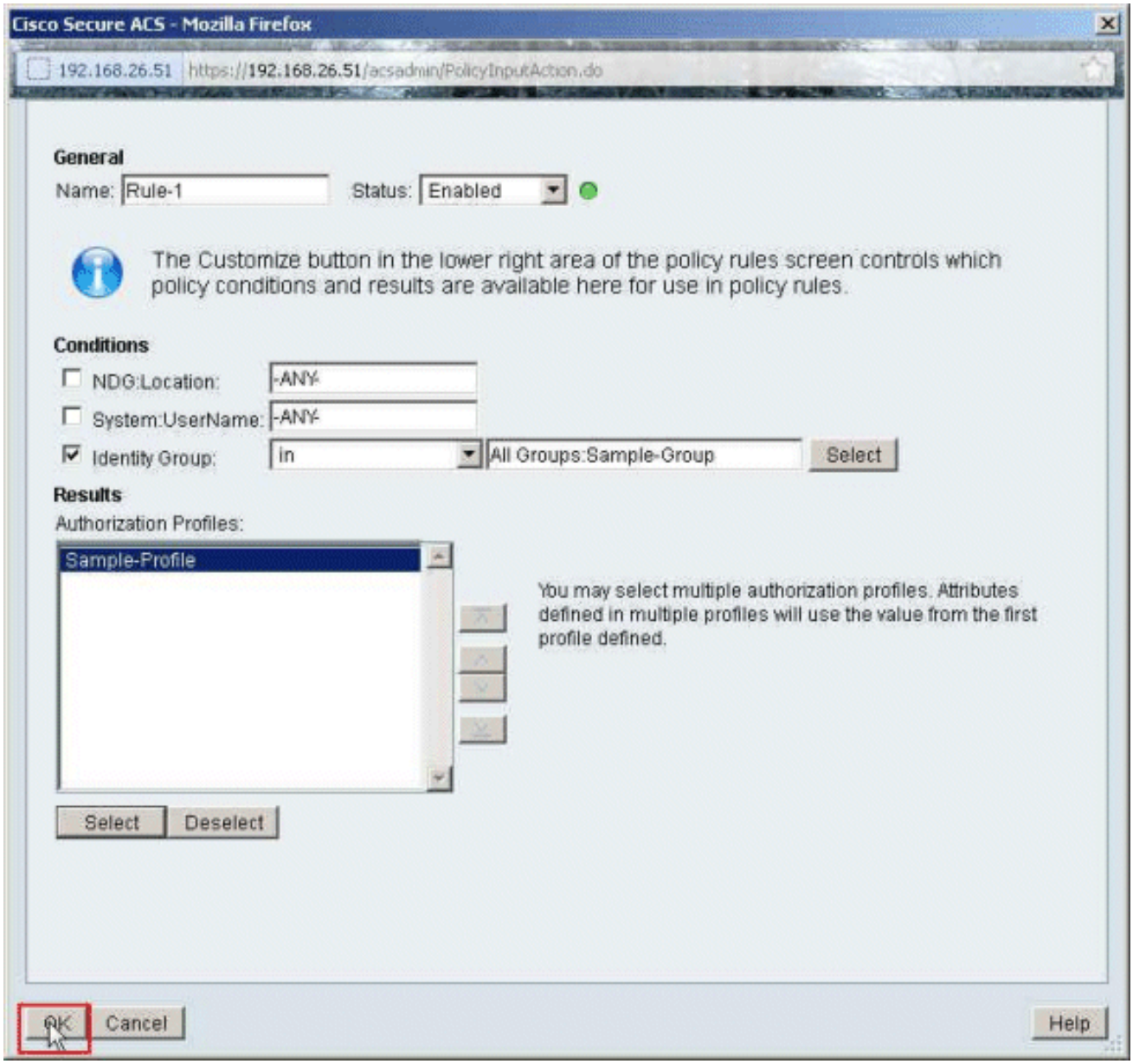


15. Scegliere il profilo di autorizzazione **Profilo di esempio** creato in precedenza e fare clic su

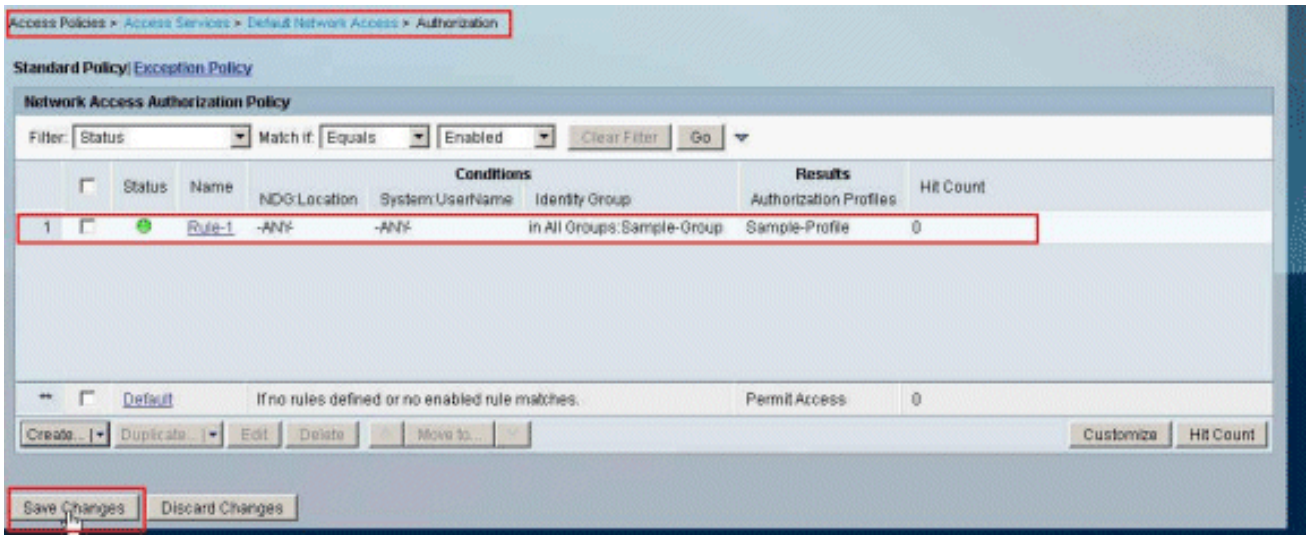
OK.



16. Fare clic su
OK.



17. Verificare che **Rule-1** sia stato creato con Identity Group **Sample-Group** come condizione e **Sample-Profile** come risultato. Fare clic su **Salva modifiche**.



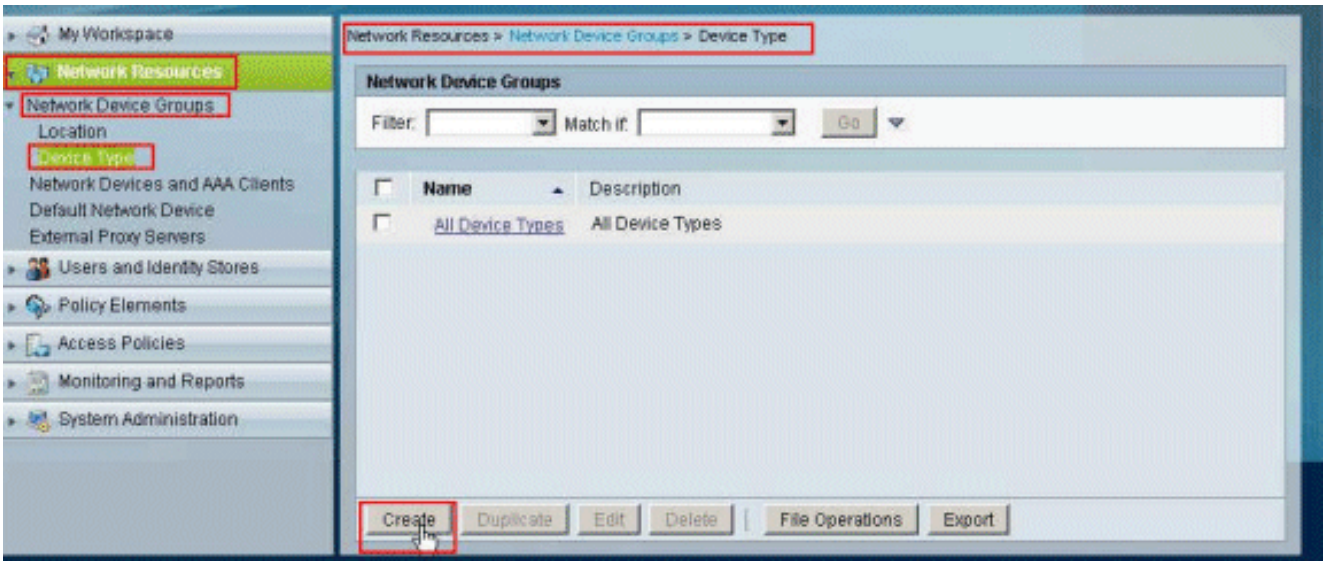
Configurazione di ACS per ACL scaricabili per un gruppo di dispositivi di rete

Completare i punti da 1 a 12 di Configure ACS for Downloadable ACL for Individual User

(Configura ACL scaricabili per un singolo utente) ed eseguire questa procedura per configurare un ACL scaricabile per un gruppo di dispositivi di rete in un ACS sicuro Cisco.

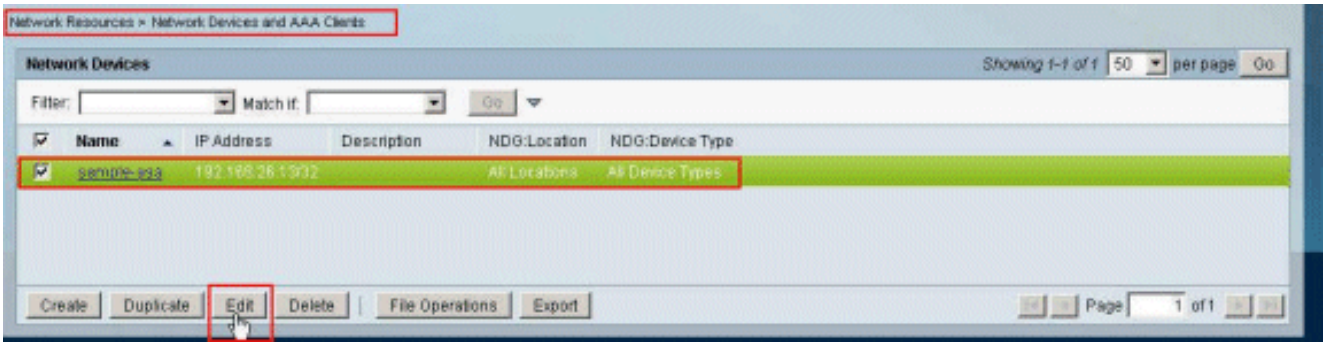
Nell'esempio, il client RADIUS (ASA) appartiene al gruppo di dispositivi di rete **VPN-Gateway**.La richiesta di autenticazione VPN proveniente dall'ASA per l'utente "cisco" viene autenticata correttamente e il server RADIUS invia un elenco degli accessi scaricabili all'appliance di sicurezza. L'utente "cisco" può accedere solo al server 10.1.1.2 e nega tutti gli altri tipi di accesso. Per verificare l'ACL, consultare la sezione ACL scaricabili per utente/gruppo.

1. Scegliere **Risorse di rete > Gruppi di dispositivi di rete > Tipo di dispositivo**, quindi fare clic su **Crea** per creare un nuovo gruppo di dispositivi di rete.

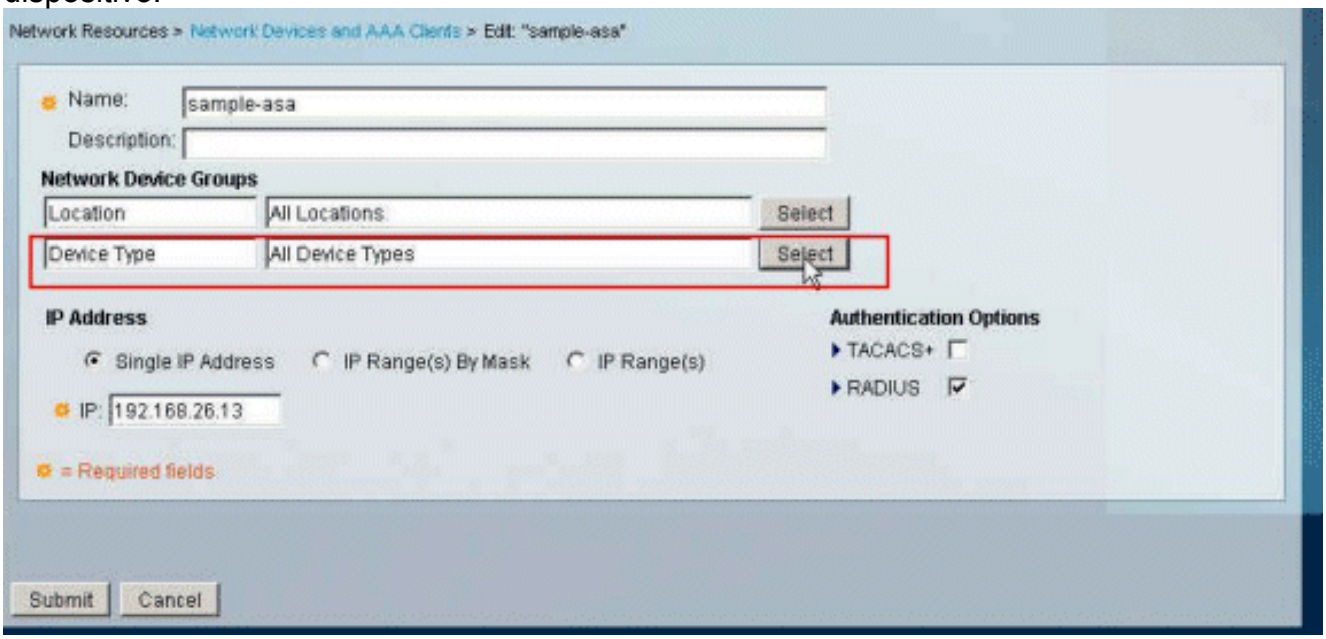


2. Specificare il nome di un **gruppo di dispositivi di rete** (**gateway VPN** in questo esempio) e fare clic su **Invia**.

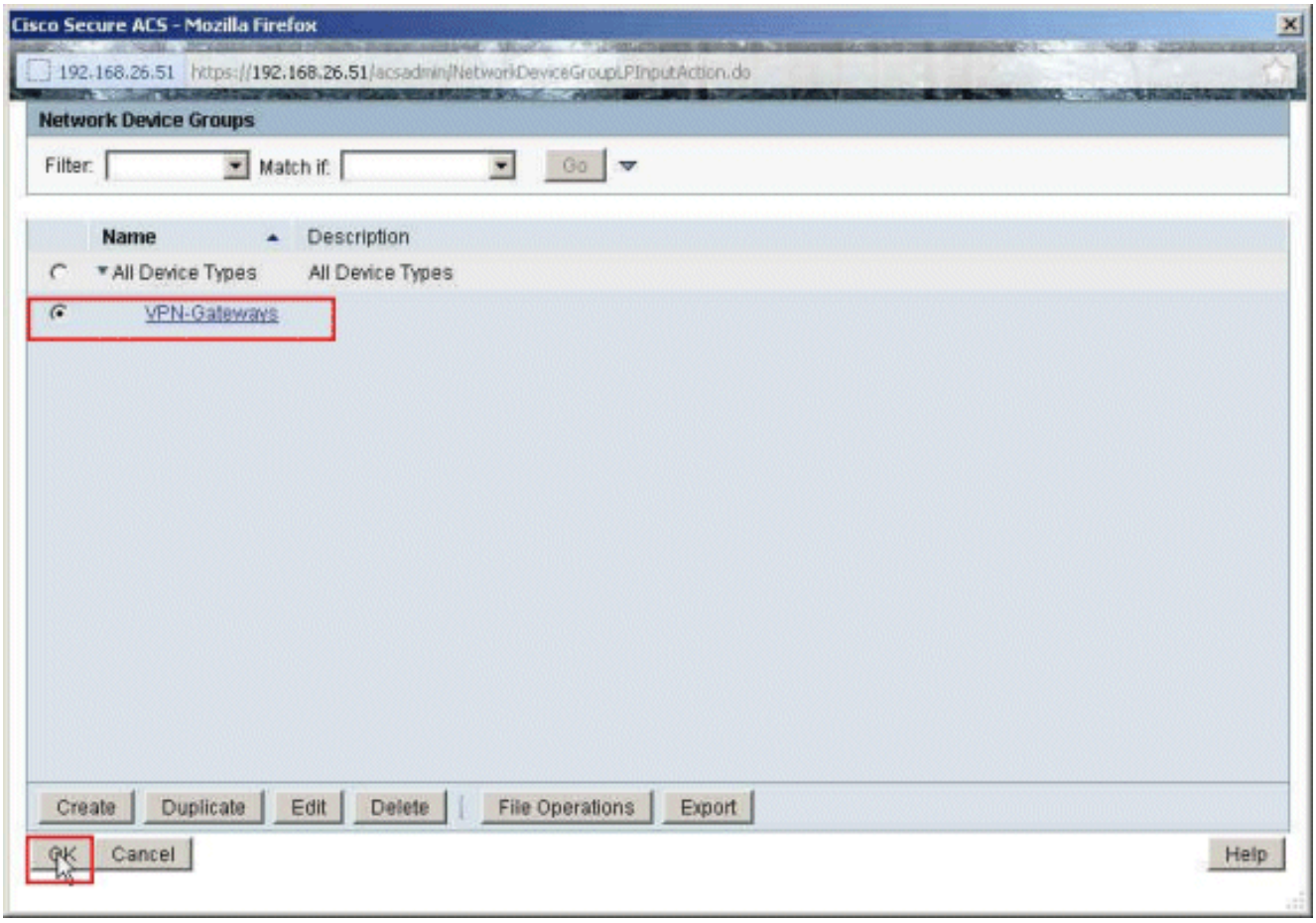
3. Scegliere **Risorse di rete > Dispositivi di rete e client AAA**, quindi selezionare il client **RADIUS campione-asa** creato in precedenza. Fare clic su **Edit** (Modifica) per modificare l'appartenenza al **gruppo di dispositivi di rete** del client RADIUS (asa).



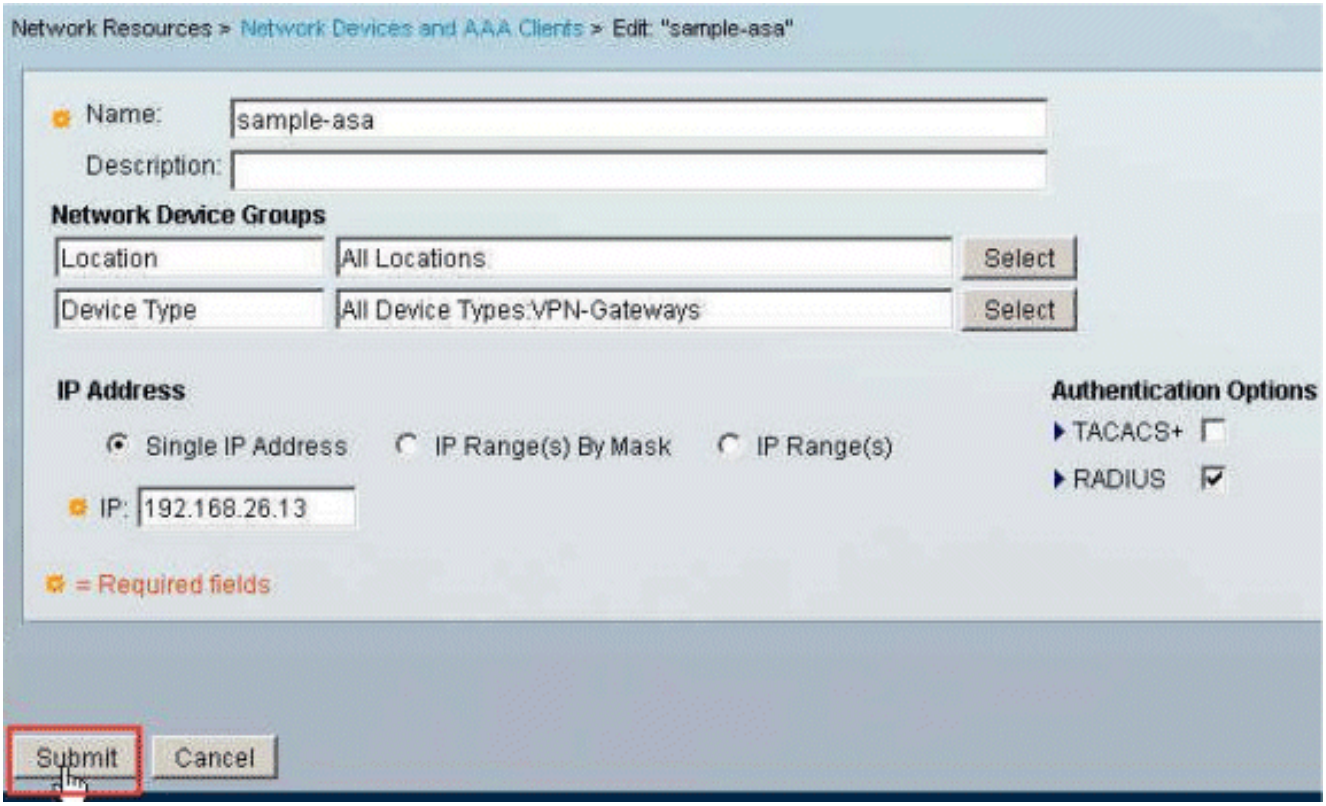
4. Fare clic su **Seleziona** accanto al Tipo di dispositivo.



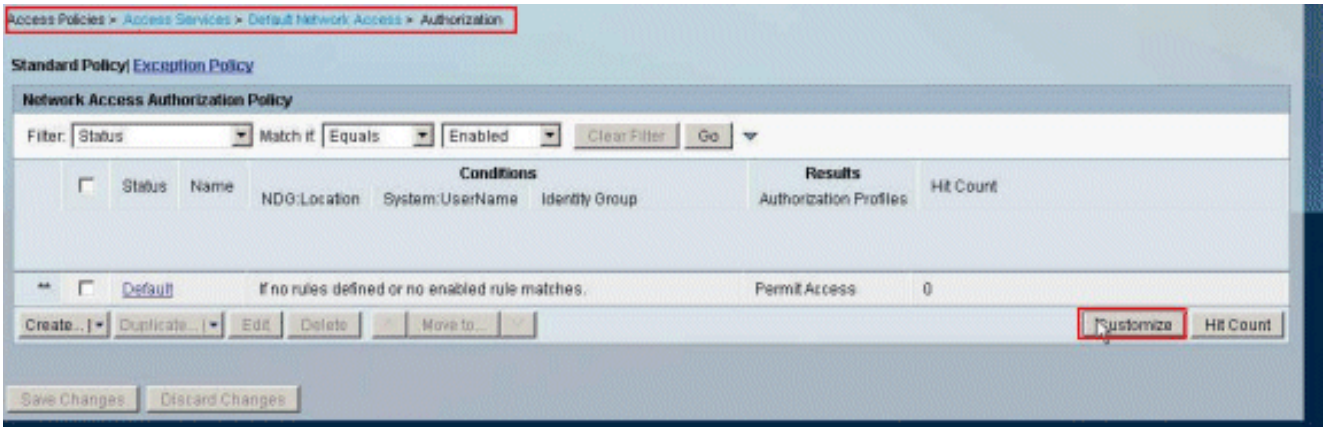
5. Selezionare il gruppo di dispositivi di rete appena creato (ovvero **VPN-Gateway**) e fare clic su **OK**.



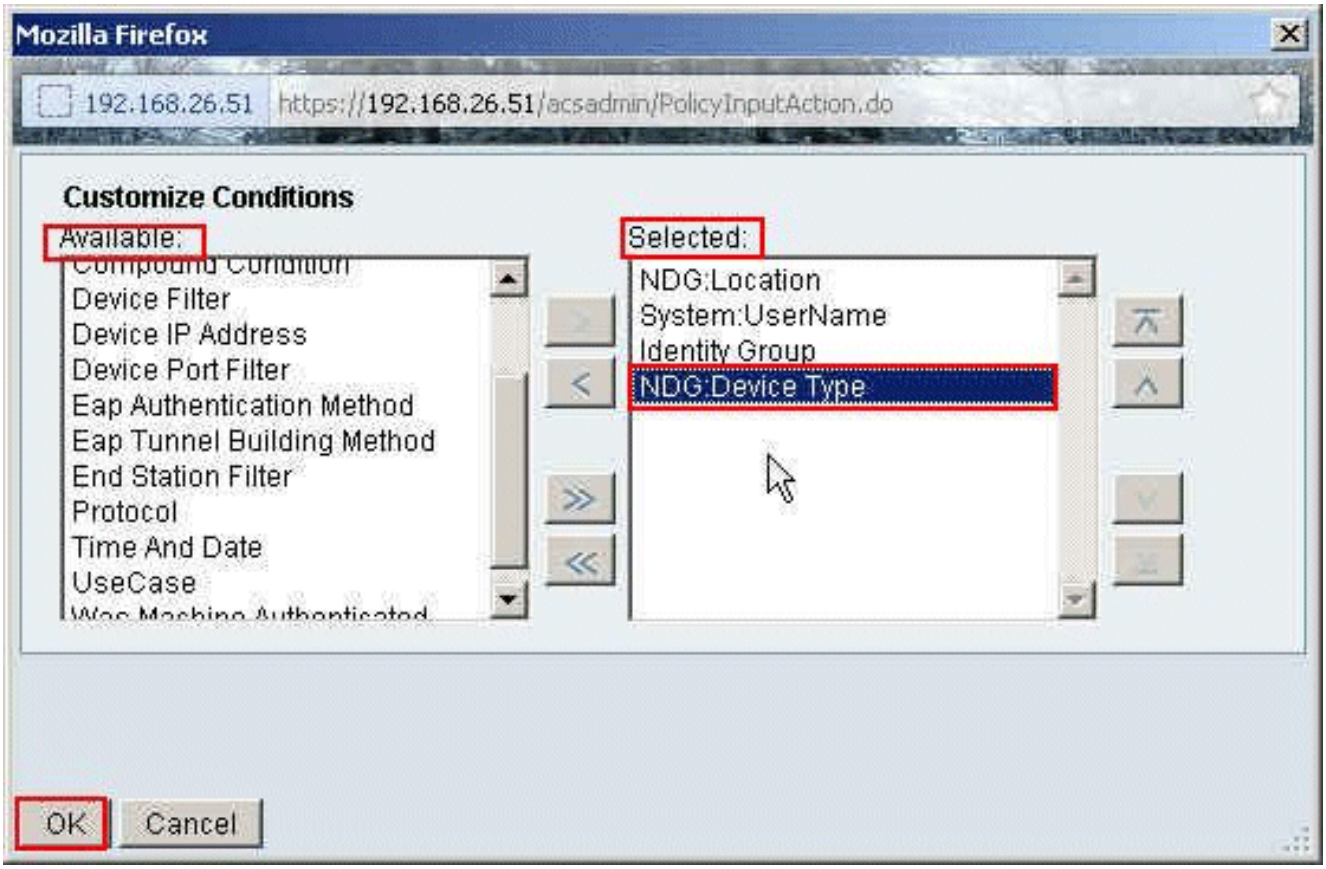
6. Fare clic su
Invia.



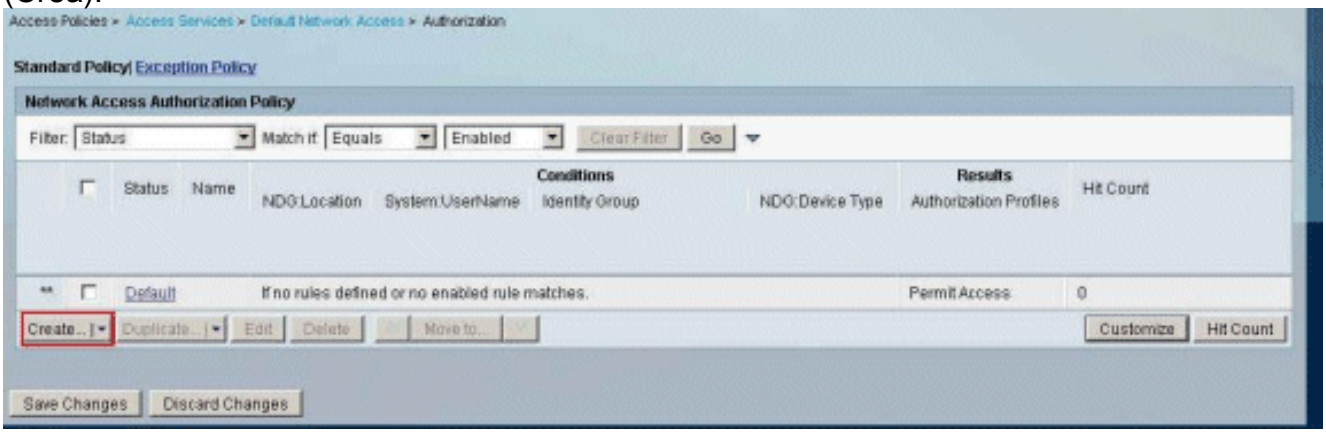
7. Scegliere Criteri di accesso > **Servizi di accesso** > **Accesso di rete predefinito** > **Autorizzazione**, quindi fare clic su
Personalizza.



8. Spostare **NDG:Tipo di dispositivo** dalla sezione **Disponibile** alla sezione **Selezionato**, quindi fare clic su
OK.

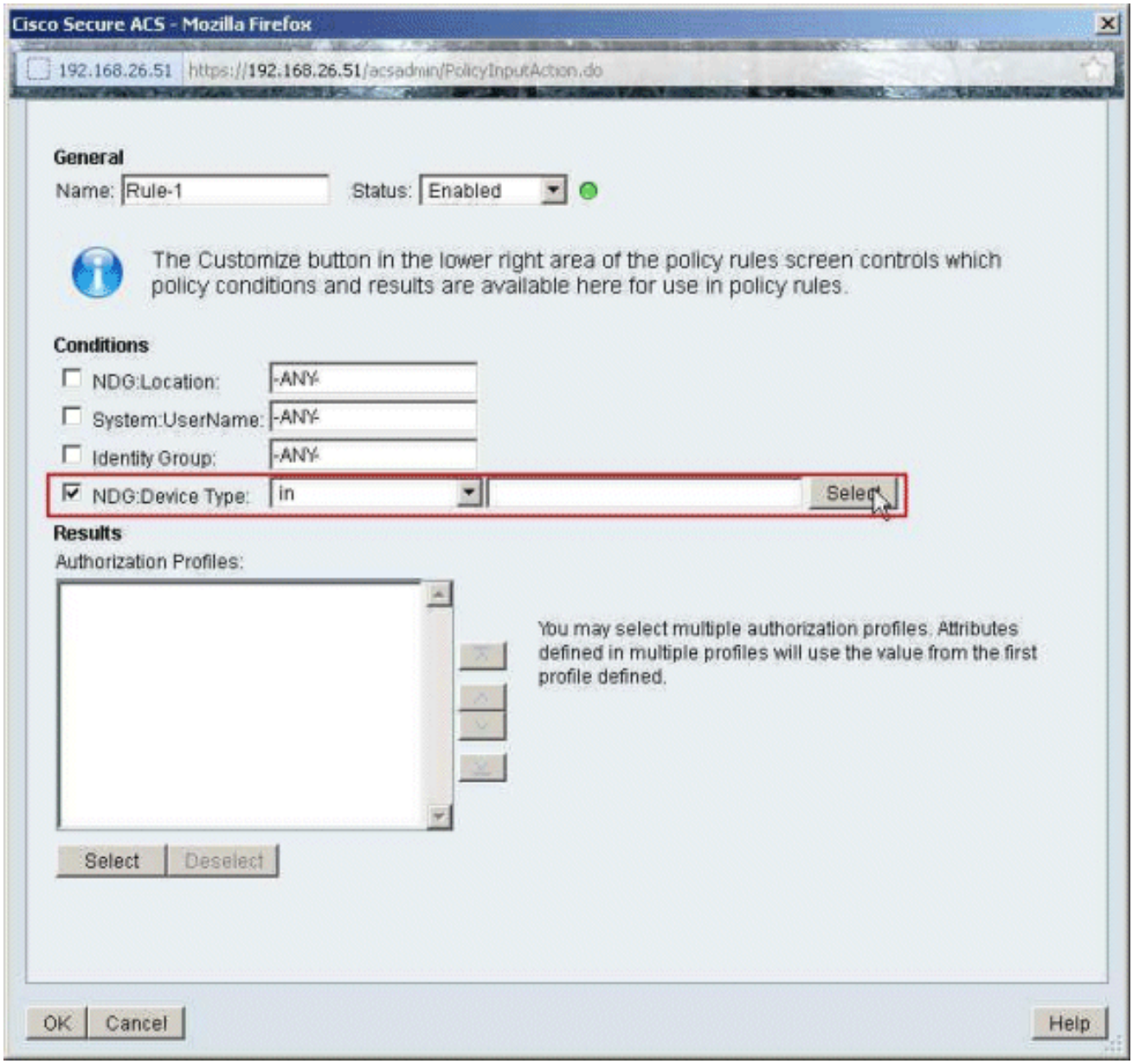


9. Per creare una nuova regola, fare clic su **Create**
(Crea).

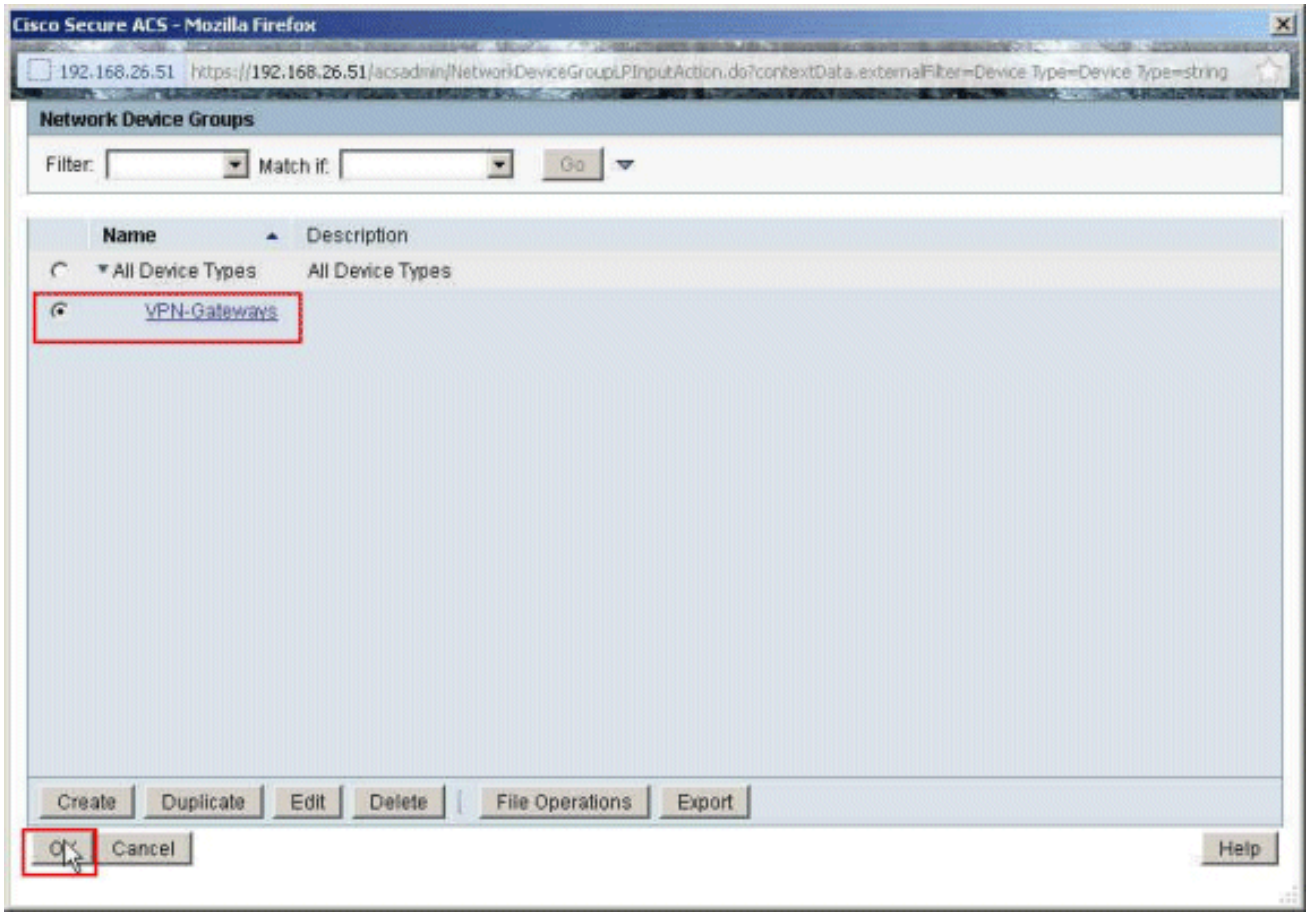


10. Assicurarsi che la casella di controllo accanto a **NDG:Tipo di dispositivo** sia selezionata e scegliere **in** dall'elenco a discesa. Fare clic su

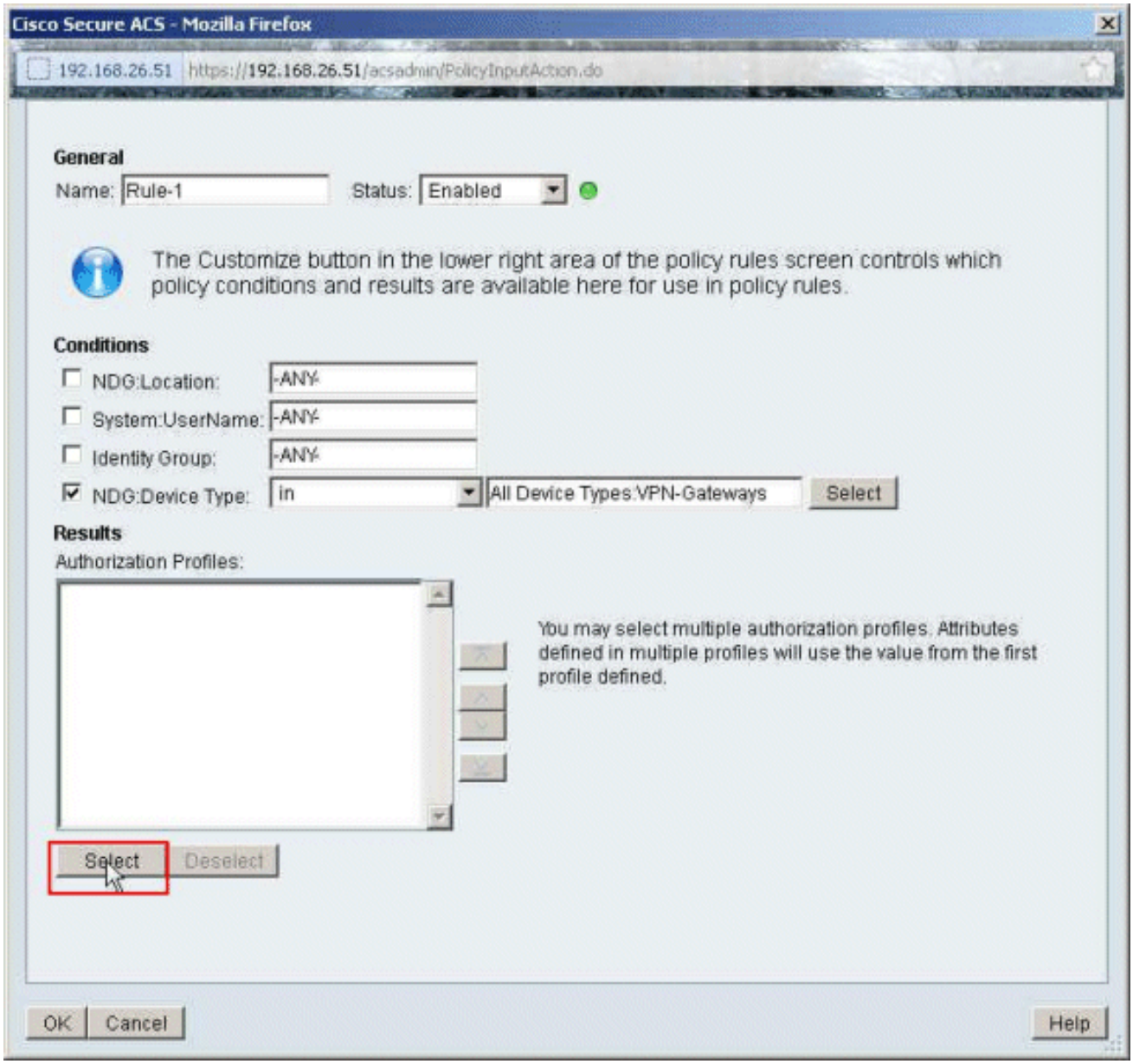
Seleziona.



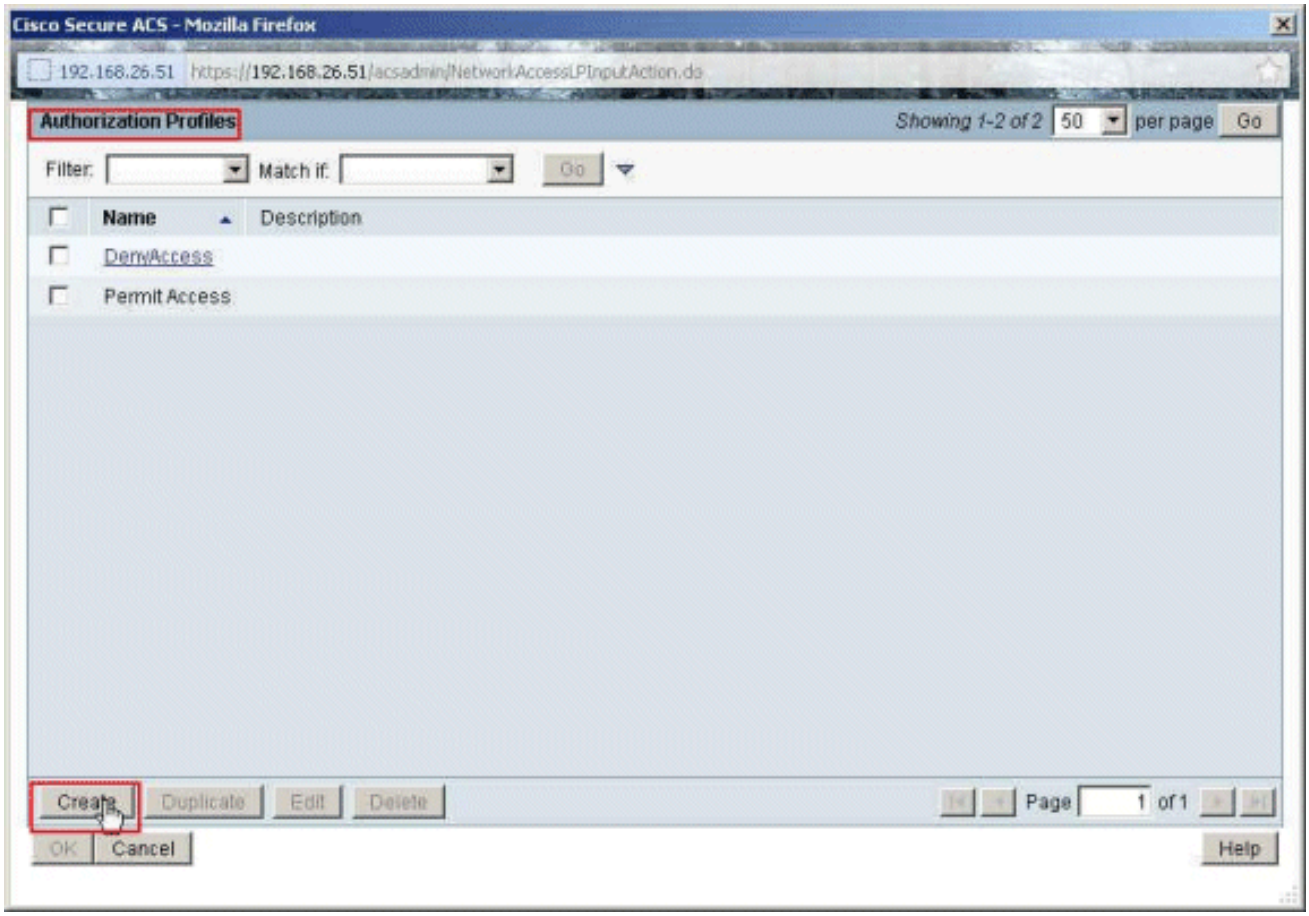
11. Scegliere il gruppo di dispositivi di rete **Gateway VPN** creato in precedenza e fare clic su **OK**.



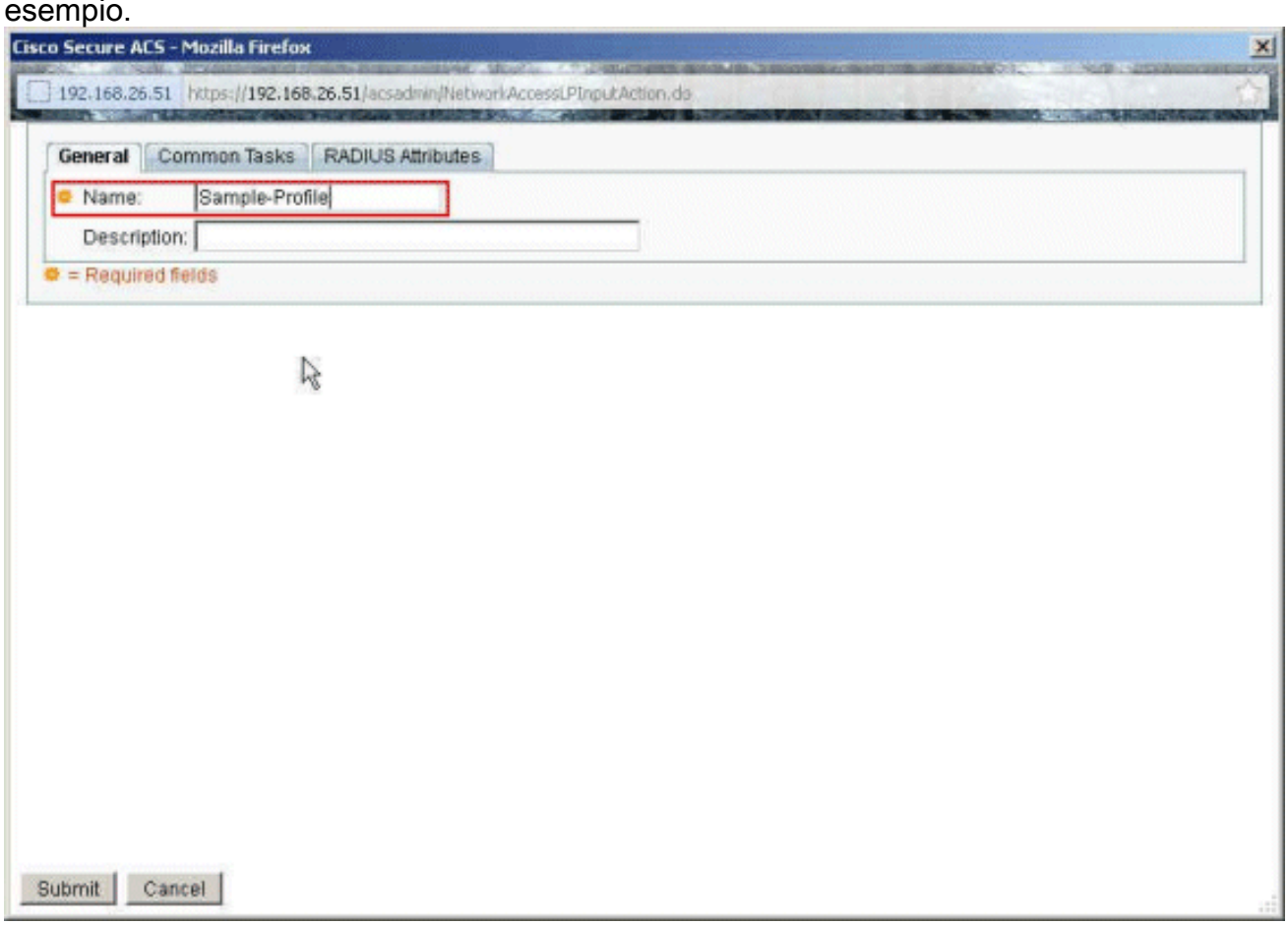
12. Fare clic su **Seleziona**.



13. Per creare un nuovo profilo di autorizzazione, fare clic su **Crea**.

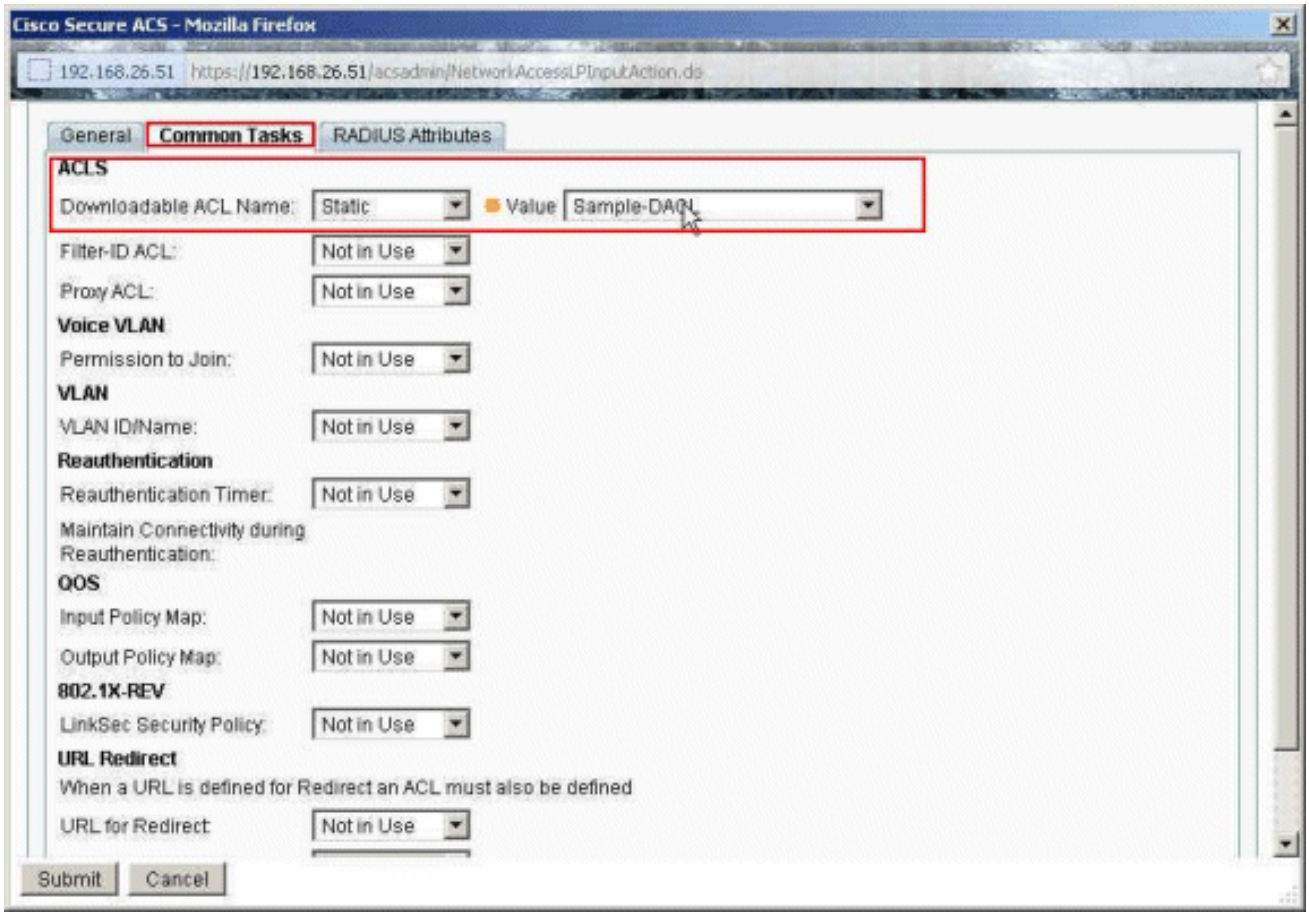


14. Specificare un nome per il **profilo di autorizzazione**. **Sample-Profile** è il nome utilizzato in questo
esempio.

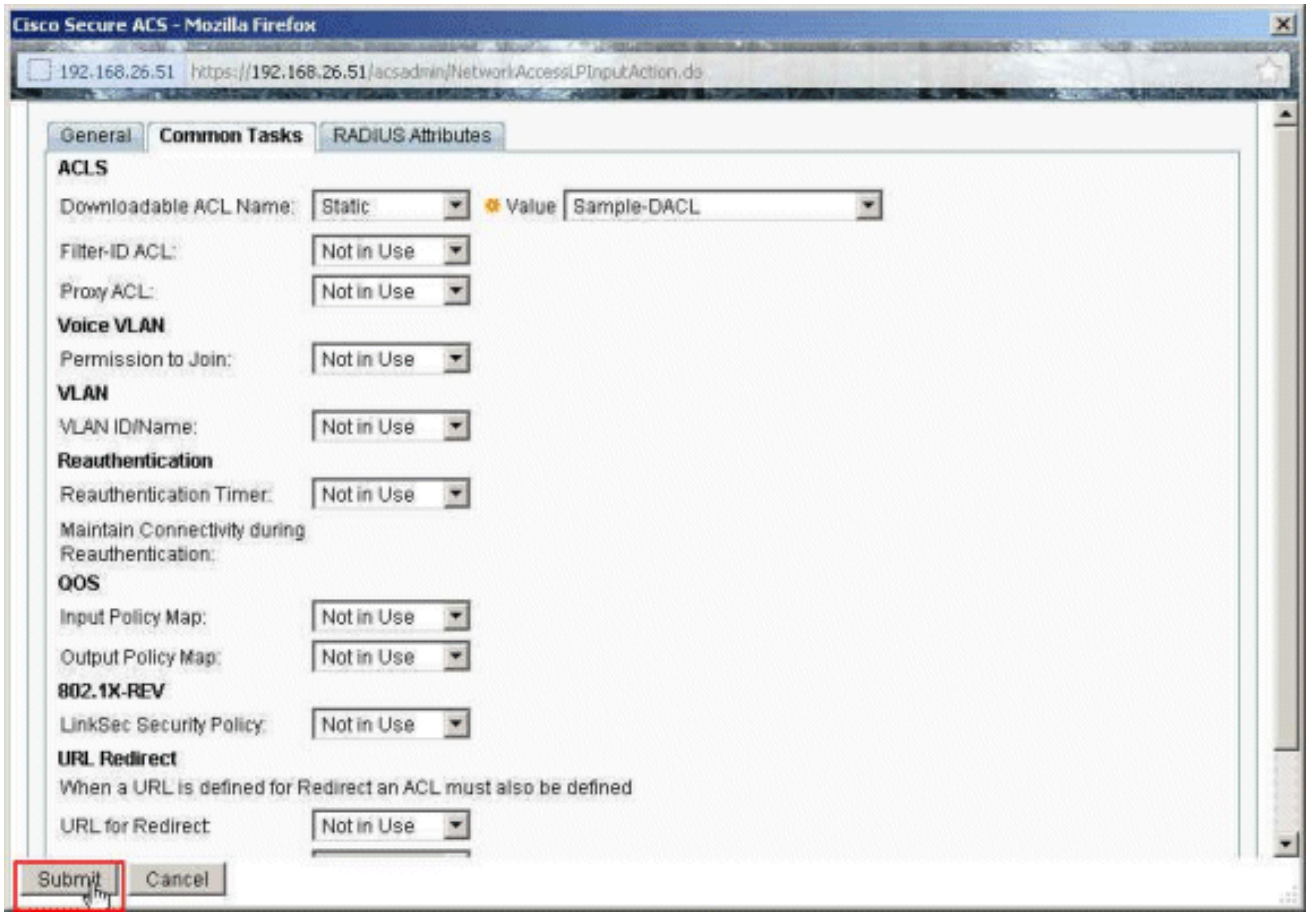


15. Scegliere la scheda **Common Tasks** e selezionare **Static** (Statica) dall'elenco a discesa per il nome dell'ACL scaricabile. Selezionare il nuovo **DACL (Sample-DACL)** creato dall'elenco

a discesa dei valori.

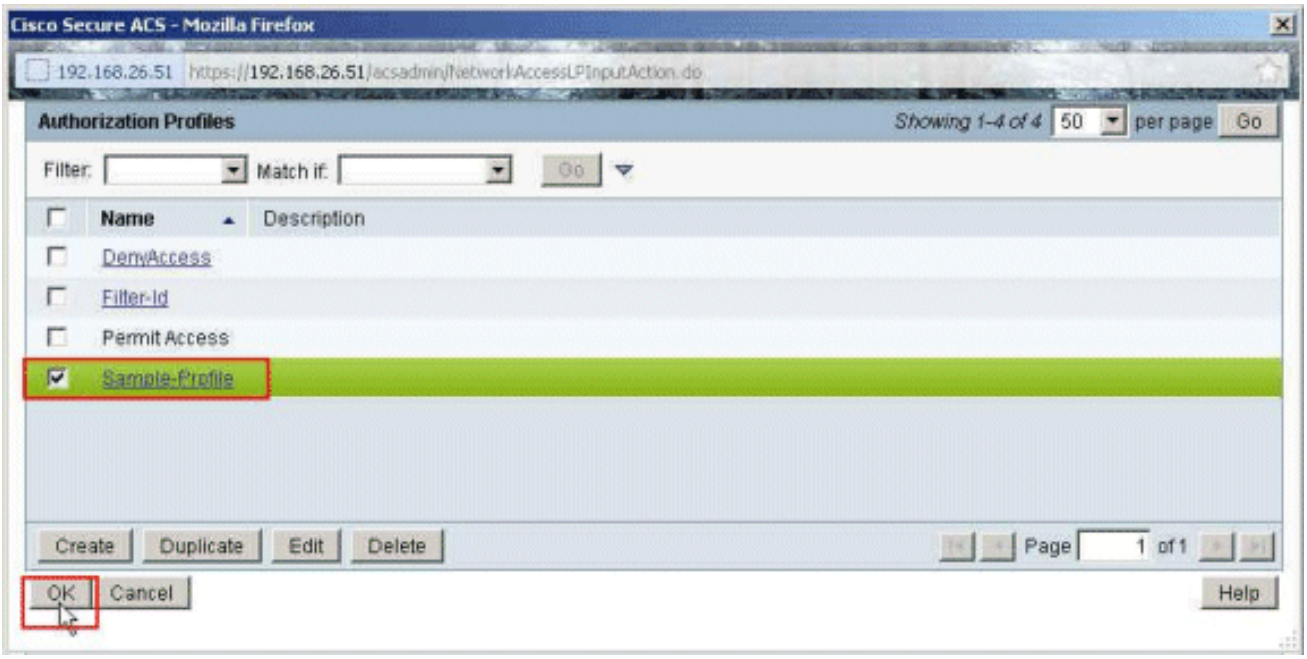


16. Fare clic su **Invia**.

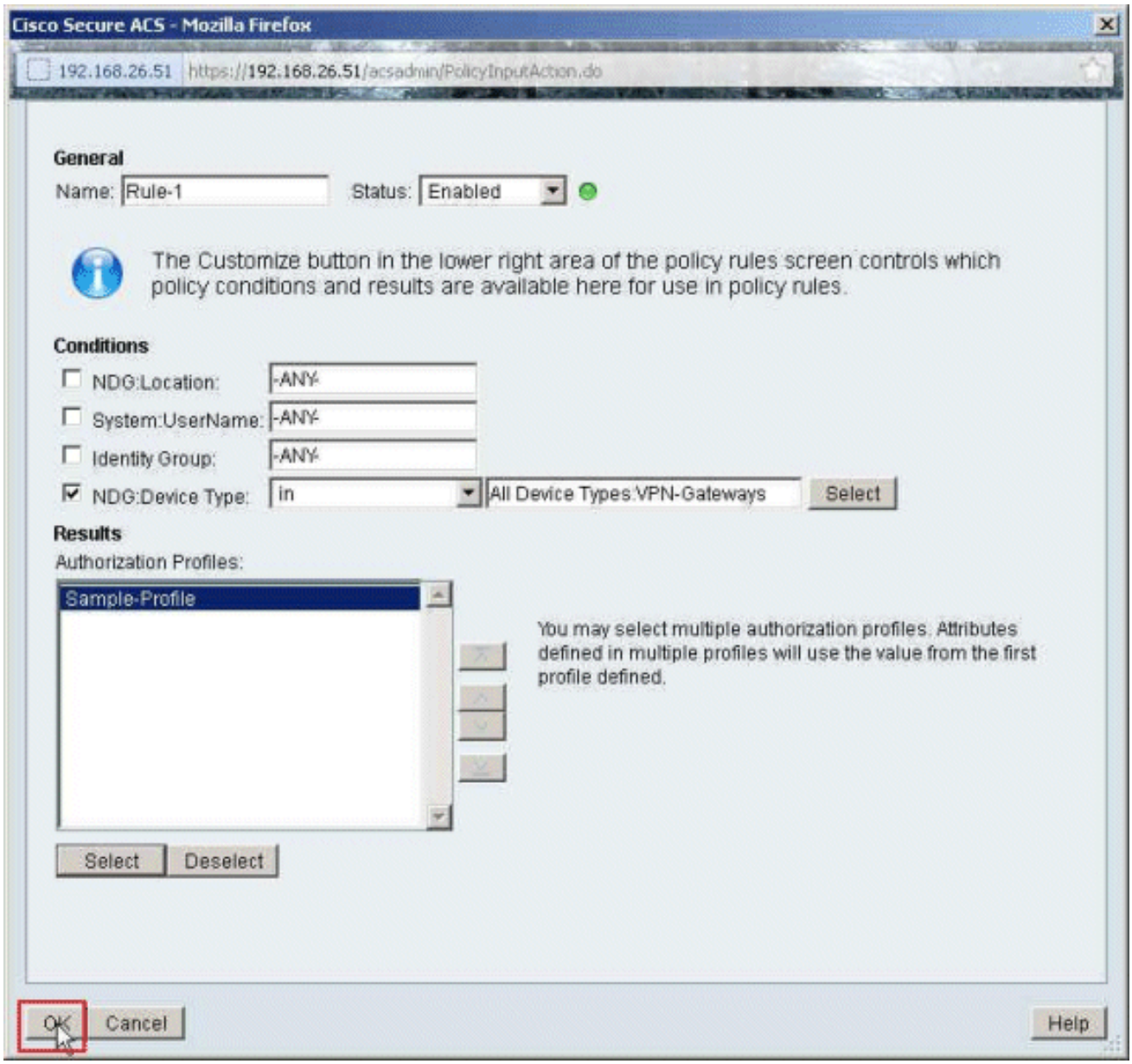


17. Selezionate **Sample-Profile** creato in precedenza e fate clic su

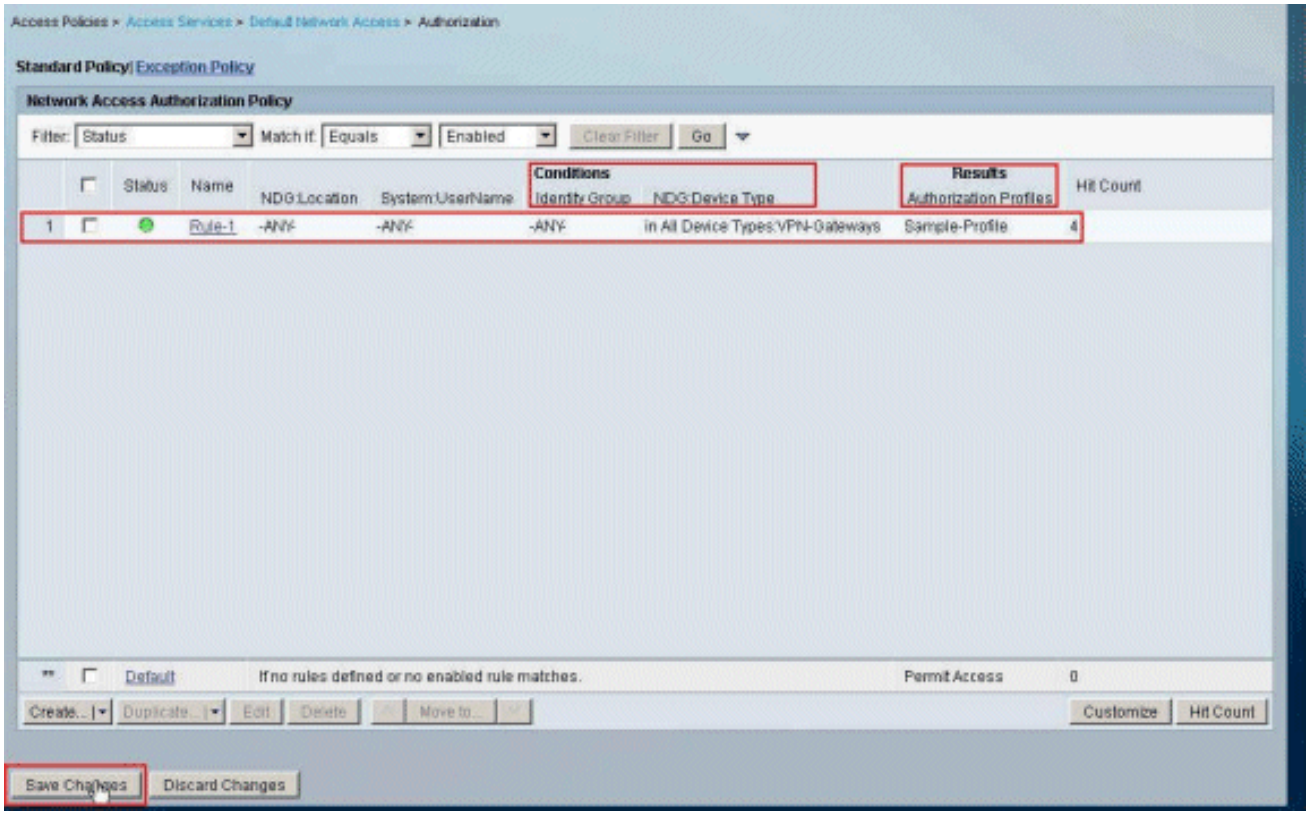
OK.



18. Fare clic su
OK.



19. Verificare che la **regola 1** venga creata con **VPN-Gateway** come condizione NDG:Device Type e come risultato **Sample-Profile**. Fare clic su **Salva modifiche**.



Configurare le impostazioni RADIUS IETF per un gruppo di utenti

Per scaricare dal server RADIUS il nome di un elenco degli accessi già creato sull'accessorio di sicurezza durante l'autenticazione, configurare l'attributo IETF RADIUS filter-id (numero attributo 11):

```
filter-id=acl_name
```

L'**utente** Sample-Group esegue l'autenticazione e il server RADIUS scarica un nome ACL (nuovo) per un elenco degli accessi già creato sull'appliance di sicurezza. L'utente "cisco" può accedere a tutti i dispositivi che si trovano all'interno della rete dell'ASA, **ad eccezione** del server 10.1.1.2. Per verificare l'ACL, consultare la sezione ACL Filter-Id.

Come mostrato nell'esempio, l'ACL con nome **new** è configurato per il filtro nell'appliance ASA:

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

Questi parametri vengono visualizzati solo quando sono veri. È stato configurato:

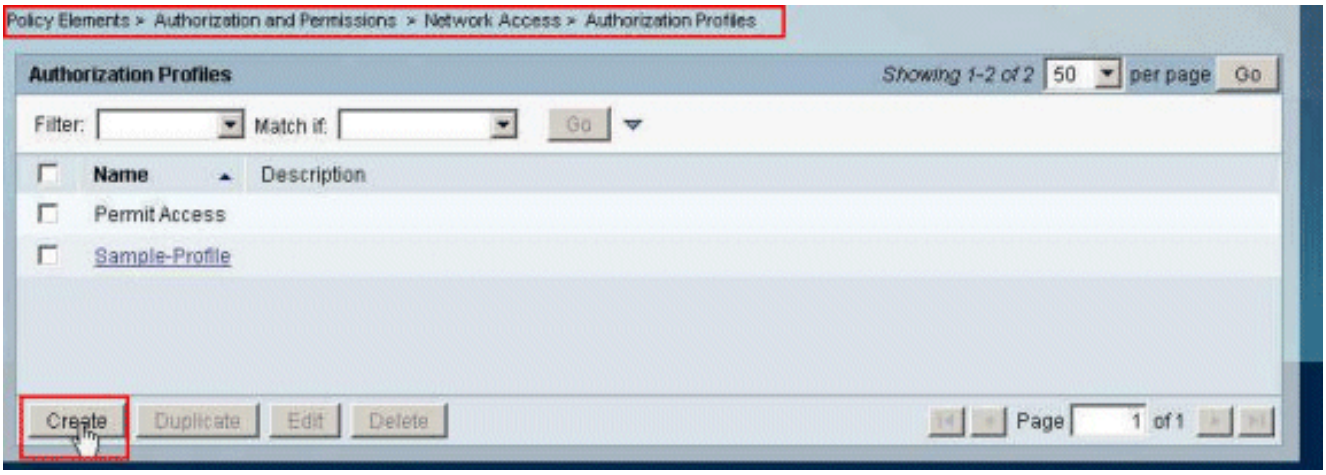
- Client AAA per utilizzare uno dei protocolli RADIUS in Configurazione rete
- Nella sezione dei risultati della regola in Access-Service viene selezionato un profilo di autorizzazione con ID filtro RADIUS (IETF).

Gli attributi RADIUS vengono inviati come profilo per ogni utente da ACS al client AAA richiedente.

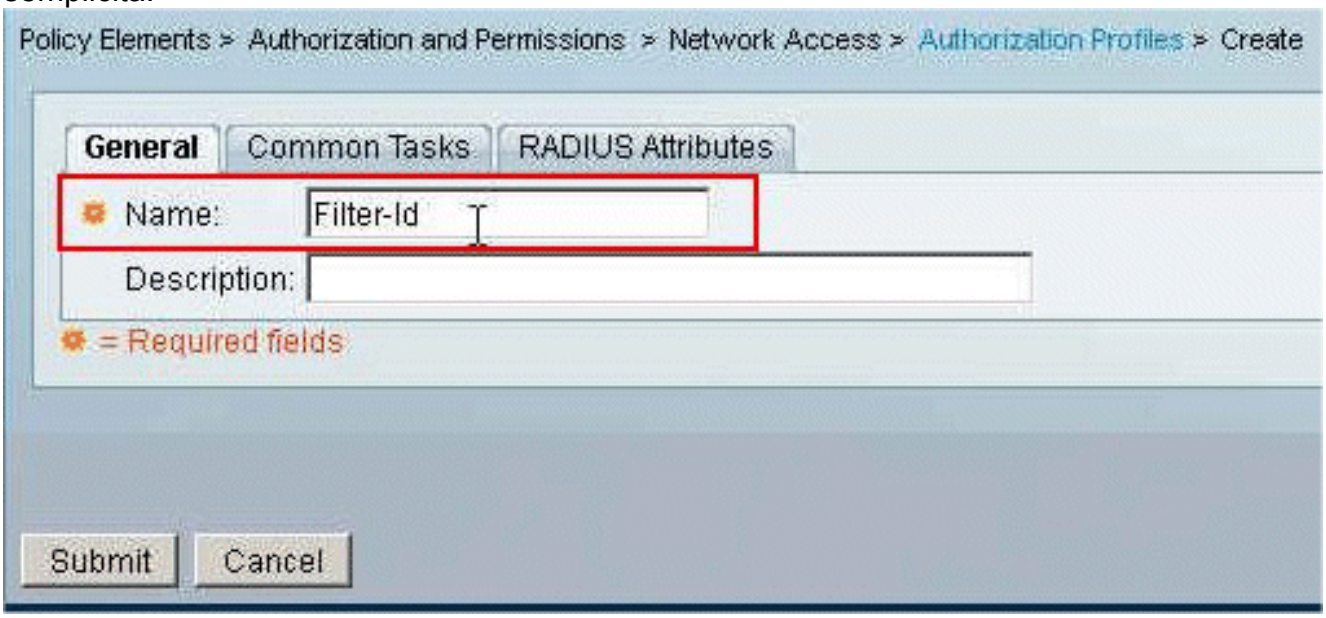
Completare i passaggi da 1 a 6 e da 10 a 12 di Configurazione di ACS per ACL scaricabili per un singolo utente, quindi i passaggi da 1 a 6 di Configurazione di ACS per ACL scaricabili per un gruppo, quindi eseguire i passaggi descritti in questa sezione per configurare Filter-Id in Cisco Secure ACS.

Per configurare le impostazioni degli attributi **RADIUS IETF** da applicare come nel profilo di autorizzazione, eseguire la procedura seguente:

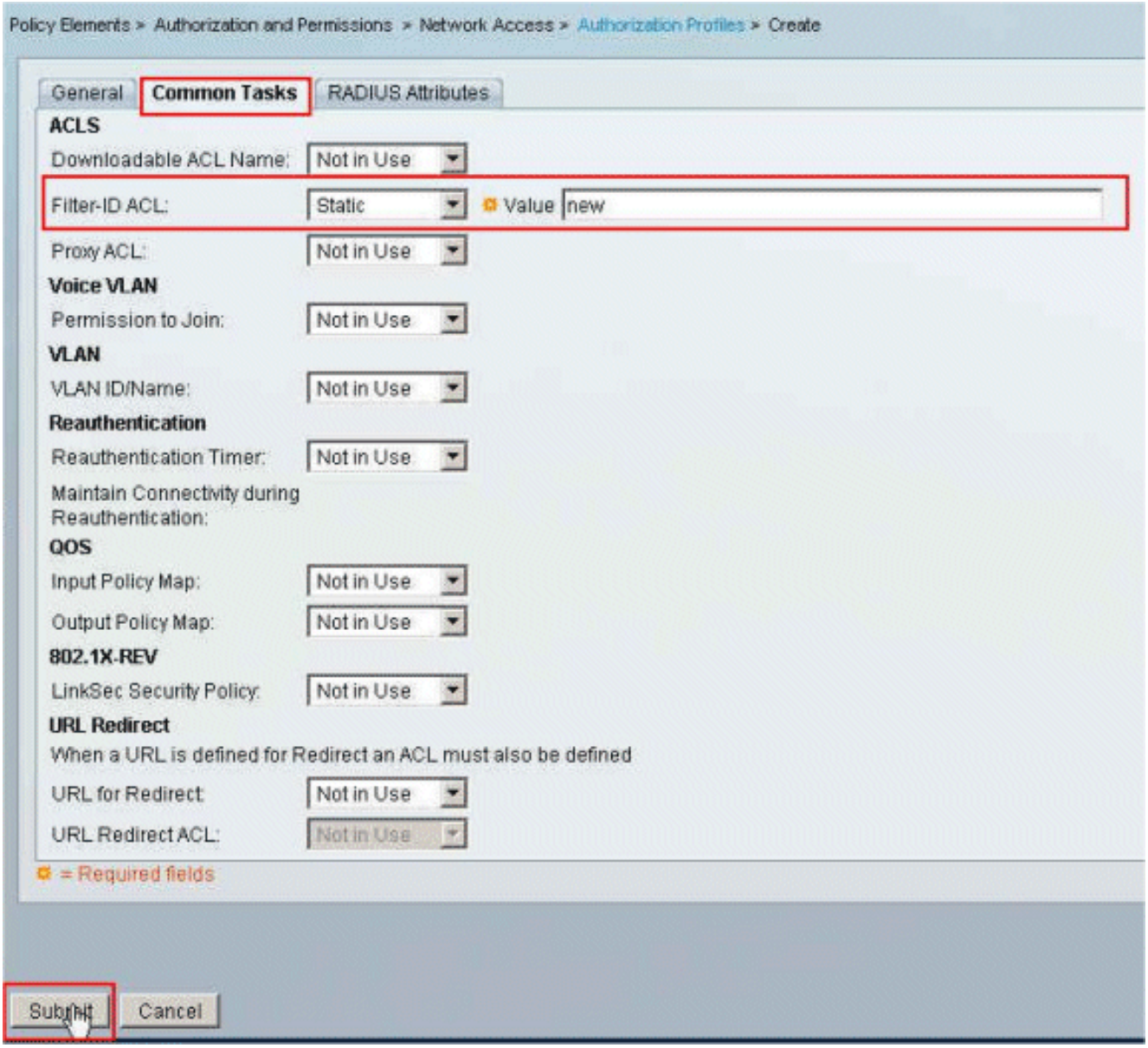
1. Scegliere Elementi dei criteri > **Autorizzazioni e autorizzazioni** > **Accesso di rete** > **Profili di autorizzazione**, quindi fare clic su **Crea** per creare un nuovo profilo di autorizzazione.



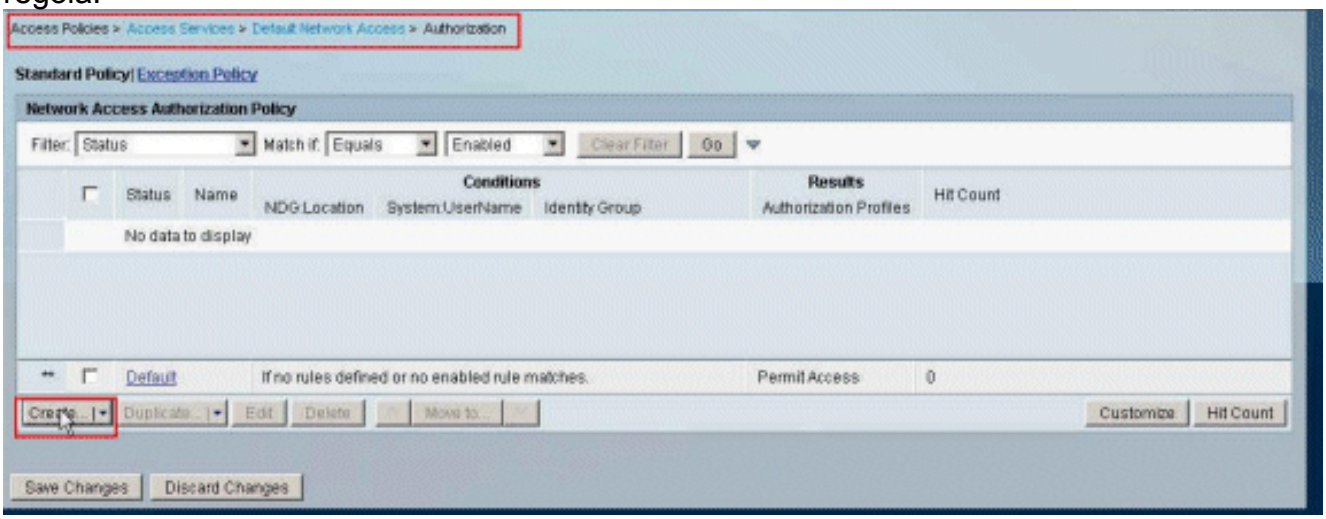
2. Specificare un nome per il **profilo di autorizzazione**. **Filter-Id** è il nome del profilo di autorizzazione scelto in questo esempio per semplicità.



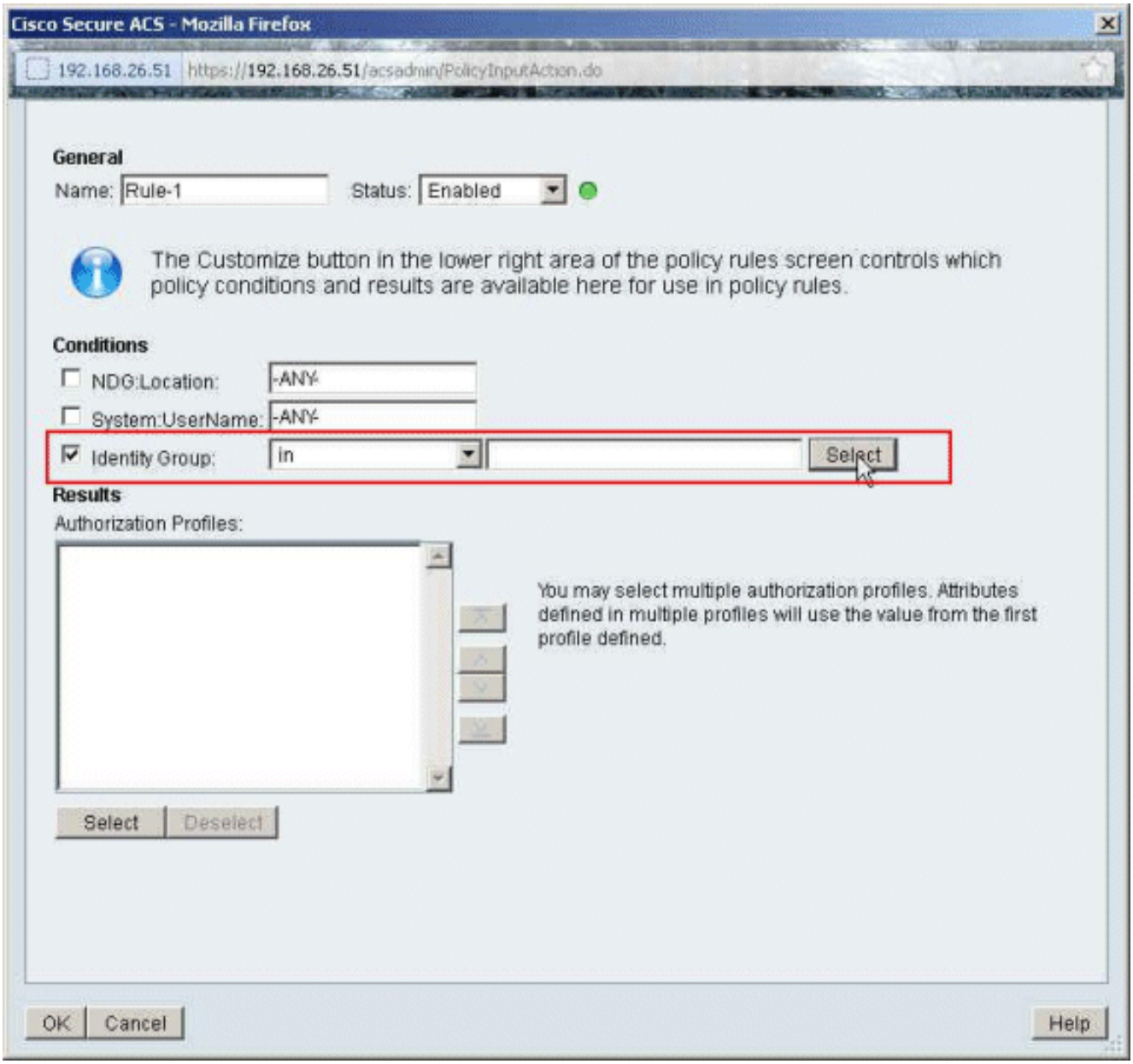
3. Fare clic sulla scheda **Attività comuni** e scegliere **Statico** dall'elenco a discesa per **ACL Filter-ID**. Immettere il nome dell'elenco accessi come **nuovo** nel campo Valore e fare clic su **Invia**.



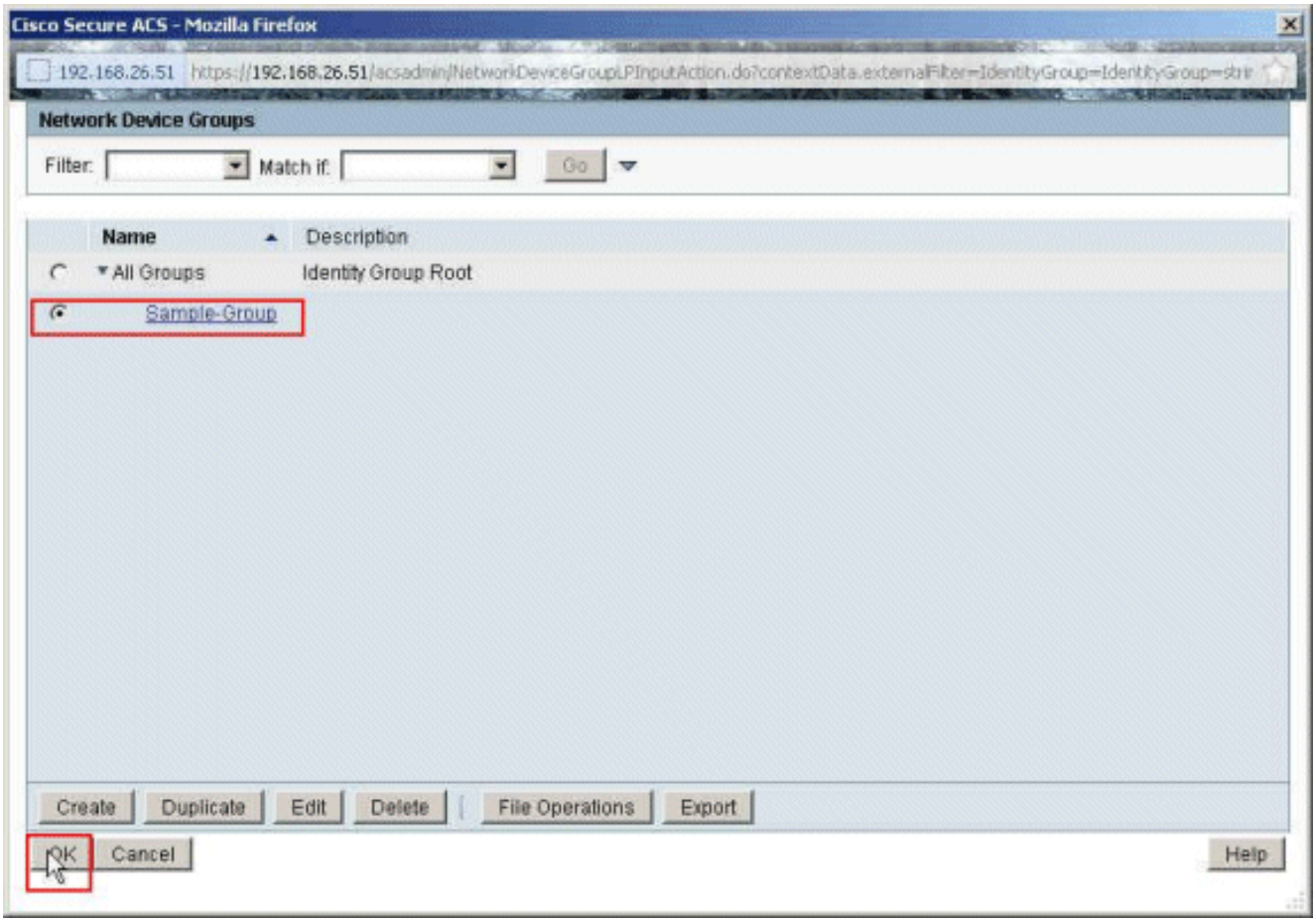
4. Scegliere Criteri di accesso > **Servizi di accesso** > **Accesso di rete predefinito** > **Autorizzazione**, quindi fare clic su **Crea** per creare una nuova regola.



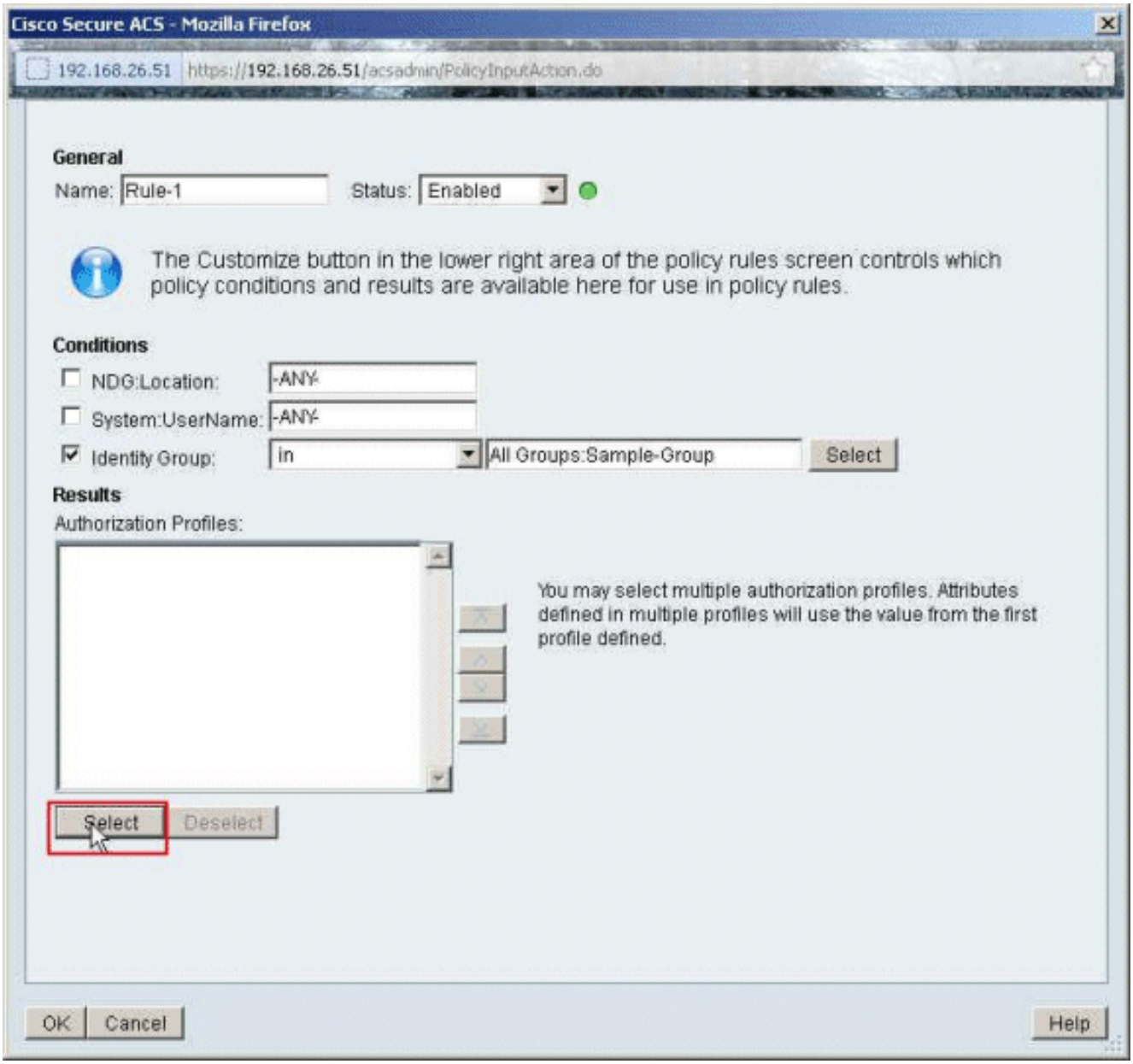
5. Verificare che la casella di controllo accanto a **Gruppo di identità** sia selezionata e fare clic su **Seleziona**.



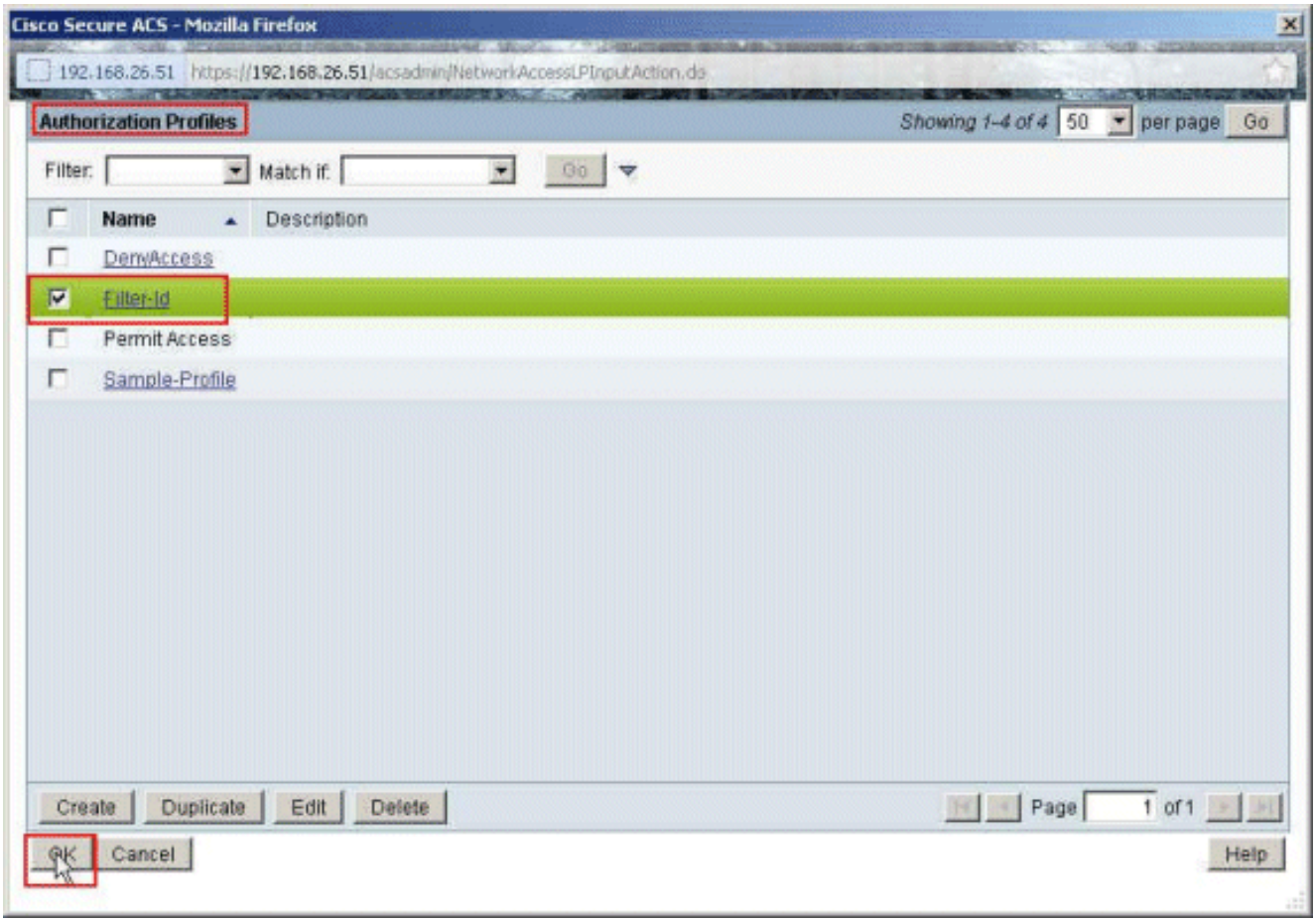
6. Selezionate **Sample-Group**, quindi fate clic su **OK**.



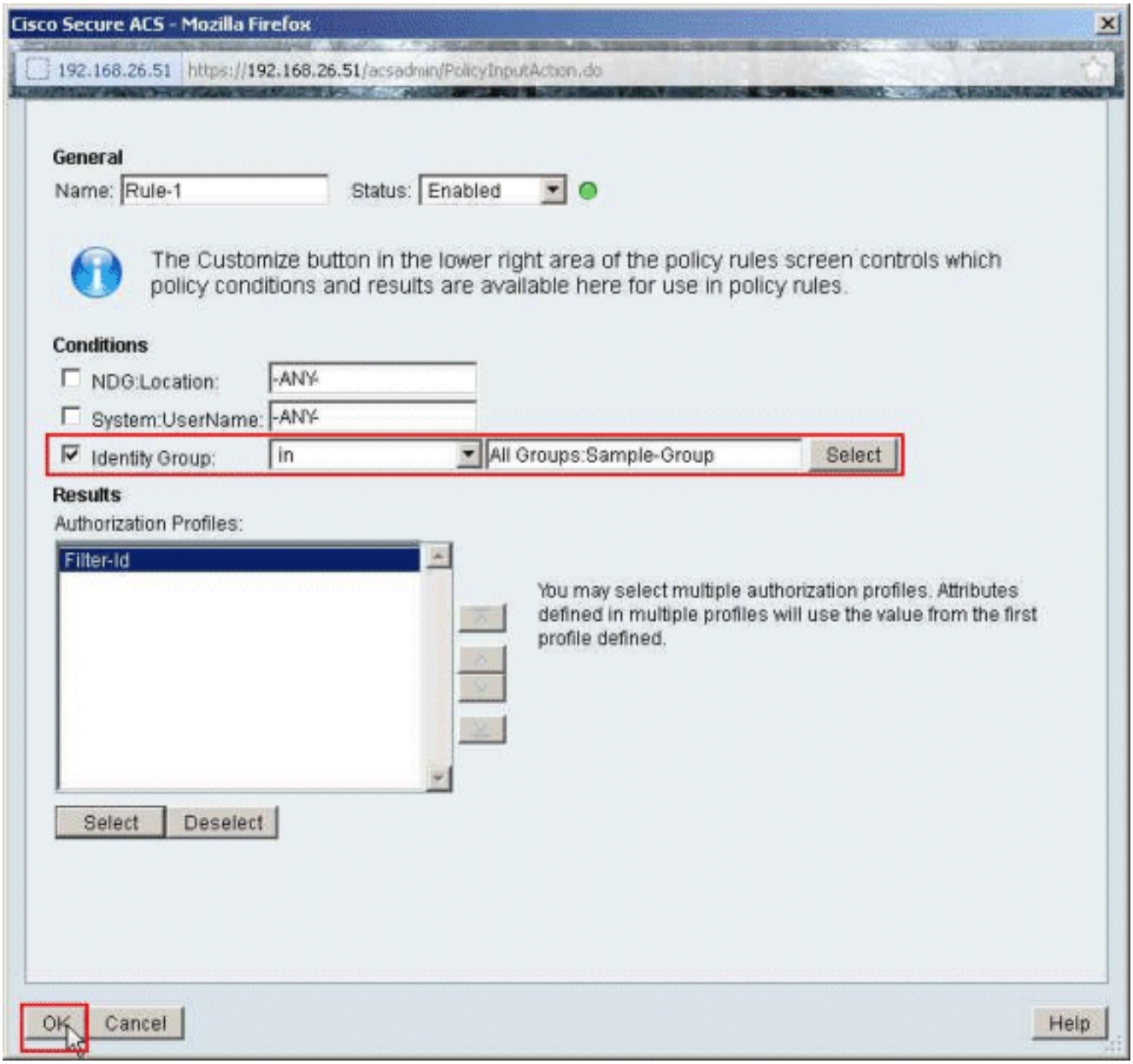
7. Fare clic su **Seleziona** nella sezione Profili di autorizzazione.



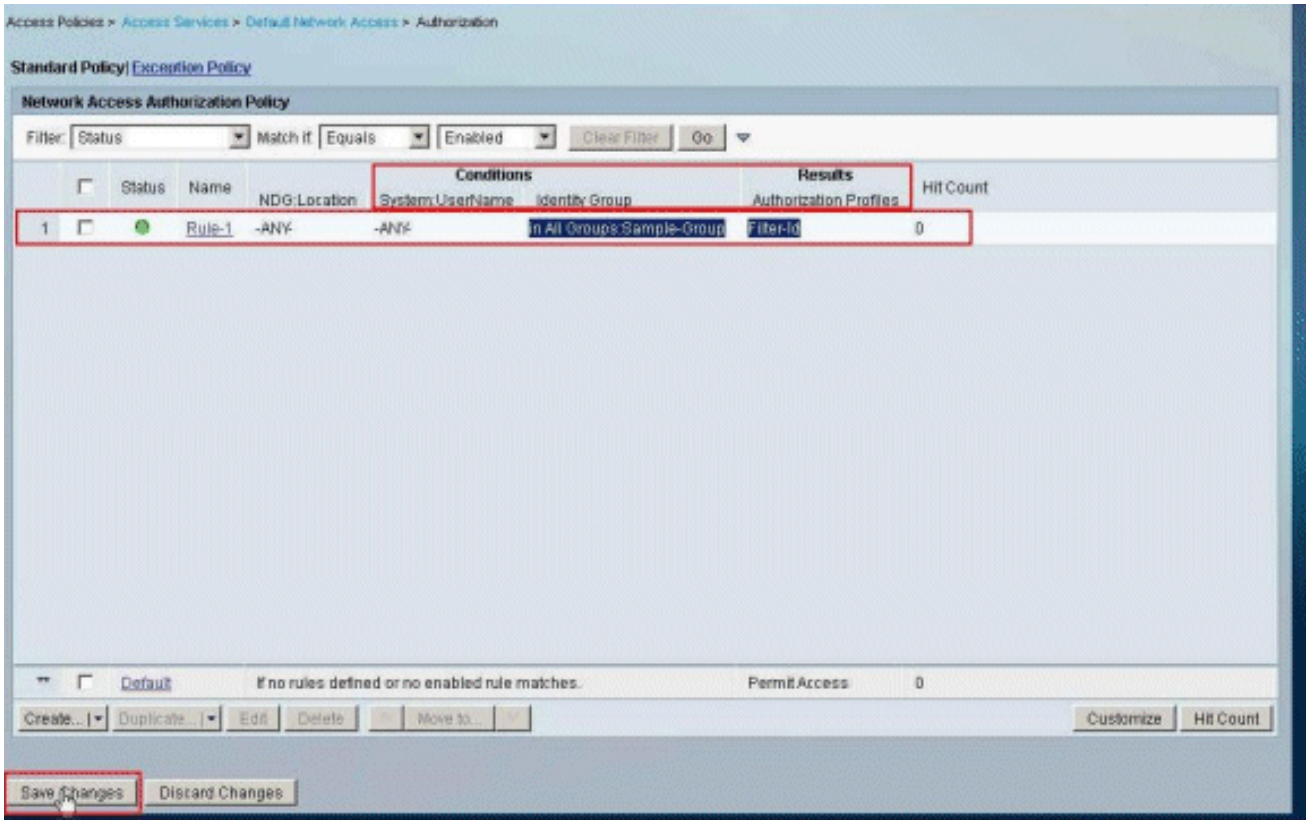
8. Scegliere l'**ID filtro del** profilo di autorizzazione creato in precedenza e fare clic su **OK**.



9. Fare clic su **OK**.



10. Verificare che **Rule-1** sia stato creato con Identity Group **Sample-Group** come condizione e **Filter-Id** come risultato. Fare clic su **Salva modifiche**.

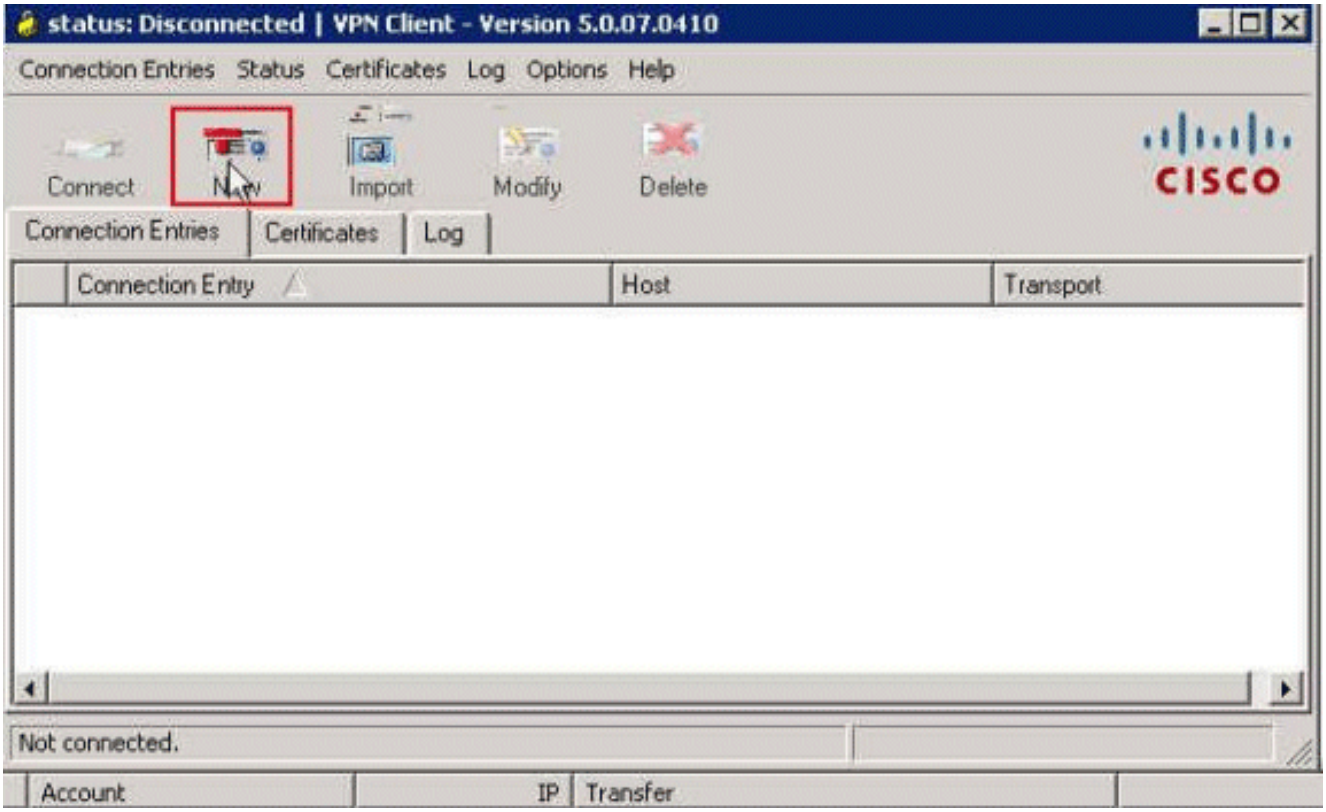


Configurazione client VPN Cisco

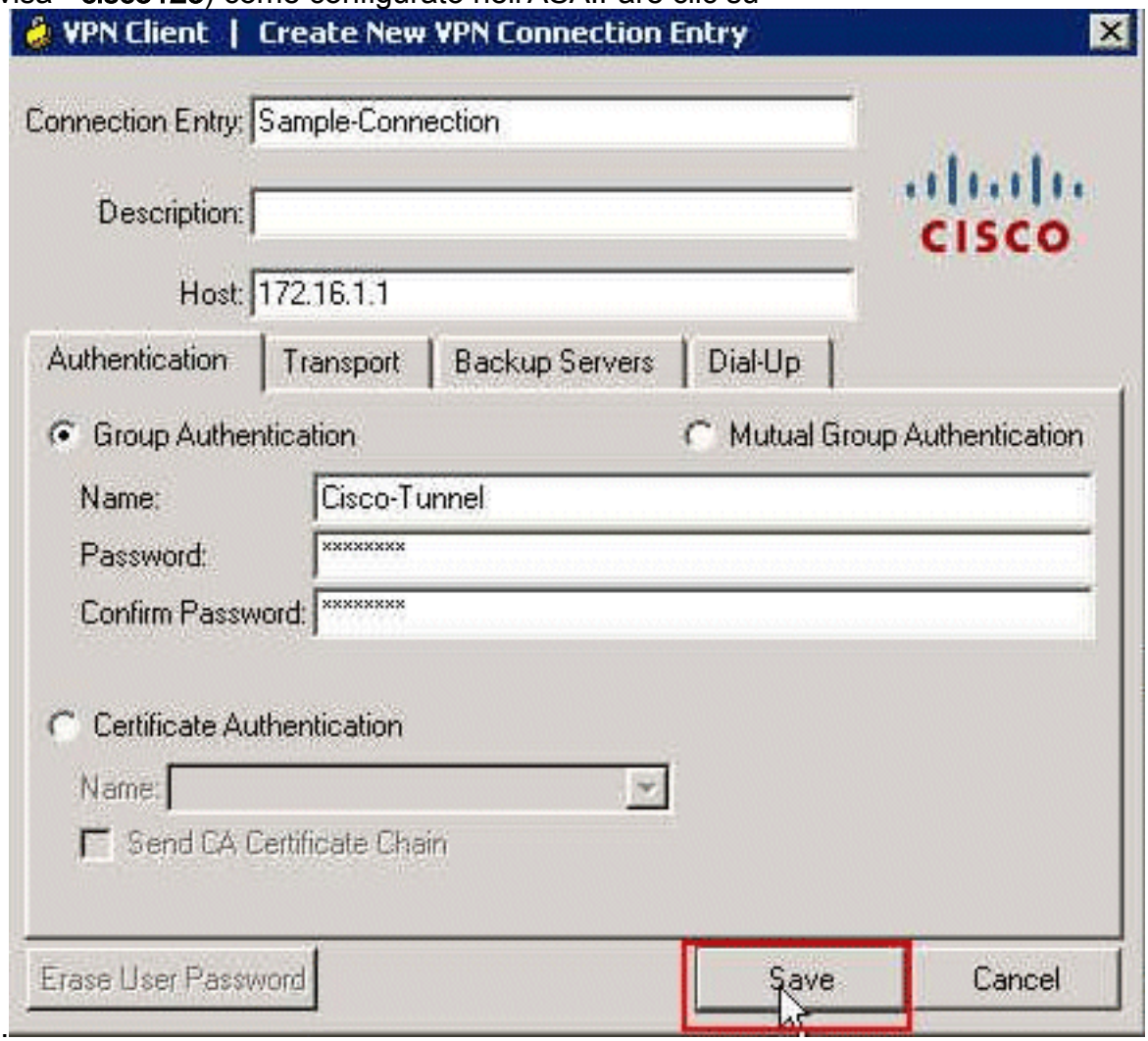
Per verificare che l'ASA sia configurata correttamente, connettersi all'appliance Cisco ASA con il client VPN Cisco.

Attenersi alla seguente procedura:

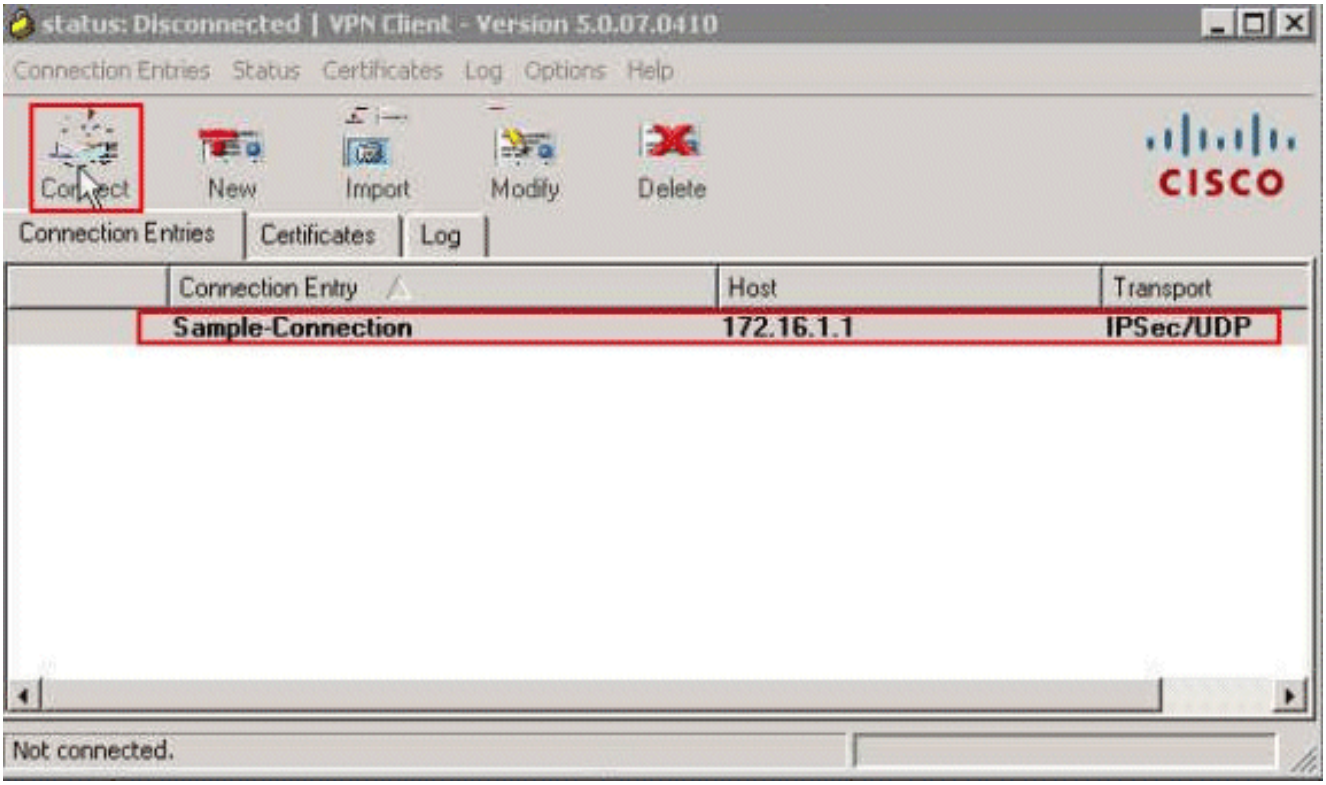
1. Scegliere **Start > Programmi > Cisco Systems VPN Client > VPN Client**.
2. Fare clic su **New** per avviare la finestra Create New VPN Connection Entry (Crea nuova voce di connessione
   VPN).



3. Specificare i dettagli della nuova connessione:Immettere il nome della voce di connessione insieme a una descrizione.Immettere l'**indirizzo IP esterno dell'appliance ASA** nella casella Host.Immettere il nome del gruppo di tunnel VPN (**Cisco-Tunnel**) e la password (chiave già condivisa - **cisco123**) come configurato nell'ASA.Fare clic su **Salva**.

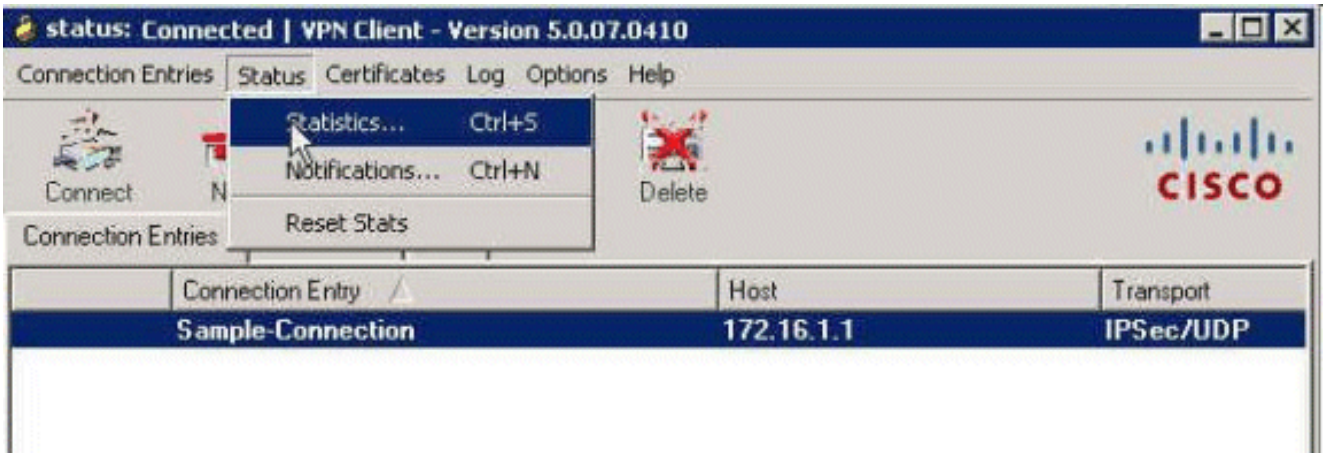


4. Fare clic sulla connessione che si desidera utilizzare e fare clic su **Connetti** nella finestra principale del client
VPN.



5. Quando richiesto, immettere il nome utente **cisco** e la password **cisco123** come configurato nell'appliance ASA per l'autenticazione e fare clic su **OK** per connettersi alla rete
remota.

6. Una volta stabilita la connessione, scegliere **Statistics** dal menu Status per verificare i dettagli del
tunnel.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Mostra comandi di crittografia

- **show crypto isakmp sa**: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.

```
ciscoasa# sh crypto isakmp sa

IKEv1 SAs:

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

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

- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

```
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 scaricabile per utente/gruppo

Verificare l'ACL scaricabile per l'utente Cisco. Gli ACL vengono scaricati dai 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 Filter-Id

L'ID filtro [011] è stato applicato al gruppo Group - Sample-Group e gli utenti del gruppo vengono filtrati in base all'ACL (nuovo) definito nell'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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione. Viene visualizzato anche l'output di esempio del comando **debug**.

Nota: per ulteriori informazioni sulla risoluzione dei problemi relativi alla VPN IPsec di accesso remoto, vedere Soluzioni per la risoluzione dei problemi relativi alla VPN IPsec di accesso remoto e L2L più comuni.

Cancella associazioni di protezione

Quando si esegue la risoluzione dei problemi, assicurarsi di cancellare le associazioni di

protezione esistenti dopo aver apportato una modifica. In modalità privilegiata di PIX, utilizzare i seguenti comandi:

- **clear [crypto] ipsec sa** - Elimina le SA IPsec attive. La parola chiave crypto è facoltativa.
- **clear [crypto] isakmp sa** - Elimina le associazioni di protezione IKE attive. La parola chiave crypto è facoltativa.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug crypto ipsec 7**: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp 7**: visualizza le negoziazioni ISAKMP della fase 1.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance - Pagina di supporto
- Riferimenti per i comandi di Cisco ASA serie 5500 Adaptive Security Appliance
- Cisco Adaptive Security Device Manager
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- Pagina di supporto per Cisco VPN Client
- Cisco Secure Access Control System
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems