ASA 8.3 en later: RADIUS-autorisatie (ACS 5.x) voor VPN-toegang met downloadbare ACL's met CLI- en ASDM-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u het security apparaat moet configureren om gebruikers te controleren op basis van een netwerktoegang. Aangezien u impliciet RADIUS-autorisaties kunt inschakelen, bevat dit document geen informatie over de configuratie van RADIUS-autorisatie op het beveiligingsapparaat. Het geeft wel informatie over hoe het beveiligingsapparaat omgaat met informatie over toegangslijsten die van RADIUS-servers wordt ontvangen.

U kunt een RADIUS-server configureren om een toegangslijst naar het beveiligingsapparaat te downloaden of een toegangslijst met naam op het moment van verificatie. De gebruiker is geautoriseerd om alleen te doen wat is toegestaan in de gebruikersspecifieke toegangslijst.

Downloadbare toegangslijsten zijn de meest schaalbare methoden wanneer u Cisco Secure Access Control Server (ACS) gebruikt om de juiste toegangslijsten voor elke gebruiker te bieden. Raadpleeg voor meer informatie over de functies van de toegangslijst en de Cisco Secure ACS het configureren van een RADIUS-server om downloadbare toegangscontrolelijsten en downloadbare IP-ACL's te verzenden.

Raadpleeg ASA/PIX 8.x: Radius Authorization (ACS) voor Netwerktoegang met behulp van downloadbare ACL met CLI en ASDM Configuration Voorbeeld voor de identieke configuratie op Cisco ASA met versies 8.2 en eerder.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de adaptieve security applicatie (ASA) volledig gebruiksklaar is en geconfigureerd om Cisco adaptieve security applicatie Manager (ASDM) of CLI in staat te stellen configuratie veranderingen door te voeren.

Opmerking: Raadpleeg HTTPS Access voor ASDM om het apparaat op afstand te kunnen configureren door de ASDM of Secure Shell (SSH).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA-softwarerelease 8.3 en hoger
- Cisco ASDM versie 6.3 en hoger
- Cisco VPN-clientversie 5.x en hoger
- Cisco Secure ACS 5.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

U kunt IP ACL's downloaden om sets ACL's (ACL's) te maken van definities die u op veel gebruikers of gebruikersgroepen kunt toepassen. Deze reeksen ACL-definities worden ACL-inhoud genoemd.

Downloadbare IP-ACL's werken op deze manier:

1. Wanneer ACS een gebruiker toegang tot het netwerk verleent, bepaalt ACS of een downloadbare IP ACL wordt toegewezen aan het machtigingsprofiel in de resultaatsectie.

2. Als ACS zich op een downloadbare IP-ACL bevindt die aan het Automation Profile is toegewezen, stuurt ACS een eigenschap (als deel van de gebruikerssessie, in het RADIUS-toegangspakket) die de genoemde ACL specificeert, en de versie van de genoemde ACL.
3. Als de AAA-client reageert dat de huidige versie van ACL in zijn cache niet beschikbaar is (dat wil zeggen dat ACL nieuw is of is gewijzigd), stuurt ACS de ACL (nieuw of bijgewerkt) naar het apparaat.

Downloadbare IP-ACL's zijn een alternatief voor de configuratie van ACL's in de RADIUS Cisco cisco-av-paareigenschap [26/9/1] van elke gebruiker of gebruikersgroep. U kunt eenmaal een downloadbare IP ACL-toegangsapparaat maken, deze een naam geven en vervolgens de downloadbare IP-naar-elk machtigingsprofiel toewijzen als u de naam ervan verwijst. Deze methode is efficiënter dan als u de RADIUS-Cisco cisco-av-paareigenschap van RADIUS vormt voor het autorisatieprofiel.

Wanneer u de ACL-definities in de ACS-web interface invoert, gebruik dan geen sleutelwoord of naamvermeldingen; Gebruik in alle andere opzichten de standaard ACL-opdrachtsyntaxis en -semantiek voor de AAA-client waarop u de downloadbare IP ACL-ACL wilt toepassen. De ACL-definities die u in ACS invoert, omvatten een of meer ACL-opdrachten. Elke ACL-opdracht moet op een aparte lijn staan.

In ACS kunt u meerdere downloadbare IP-ACL's definiëren en gebruiken in verschillende autorisatieprofielen. Gebaseerd op de voorwaarden in de regels van de Vergunning van de Toegangsdienst kunt u verschillende Bewerkingen van de Vergunning verzenden die IP ACLs bevatten kunnen downloaden naar verschillende AAA klanten.

Verder kunt u de volgorde van de ACL-inhoud wijzigen in een downloadbare IP-ACL. ACS onderzoekt ACL-inhoud, vanaf de bovenkant van de tabel, en downloads de eerste ACL-inhoud die deze vindt. Wanneer u de volgorde instelt, kunt u de systeemefficiëntie garanderen als u de meest toepasselijke ACL-inhoud hoger in de lijst plaatst.

Om IP ACL op een bepaalde AAA-client te kunnen downloaden, moet de AAA-client deze regels naleven:

- Gebruik RADIUS voor verificatie
- Ondersteuning van downloadbare IP ACL's

Dit zijn voorbeelden van Cisco-apparaten die IP ACL's ondersteunen die kunnen worden gedownload:

- ASA
- Cisco-apparaten die IOS versie 12.3(8)T en hoger uitvoeren

Dit is een voorbeeld van het formaat dat u moet gebruiken om ASA ACLs in het vak ACL-definities in te voeren:

```
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
```

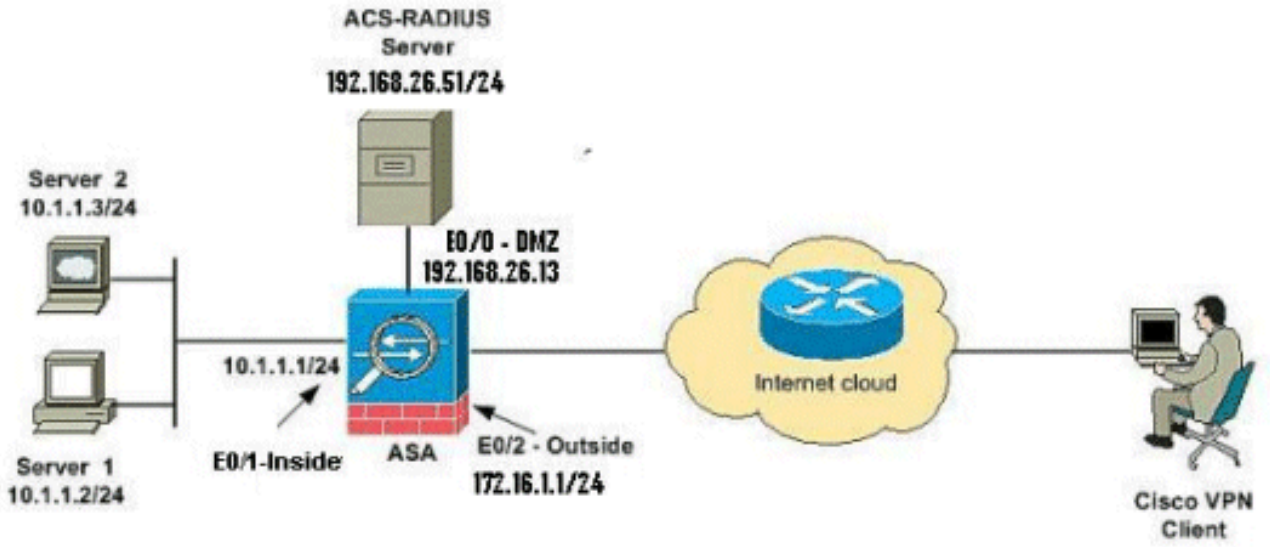
```
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



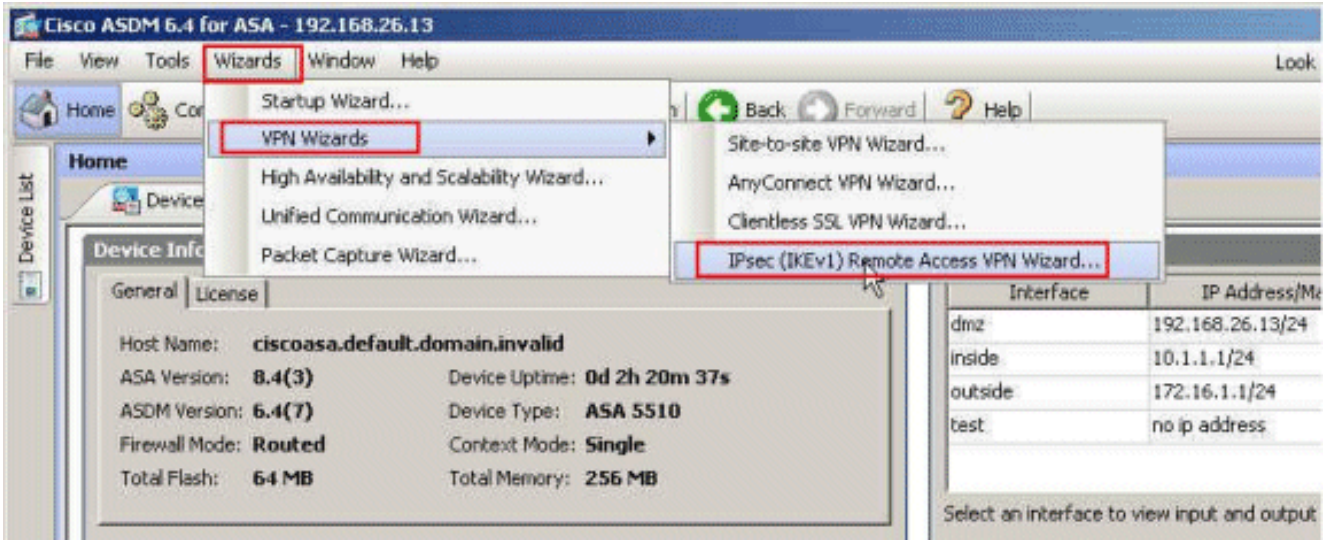
Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918-adressen die in een labomgeving werden gebruikt.

Externe toegang instellen (IPsec)

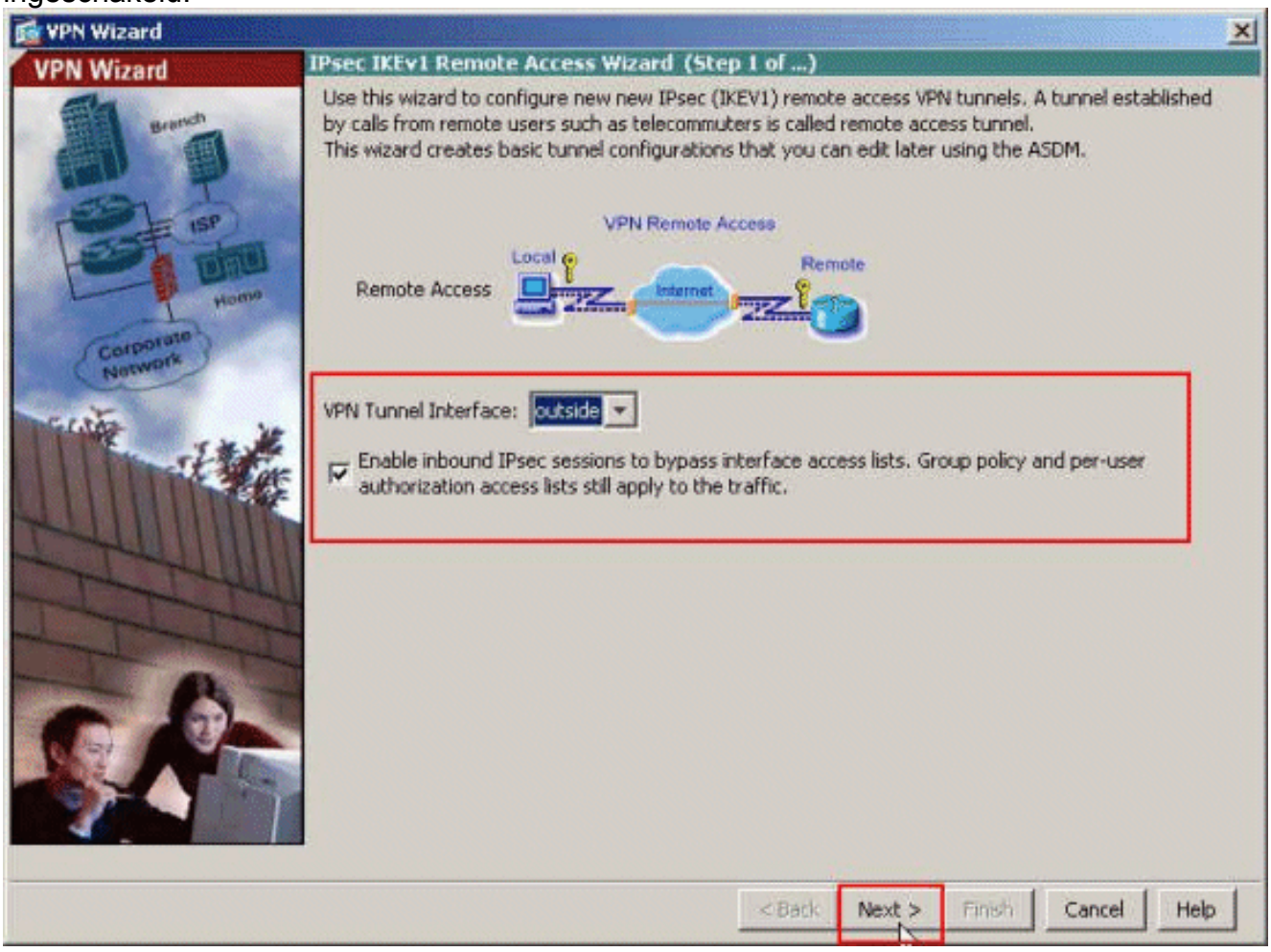
ASDM-procedure

Voltooi deze stappen om de externe VPN-toegang te configureren:

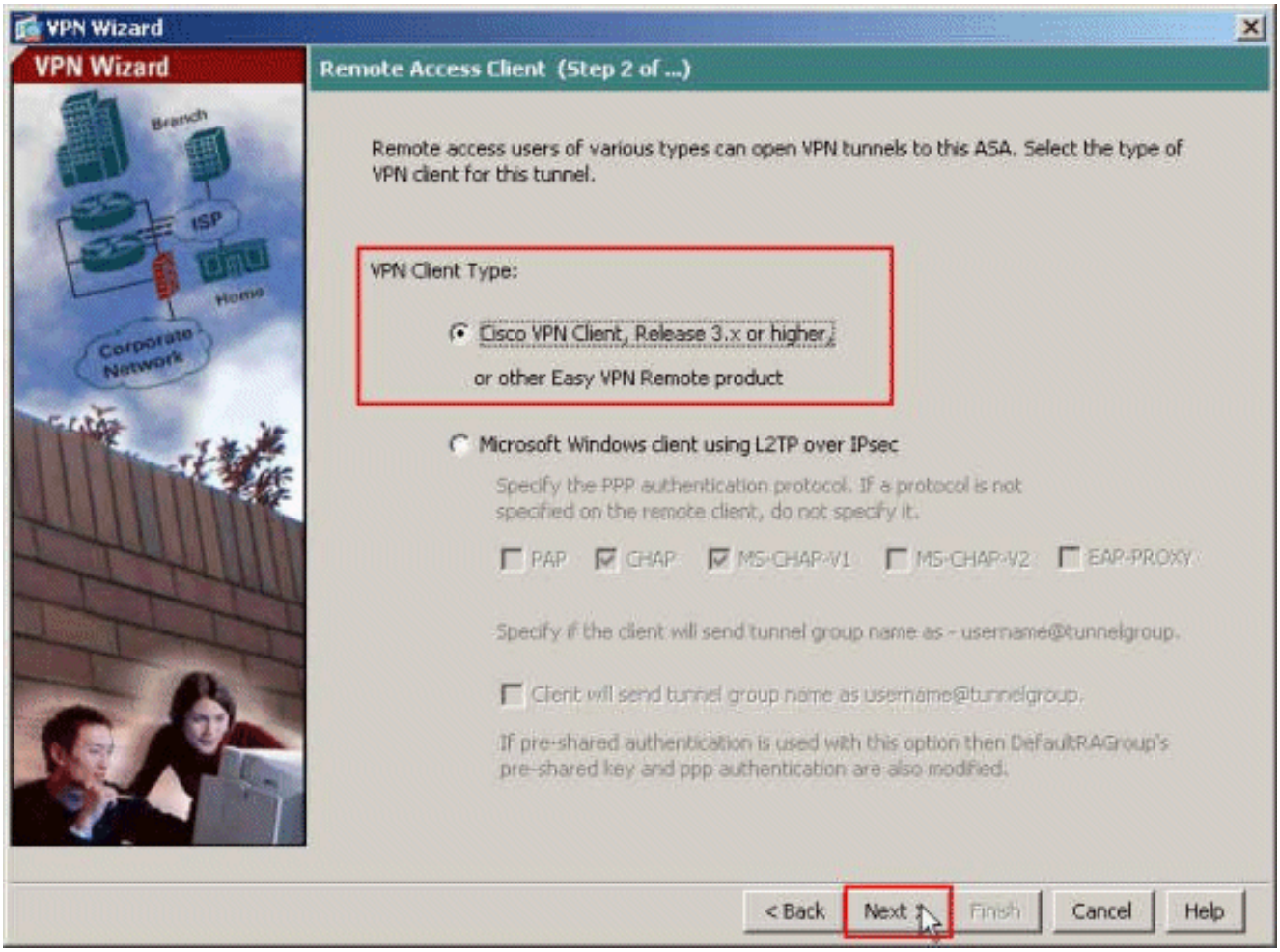
1. Selecteer **Wizard > VPN-wizard > IPsec (IKEv1) externe VPN-toegangswizard** vanuit het Home
venster.



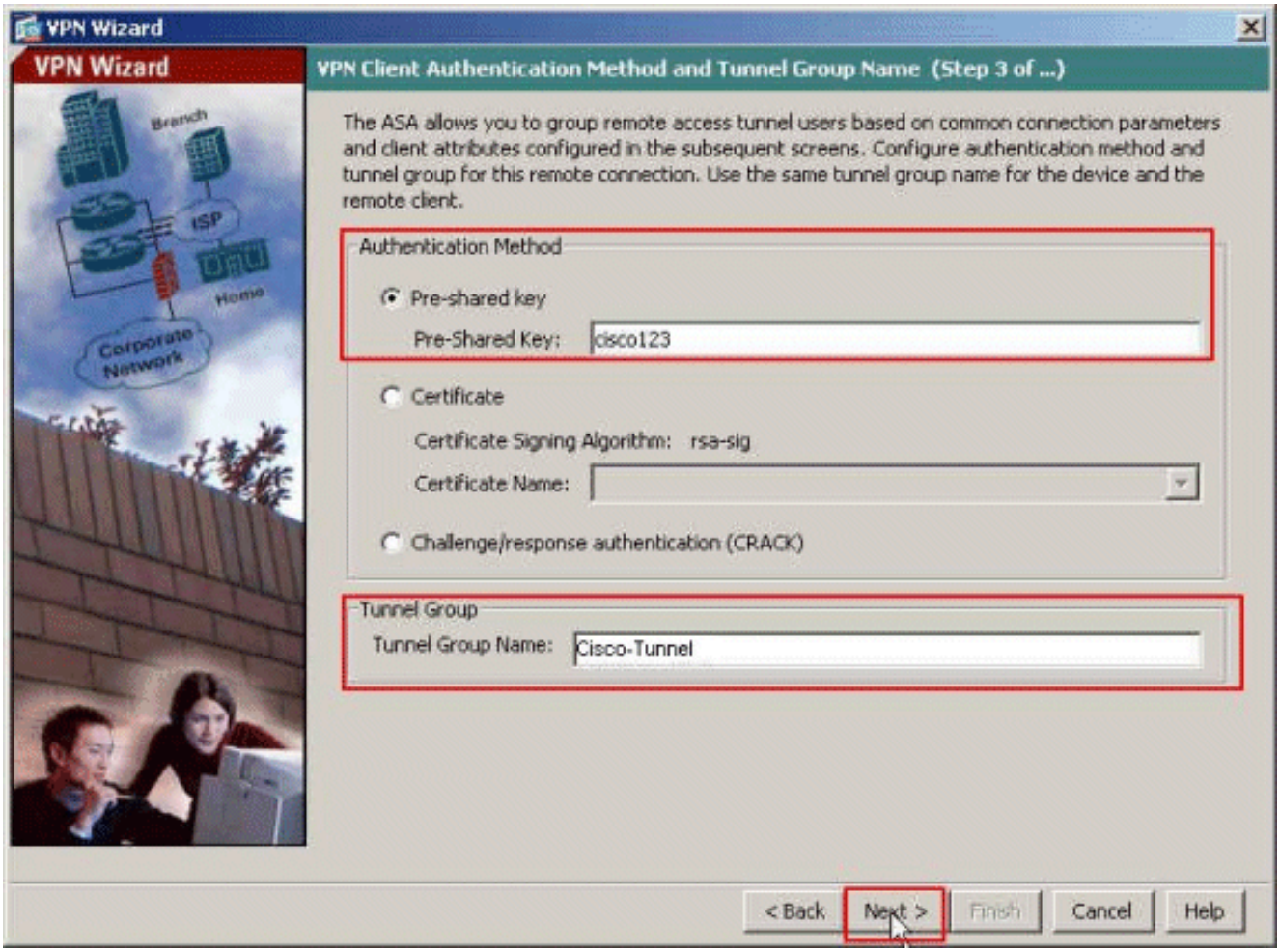
2. Selecteer de gewenste **VPN-tunnelinterface** (**Buiten**, in dit voorbeeld) en zorg er ook voor dat het selectieteken naast **IPsec-sessies inschakelen om de toegangslijsten van de interface te omzeilen** is ingeschakeld.



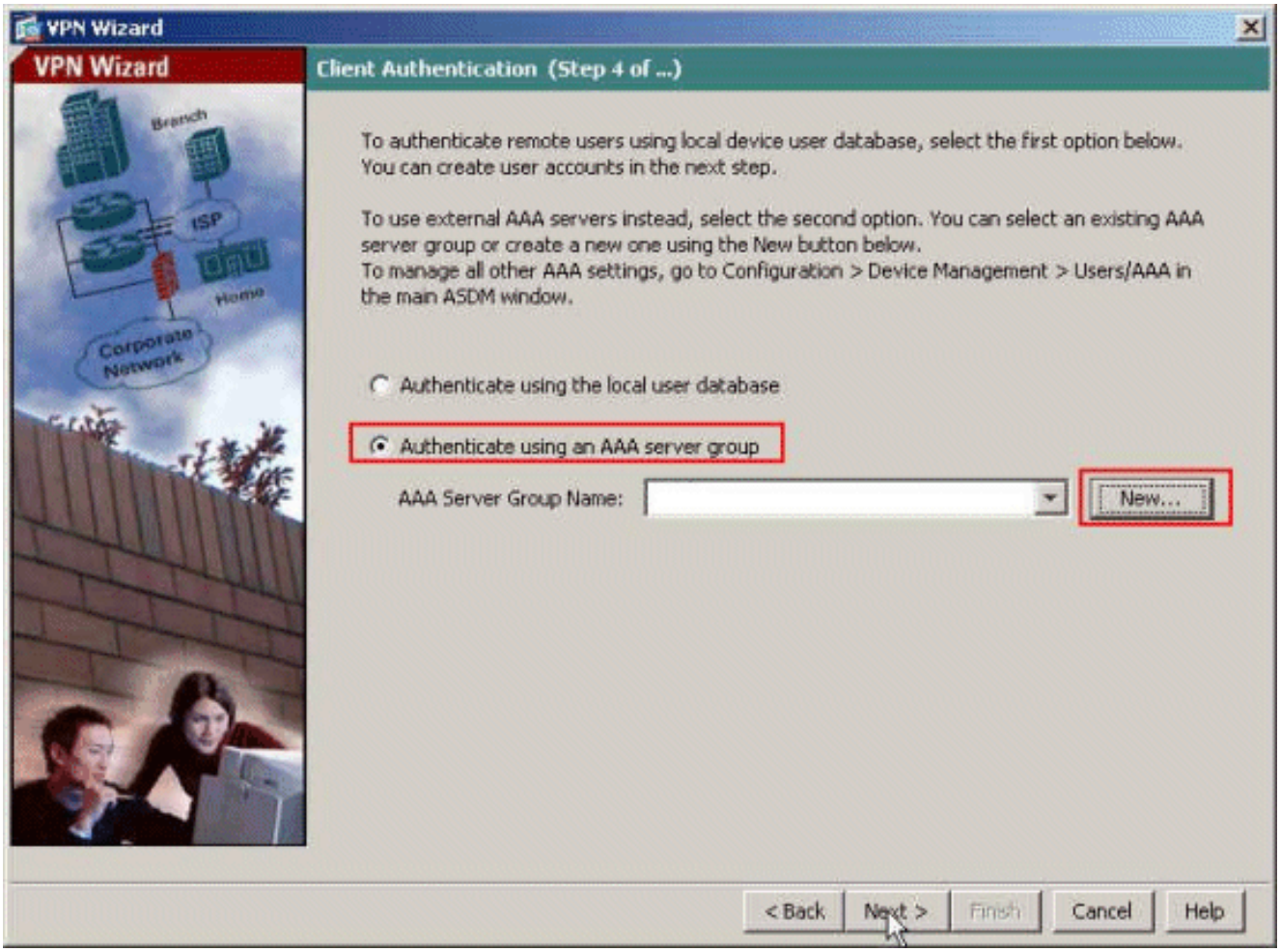
3. Kies het VPN-clienttype als **Cisco VPN-client, release 3.x of hoger**. Klik op **Volgende**.



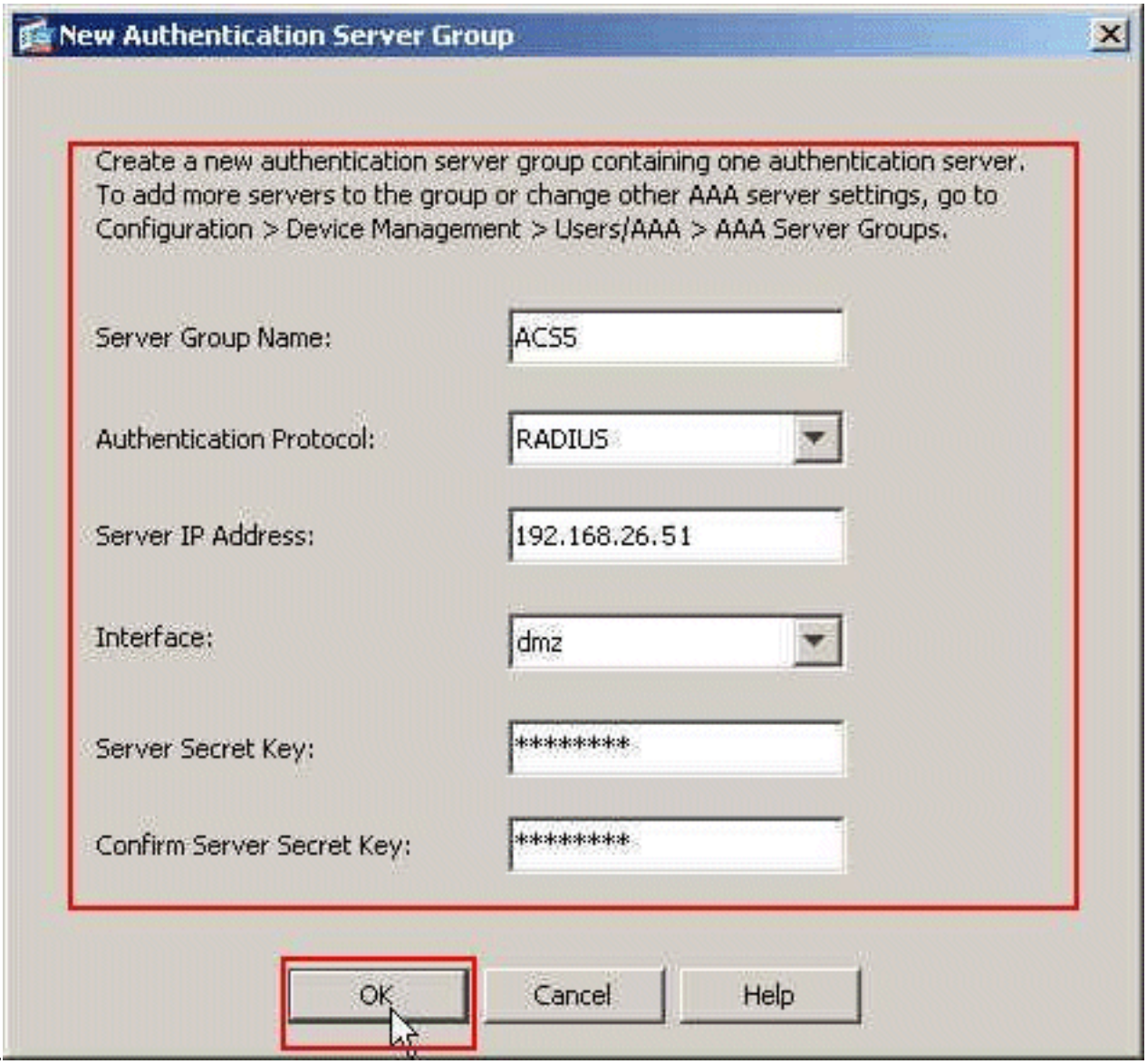
4. Kies de **verificatiemethode** en voer de verificatieinformatie in. De hier gebruikte verificatiemethode is **Vooraf gedeelde sleutel**. Typ ook een naam **van de Tunnelgroep** in de meegeleverde ruimte. De **Vooraf gedeelde sleutel** die hier wordt gebruikt is **Cisco123** en de **naam van de Tunnelgroep** die hier wordt **Cisco-Tunnel**. Klik op **Volgende**.



5. Kies of u externe gebruikers wilt geauthentiseerd worden naar de lokale gebruikersdatabase of naar een externe AAA server groep. Hier kiezen we voor **Authenticate aan het gebruik van een AAA server groep**. Klik op **Nieuw** naast het veld Naam AAA-servergroep om een nieuwe naam voor de AAA-servergroep te
maken.

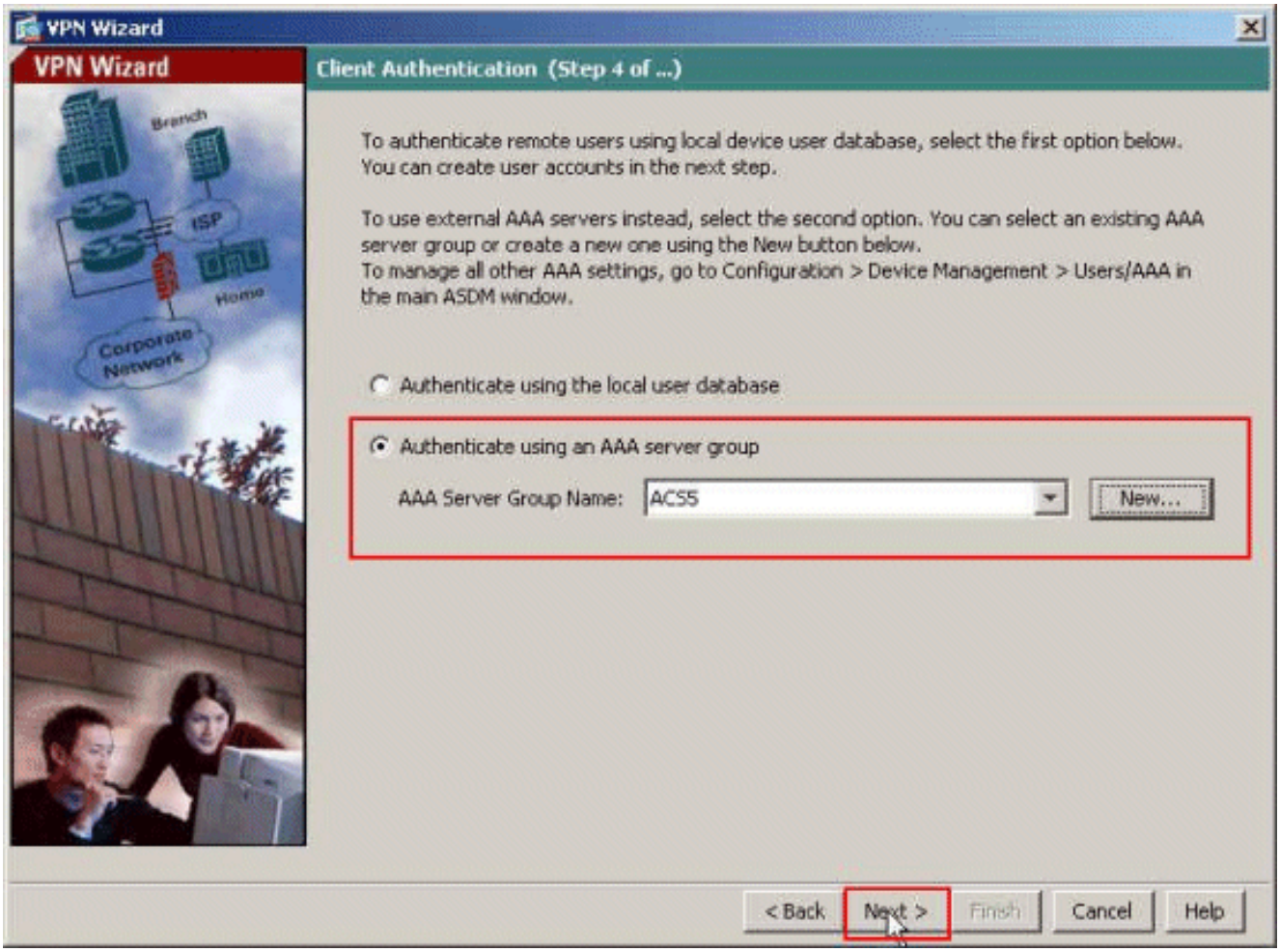


6. Typ de naam van de servergroep, het verificatieprotocol, het IP-adres van de server, de interfacenaam en de beveiligingstoets van de server in de betreffende ruimtes en klik op

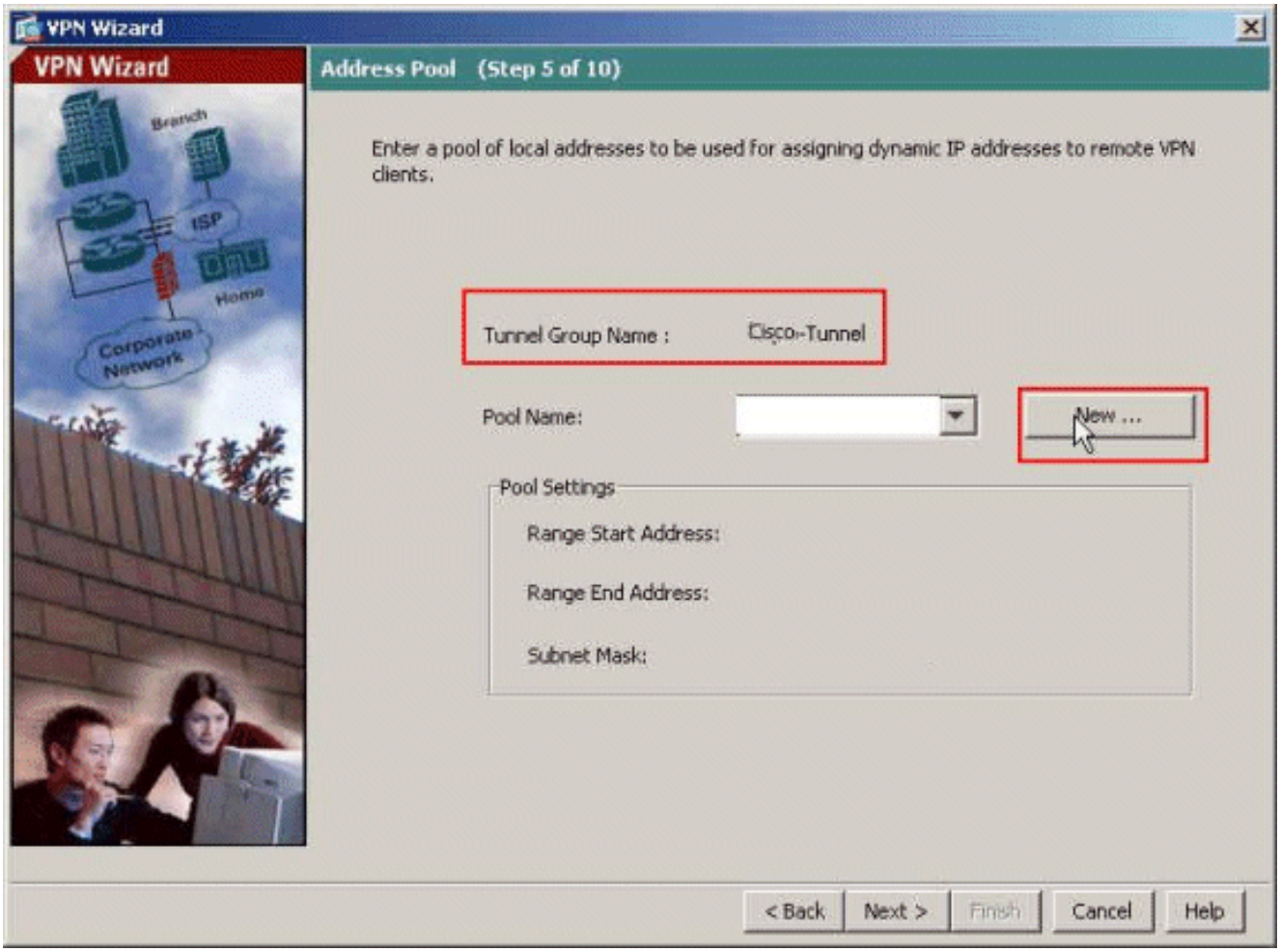


OK.

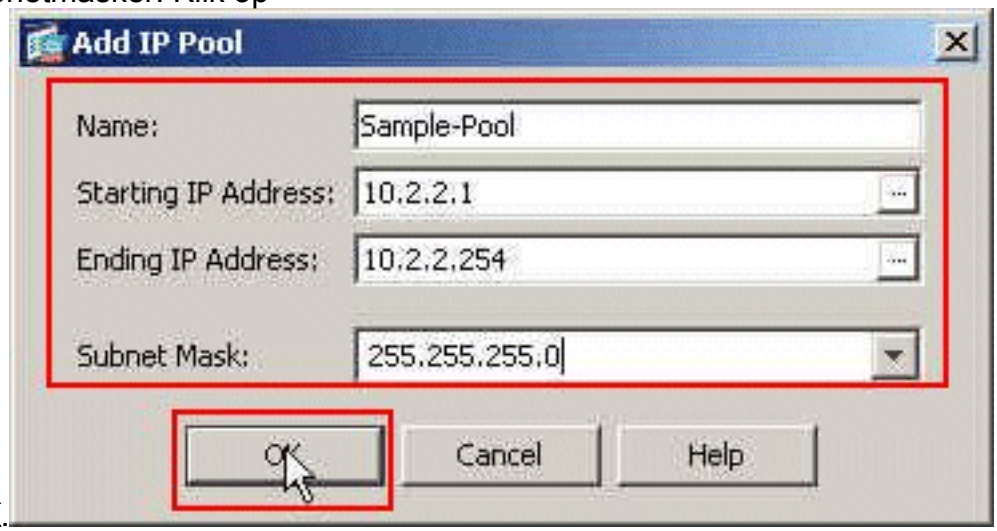
7. Klik op **Volgende**.



8. Defineert een pool van lokale adressen die dynamisch aan externe VPN-clients moeten worden toegewezen wanneer ze verbinding maken. Klik op **Nieuw** om een nieuw Pool van lokaal adres te
maken.

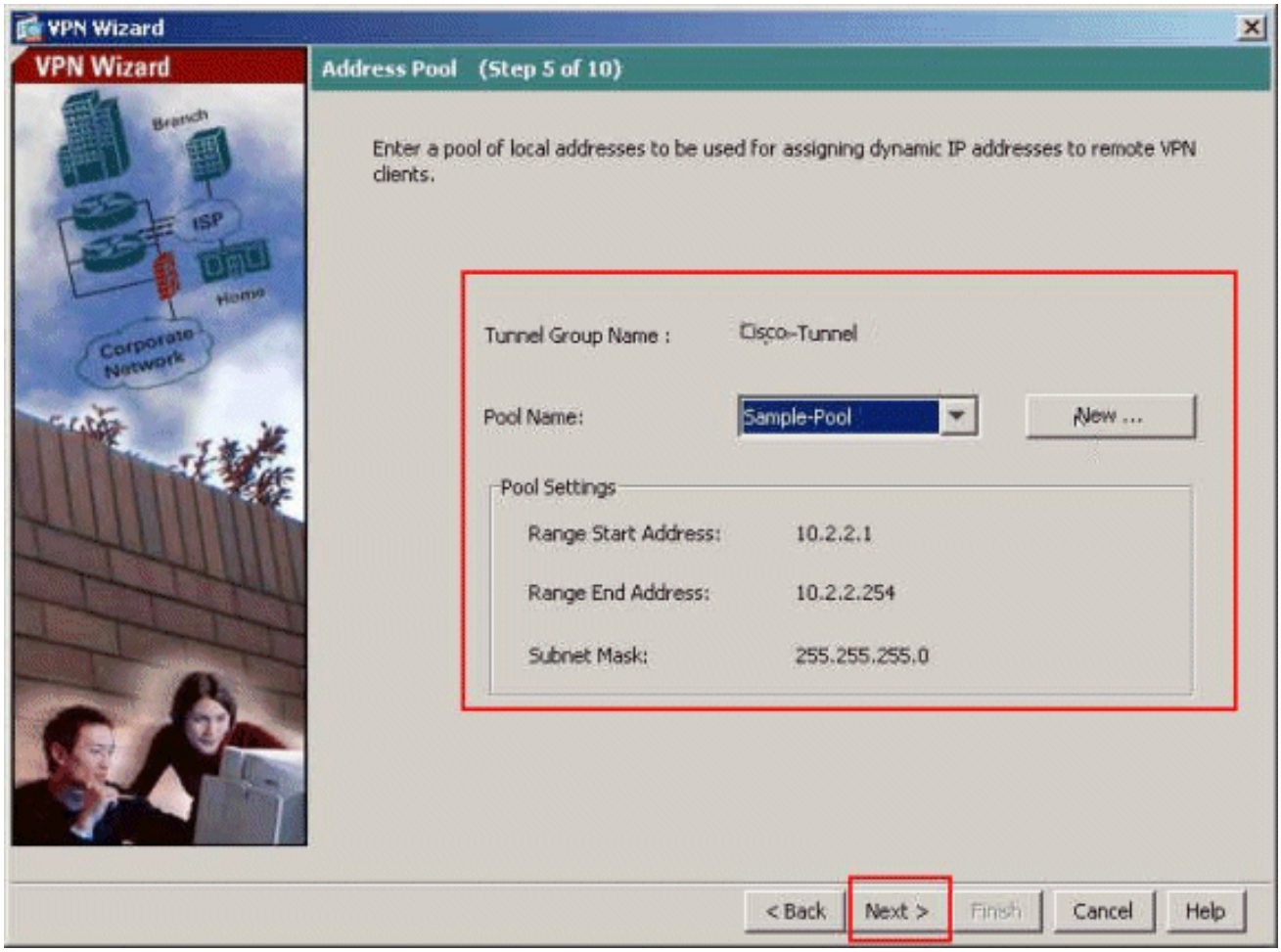


9. Typ in het venster Pool toevoegen de poolnaam, Start IP-adres, Eind IP-adres en het subnetmasker. Klik op

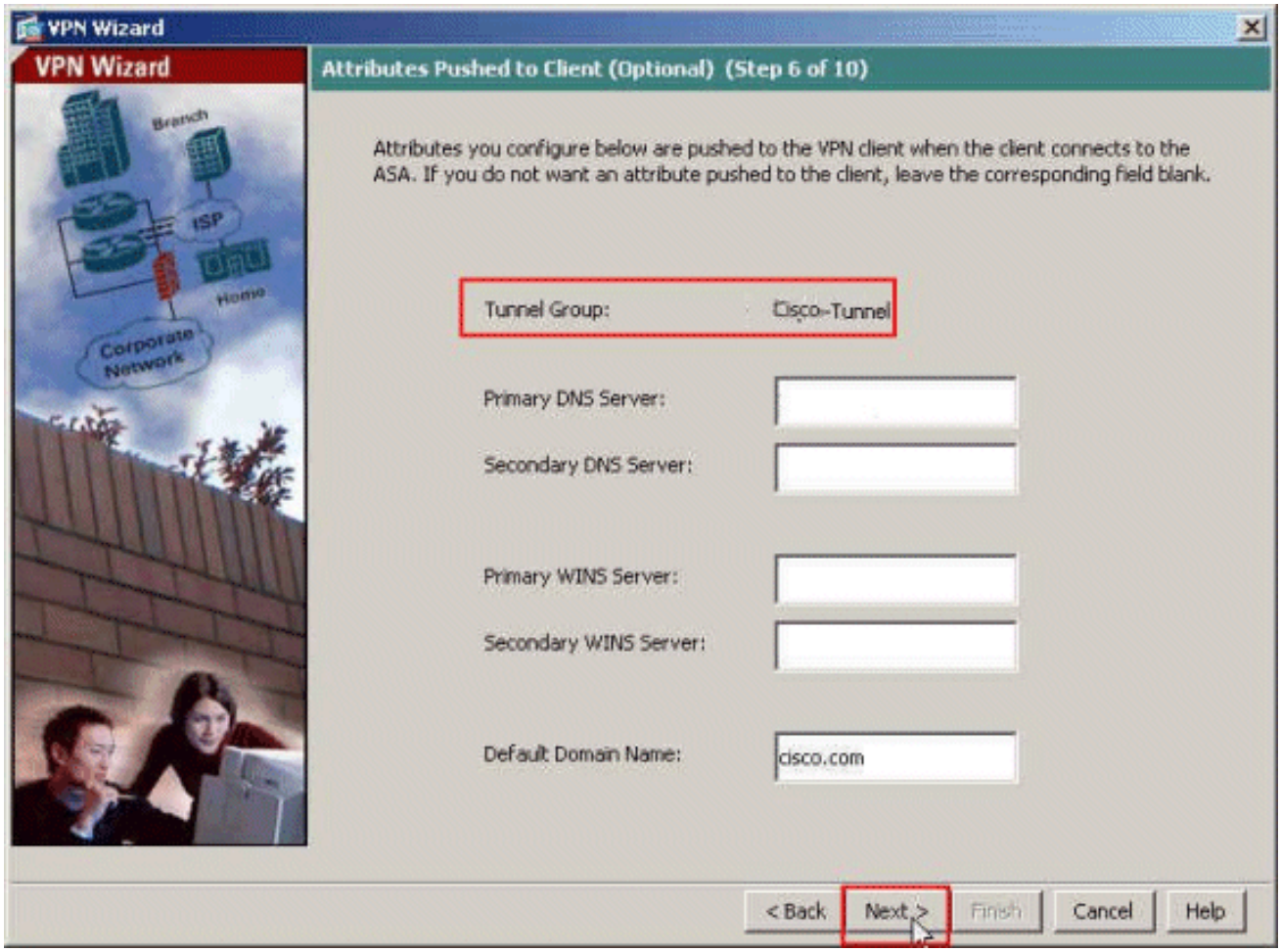


OK.

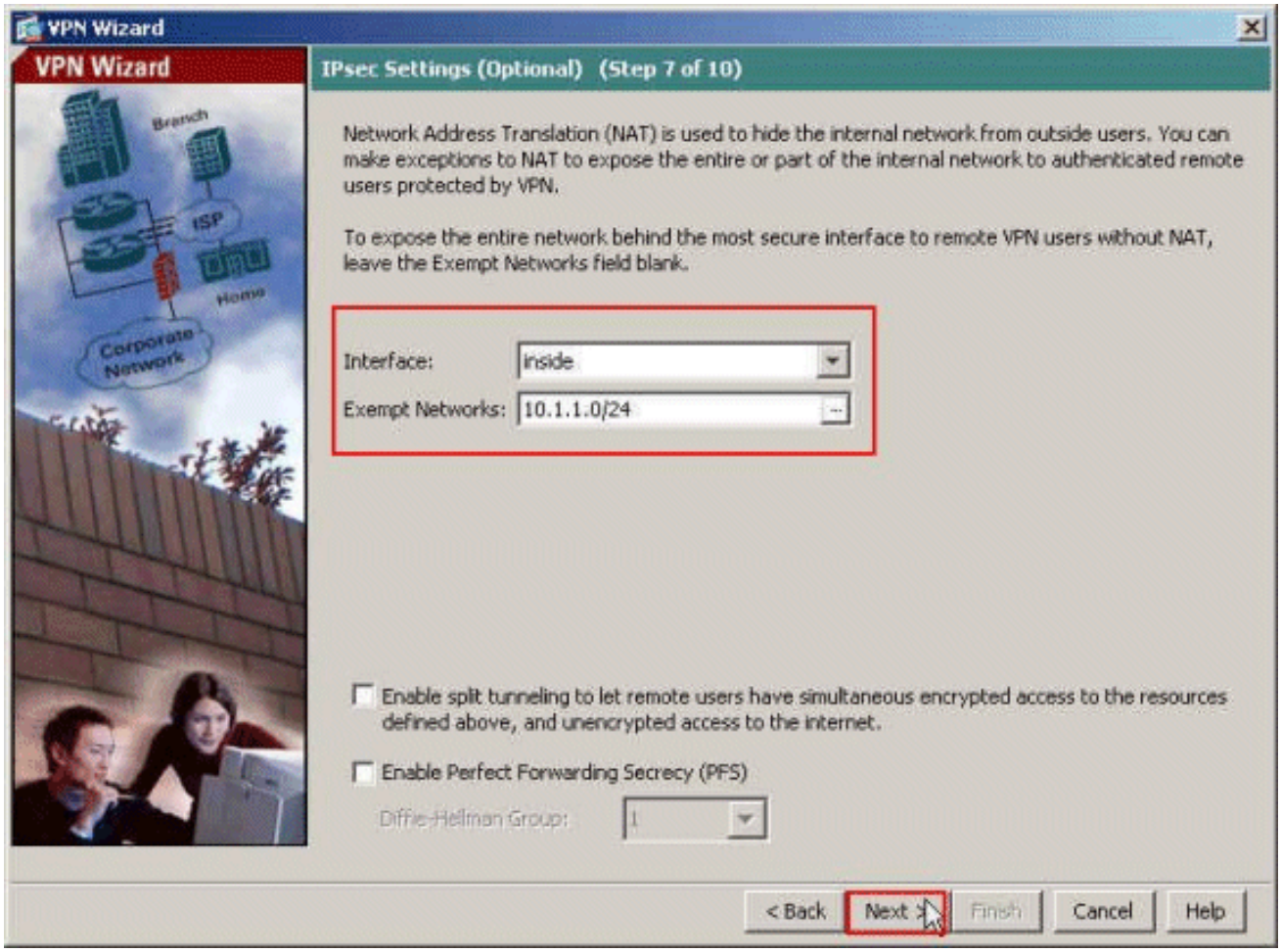
10. Selecteer de poolnaam in de vervolgkeuzelijst en klik op **Volgende**. Het voorbeeld Pool Name voor dit voorbeeld is **Sample-Pool** die in Stap 9 is gemaakt.



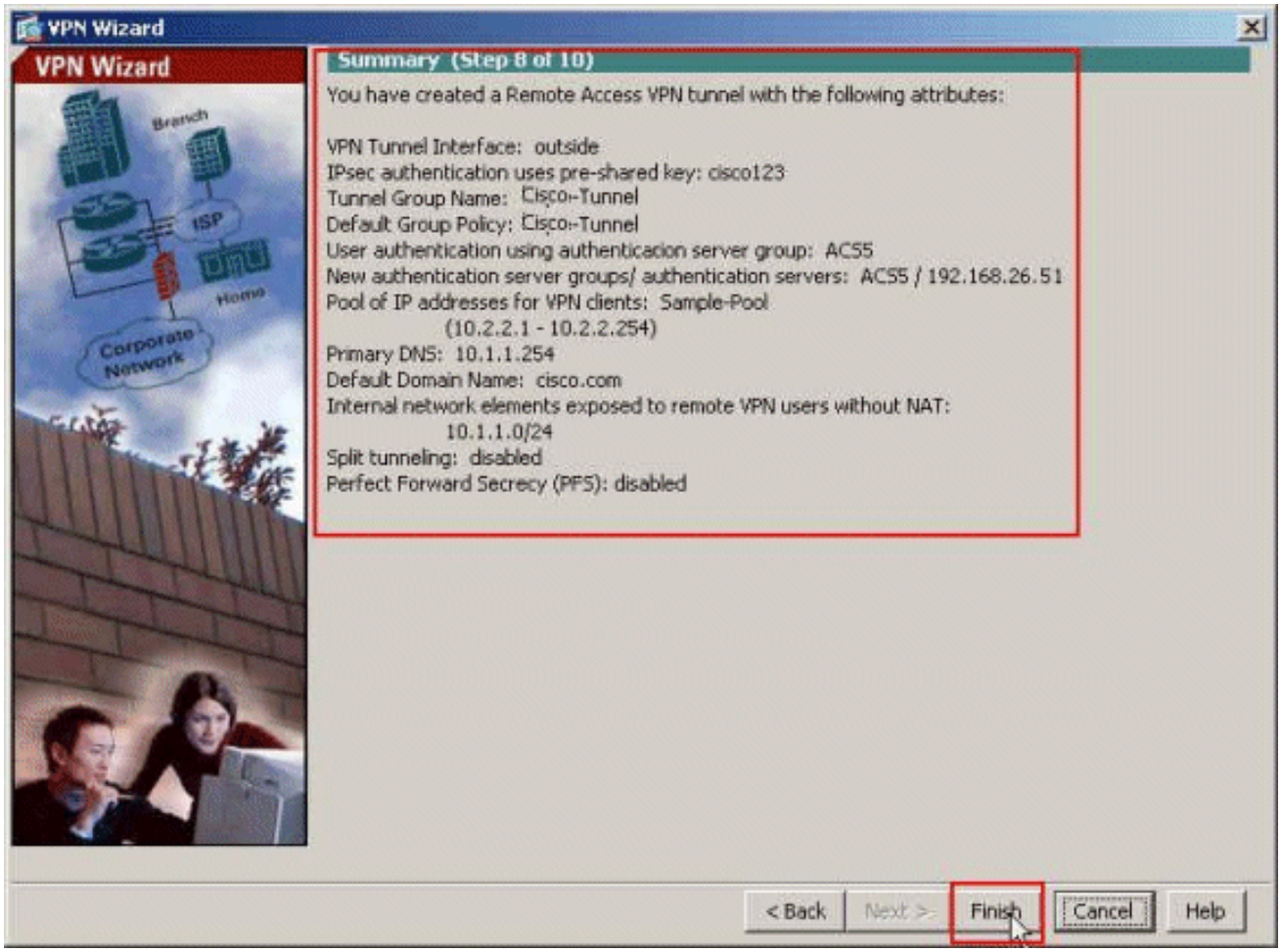
11. *Optioneel:* Specificeer de DNS- en WINS-serverinformatie en een standaardnaam voor domeinen die naar externe VPN-clients moet worden geduwd.



12. Specificeer welke, als om het even welke, interne hosts of netwerken zouden moeten worden blootgesteld aan externe VPN-gebruikers. Klik op **Volgende** na het opgeven van de interfacenaam en de netwerken die moeten worden vrijgesteld in het veld Uitzonderde netwerken.Als u deze lijst leeg laat, staat het externe VPN-gebruikers toe om toegang te krijgen tot het gehele binnennetwerk van de ASA.U kunt ook gesplitste tunneling in dit venster inschakelen. Split-tunneling versleutelt het verkeer naar de bronnen die eerder in deze procedure zijn gedefinieerd en geeft onversleutelde toegang tot internet in het algemeen door dat verkeer niet uit te schakelen. Als gesplitste tunneling *niet* ingeschakeld is, wordt al het verkeer van externe VPN-gebruikers naar de ASA gekanaliseerd. Dit kan zeer bandbreedte en processor intensief worden, gebaseerd op uw configuratie.



13. Dit venster geeft een samenvatting van de maatregelen die u hebt genomen. Klik op **Voltooien** als u tevreden bent met de configuratie.



ASA met CLI configureren

Dit is de CLI-configuratie:

Configuratie op het ASA-apparaat uitvoeren

```
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#
```

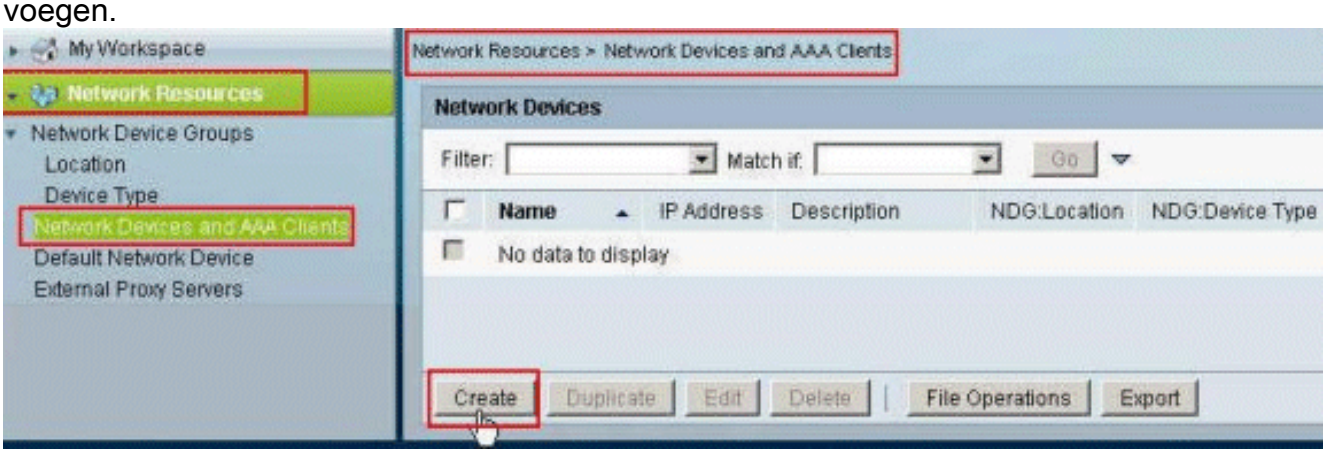
ACS voor downloadbare ACL voor individuele gebruiker configureren

U kunt downloadbare toegangslijsten op Cisco Secure ACS 5.x configureren als een benoemde toegangsobject voor toegangsrechten en deze vervolgens toewijzen aan een autorisatieprofiel dat geselecteerd wordt in de resulterende sectie van de regel in de toegangsservice.

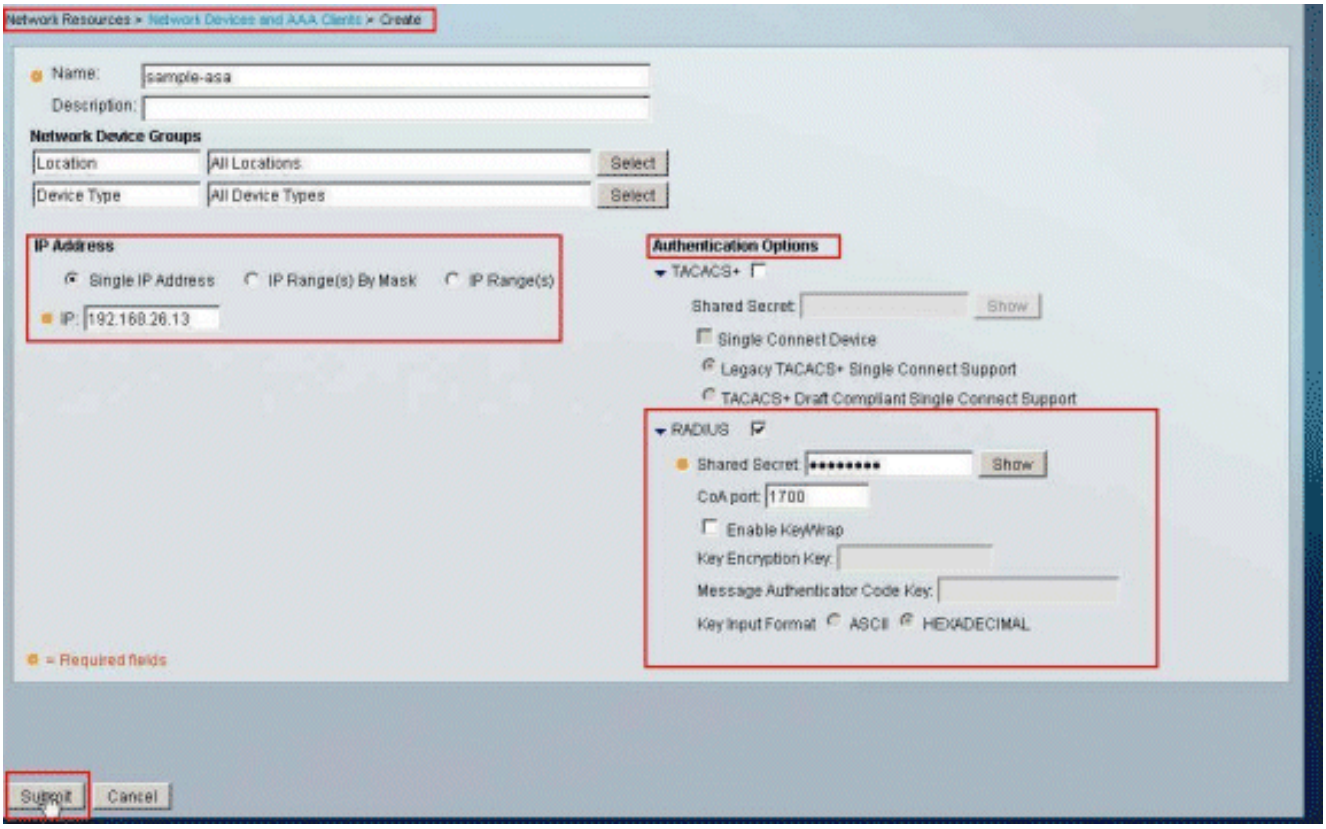
In dit voorbeeld authenticeert de IPsec VPN-gebruiker **Cisco** en de RADIUS-server stuurt een downloadbare toegangslijst naar het security apparaat. De gebruiker "cisco" heeft alleen toegang tot de 10.1.1.2 server en ontkent alle andere toegang. Om ACL te controleren, zie de Downloadbare ACL voor Gebruiker/Groep.

Voltooi deze stappen om een RADIUS-client te configureren in een Cisco Secure ACS 5.x:

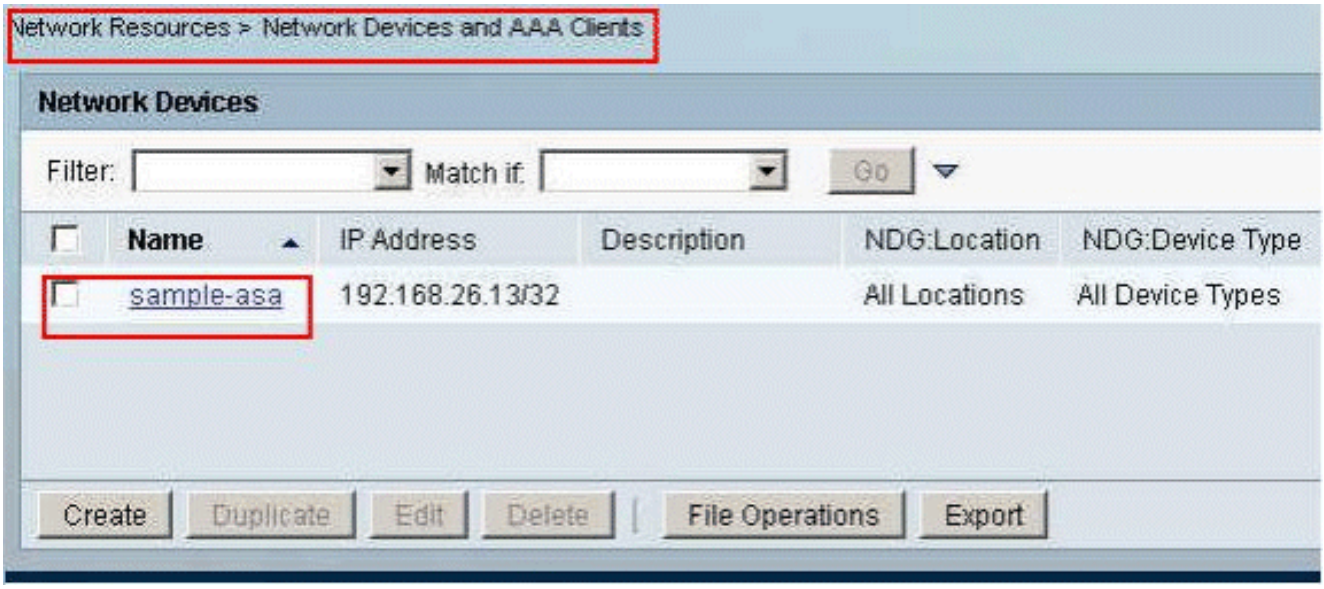
1. Kies **Netwerkbronnen > Netwerkapparaten en AAA-clients** en klik op **Maken** om een bestandsindeling voor de ASA in de RADIUS-serverdatabase toe te voegen.



2. Voer een lokaal significante naam voor de ASA in (**monster-asa**, in dit voorbeeld) en voer in het veld IP-adres **192.168.26.13** in. Kies **RADIUS** in het gedeelte Verificatieopties door het selectieteken **RADIUS** te controleren en voer **cisco123** in voor het veld Gedeeld geheim. Klik op **Inzenden**.

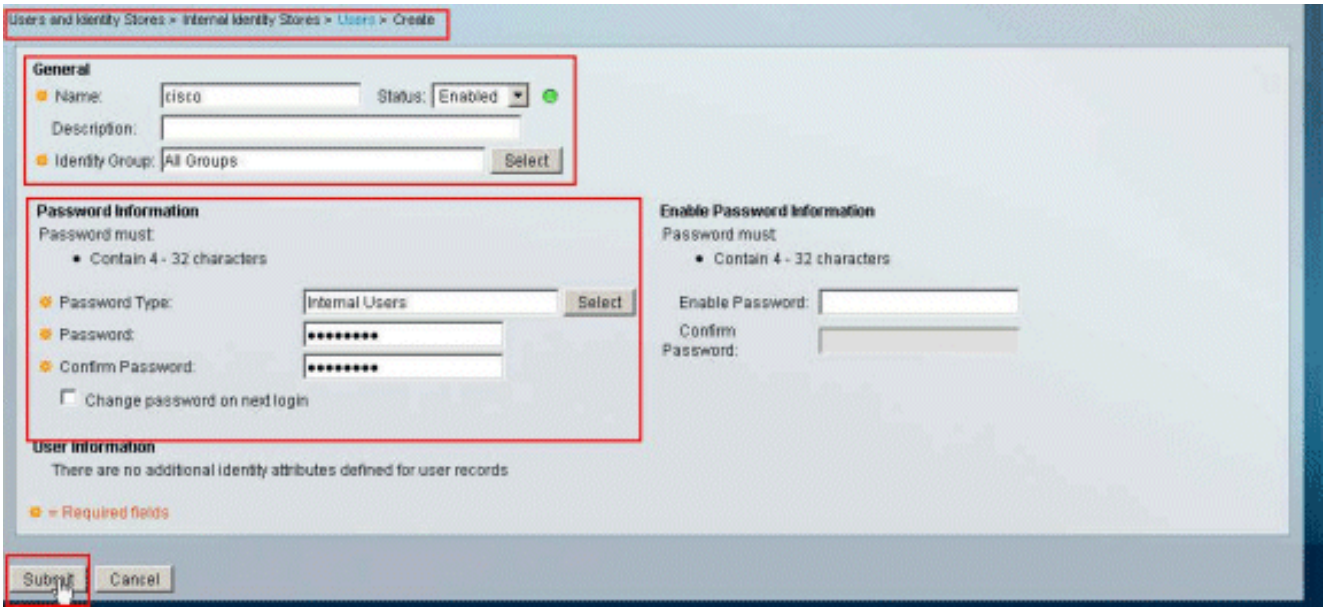


3. De ASA wordt met succes toegevoegd aan de RADIUS server (ACS) database.

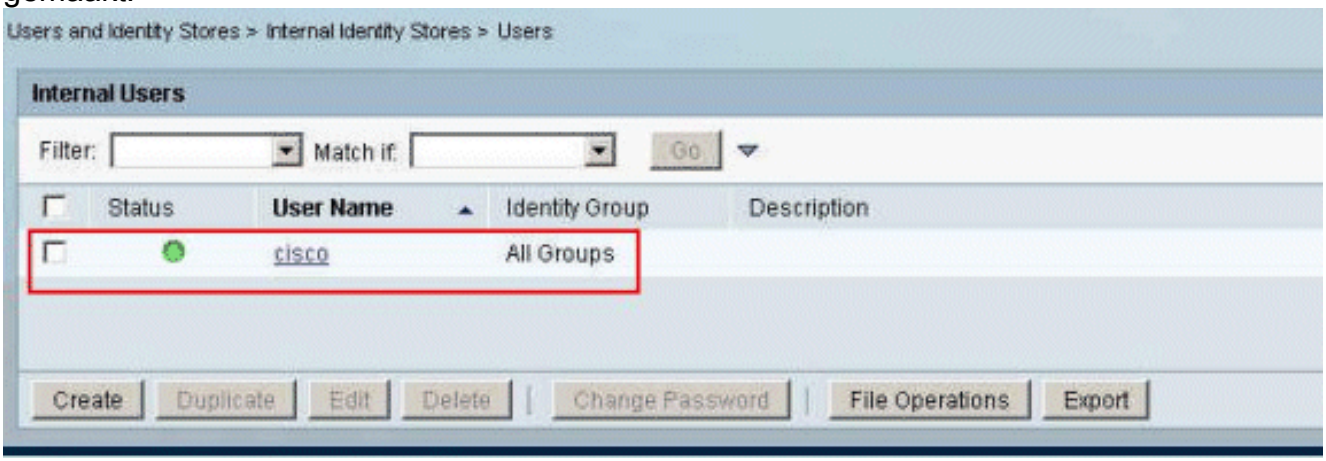


4. Kies **gebruikers en identiteitsopslag > Interne identiteitsopslag > gebruikers**, en klik **Maken** om een gebruiker in de lokale gegevensbank van ACS voor VPN-verificatie te maken.

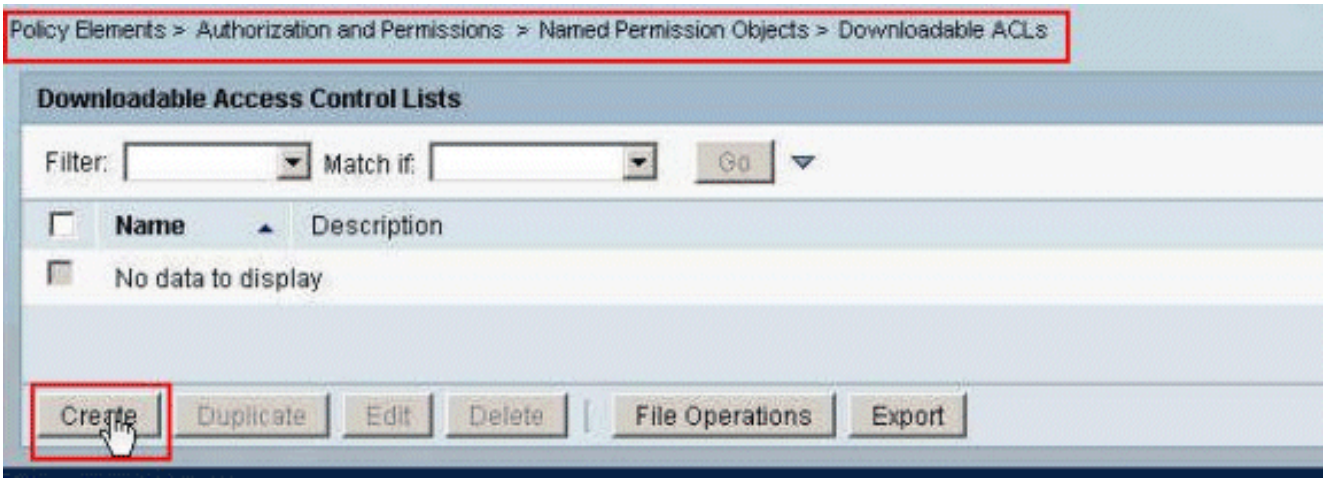
5. Voer de gebruikersnaam in **cisco**. Selecteer het wachtwoordtype als **interne gebruikers** en voer het wachtwoord in (**cisco123**, in dit voorbeeld). Bevestig het wachtwoord en klik op **Indienen**.



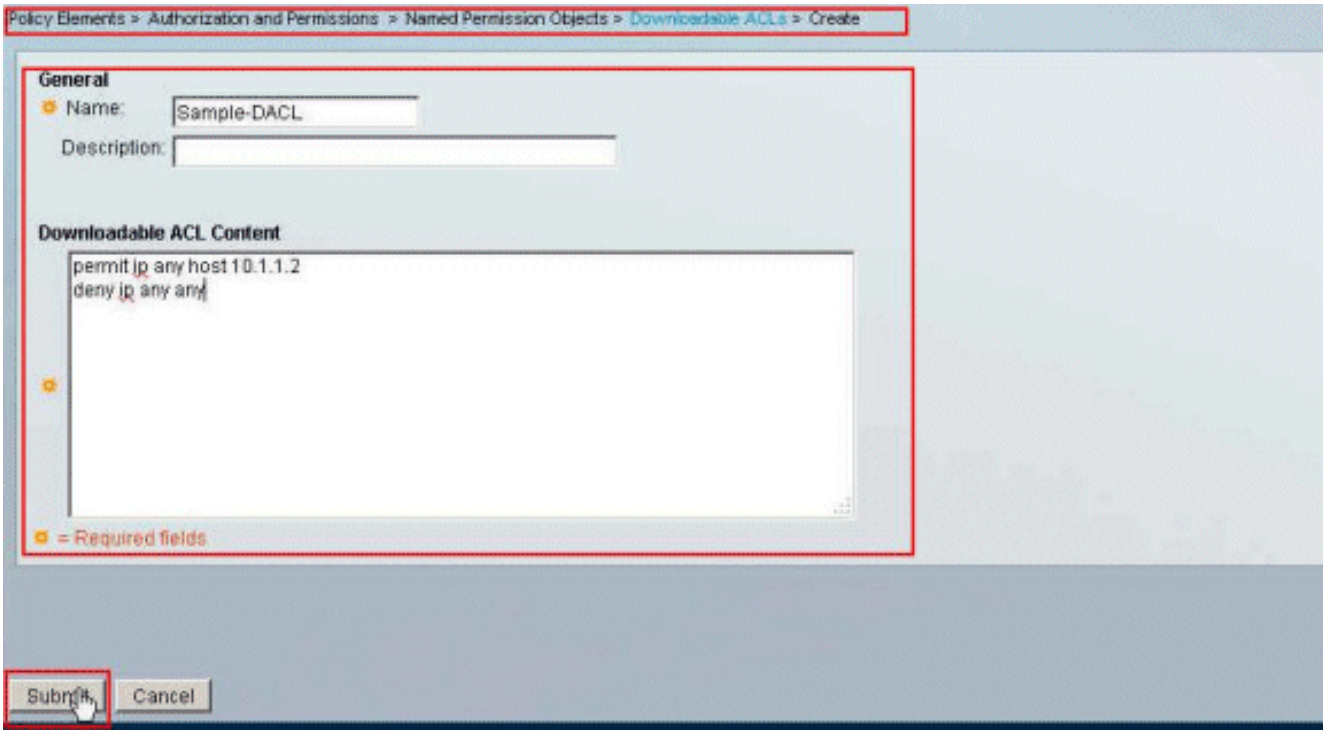
6. De gebruikersinterface **cisco** is gemaakt.



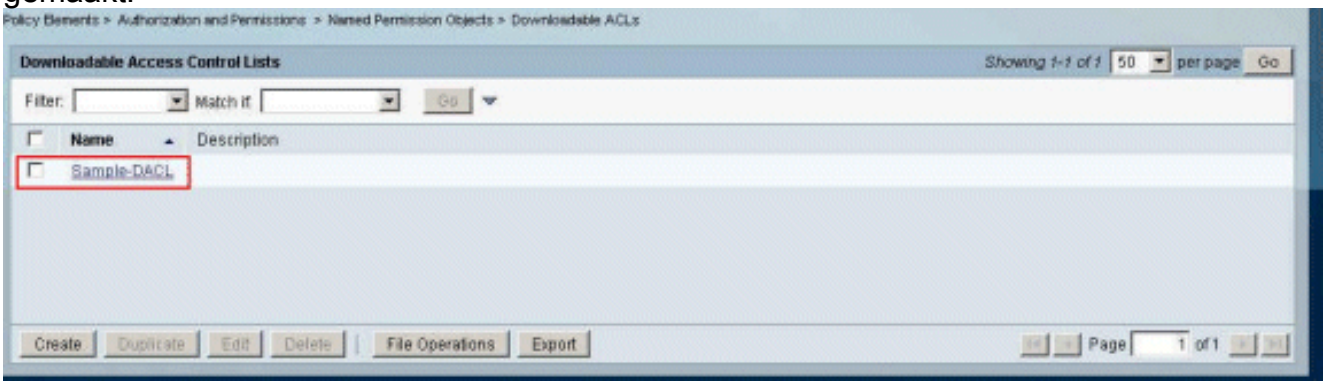
7. Om een downloadbare ACL te maken, kiest u **Beleidselementen > Verificatie en toegangsrechten > Benoemde toegangsobjecten > Downloadbare ACL's** en klikt u op **Maken.**



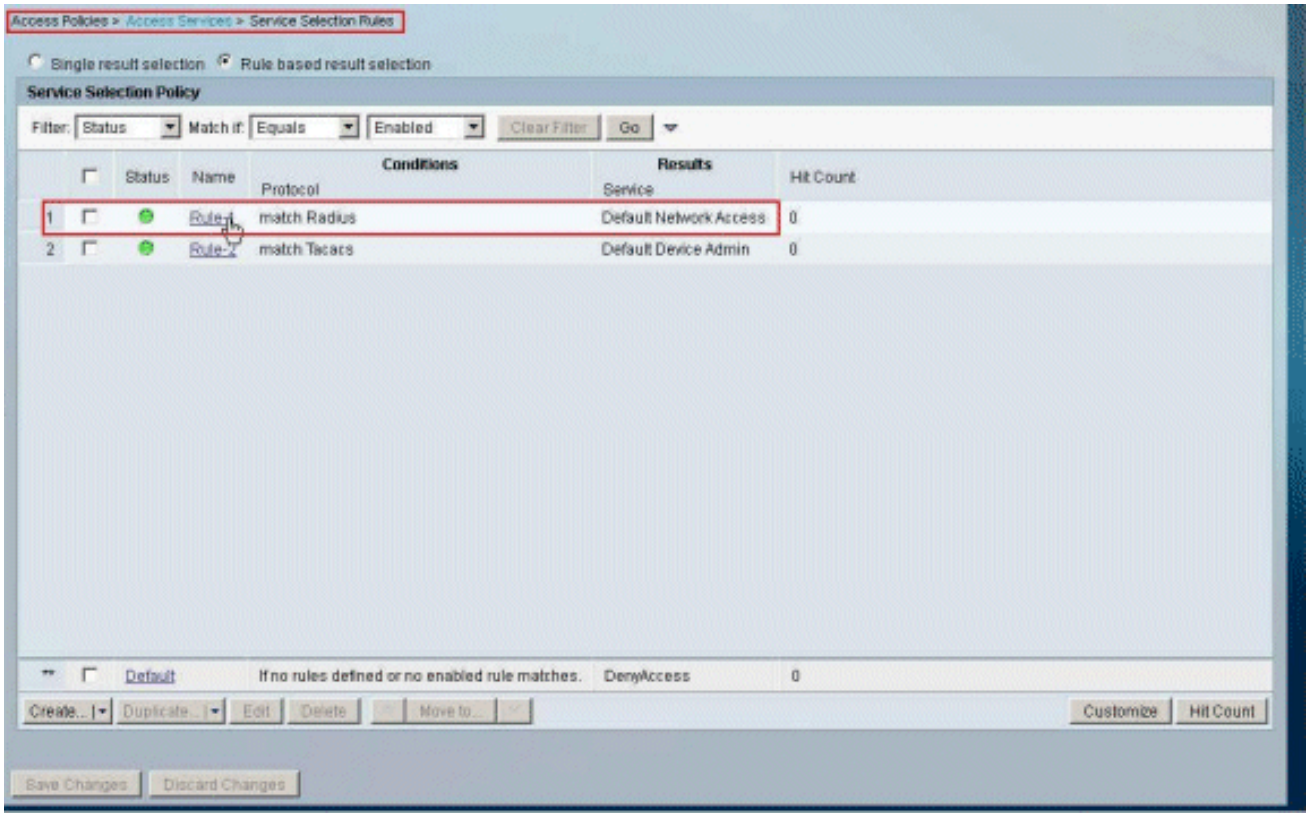
8. Typ de **naam** voor de downloadbare ACL's en de **ACL-inhoud**. Klik op **Inzenden**.



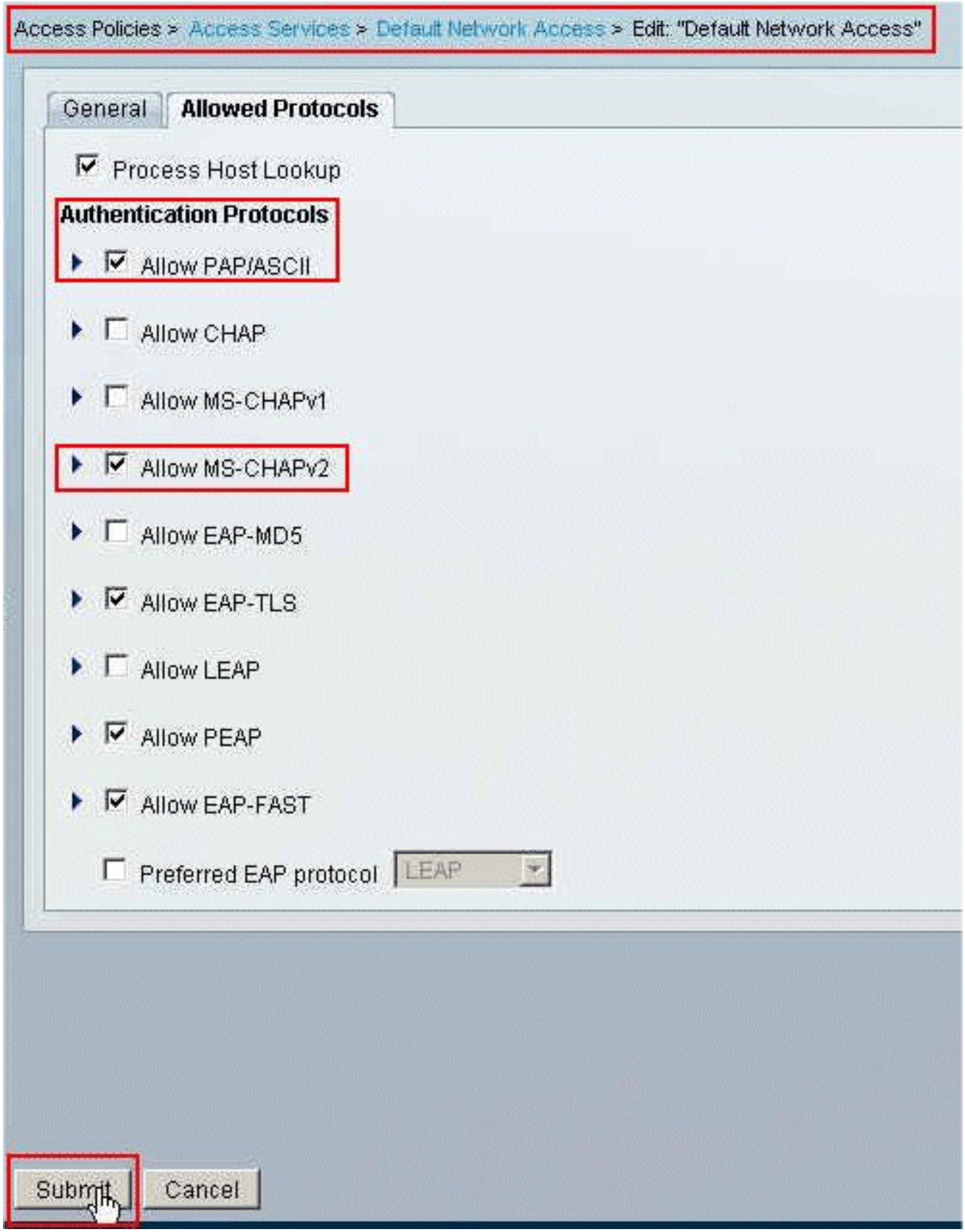
9. De downloadbare ACL-**monster-DACL** wordt gemaakt.



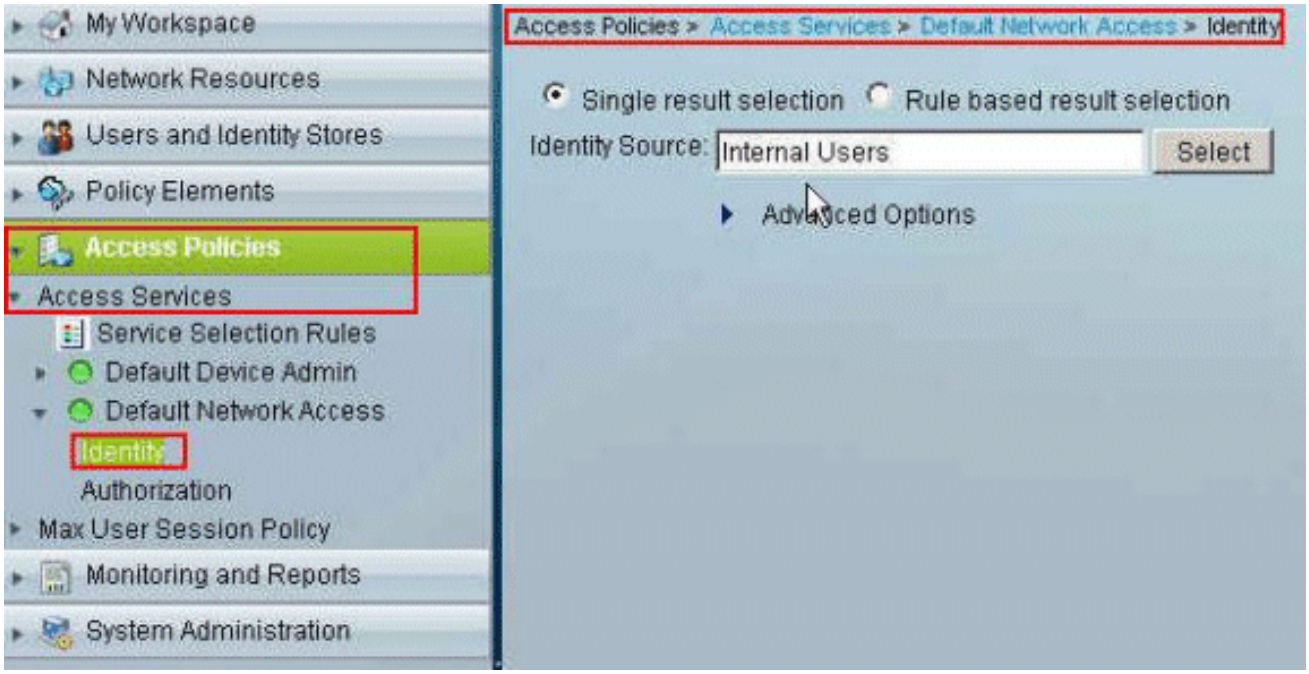
10. Om het Access-beleid voor VPN-verificatie te configureren kiest u **Toegangsbeleid > Toegangsservices > Servicesselectieregels** en bepaalt u welke service aan het RADIUS-protocol gekoppeld is. In dit voorbeeld komt **Regel 1** overeen met **RADIUS** en de standaard toegang tot het netwerk behandelt het RADIUS-verzoek.



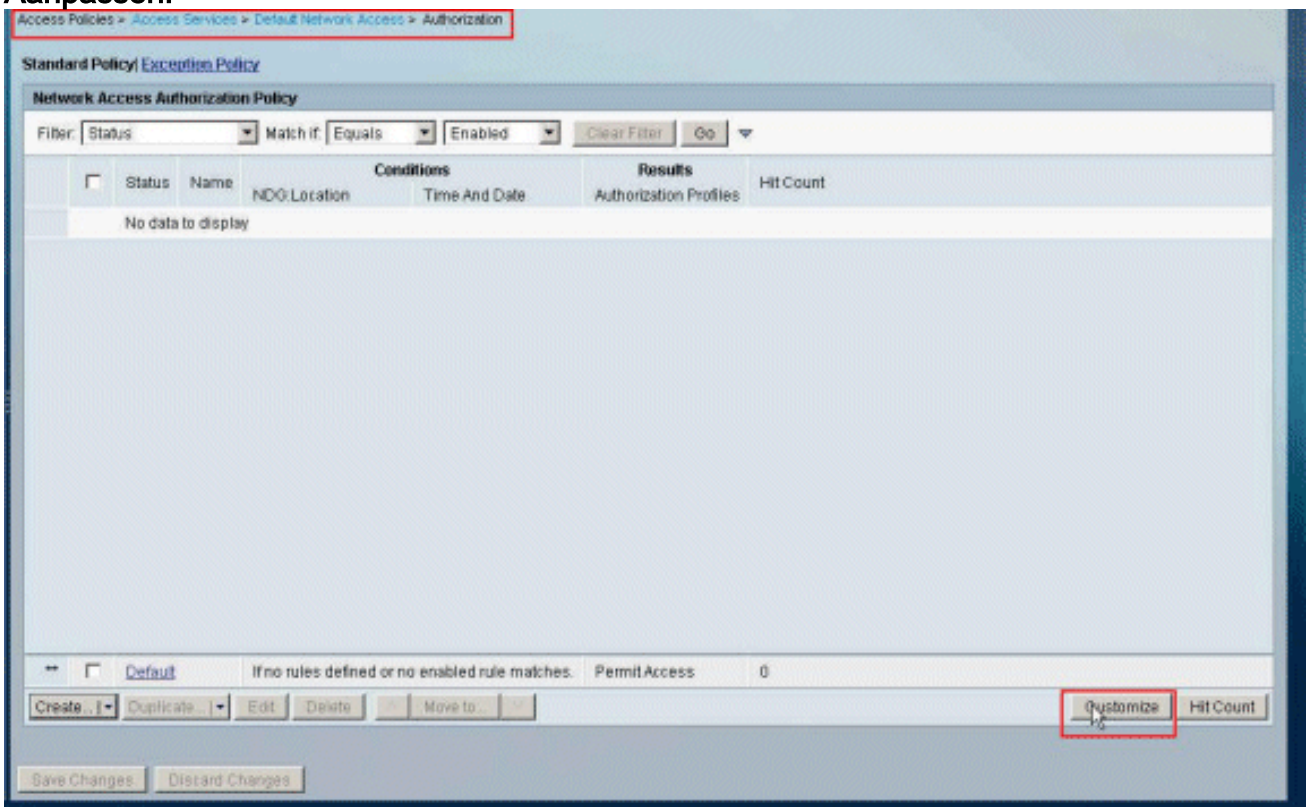
11. Kies de **toegangsservice** die is ingesteld in stap 10. In dit voorbeeld wordt **standaard netwerktoegang** gebruikt. Kies het tabblad **Toegestane protocollen** en zorg ervoor dat **PAP/ASCII toestaan** en **MS-CHAPv2** toestaan is geselecteerd .Klik op **Indienen**.



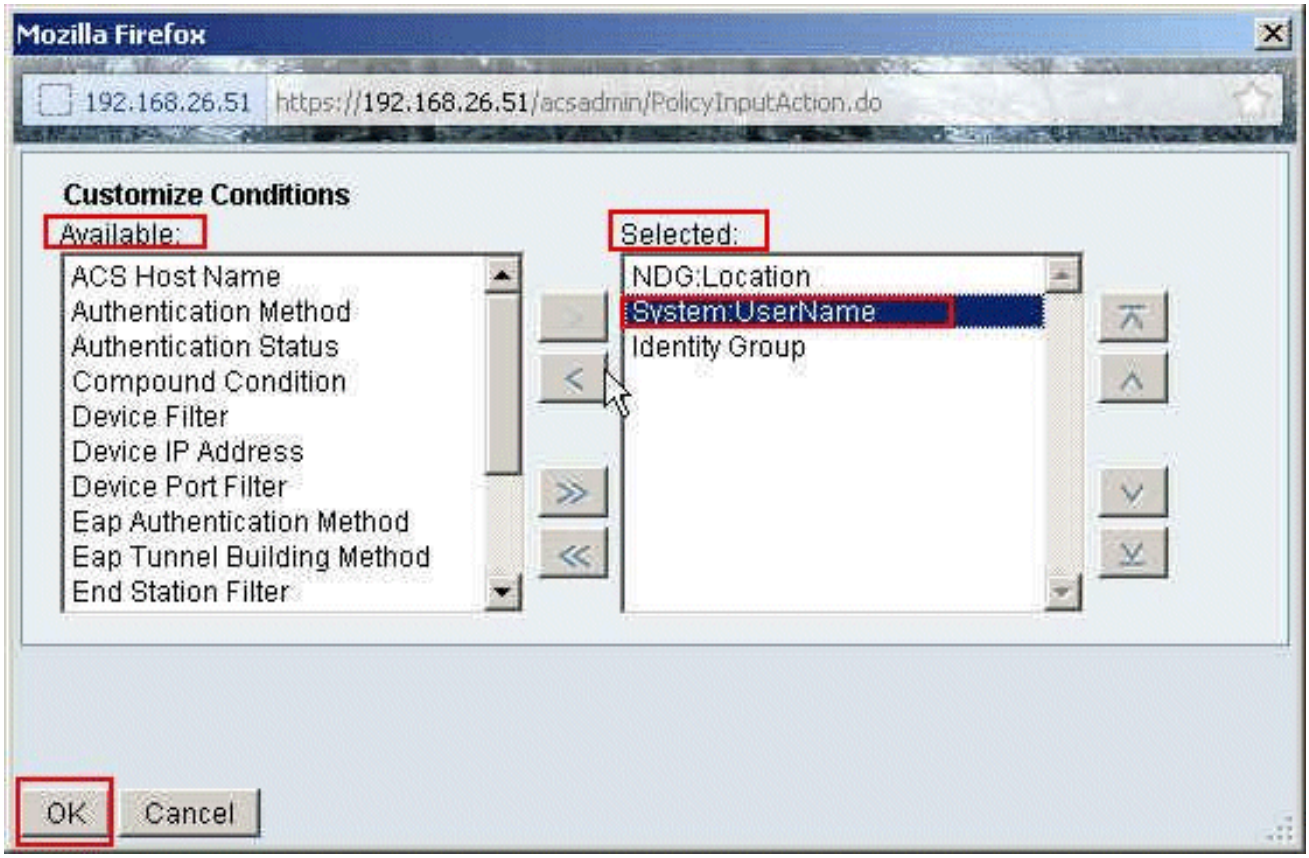
12. Klik op het **gedeelte Identity** van de **Access Services** en zorg ervoor dat de **interne gebruikers** zijn geselecteerd als de Identity Source. In dit voorbeeld hebben we standaard netwerktoegang.



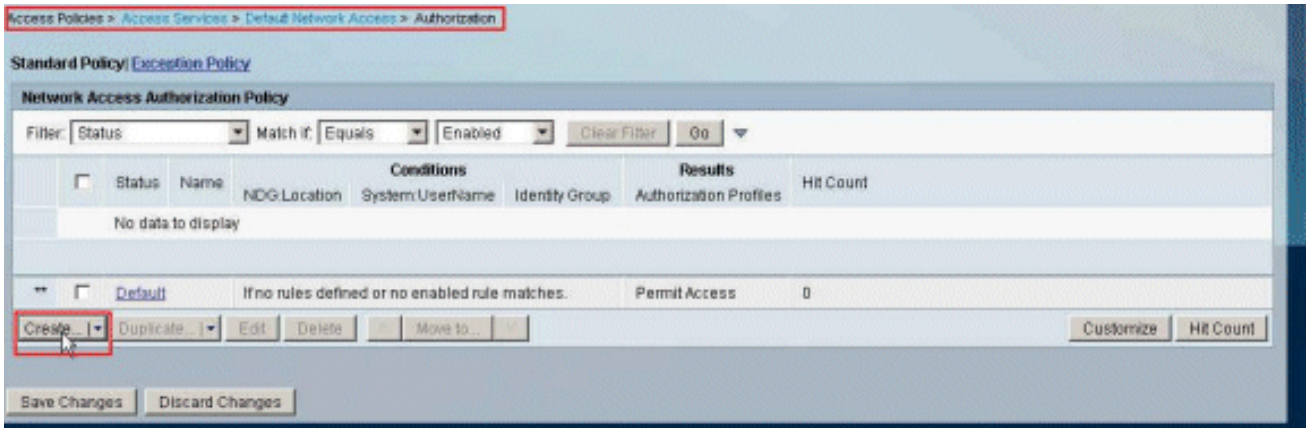
13. Kies **Toegangsbeleid** > **Toegangsservices** > **Standaardnetwerktoegang** > **autorisatie** en klik **op**
Aanpassen.



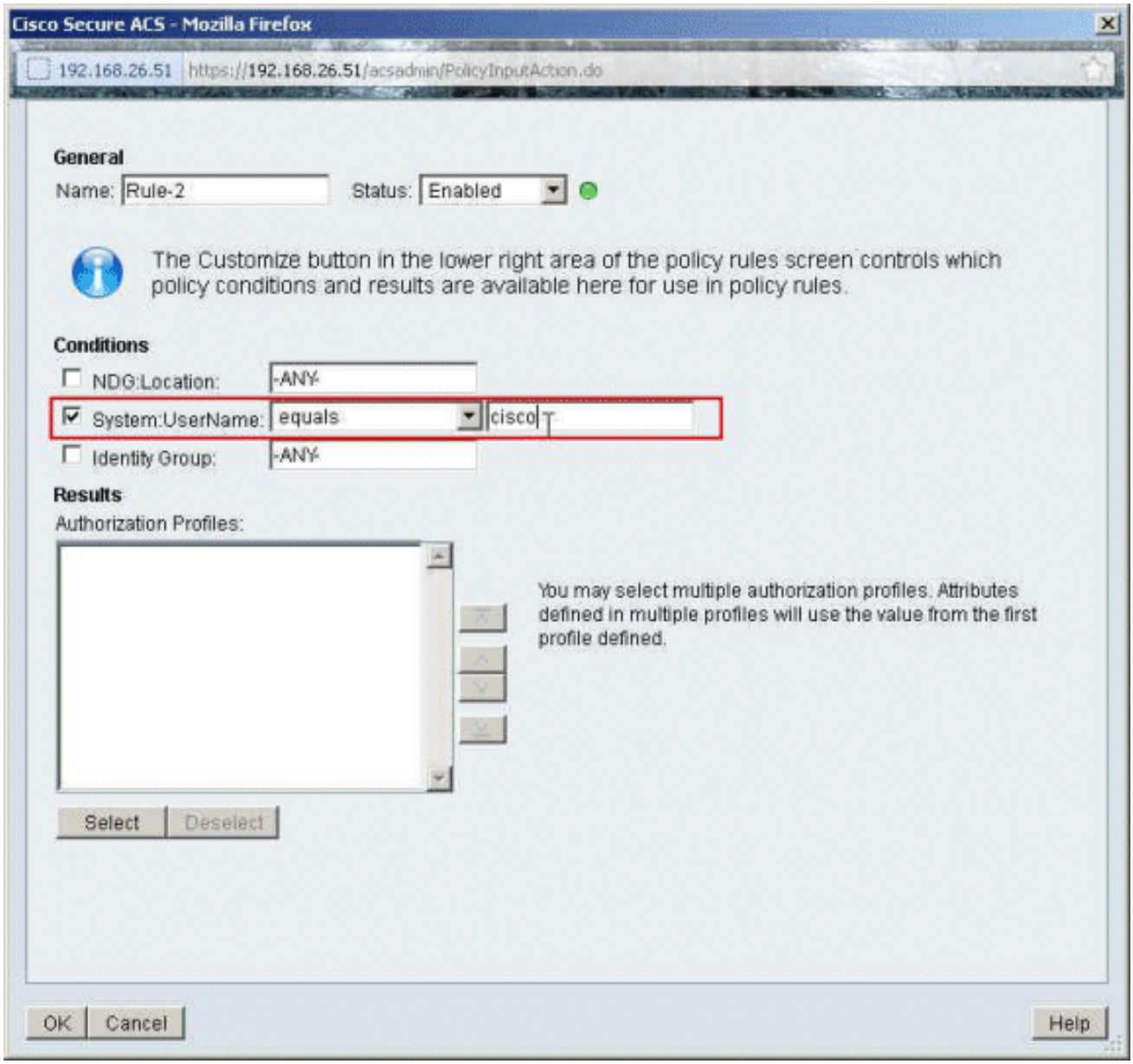
14. Verplaats **Systeem:**GebruikerNaam uit de **Beschikbare** kolom in de **geselecteerde** kolom en klik op
OK.



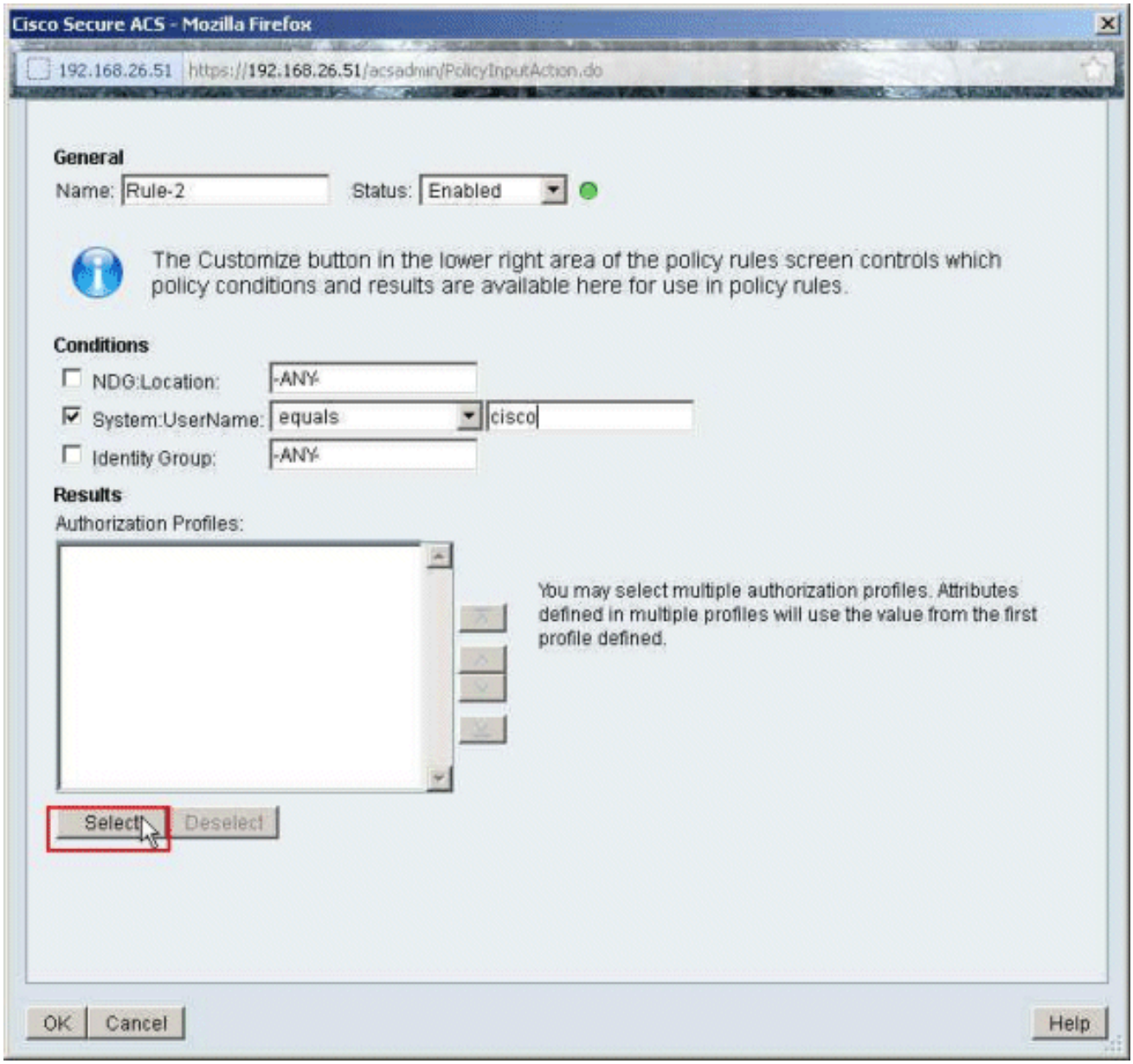
15. Klik op **Maken** om een nieuwe Regel te maken.



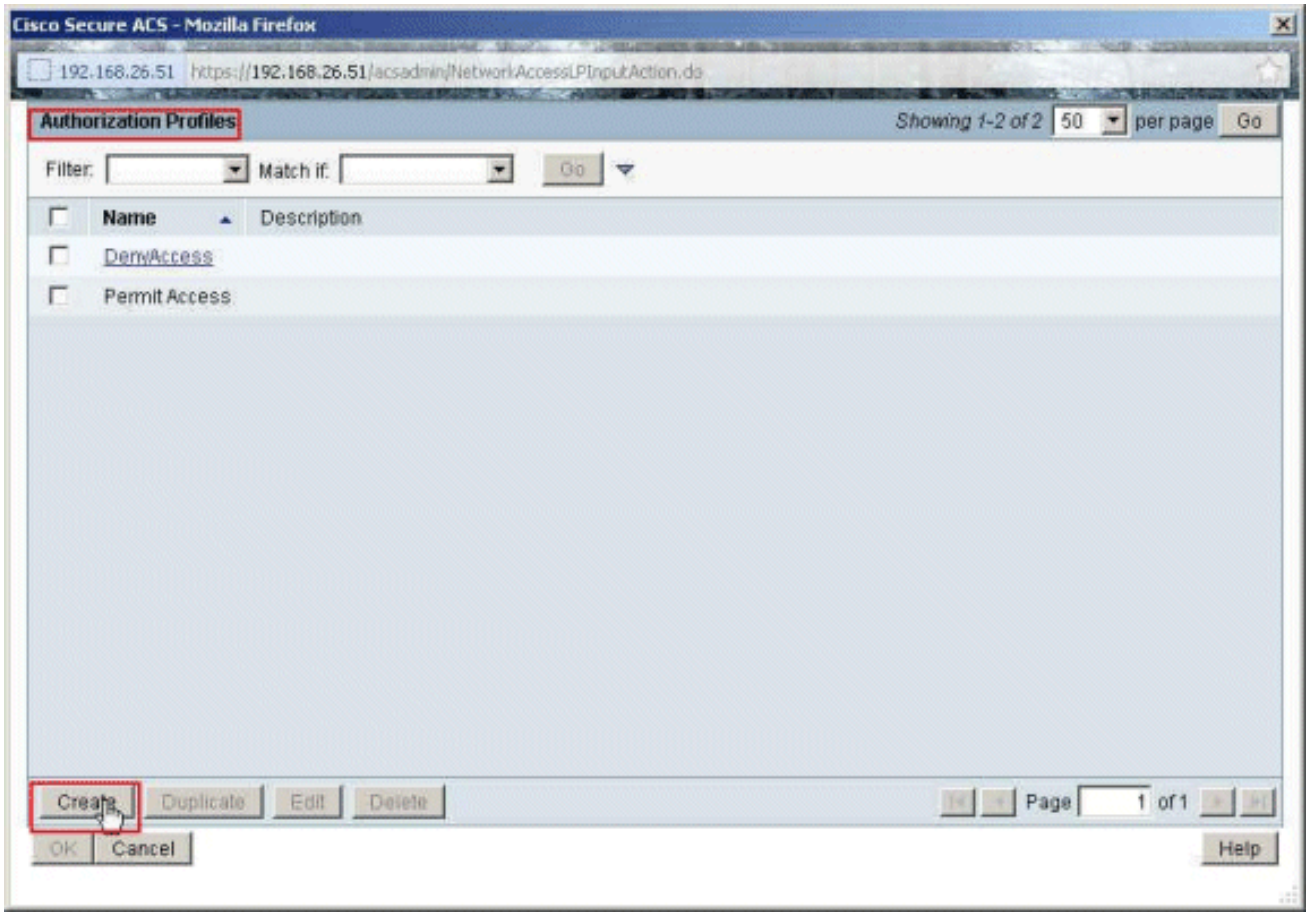
16. Zorg dat het selectieteken naast **Systeem:UserName** is geselecteerd, kies **gelijken** uit de vervolgkeuzelijst en voer de gebruikersnaam **cisco in**.



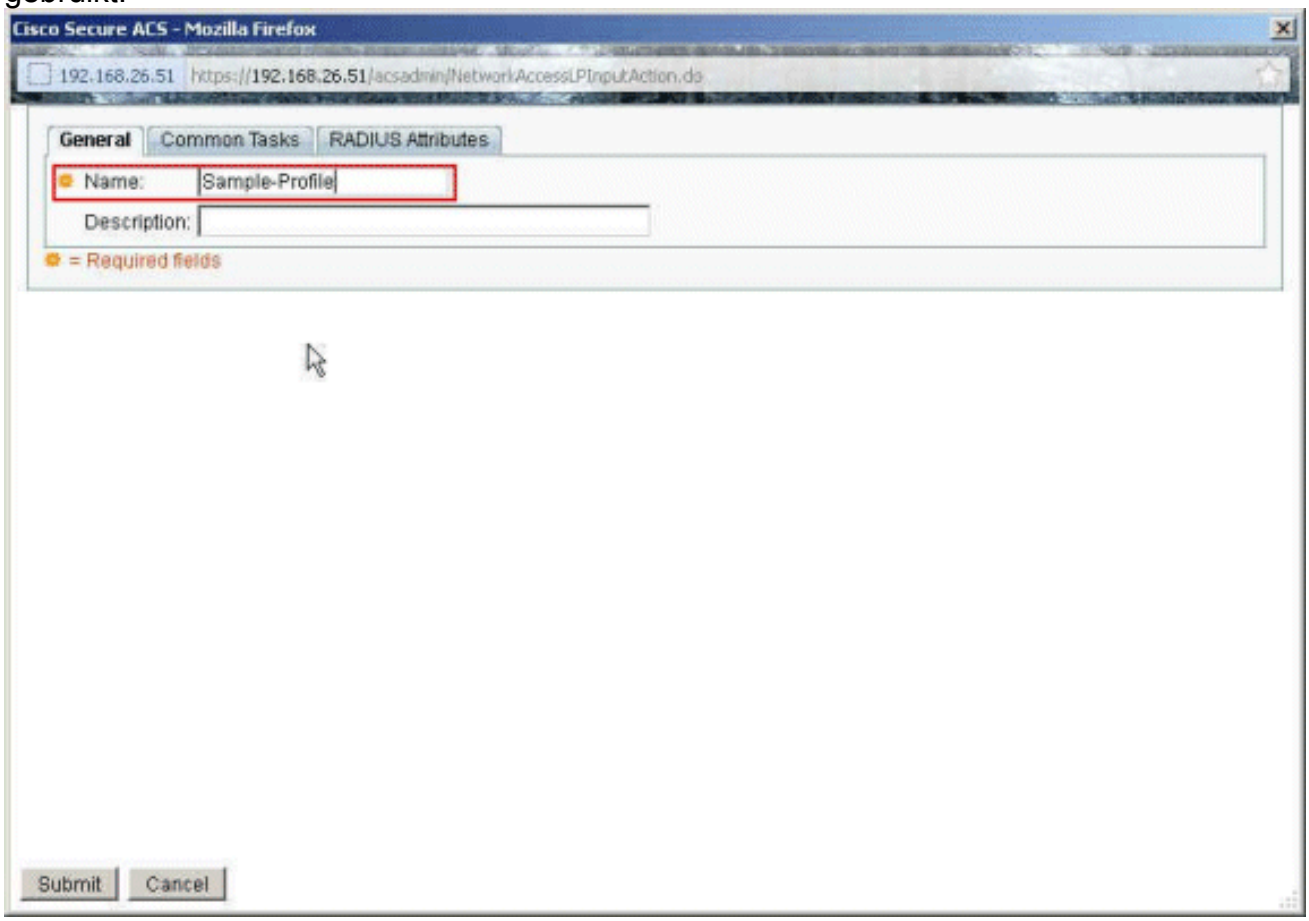
17. Klik op **Selecteren**.



18. Klik op **Maken** om een nieuw Auditprofiel te maken.

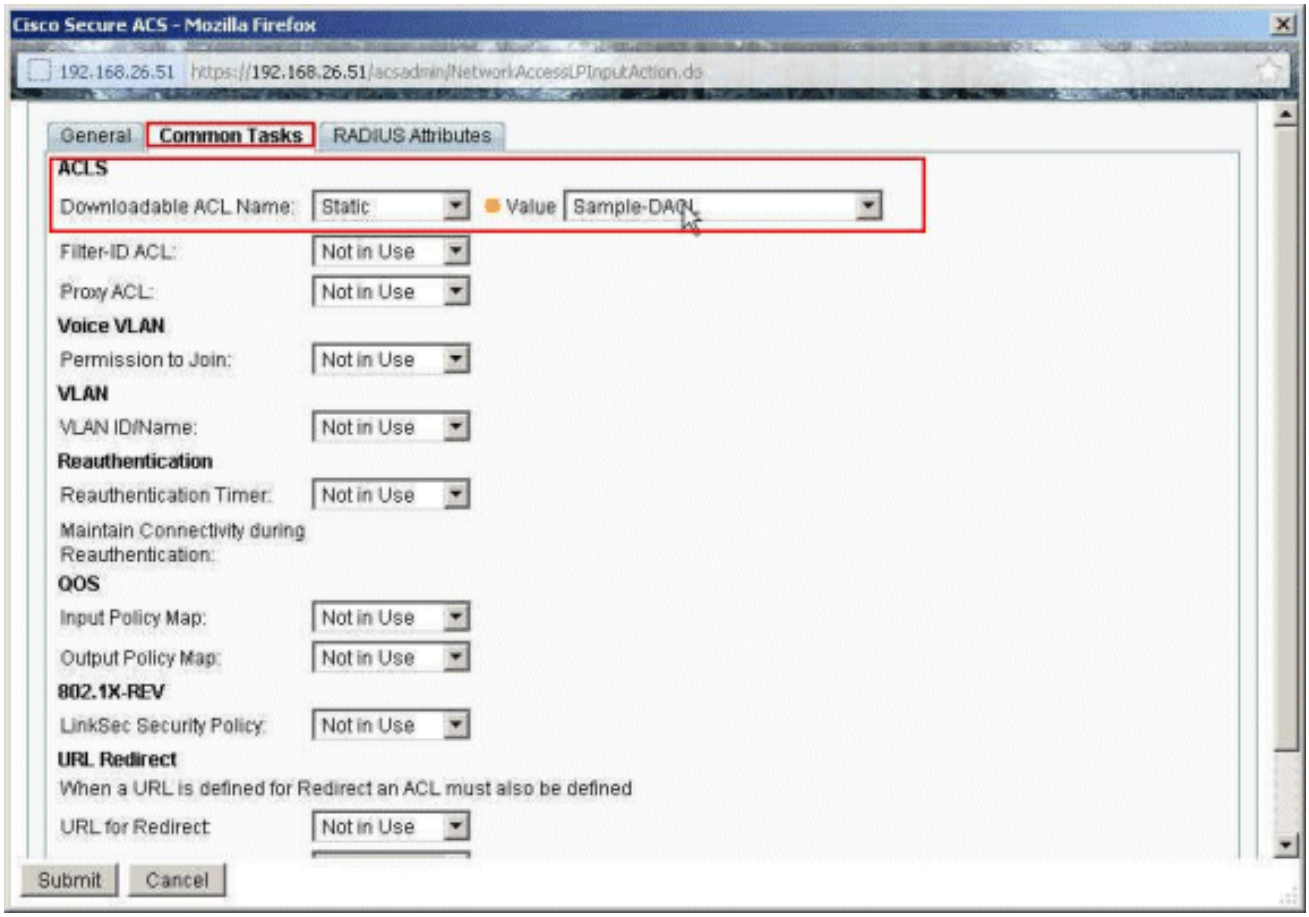


19. Geef een naam op voor het **machtigingsprofiel**. In dit voorbeeld wordt **een voorbeeldprofiel** gebruikt.

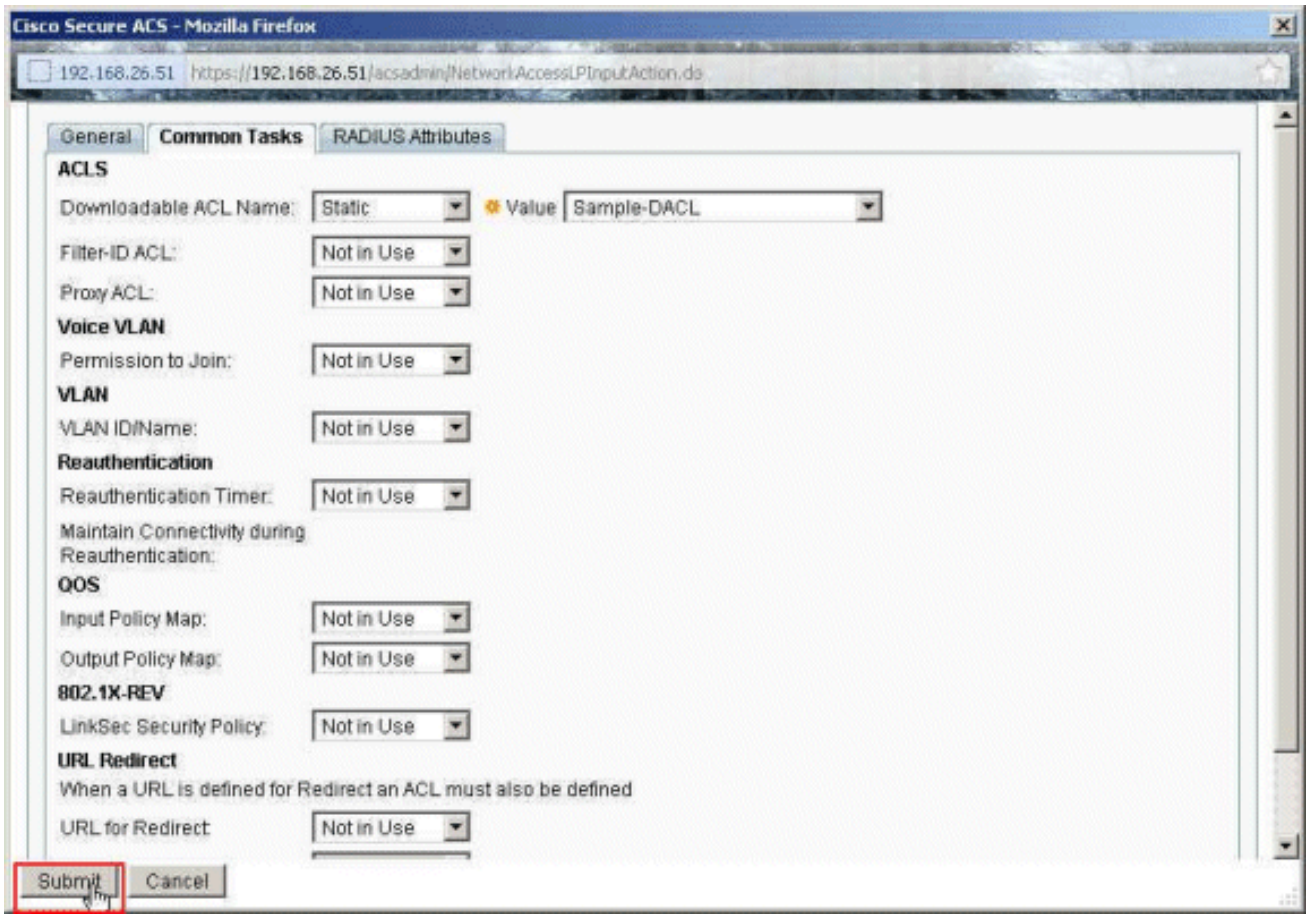


20. Kies het tabblad **Gemeenschappelijke taken** en selecteer **Statisch** uit de vervolgkeuzelijst voor de **downloadbare ACL-naam**. Kies de nieuwe **DACL (Steekproef -DACL)** uit de vervolgkeuzelijst

waarde.

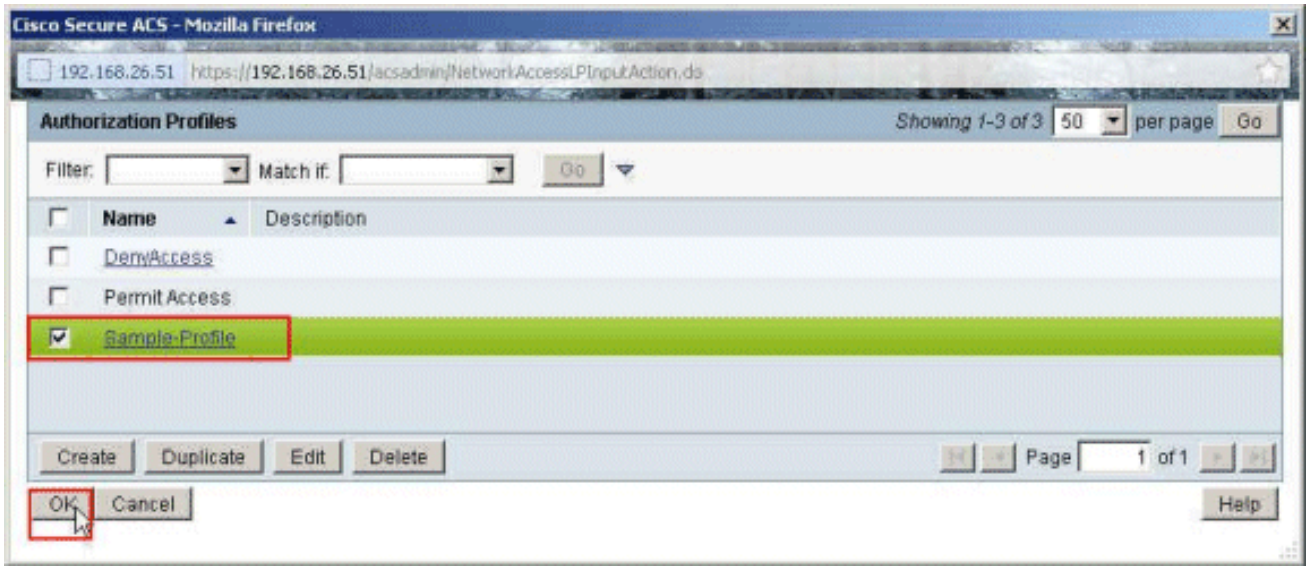


21. Klik op **Inzenden**.

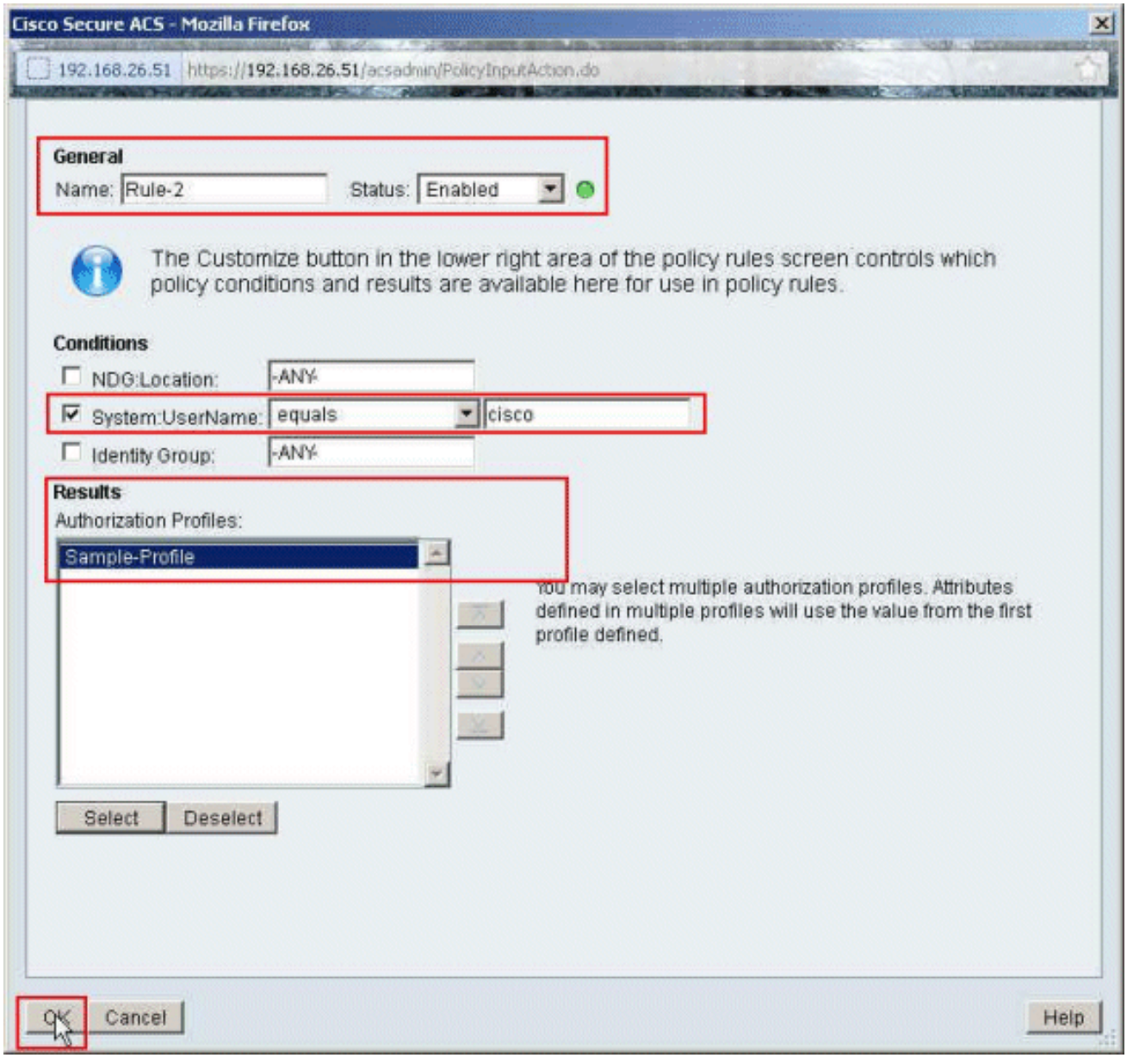


22. Controleer of het selectieteken naast **profiel** van het **monster** (het nieuw gemaakte machtigingsprofiel) is ingeschakeld en klik op

OK.

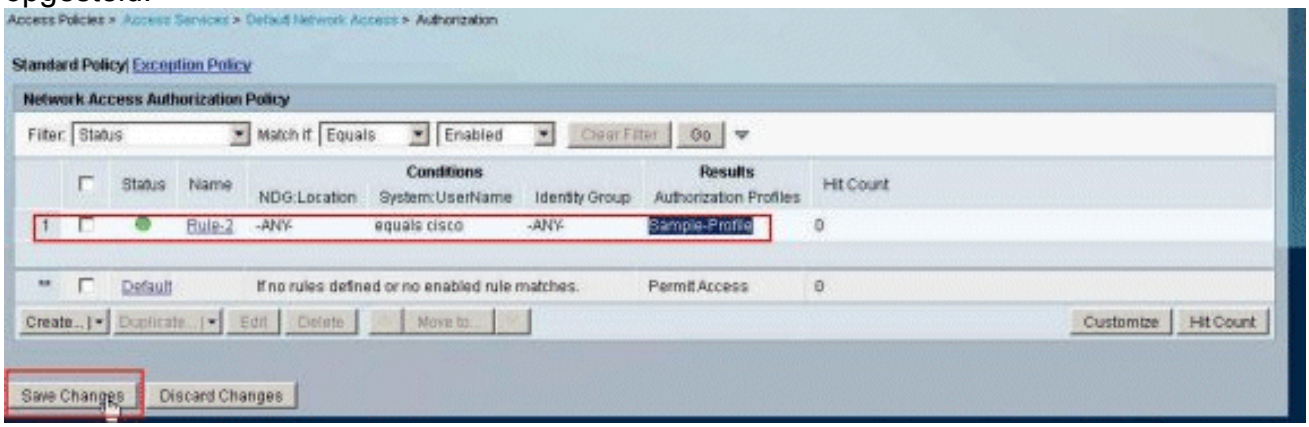


23. Nadat u hebt geverifieerd dat het nieuwe **voorbeeldprofiel** is geselecteerd in het veld **Verificatieprofielen**, klikt u op
OK.



24. Controleer dat de nieuwe regel (**regel-2**) met System:UserName **is** gelijk aan **cisco-**voorwaarden en **voorbeeldprofiel** als resultaat. Klik op **Wijzigingen opslaan**. Regel 2 wordt

succesvol opgesteld.



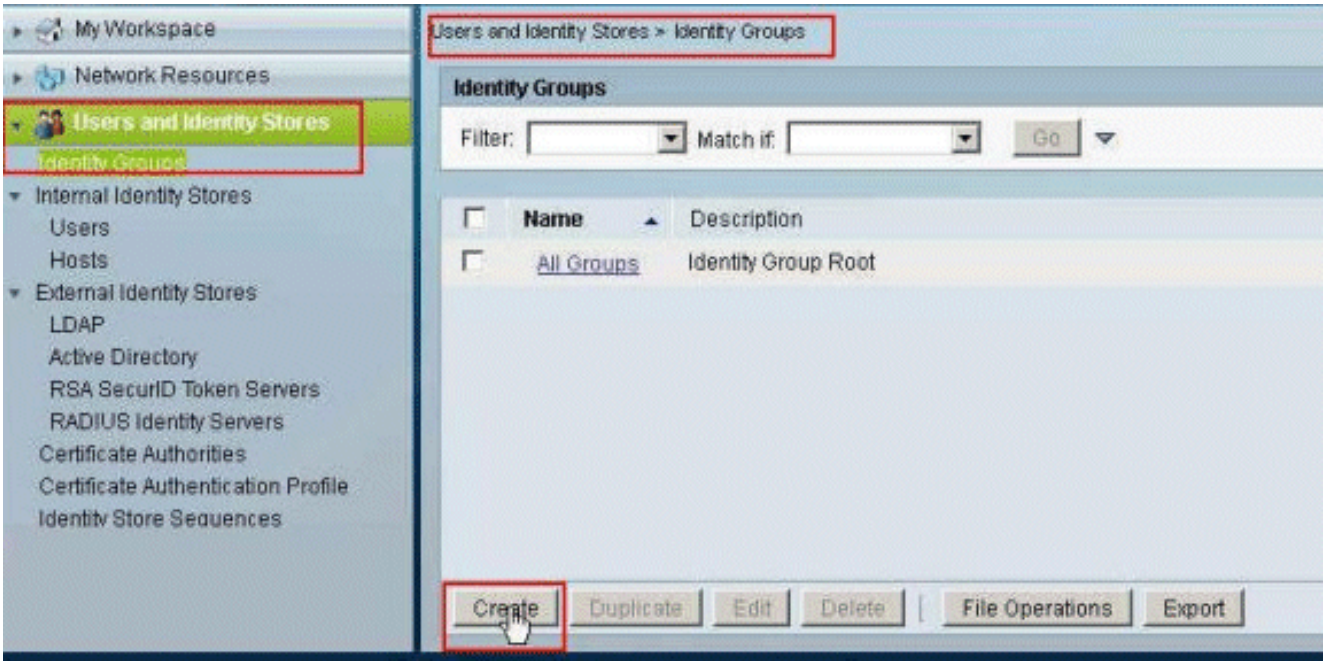
ACS voor downloadbare ACL voor groep configureren

Voltooi stap 1 tot en met 12 van het configureren ACS voor downloadbare ACL voor individuele gebruiker en voer deze stappen uit om downloadbare ACL voor groep te configureren in een Cisco Secure ACS.

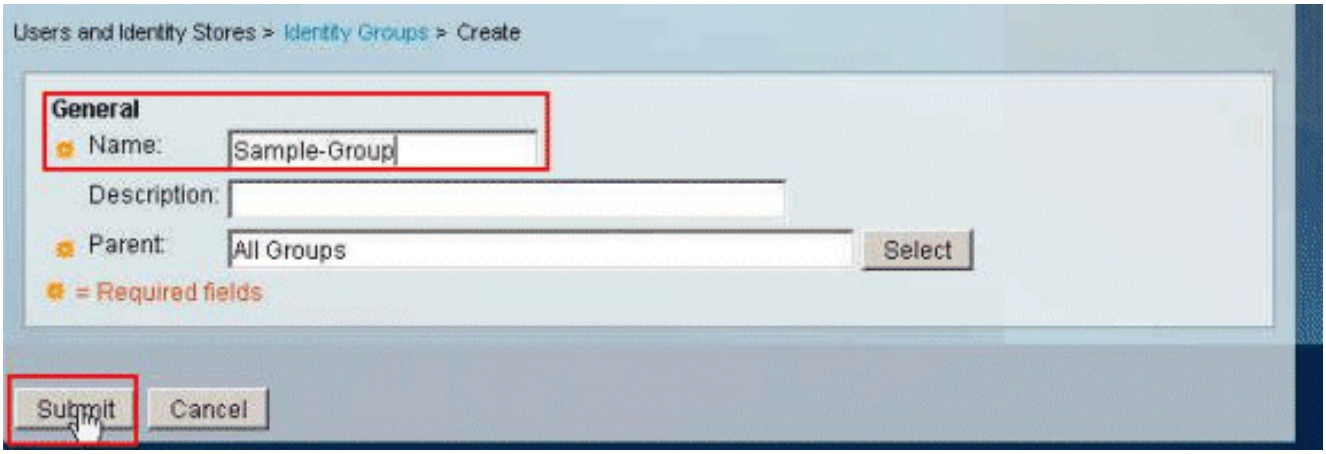
In dit voorbeeld hoort de IPsec VPN-gebruiker "cisco" tot de **voorbeeldgroep**.

De **Cisco-voorbeeldgebruiker** is geauthentiek en de RADIUS-server stuurt een downloadbare toegangslijst naar het beveiligingsapparaat. De gebruiker "cisco" heeft alleen toegang tot de 10.1.1.2 server en ontkent alle andere toegang. Raadpleeg het gedeelte Downloadbare ACL's om de ACL's te controleren.

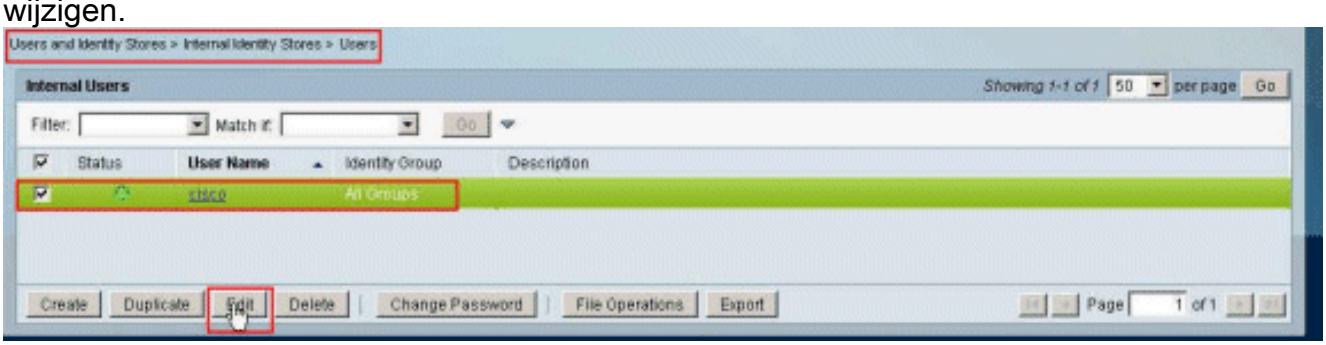
1. Klik in de navigatiebalk op **Gebruikers en identiteitsopslag** > **Identiteitsgroepen** en klik op **Maken** om een nieuwe groep te maken.



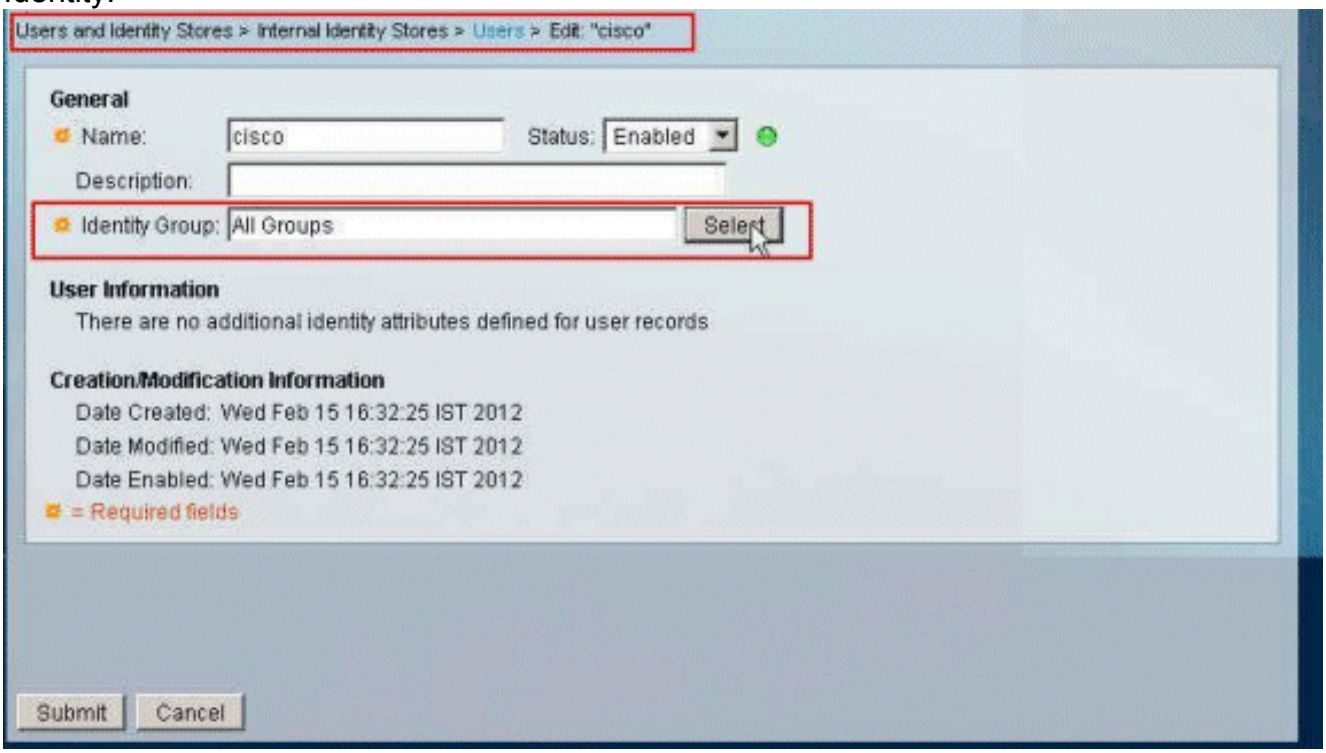
2. Typ een groepsnaam (**voorbeeldgroep**) en klik op **Indienen**.



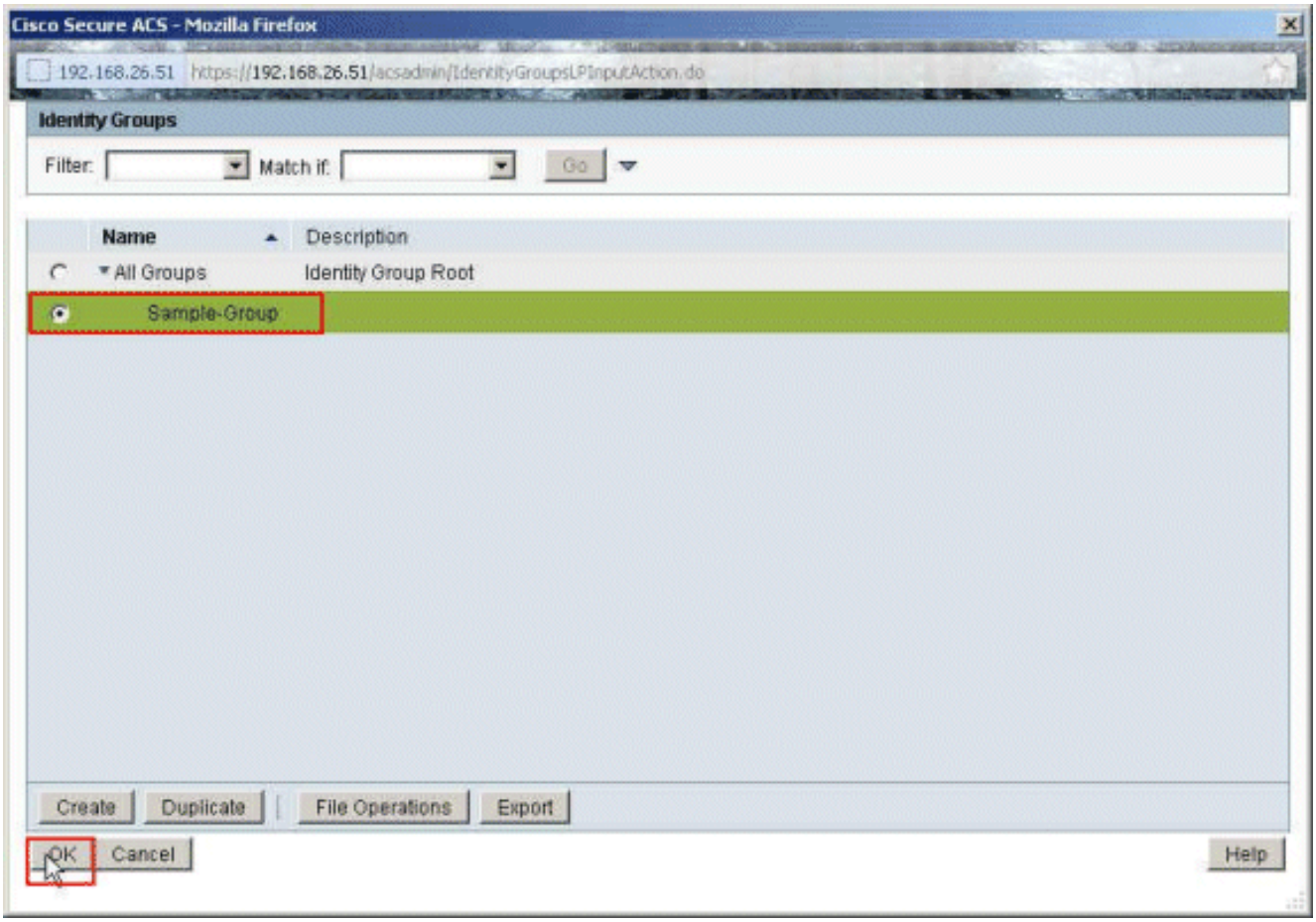
3. Kies **Gebruiker identiteitsopslag > Interne identiteitsopslag > Gebruikers** en selecteer de gebruiker **cisco**. Klik op **Bewerken** om het groepslidmaatschap van deze gebruiker te wijzigen.



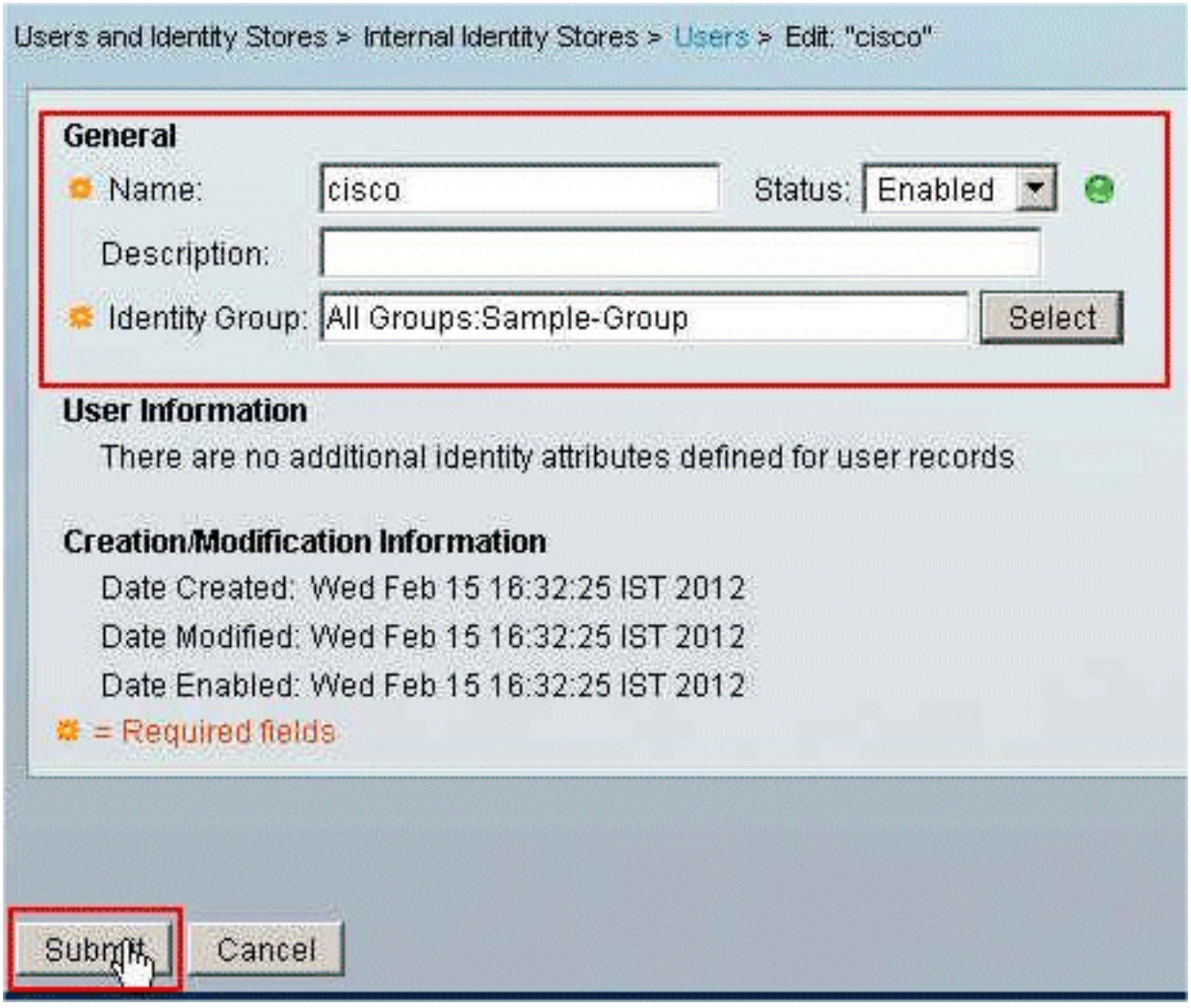
4. Klik op **Selecteer** naast de groep Identity.



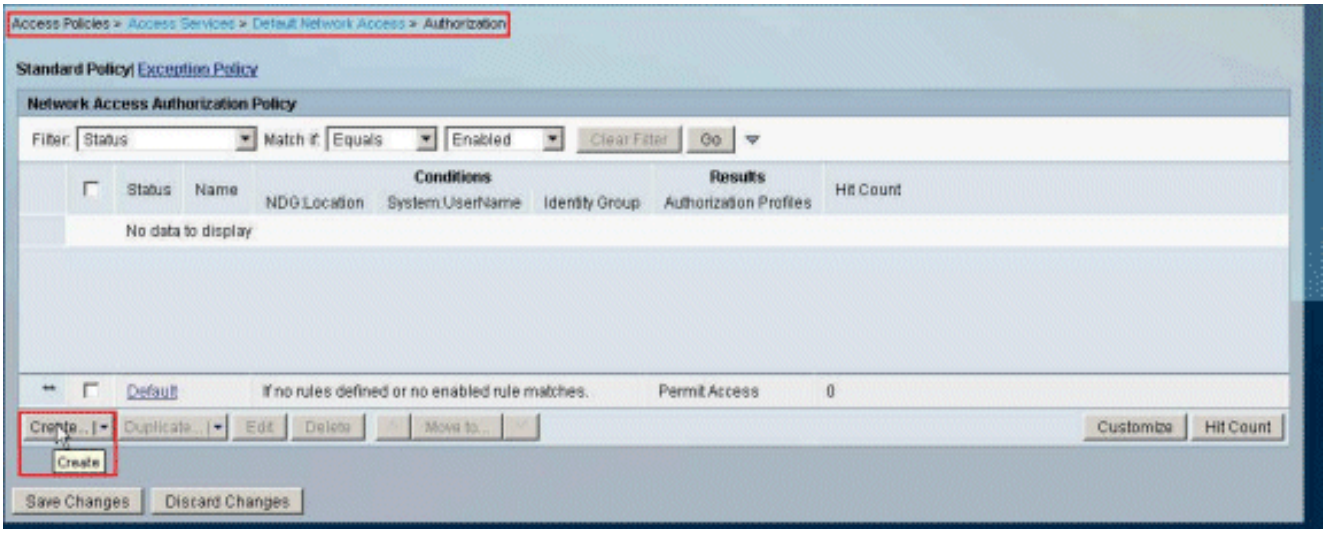
5. Selecteer de nieuwe groep (dat wil zeggen de **voorbeeldgroep**) en klik op **OK**.



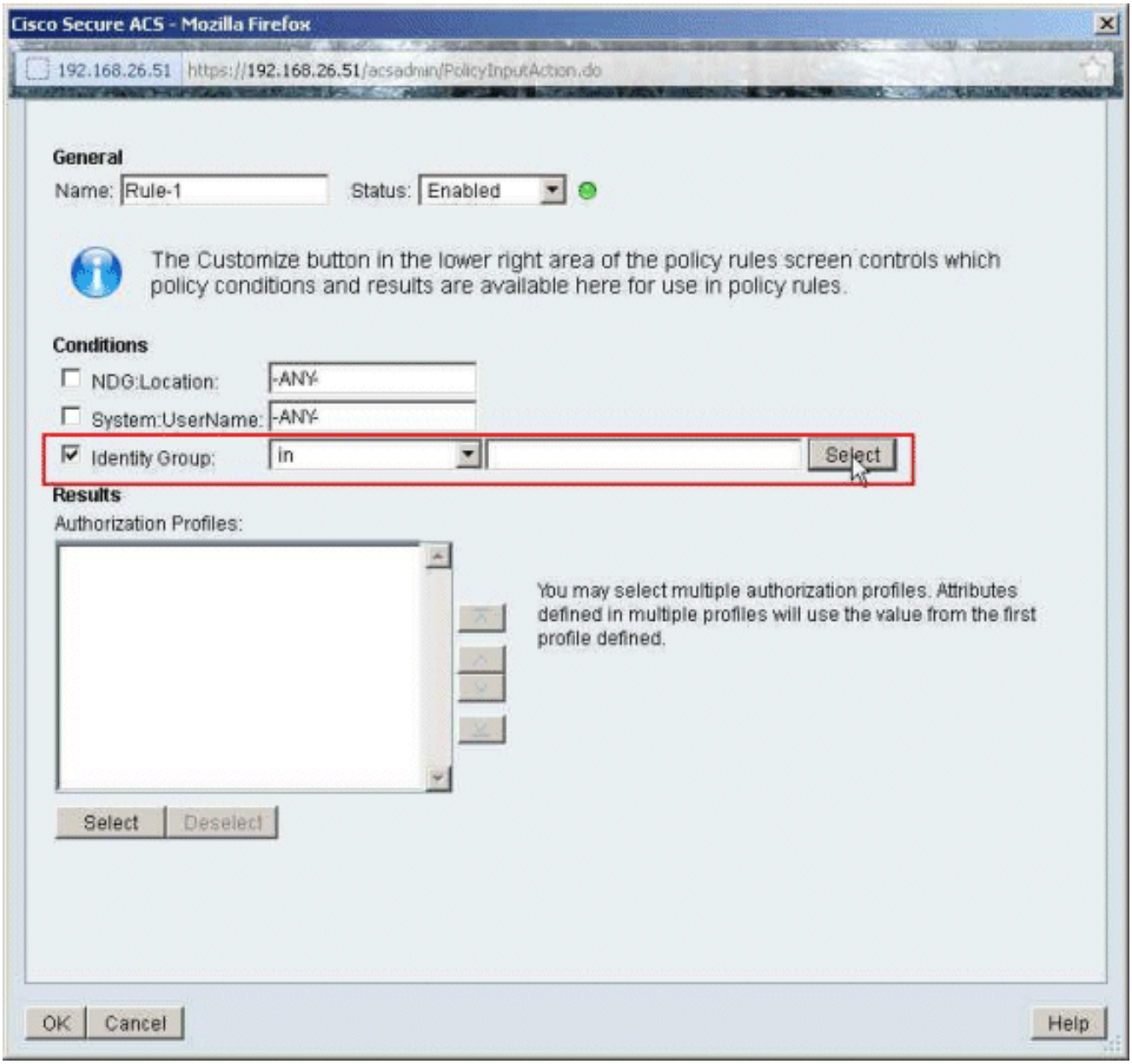
6. Klik op **Inzenden**.



7. Kies **Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang > autorisatie** en klik op **Maken om een nieuwe regel te maken.**

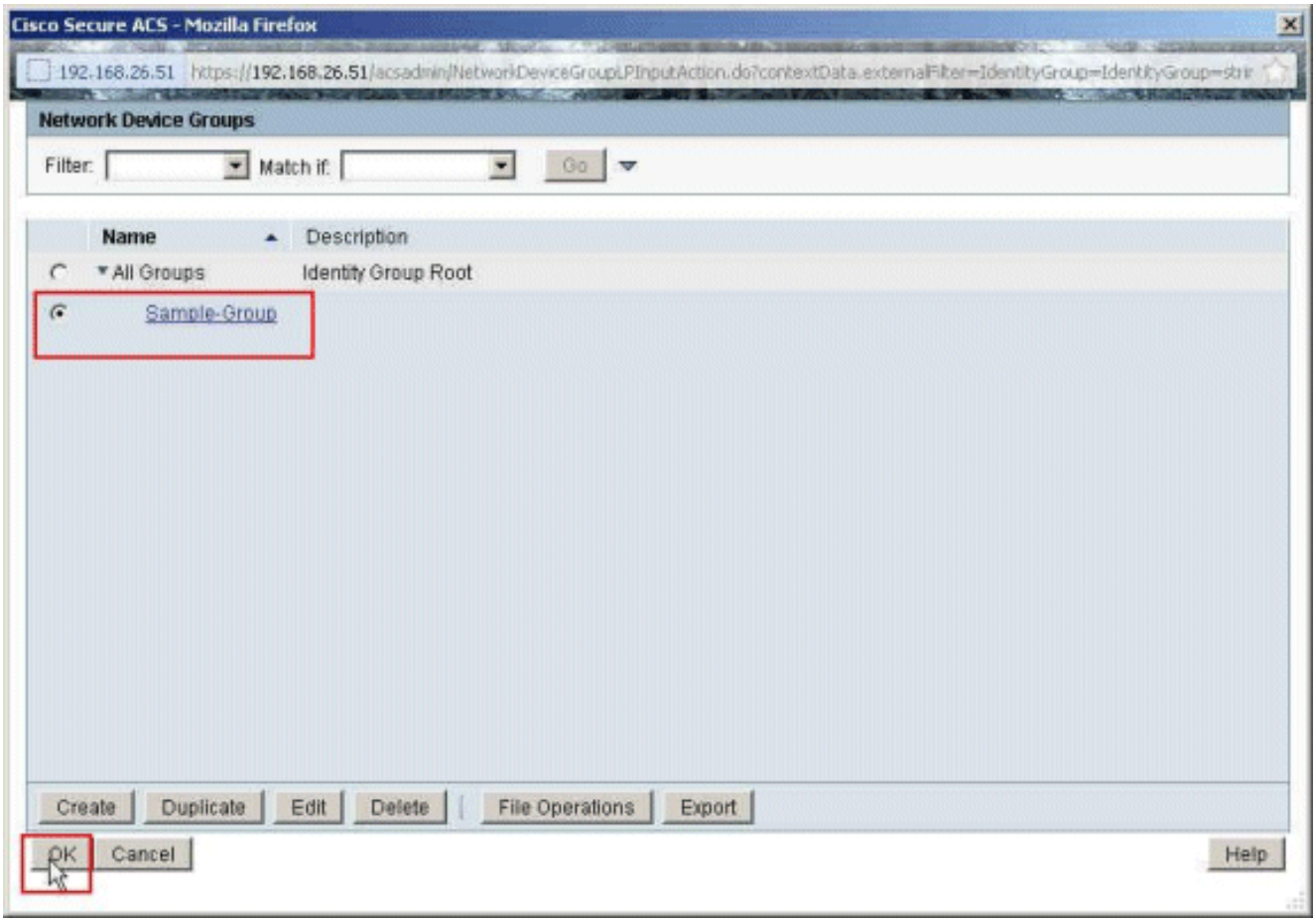


8. Controleer of het selectieteken naast **Identity Group** ingeschakeld is en klik vervolgens op **Selecteren**.

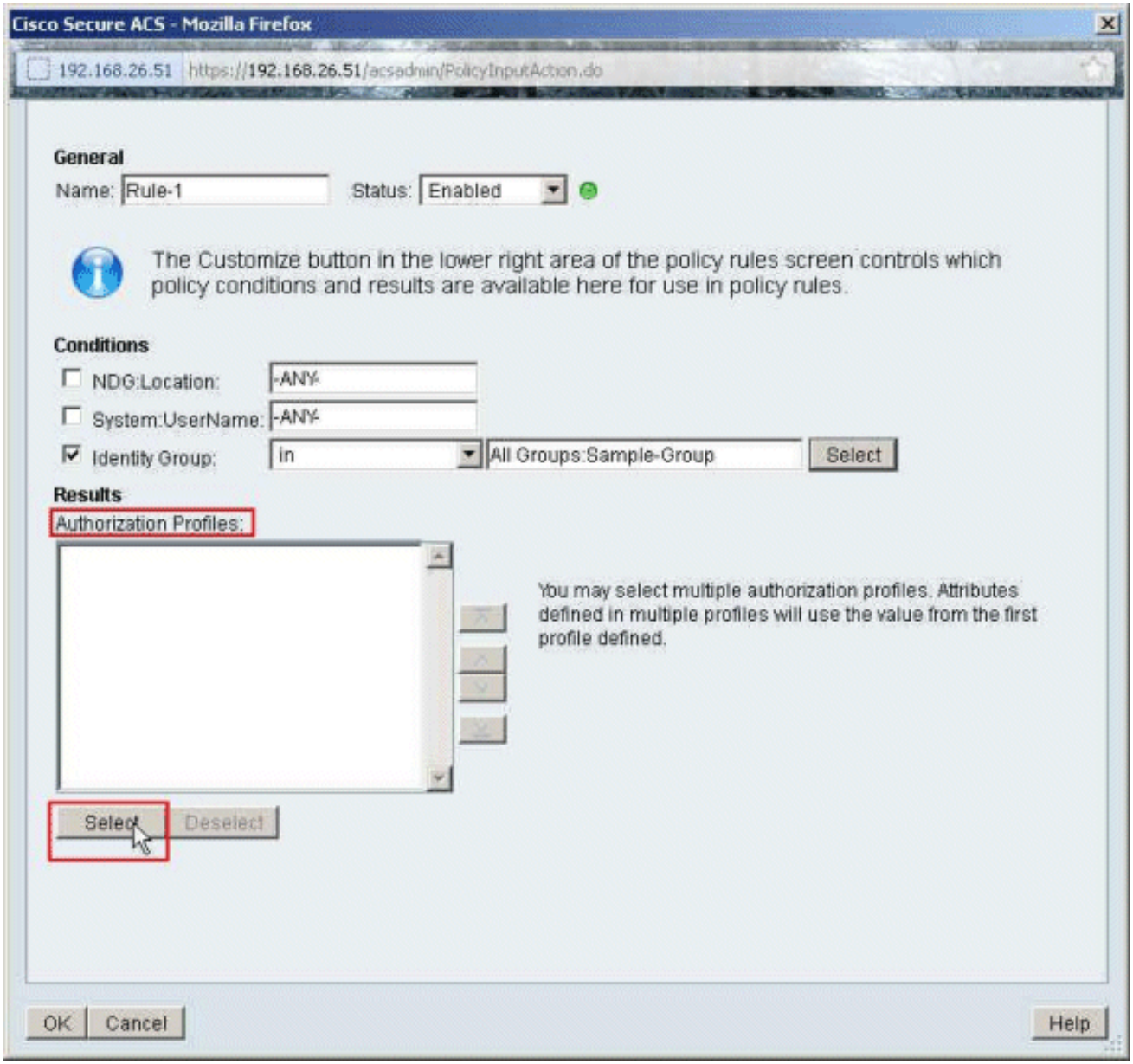


9. Kies **een voorbeeldgroep** en klik op

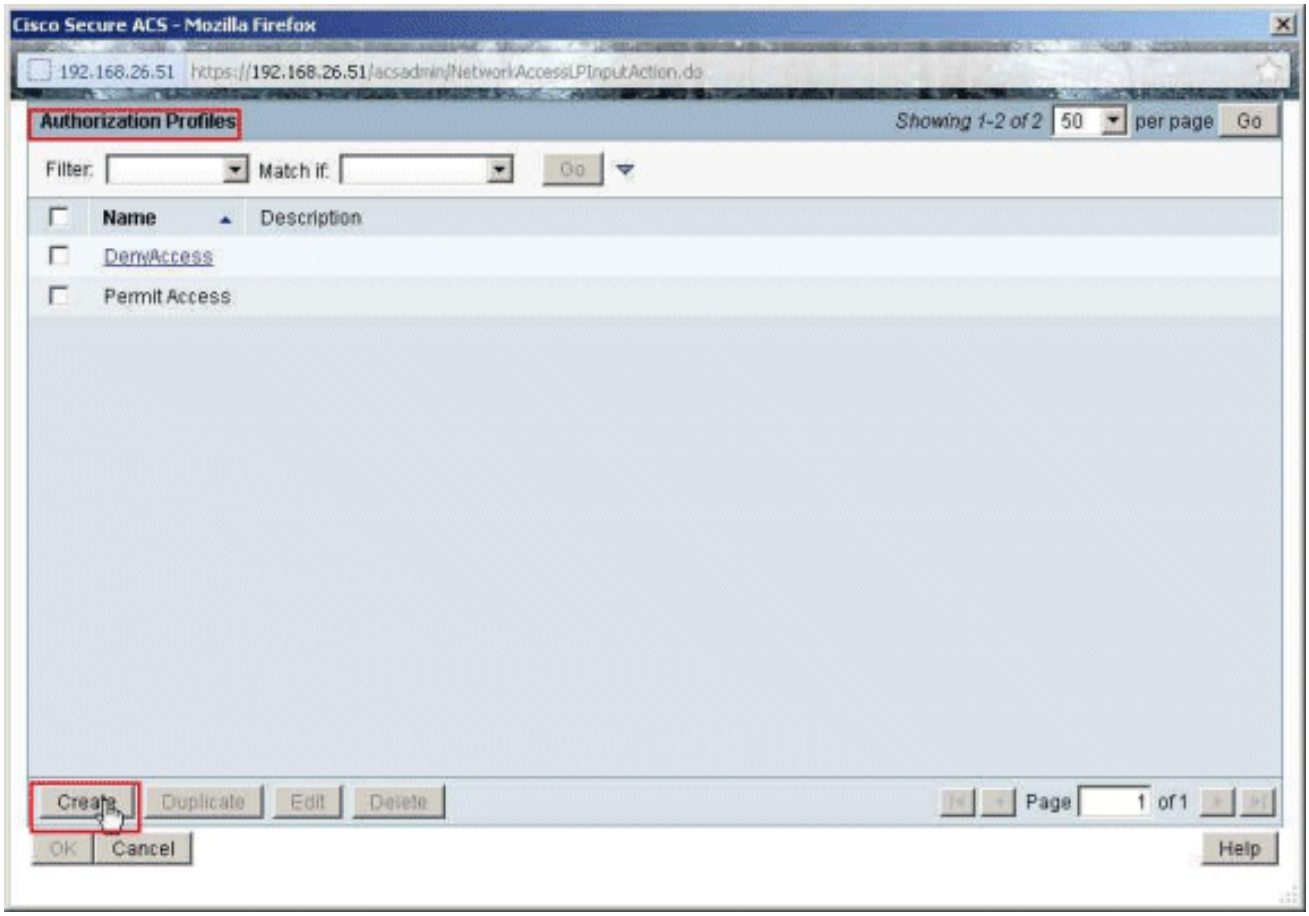
OK.



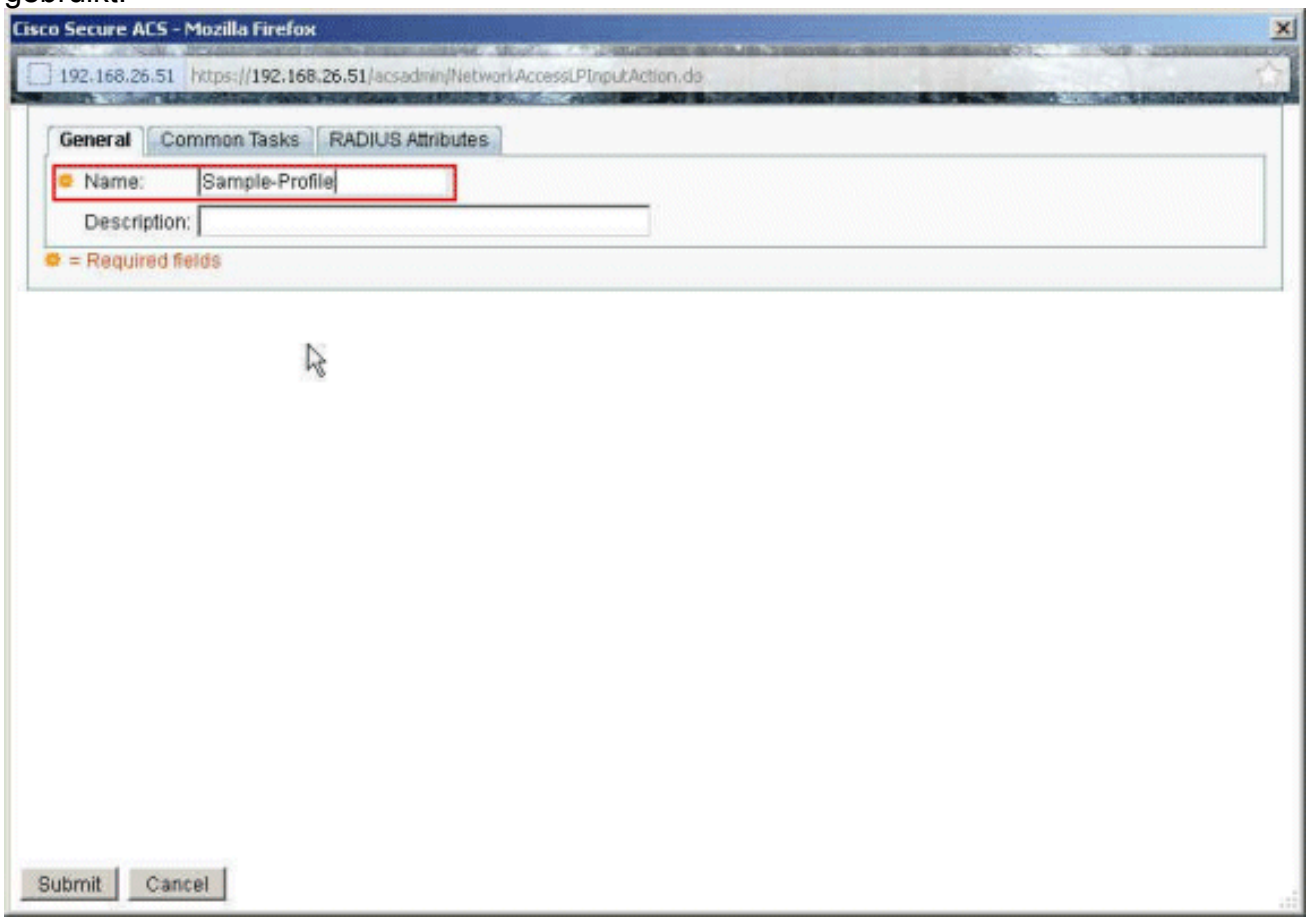
10. Klik op **Selecteren** in het gedeelte Automation Profiles.



11. Klik op **Maken** om een nieuw Auditprofiel te maken.

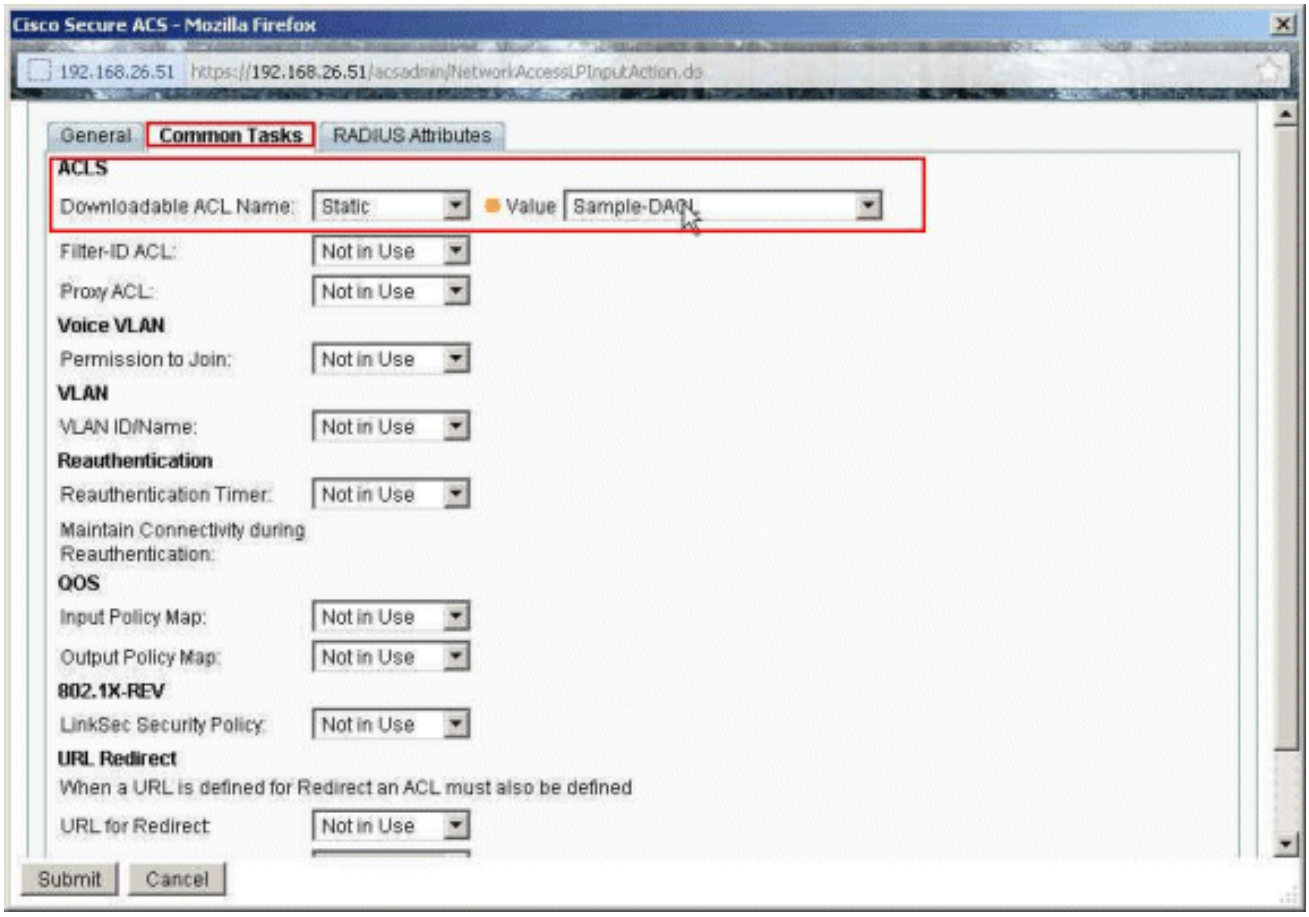


12. Geef een naam op voor het **machtigingsprofiel**. **Monster-profiel** is de naam die in dit voorbeeld wordt
gebruikt.

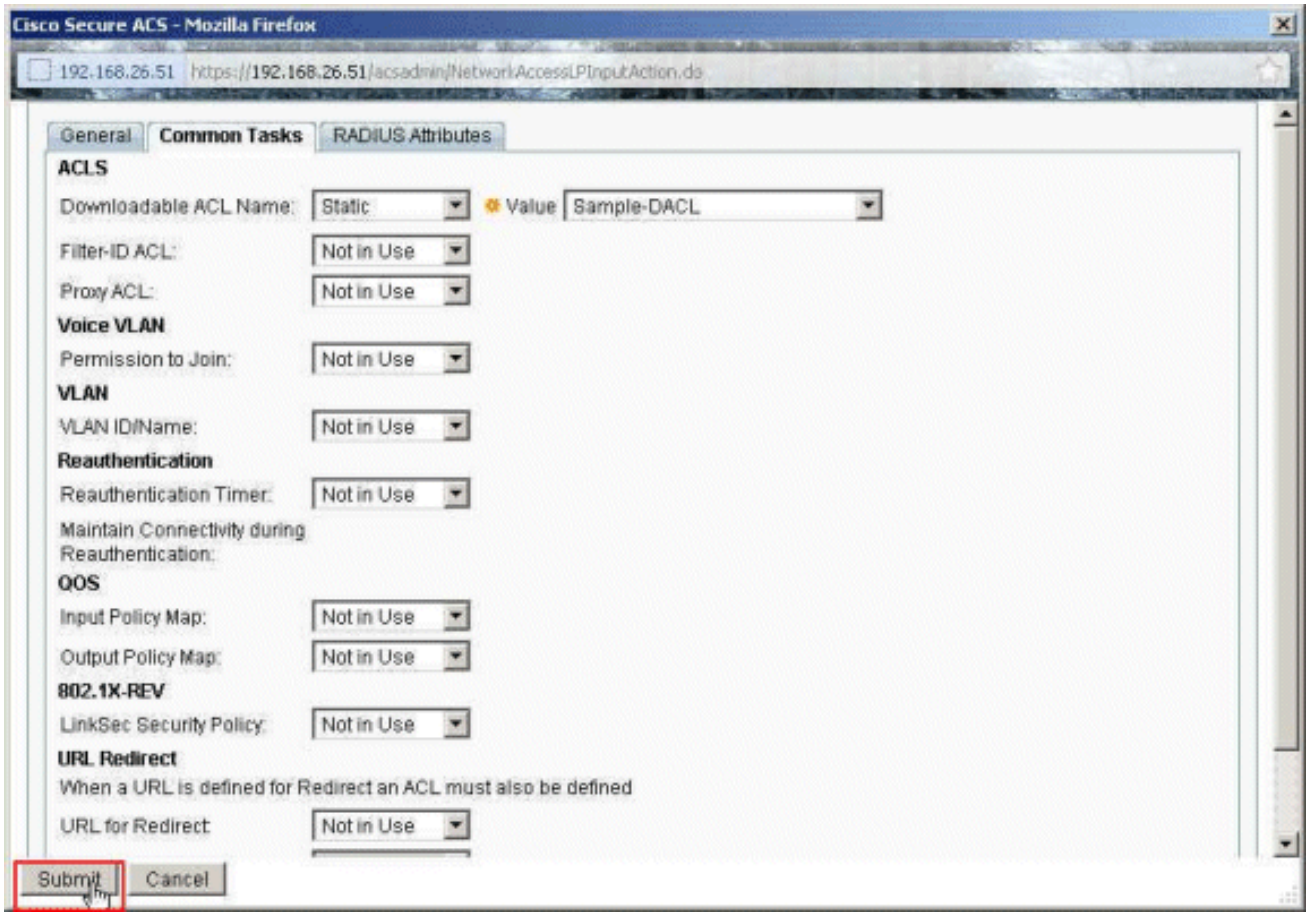


13. Kies het tabblad **Gemeenschappelijke taken** en selecteer **Statisch** uit de vervolgkeuzelijst voor de **downloadbare ACL-naam**. Kies de nieuwe **DACL (Steekproef -DACL)** van de

vervolgkeuzelijst
Waarde.

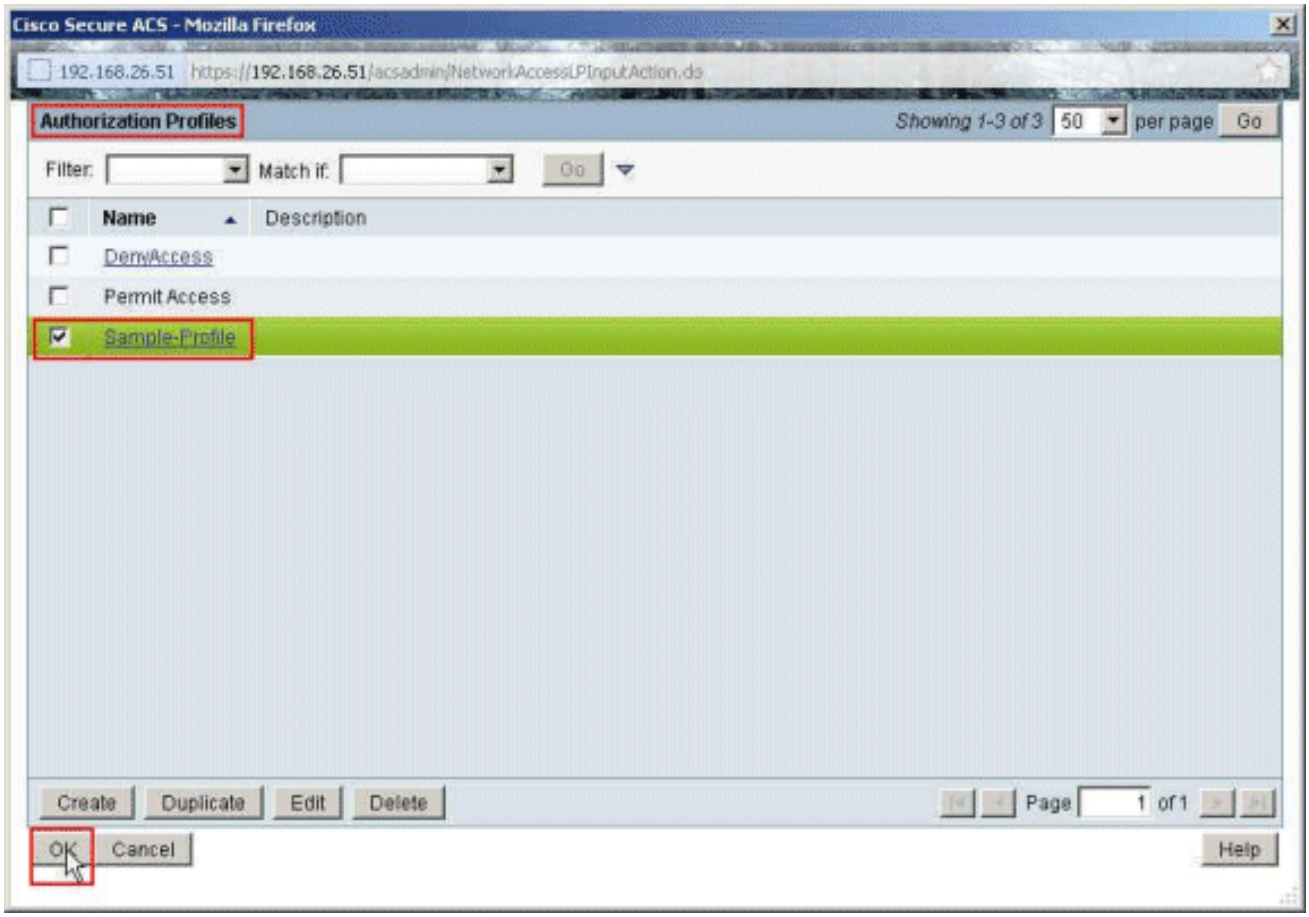


14. Klik op
Inzenden.

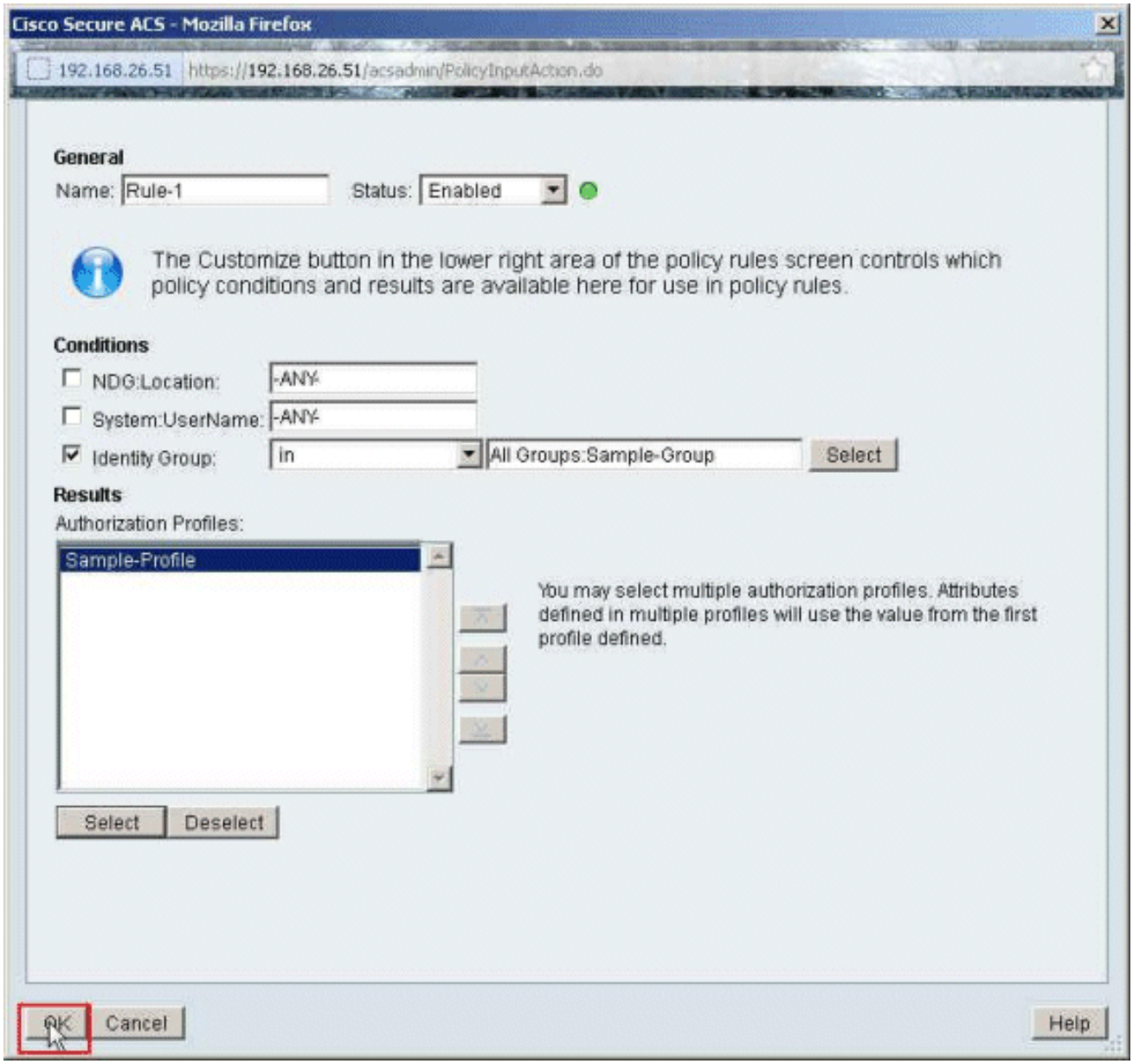


15. Kies het **voorbeeldprofiel** van het autorisatieprofiel dat eerder is gemaakt en klik op

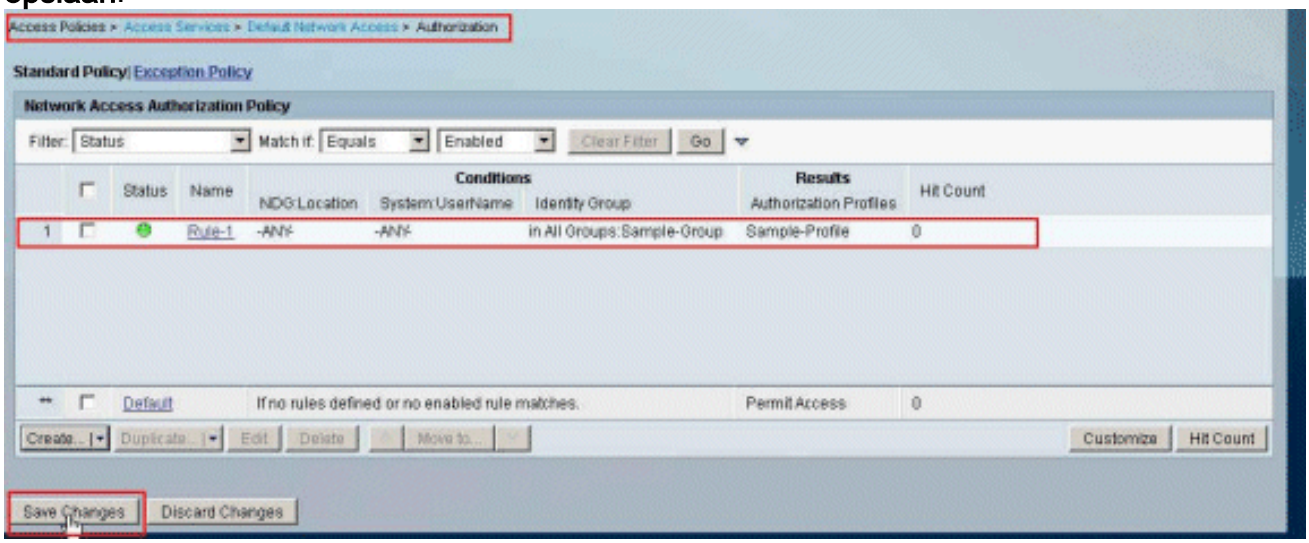
OK.



16. Klik op
OK.



17. Controleer dat **regel-1** met de **voorbeeldgroep** van de Identity Group als voorwaarde en **voorbeeldprofiel** als resultaat wordt gemaakt. Klik op **Wijzigingen opslaan**.



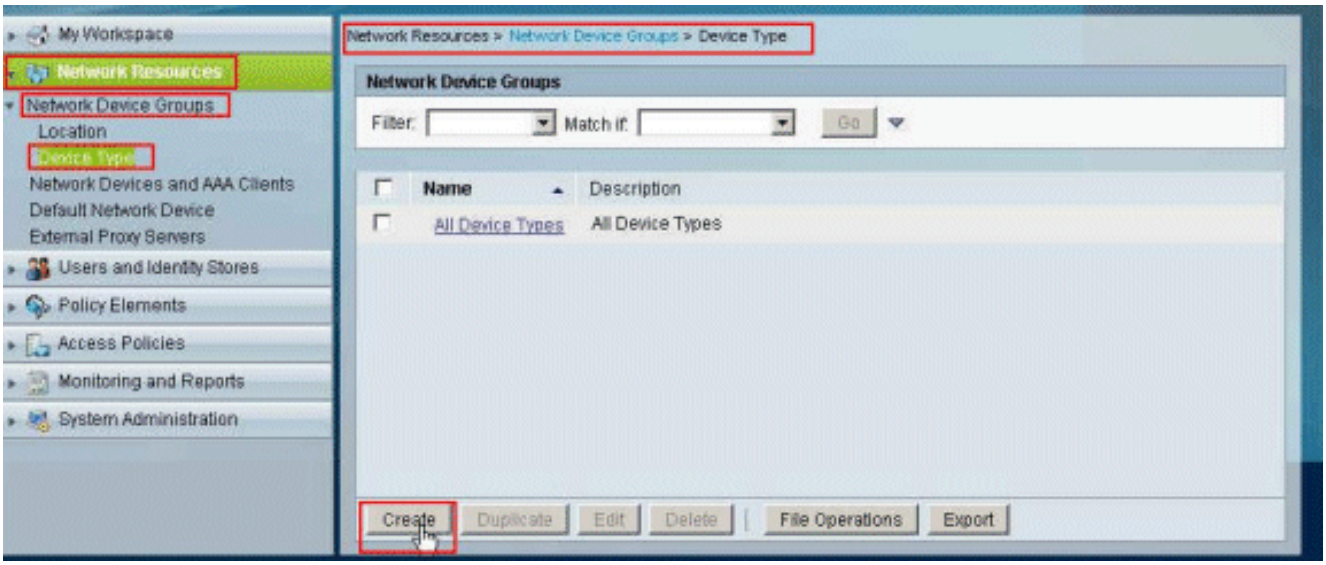
ACS voor downloadbare ACL voor een netwerkapparaatgroep configureren

Voltooi stap 1 tot en met 12 van het configureren ACS voor downloadbare ACL voor individuele

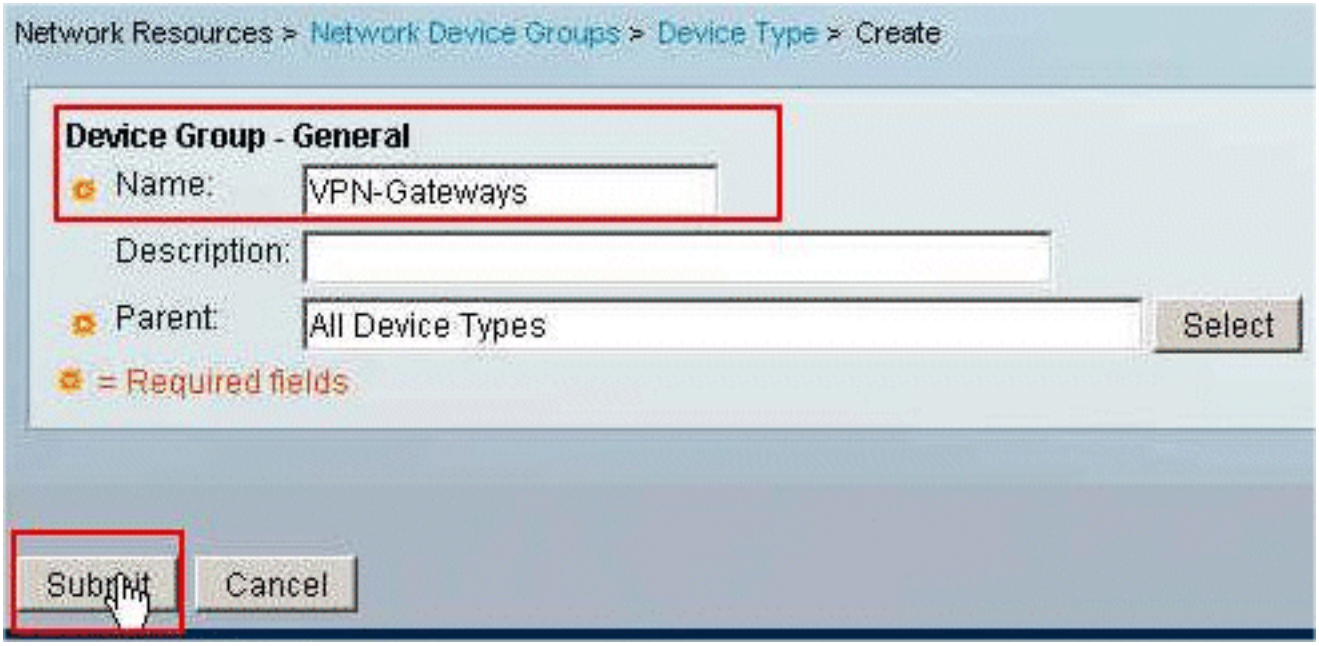
gebruiker en voer deze stappen uit om downloadbare ACL voor een netwerkapparaatgroep in een Cisco Secure ACS te configureren.

In dit voorbeeld behoort de RADIUS-client (ASA) tot de **VPN-gateways** van de netwerkapparaatgroep.De VPN-verificatieaanvraag afkomstig van ASA voor gebruiker 'cisco'-authenticeert met succes en de RADIUS-server stuurt een downloadbare toegangslijst naar het beveiligingsapparaat. De gebruiker "cisco" heeft alleen toegang tot de 10.1.1.2 server en ontkent alle andere toegang. Raadpleeg het gedeelte Downloadbare ACL's om de ACL's te controleren.

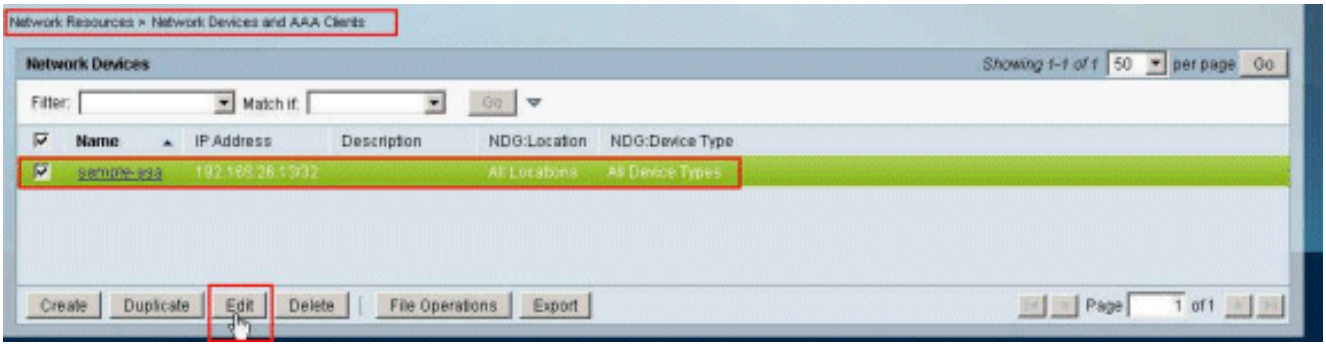
1. Kies **Netwerkbronnen > Netwerkapparaatgroepen > Apparaattype** en klik **op** Maken om een nieuwe netwerkapparaatgroep te maken.



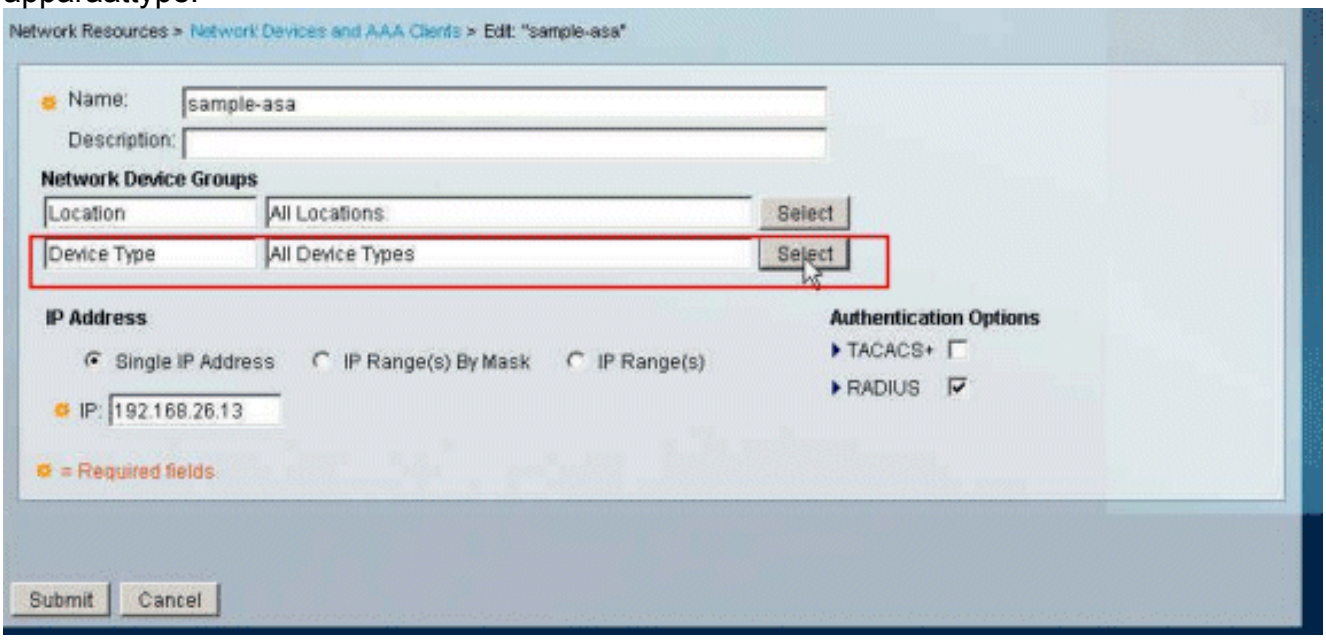
2. Geef een naam **van de Netwerkgroep op** (**VPN-gateways** in dit voorbeeld) en klik op **Inzenden**.



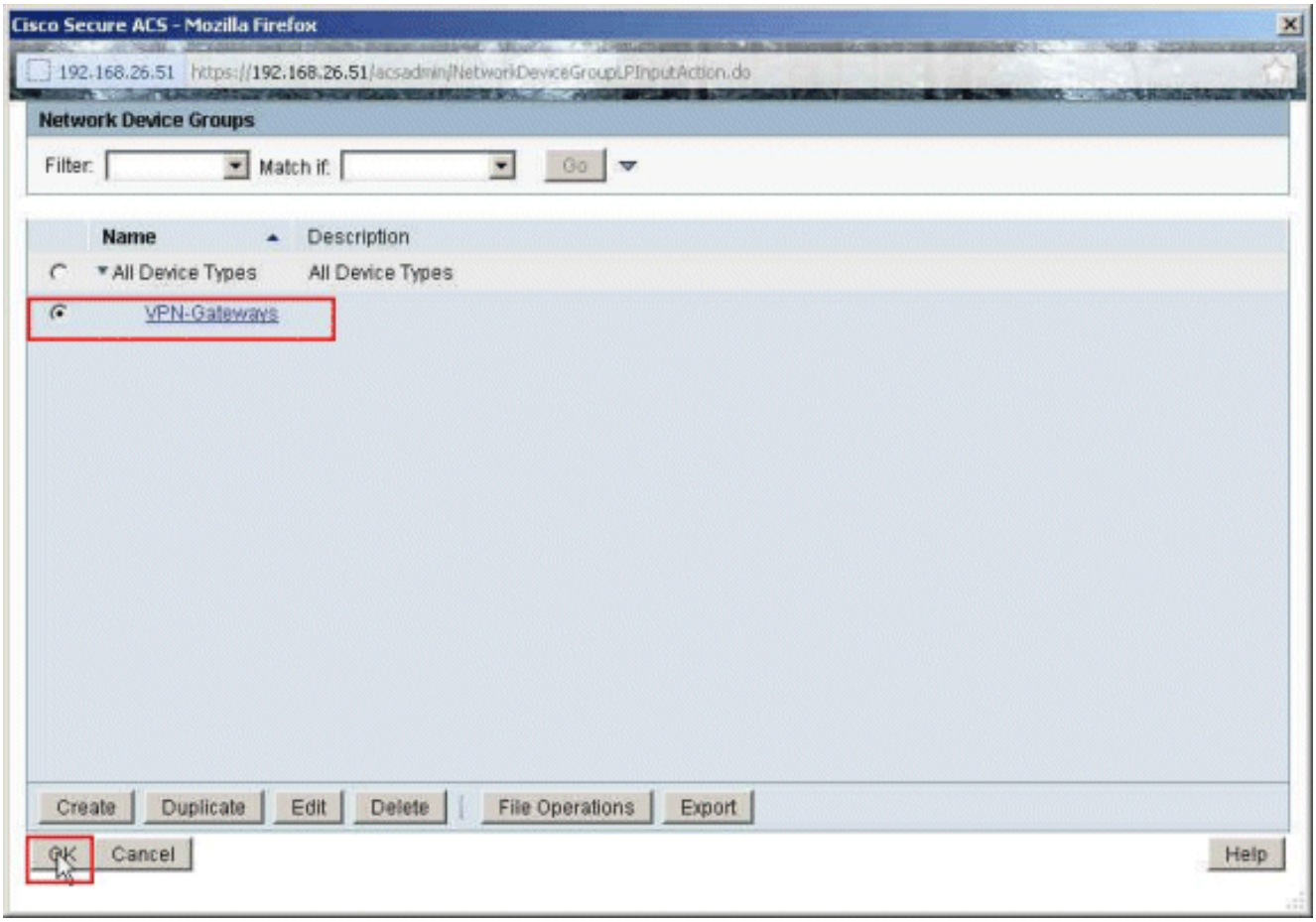
3. Kies **Netwerkbronnen > Netwerkapparaten en AAA-clients** en selecteer de **voorbeeldweergave** van de **RADIUS**-client. Klik op **Bewerken** om het lidmaatschap van de **Netwerkgroep** van deze RADIUS-client (ASA) te wijzigen.



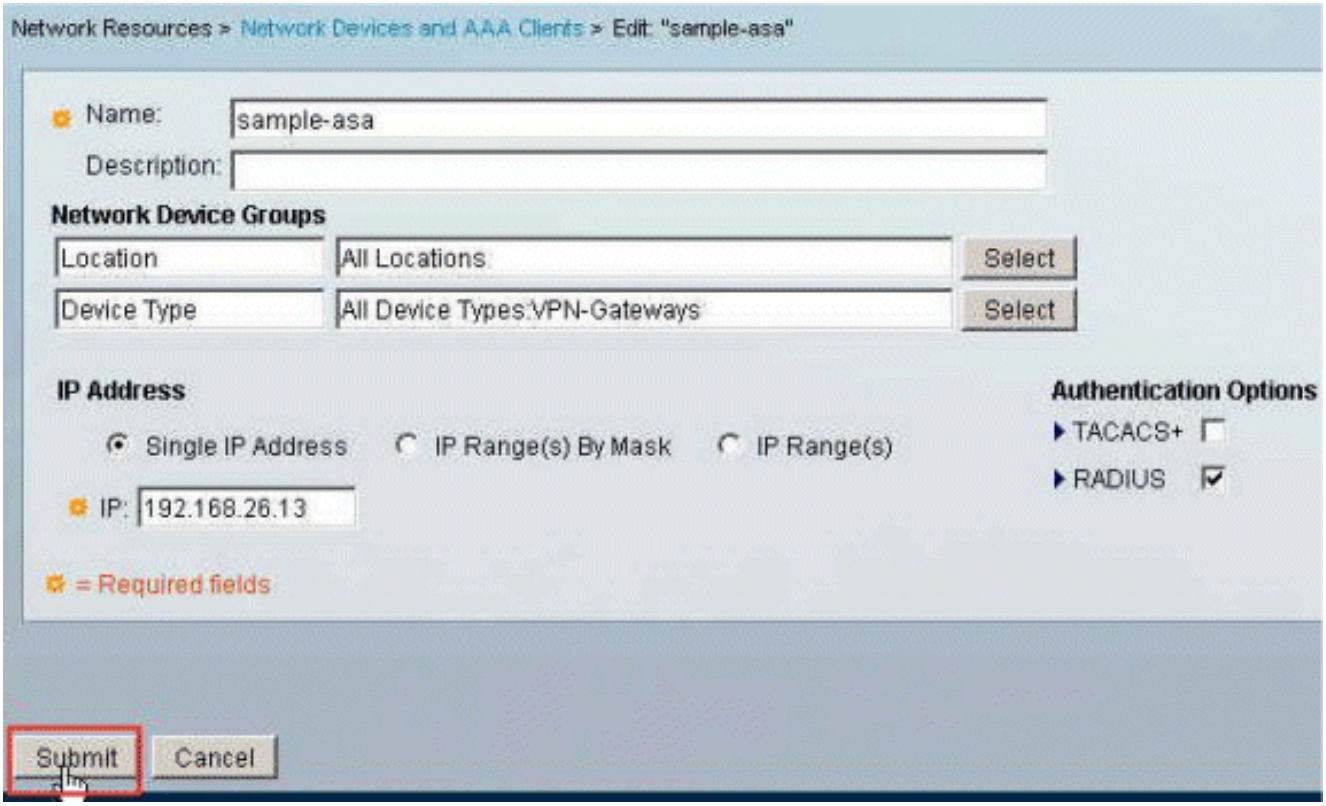
4. Klik op **Selecteer** naast het apparaattype.



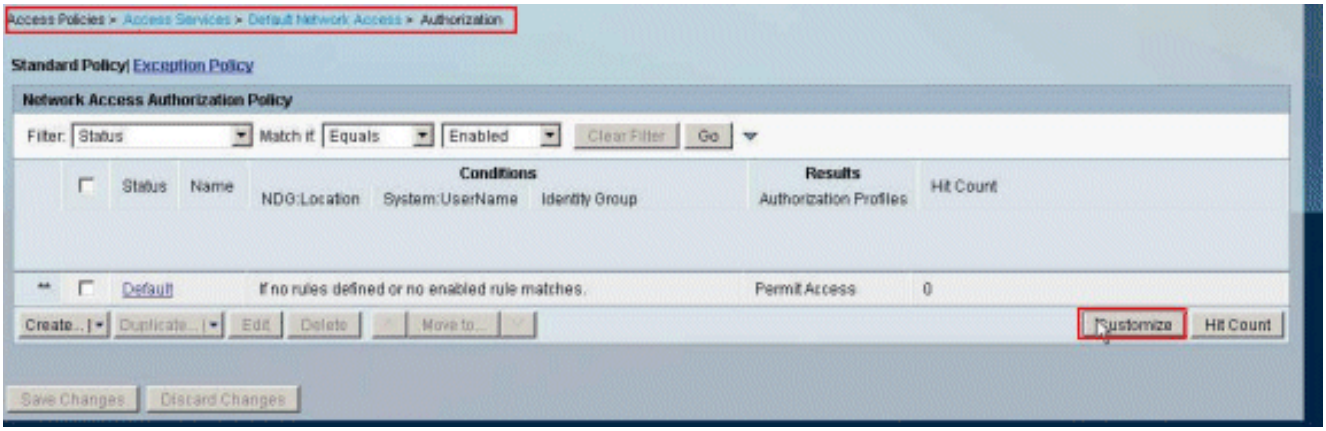
5. Selecteer de nieuwe groep van het Netwerkapparaat (**VPN-gateways**) en klik op **OK**.



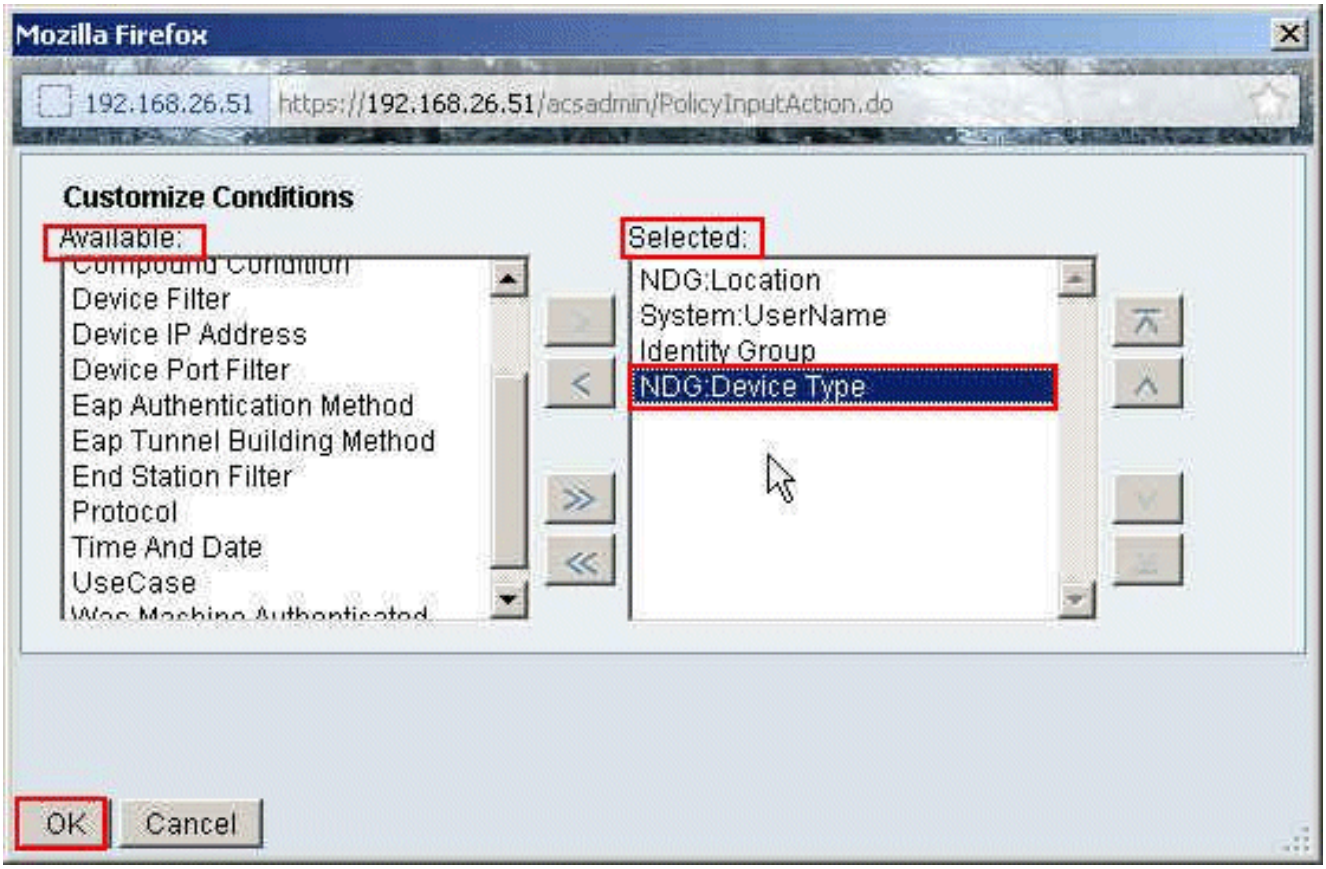
6. Klik op
Inzenden.



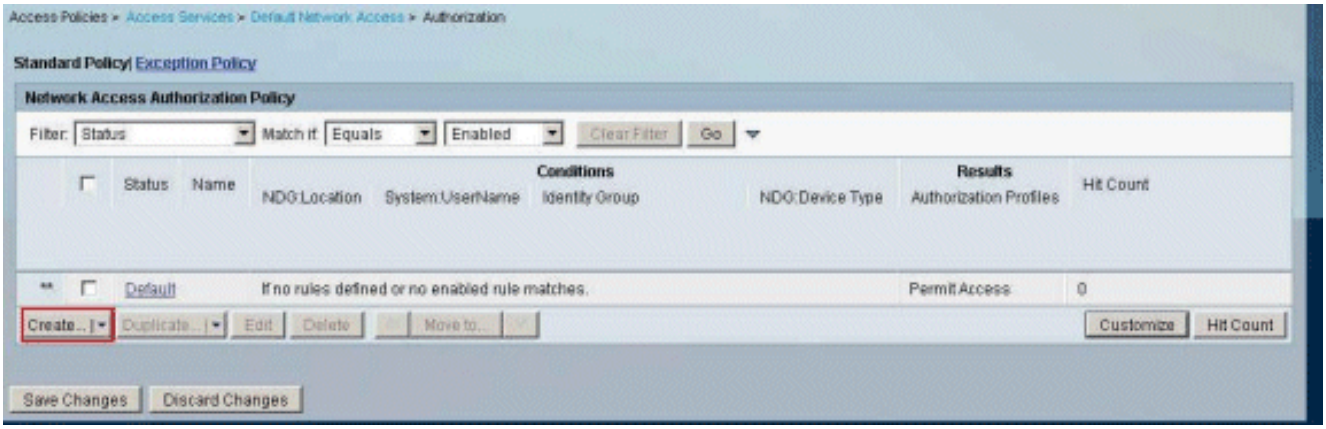
7. Kies **Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang > autorisatie** en klik **op**
Aanpassen.



8. Verplaats **NDG:Apparaattype** van het **Beschikbare** gedeelte naar het **geselecteerde** gedeelte en klik op
OK.

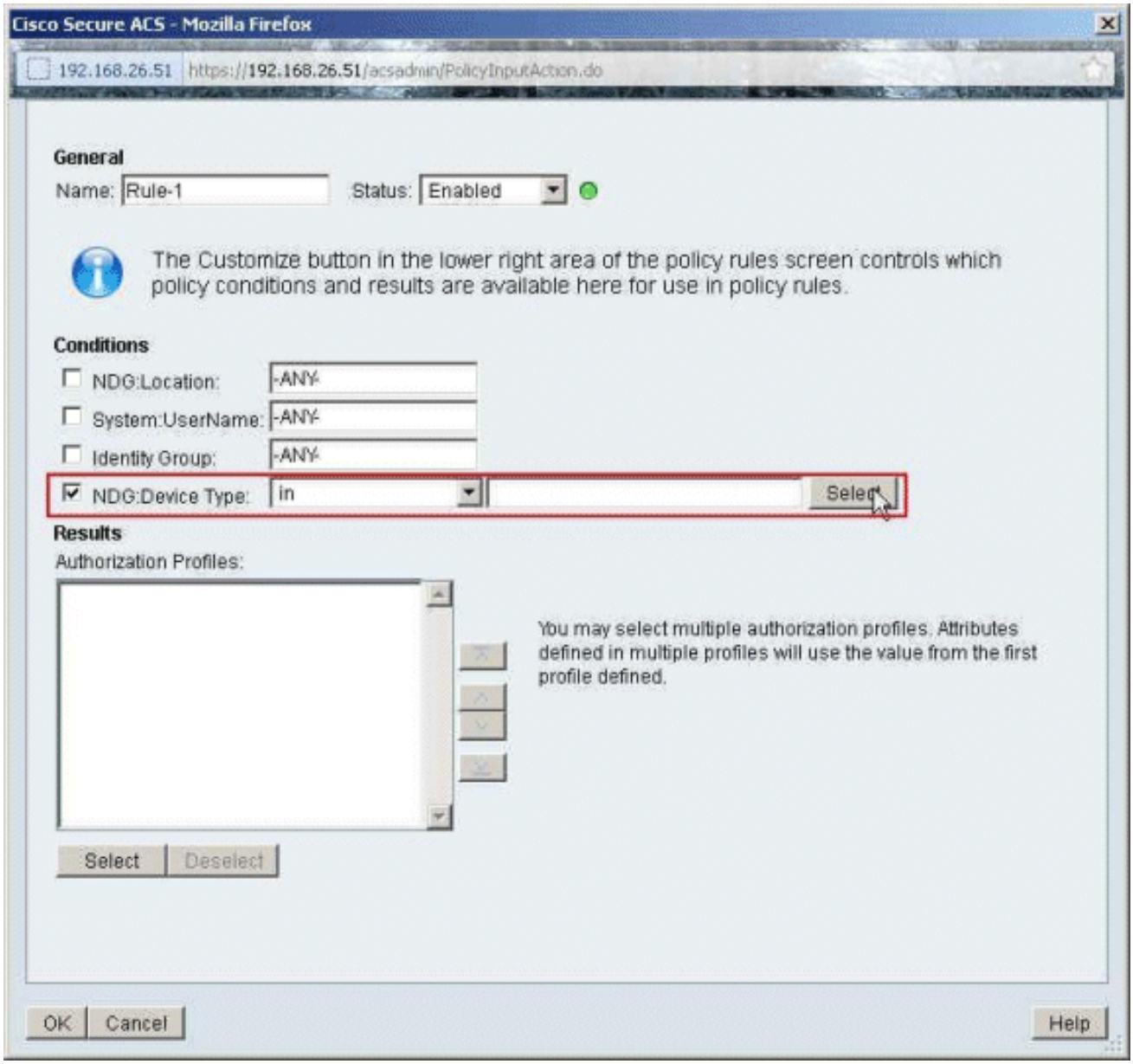


9. Klik op **Maken** om een nieuwe Regel te maken.

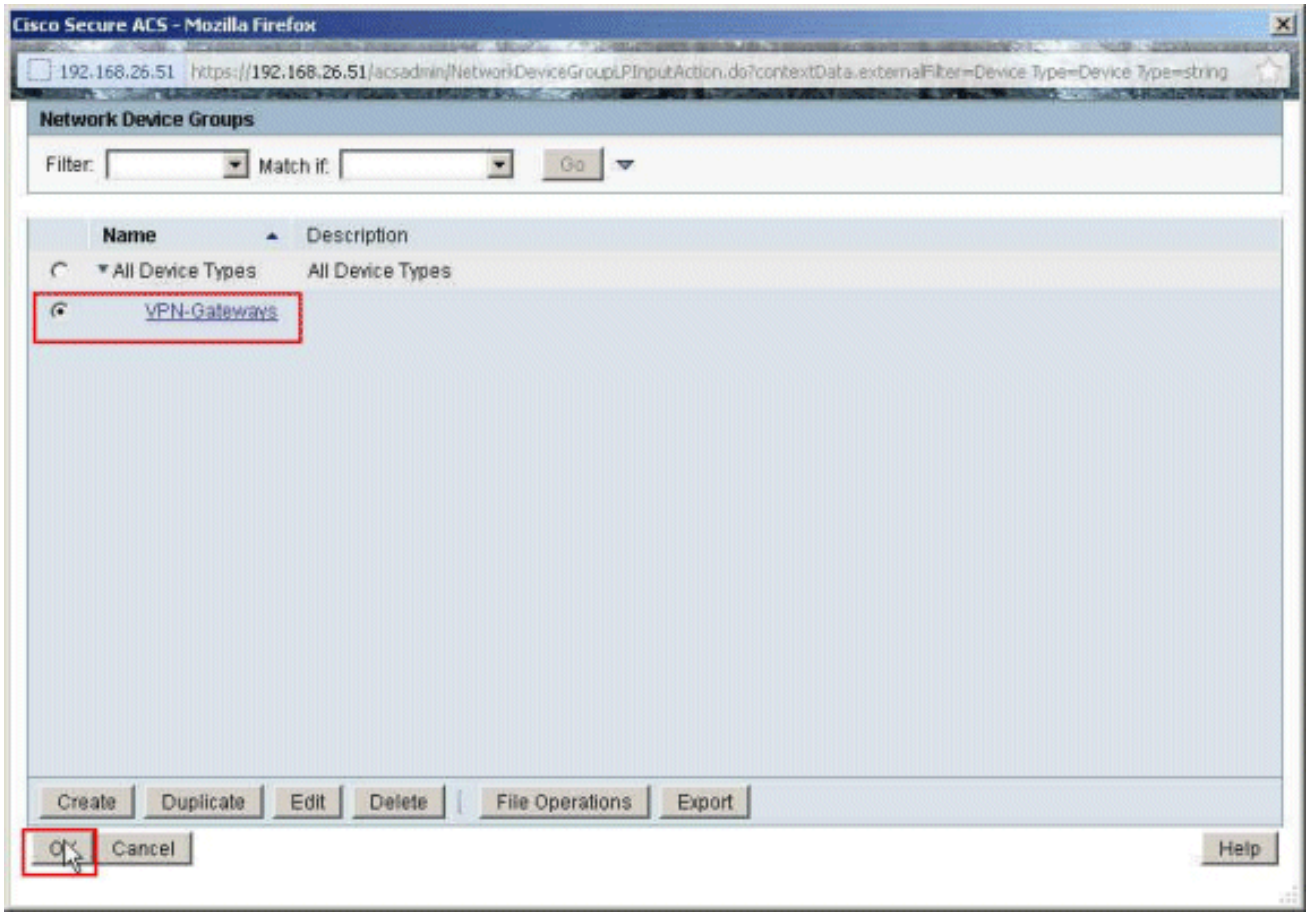


10. Zorg dat het selectieteken naast **NDG:Het type apparaat** is geselecteerd en kies **in** de vervolgkeuzelijst. Klik op

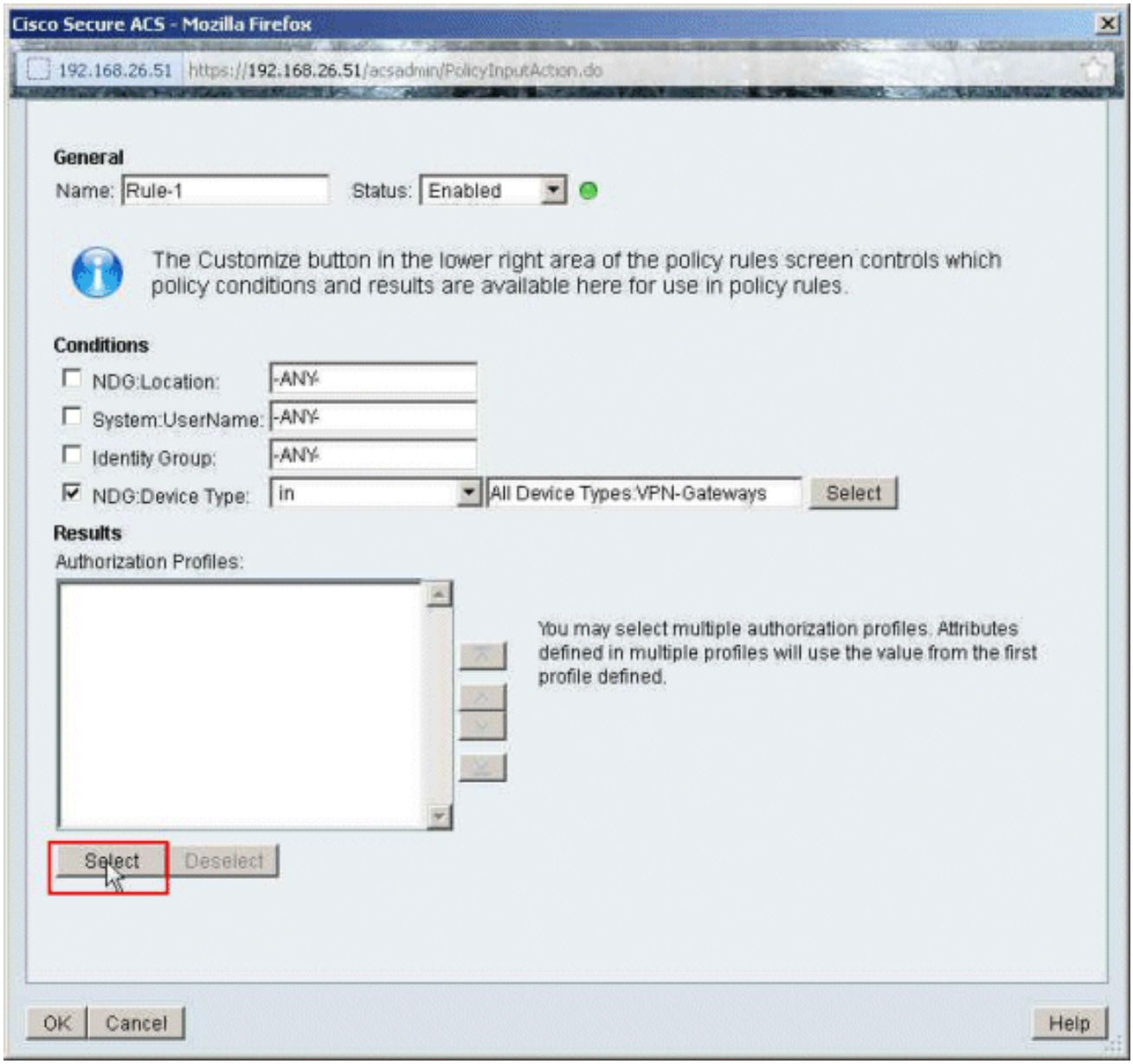
Selecteren.



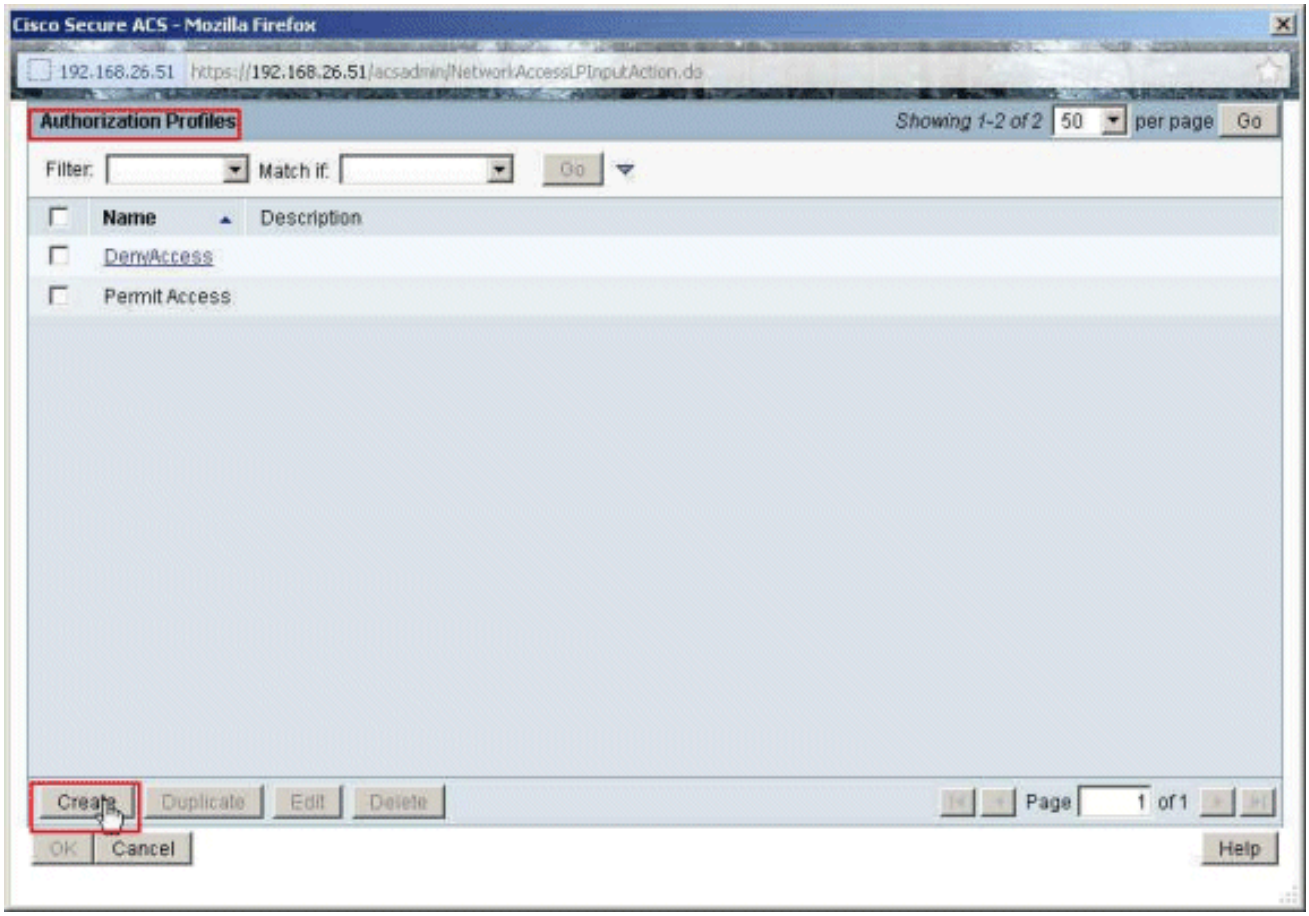
11. Kies de **VPN-gateways** van de netwerkgroep die eerder zijn gemaakt en klik op **OK**.



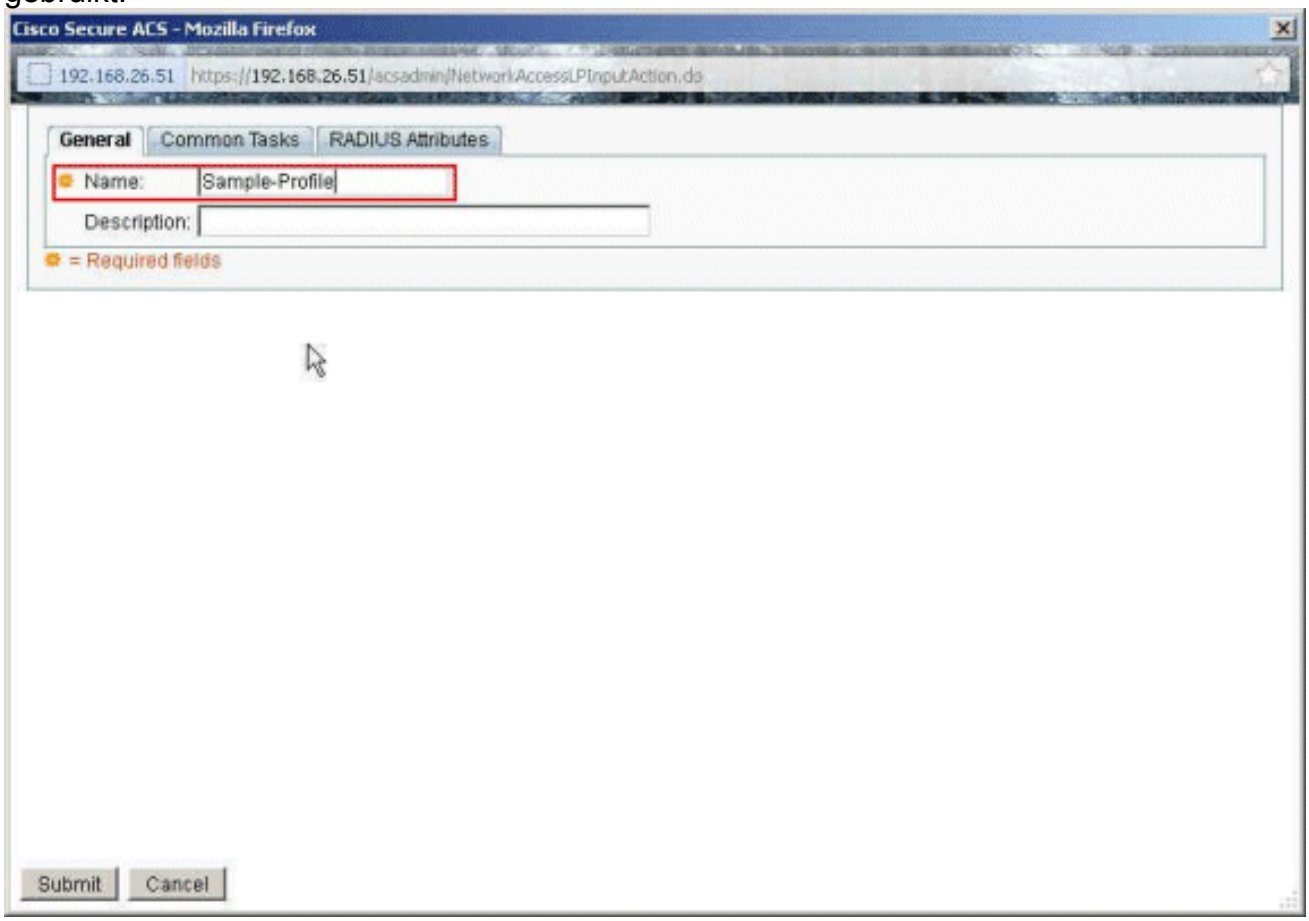
12. Klik op **Selecteren**.



13. Klik op **Maken** om een nieuw Auditprofiel te maken.

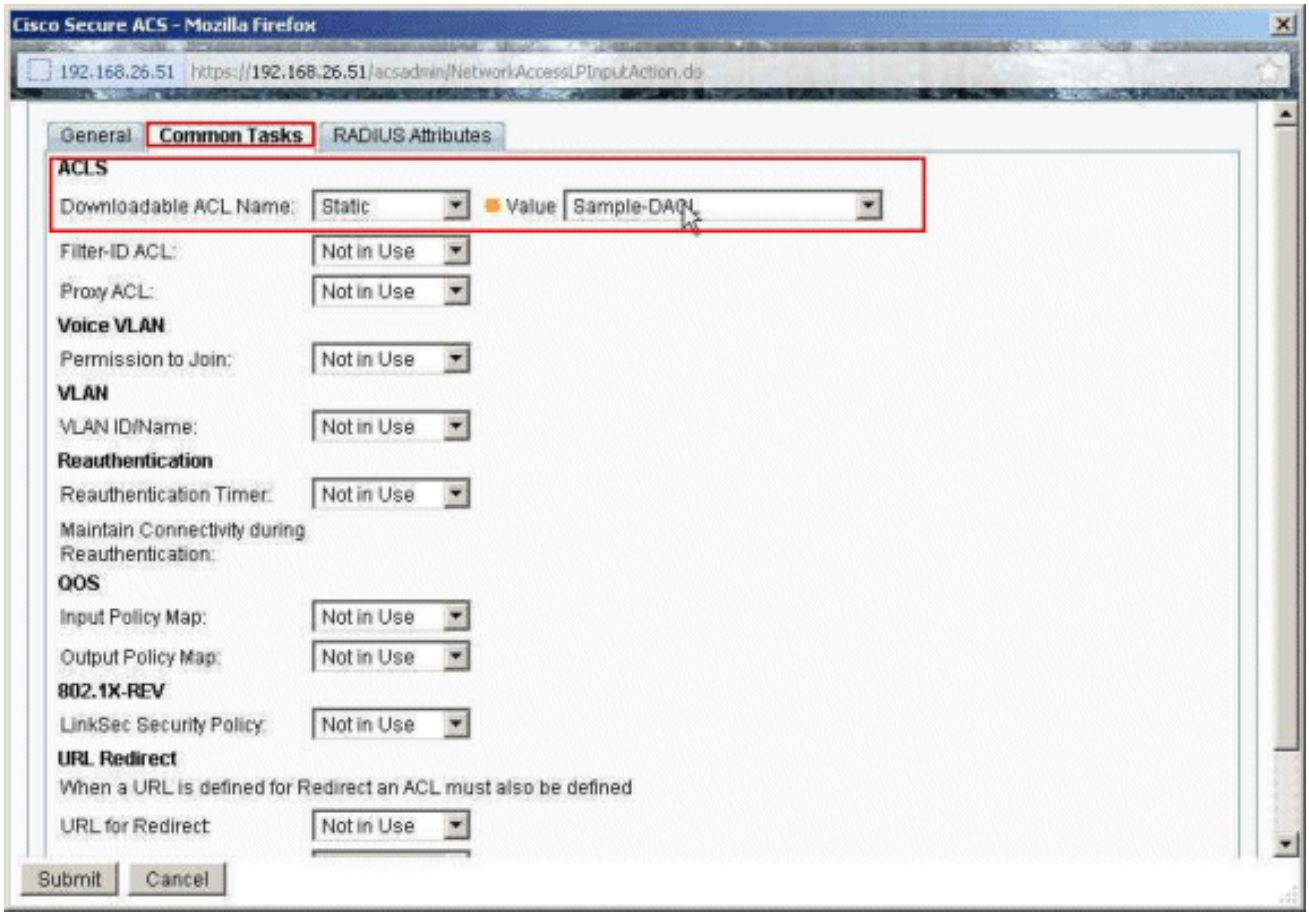


14. Geef een naam op voor het **machtigingsprofiel**. **Monster-profiel** is de naam die in dit voorbeeld wordt
gebruikt.

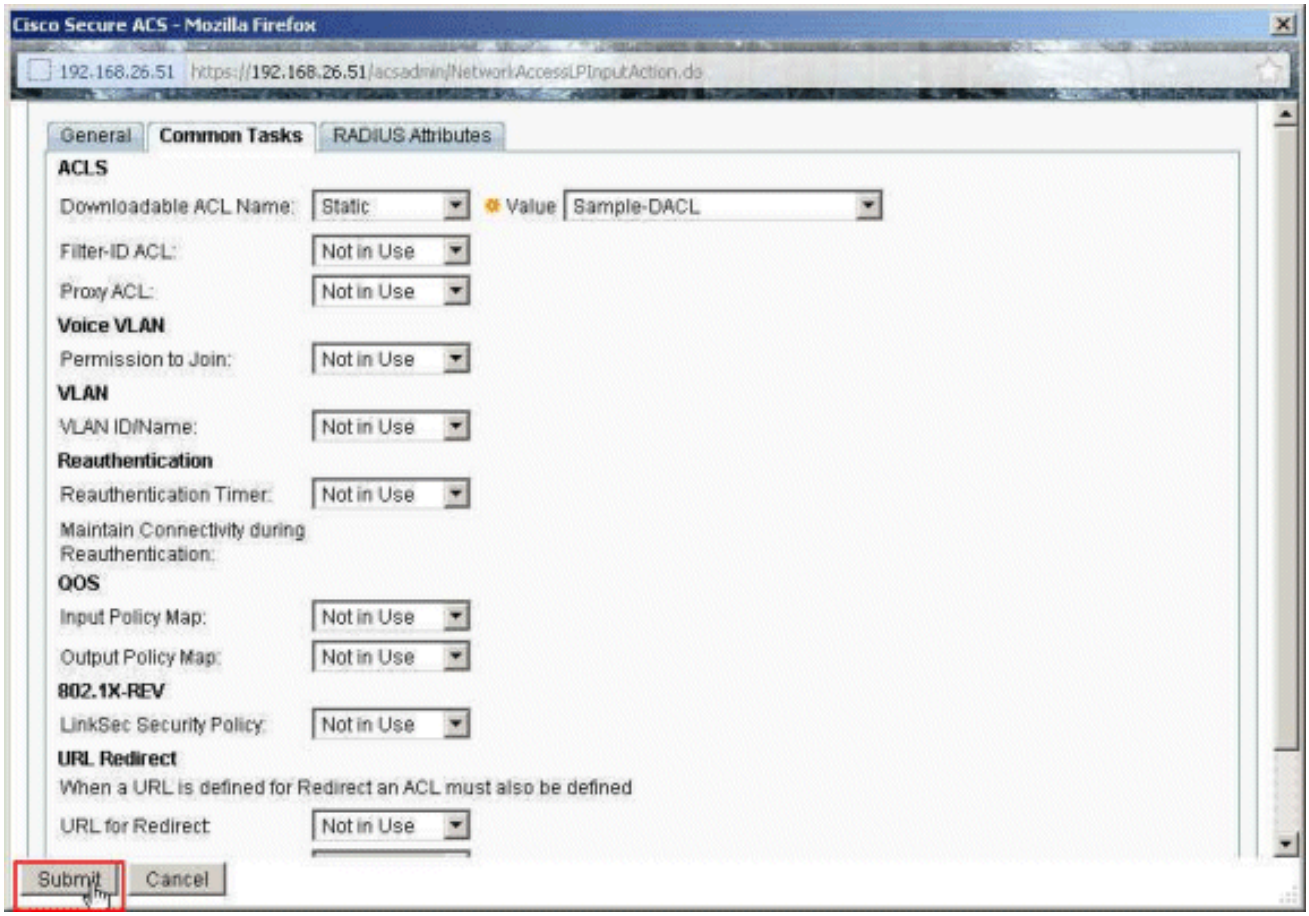


15. Kies het tabblad **Gemeenschappelijke taken** en selecteer **Statisch** uit de vervolgkeuzelijst voor de downloadbare ACL-naam. Kies de nieuwe **DACL (Steekproef-DACL)** uit de

vervolgkeuzelijst
waarde.

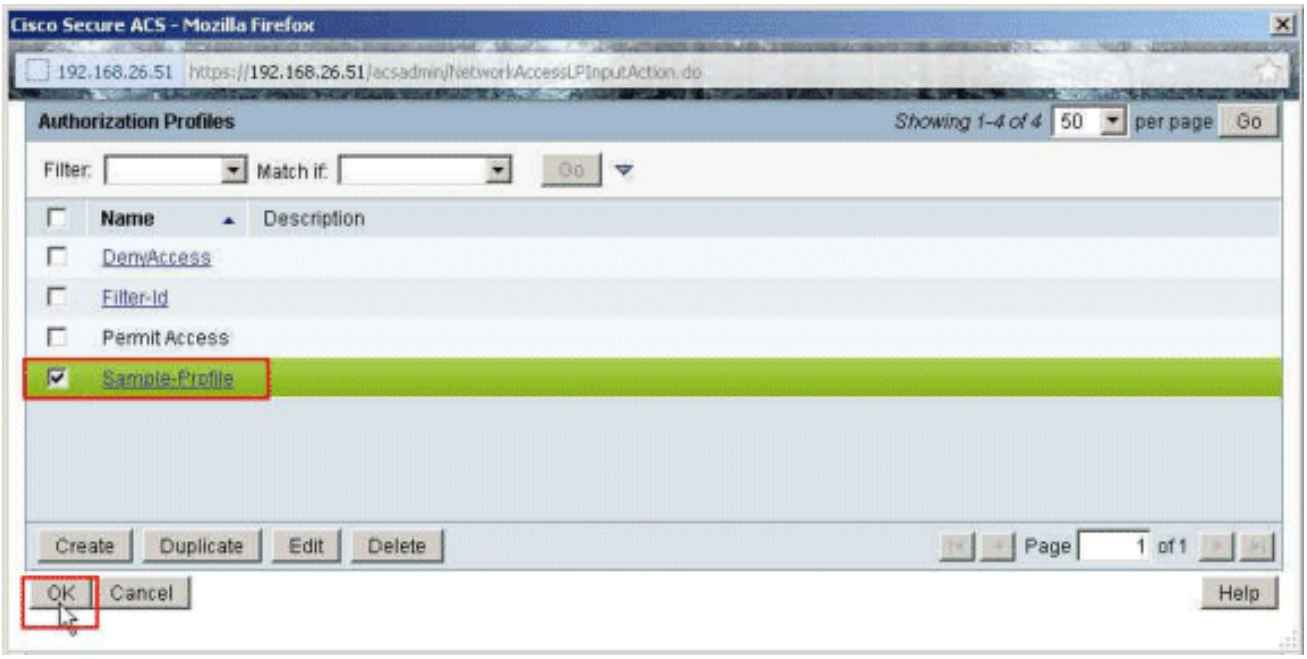


16. Klik op
Inzenden.

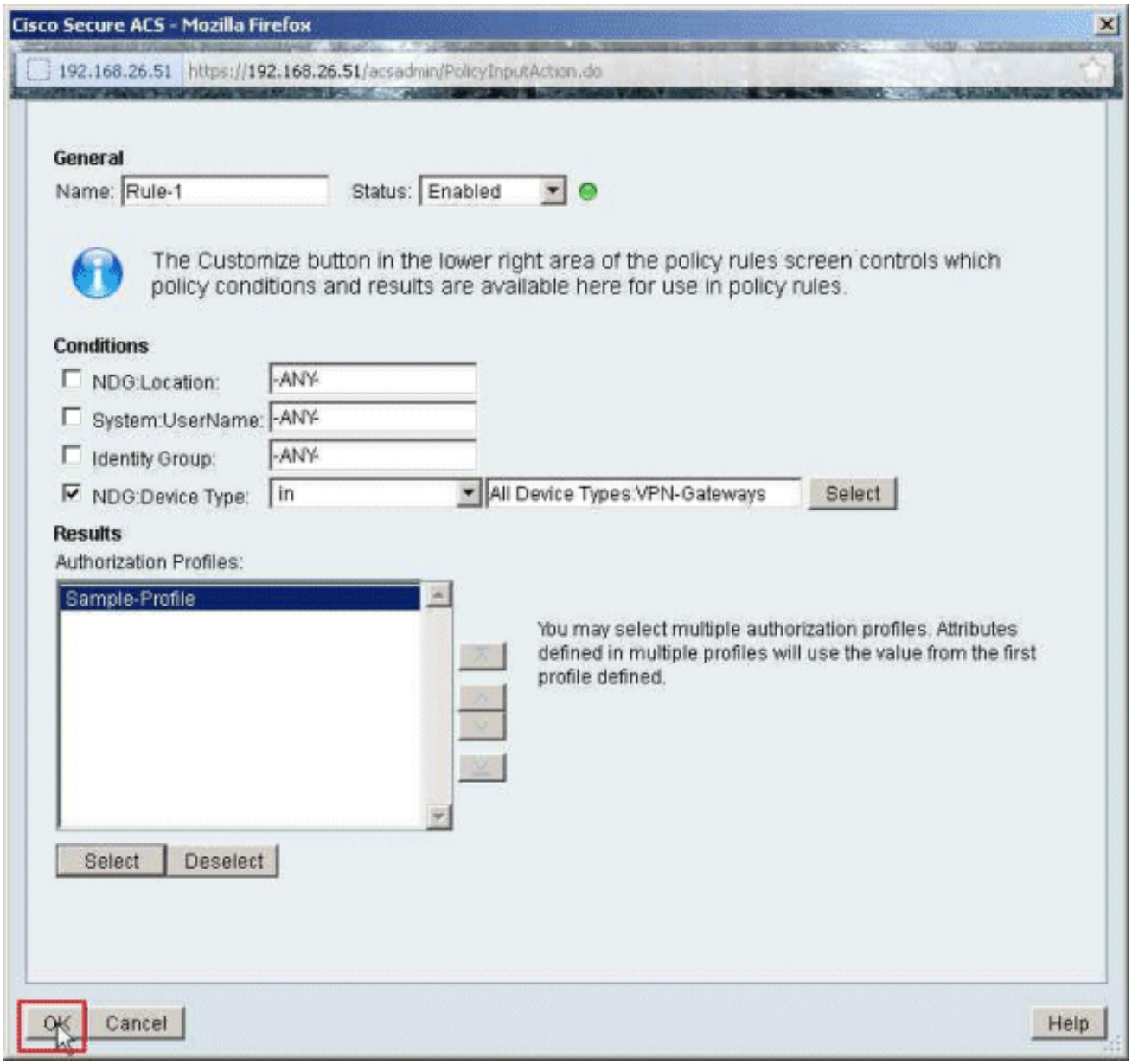


17. Selecteer **Monster-profiel dat** eerder is gemaakt en klik op

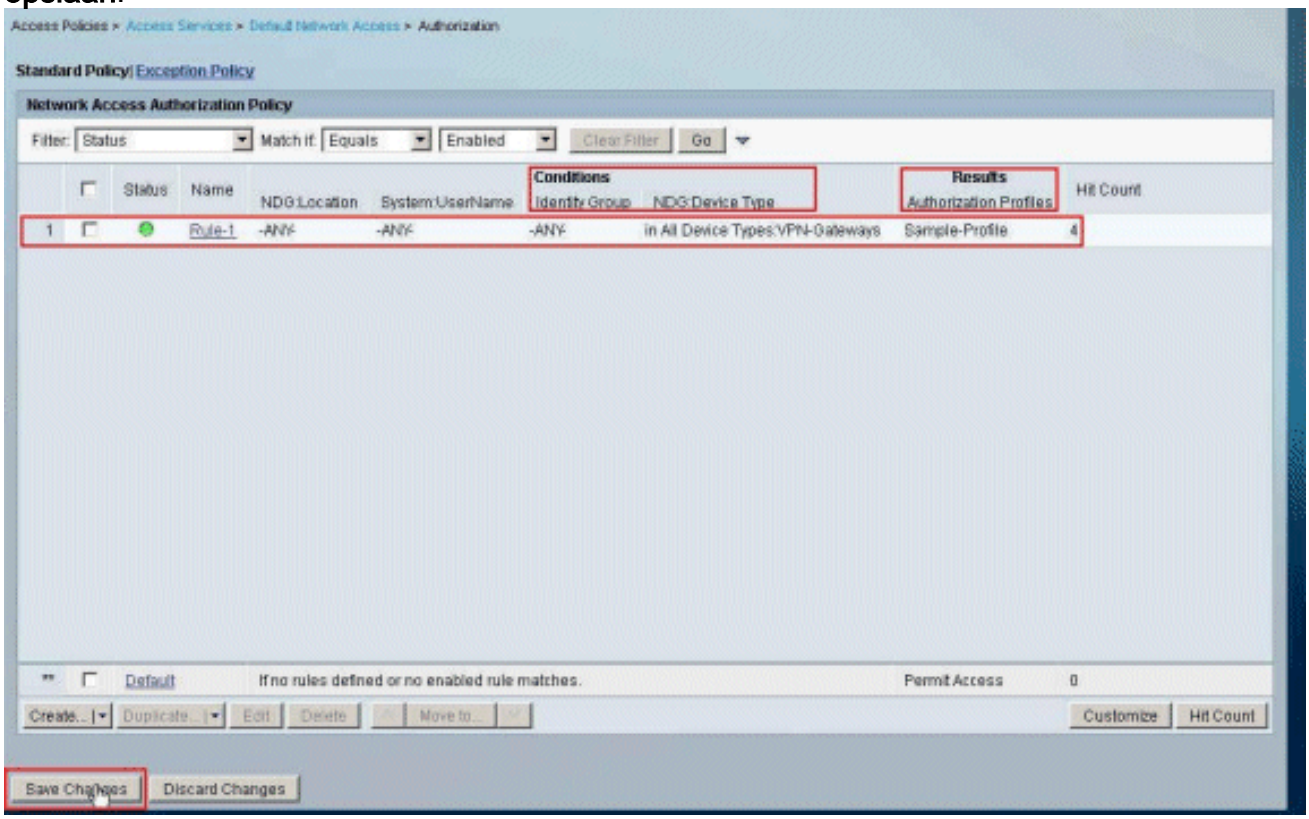
OK.



18. Klik op
OK.



19. Controleer dat **regel-1** met **VPN-gateways** als NDG:Apparaattype als conditie en **voorbeeldprofiel** als resultaat. Klik op **Wijzigingen opslaan**.



RADIUS-instellingen voor IETF configureren voor een gebruikersgroep

Om een naam voor een toegangslijst te downloaden die u al op het security apparaat hebt gemaakt, vanaf de RADIUS-server wanneer een gebruiker voor authenticatie verantwoordelijk is, moet u de eigenschap IETF RADIUS-filter-id (attribuut nummer 11) configureren:

```
filter-id=acl_name
```

Het Sample-Group **subsysteem** is gecertificeerd en de RADIUS-server downloads een ACL-naam (nieuw) voor een toegangslijst die u al op het security apparaat hebt gemaakt. De gebruiker "cisco" kan toegang hebben tot alle apparaten die binnen het netwerk van de ASA **behalve** de 10.1.1.2 server zijn. Zie het gedeelte Filter-ID ACL om de ACL te controleren.

Zoals in het voorbeeld, wordt ACL genoemd **nieuw** gevormd voor het filteren in ASA:

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

Deze parameters verschijnen alleen wanneer ze waar zijn. U hebt ingesteld:

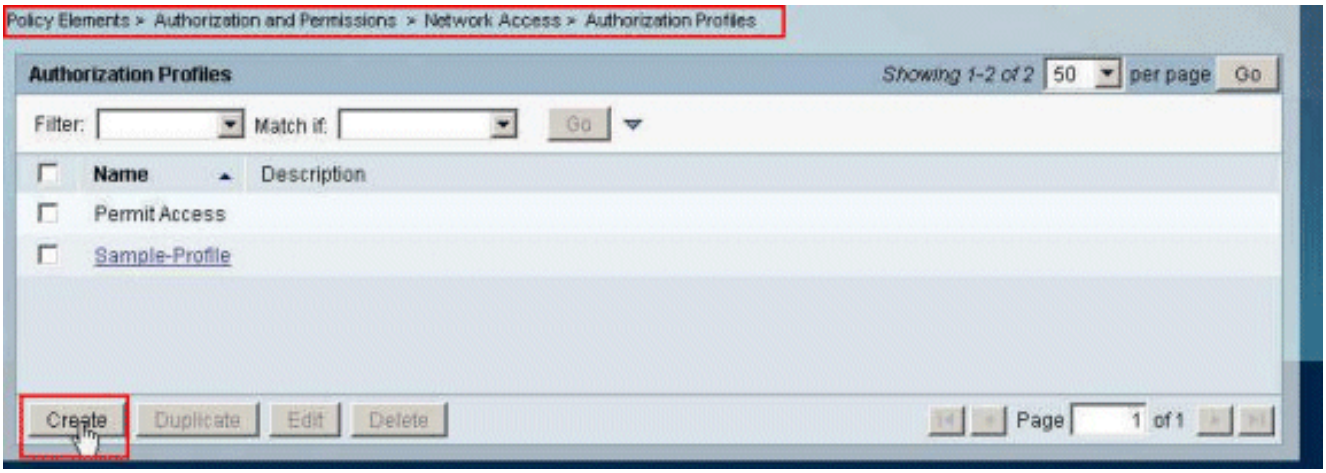
- AAA-client voor gebruik van een RADIUS-protocol in netwerkconfiguratie
- Een autorisatieprofiel met RADIUS-filter-ID (IETF) wordt geselecteerd onder het resultaatgedeelte van de regel in de Access-Service.

RADIUS-eigenschappen worden als profiel voor elke gebruiker van ACS naar de verzoekende AAA-client verzonden.

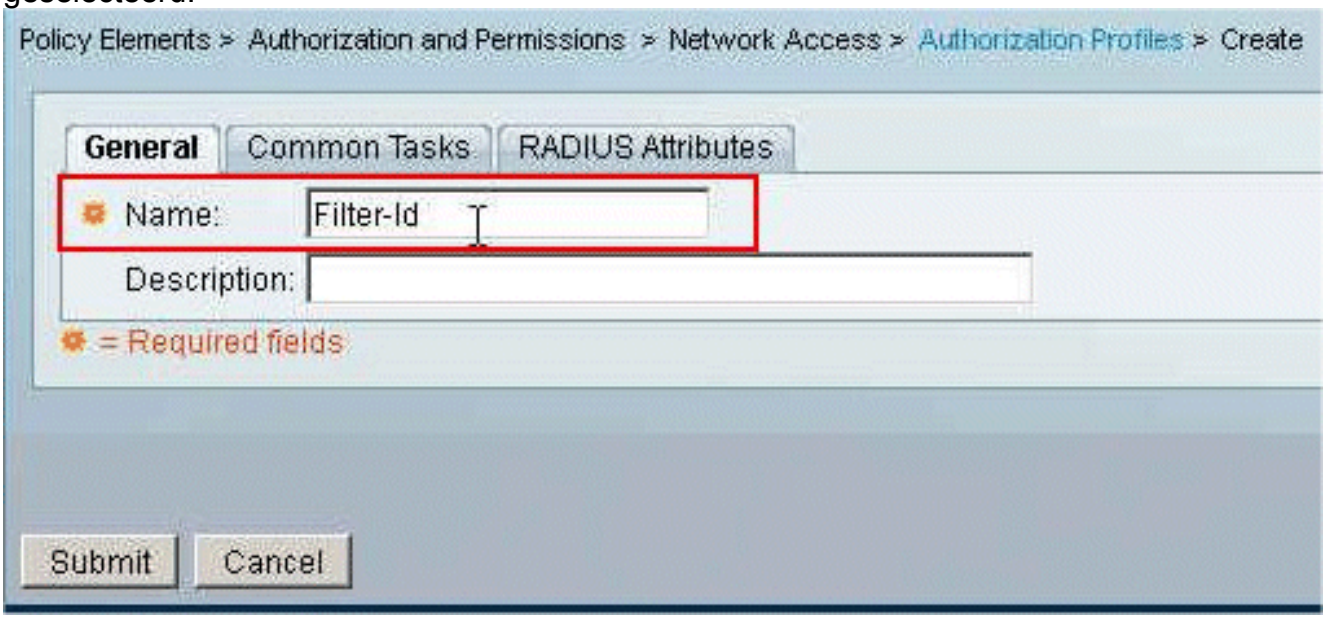
Voltooi stappen 1 tot en met 6 en 10 tot en met 12 van het configureren ACS voor downloadbare ACL voor individuele gebruiker, gevolgd door stappen 1 tot en met 6 van het configureren ACS voor downloadbare ACL voor groep, en voer deze stappen in deze sectie uit om filter-ID in Cisco Secure ACS te configureren.

Om de instellingen van de eigenschap **RADIUS** van **IETF** te configureren om deze toe te passen zoals in autorisatieprofiel, voert u deze stappen uit:

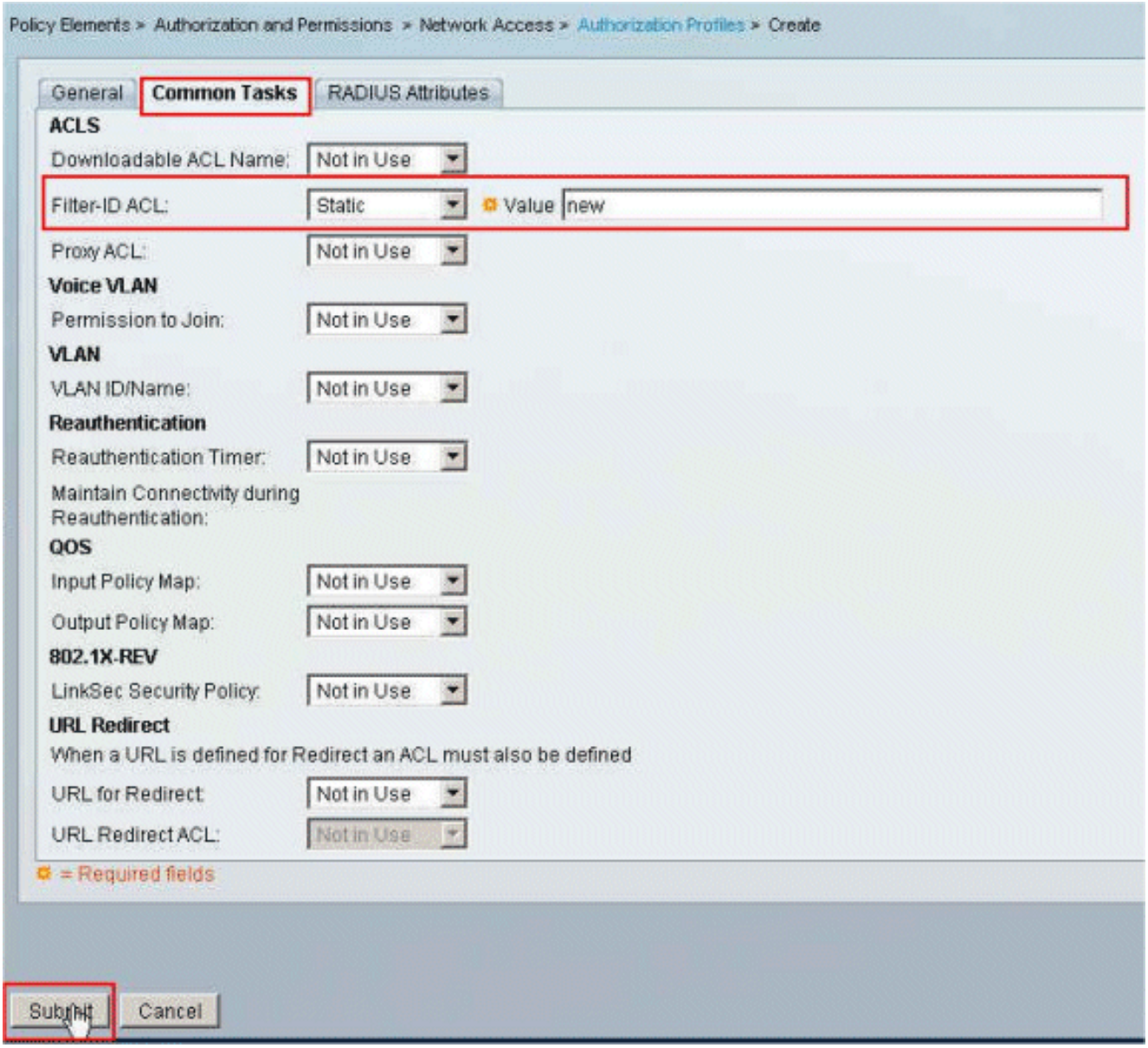
1. Kies **Beleidselementen > Vergunning en toegangsrechten > Toegang tot netwerk > Verificatieprofielen** en klik **op Maken om een nieuw vergunningsprofiel te maken.**



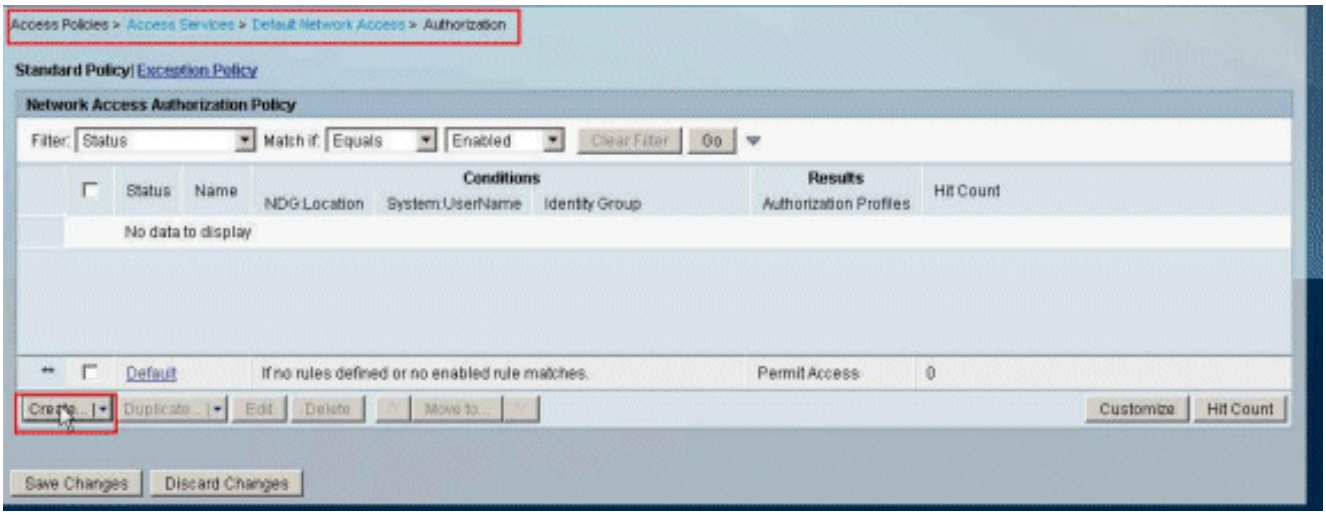
2. Geef een naam op voor het **machtigingsprofiel**. **Filter-ID** is de naam van het machtigingsprofiel die in dit voorbeeld voor eenvoud is geselecteerd.



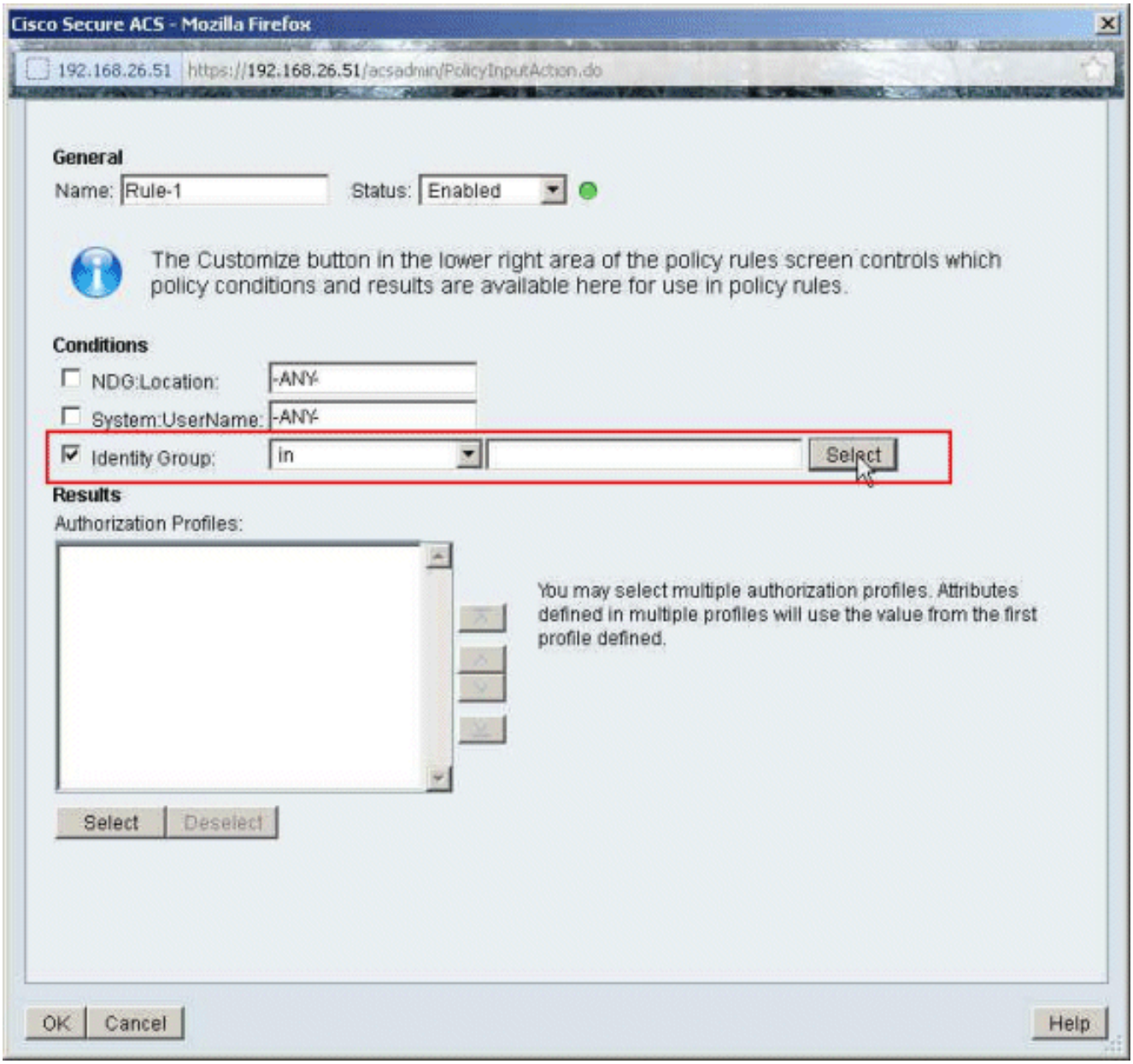
3. Klik op het tabblad **Gemeenschappelijke taken** en kies **Static** in de vervolgkeuzelijst voor **Filter-ID ACL**. Voer de naam van de toegangslijst in als **nieuw** in het veld Waarde en klik op **Inzenden**.



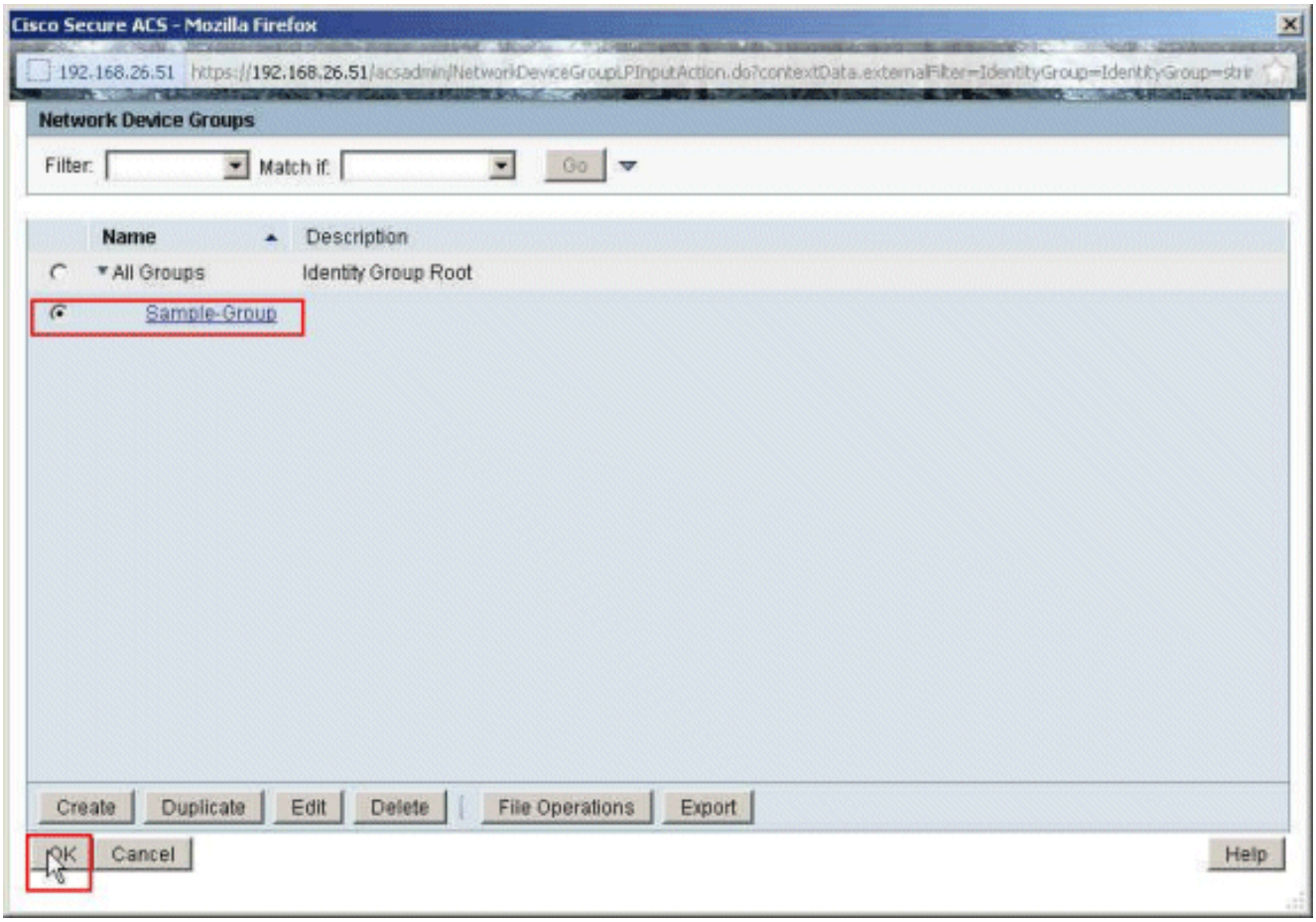
4. Kies **Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang > autorisatie** en klik **op Maken om een nieuwe regel te maken.**



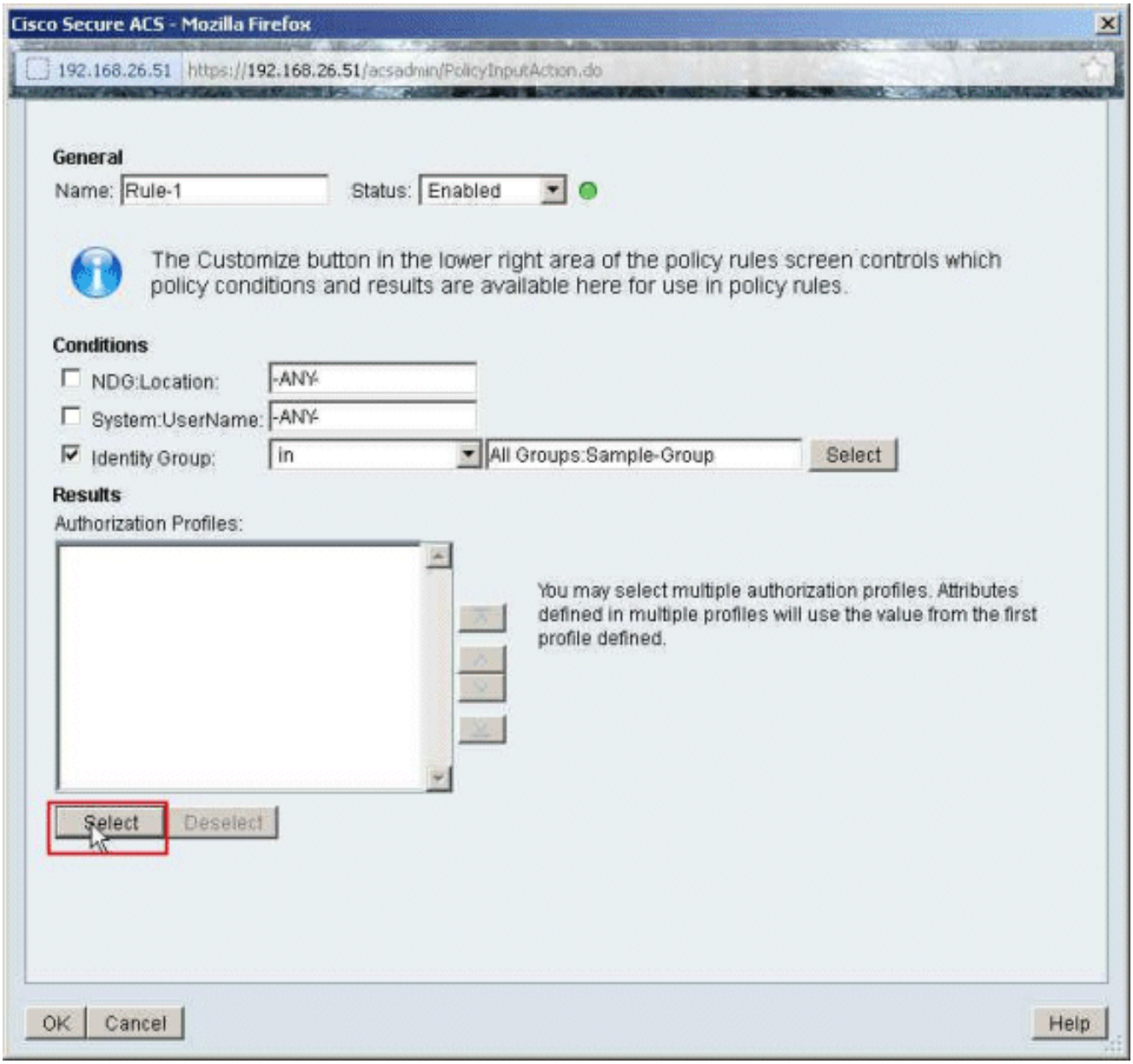
5. Controleer of het selectieteken naast **Identity Group** ingeschakeld is en klik vervolgens op **Selecteren**.



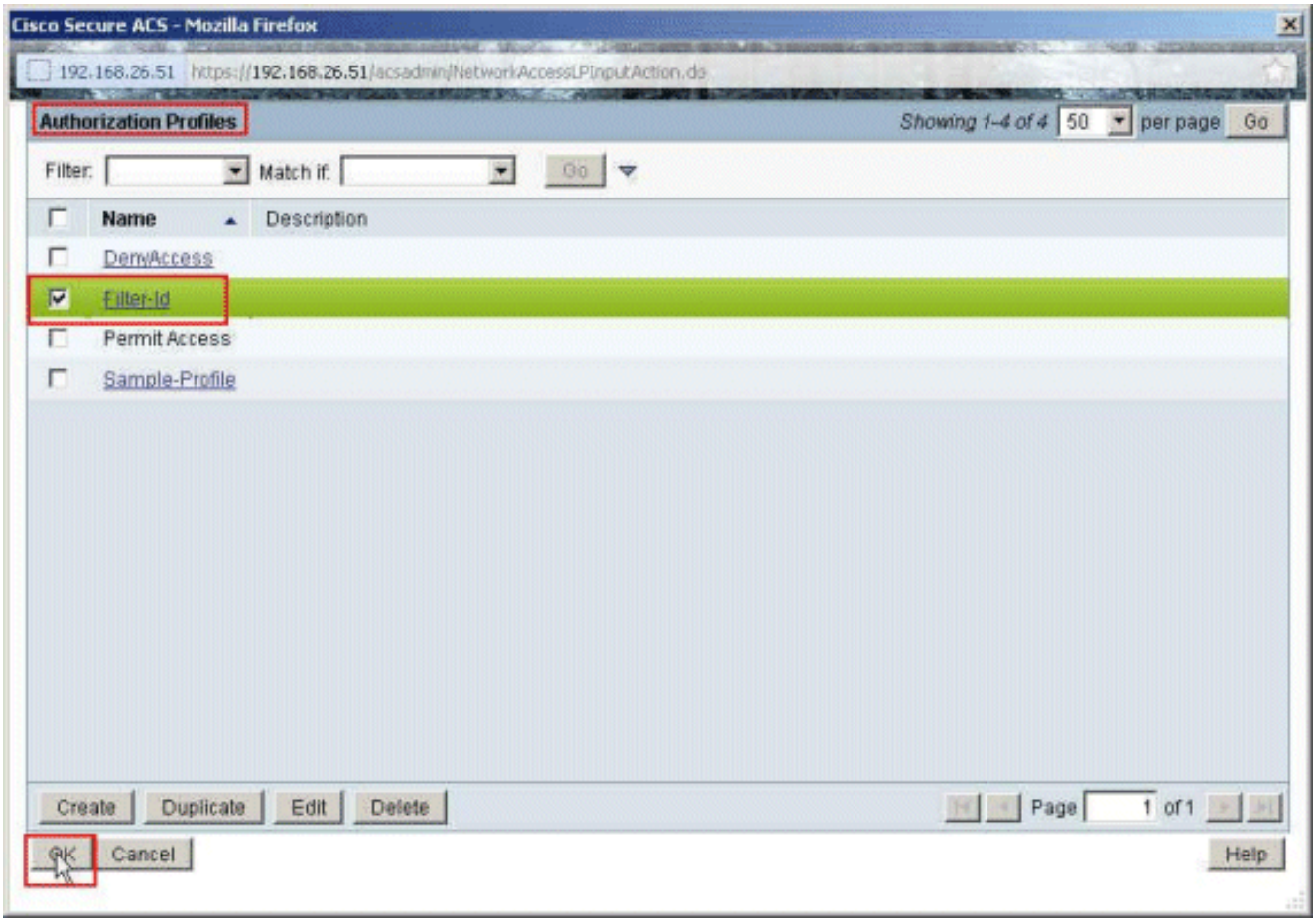
6. Kies **een voorbeeldgroep** en klik op **OK**.



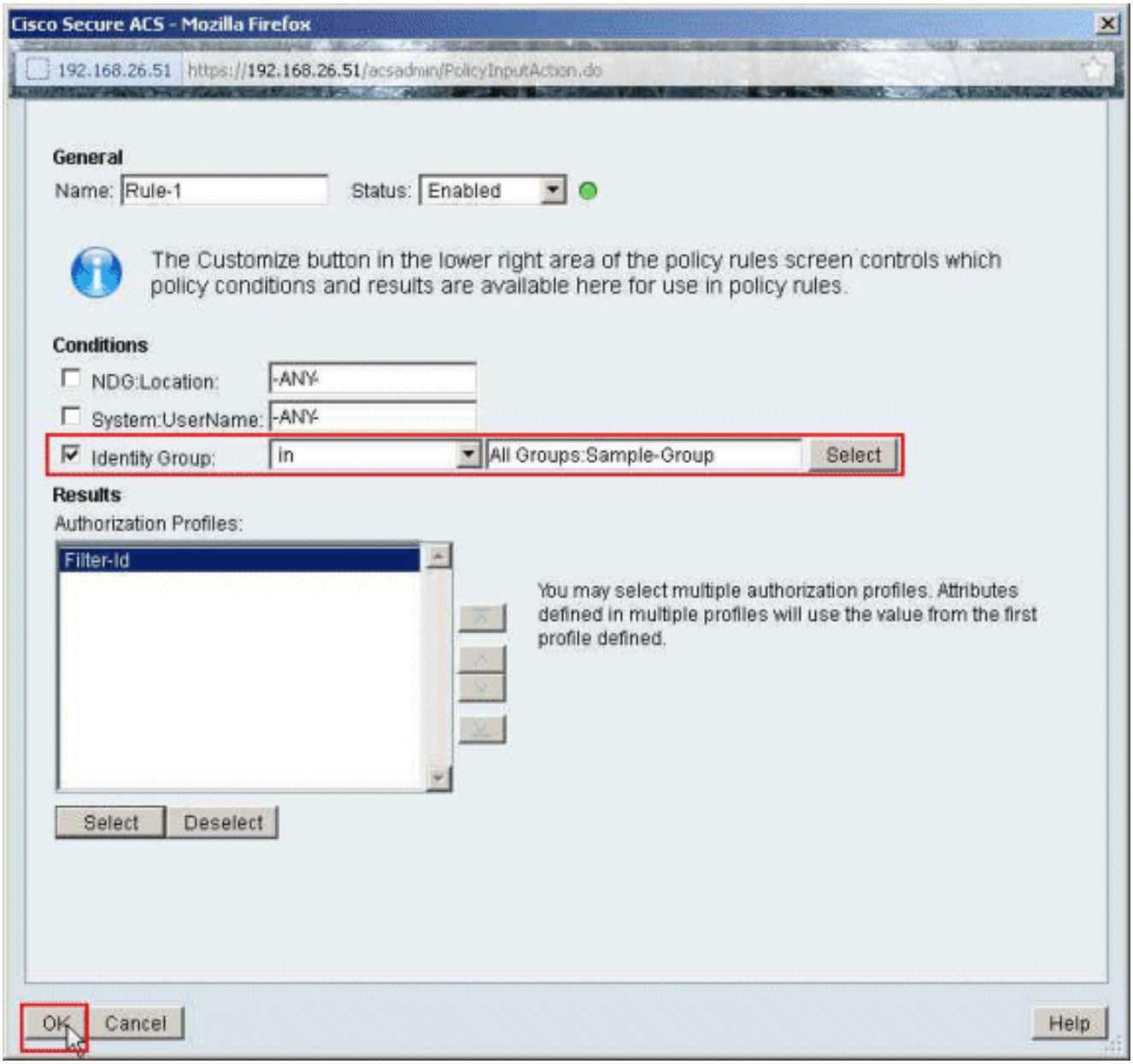
7. Klik op **Selecteer** in het gedeelte Automation Profiles.



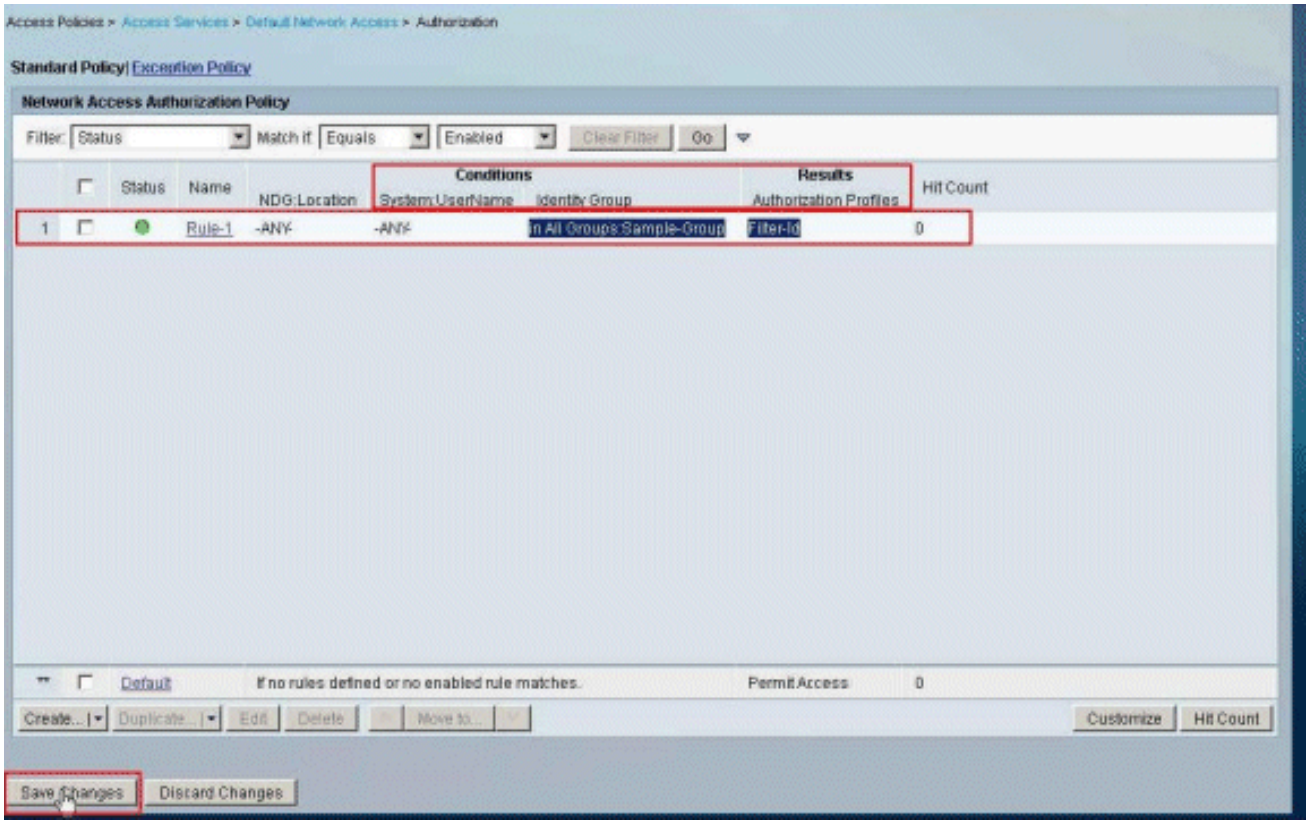
8. Kies de eerder gemaakte **filter-ID van het** autorisatieprofiel en klik op **OK**.


Cisco Secure ACS - Mozilla Firefox
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do
Authorization Profiles
Showing 1-4 of 4 50 per page Go
Filter: Match if: Go
Name Description
DenyAccess
Filter-Id
Permit Access
Sample-Profile
Create Duplicate Edit Delete
Page 1 of 1
OK Cancel
Help

9. Klik op
   OK.



10. Controleer dat **regel-1** met de **voorbeeldgroep** van de Identity Group wordt gemaakt als **filter-ID** als resultaat. Klik op **Wijzigingen opslaan**.

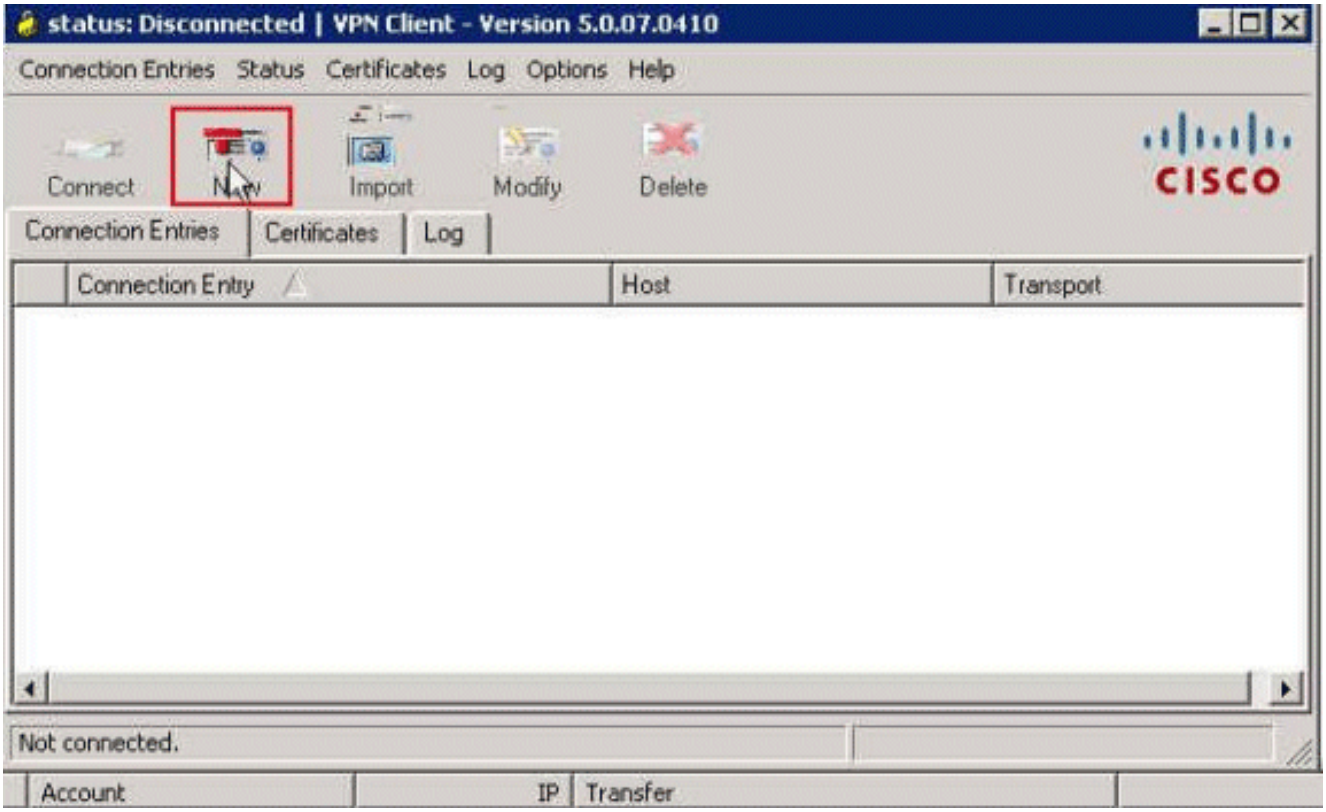


Cisco VPN-clientconfiguratie

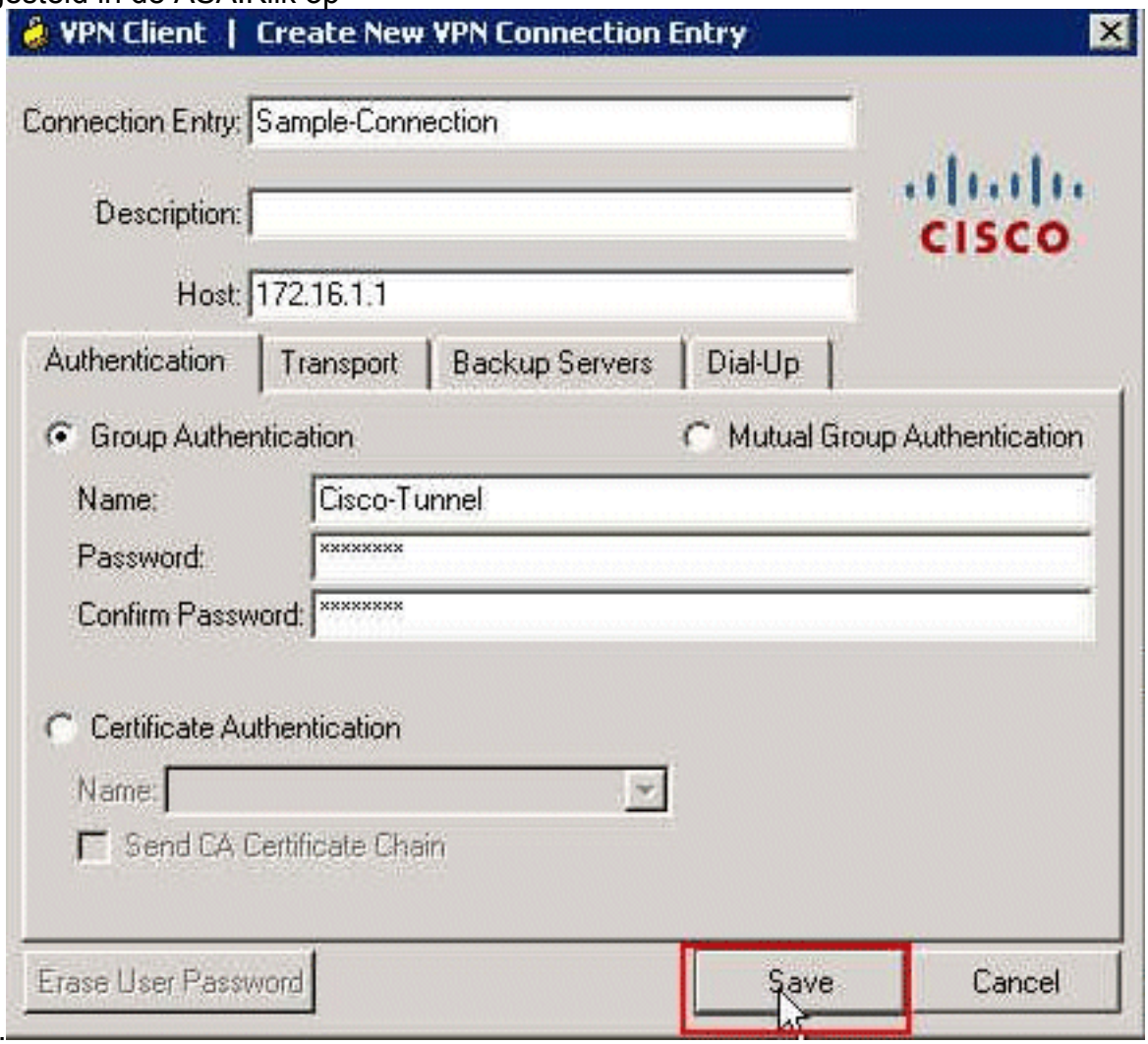
Sluit aan op de Cisco ASA met de Cisco VPN-client om te controleren of de ASA met succes is geconfigureerd.

Voer de volgende stappen uit:

1. Kies **Start > Programma's > Cisco Systems VPN-client > VPN-client**.
2. Klik op **Nieuw** om het venster Nieuwe VPN-verbinding maken te starten.

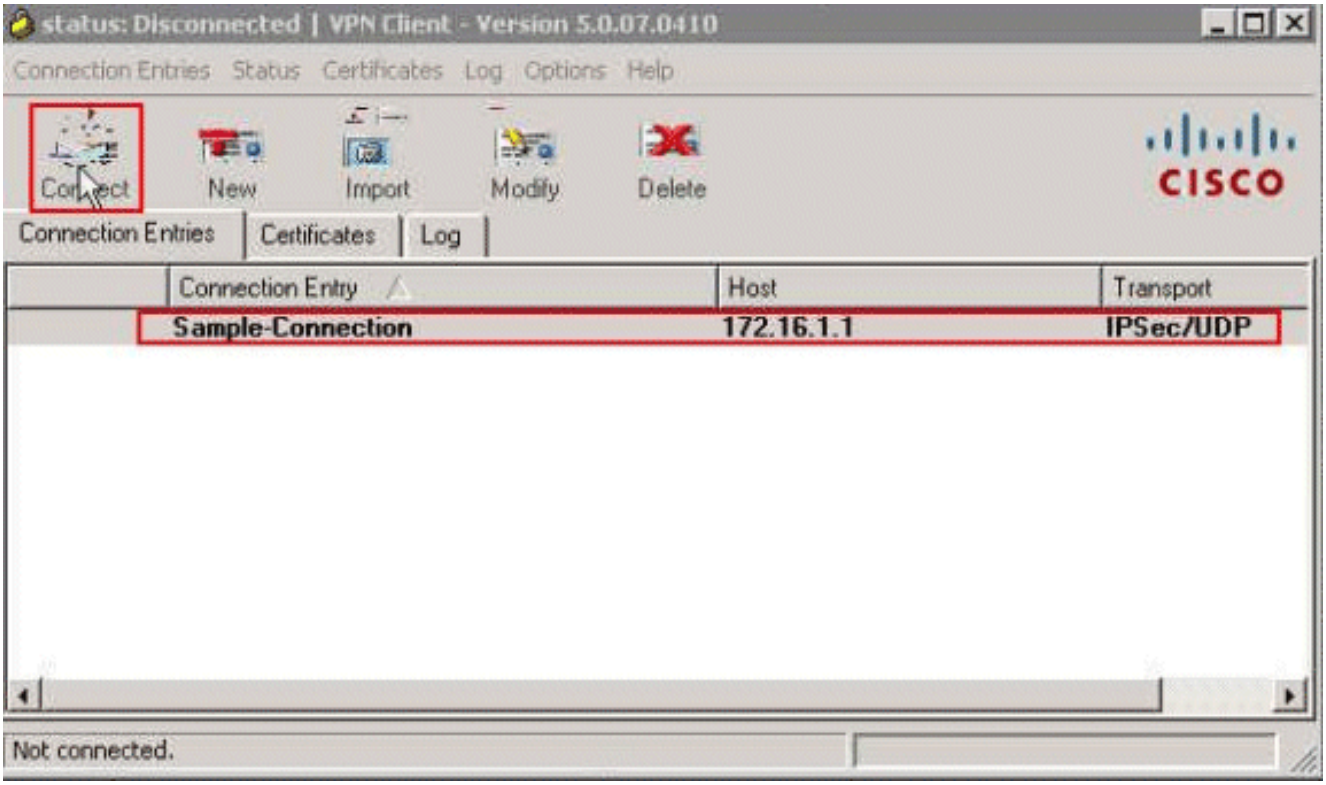


3. Geef de details op van uw nieuwe aansluiting:Voer de naam van de verbindingsbocht in samen met een beschrijving.Voer het **externe IP-adres van de ASA** in het hostvak in.Voer de VPN Tunnel Group Name (**Cisco-Tunnel**) en het wachtwoord in (Pre-Shared Key - **cisco123**) zoals ingesteld in de ASA.Klik op



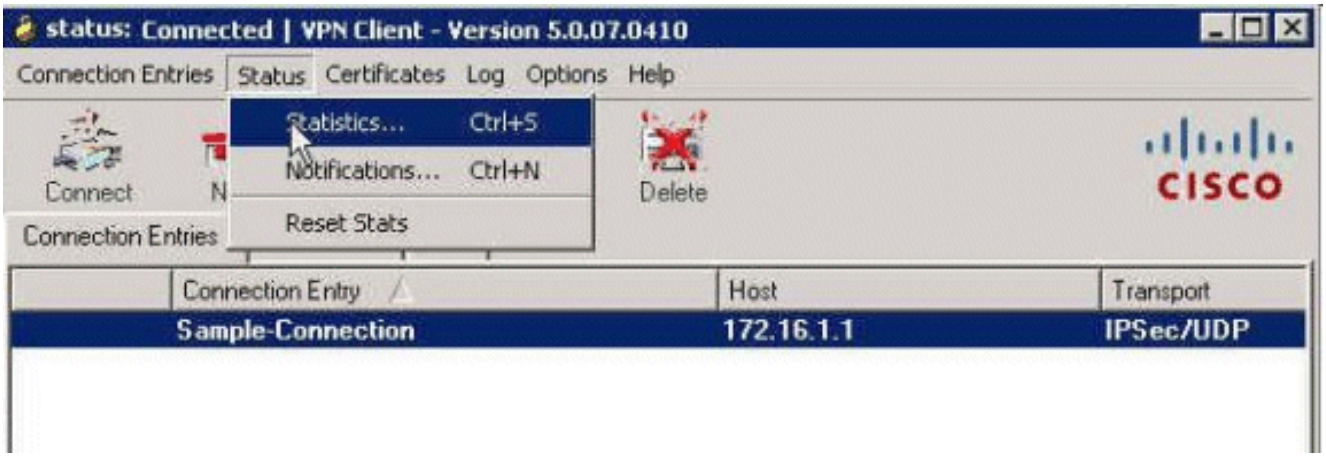
Opslaan.

4. Klik op de verbinding die u wilt gebruiken en klik op **Connect** vanuit het hoofdvenster van VPN-
client.



5. Voer desgevraagd de **Cisco**-naam **en cisco**123 van het wachtwoord in zoals in de ASA is ingesteld voor verificatie en klik op **OK** om verbinding te maken met het externe netwerk.

6. Zodra de verbinding met succes is tot stand gebracht, kiest u **Statistieken** uit het menu Status om de details van de tunnel te
controleren.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Crypto opdrachten tonen

- **toon crypto isakmp sa** - laat alle huidige IKE Security Associations (SA's) bij een peer zien.

```
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#
```

- **toon crypto ipsec sa** - toont de instellingen die door huidige SA's worden gebruikt.

```
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
```

Downloadbare ACL voor gebruiker/groep

Controleer de downloadbare ACL voor de gebruiker Cisco. ACL's worden gedownload van de CSACS.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list #ACSACL#-IP-Sample-DACL-4f3b9117; 2 elements; name hash: 0x3c878038
   (dynamic)
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 1 extended permit ip any host
   10.1.1.2 (hitcnt=0) 0x5e896ac3
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 2 extended deny ip any any
   (hitcnt=130) 0x19b3b8f5
```

Filter-ID ACL

De [011] Filter-ID is toegepast voor de groep - Steekproef-groep, en gebruikers van de groep worden gefilterd volgens de ACL (nieuw) die in de ASA is gedefinieerd.

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. De voorbeelduitvoer **van debug** wordt ook weergegeven.

Opmerking: Raadpleeg voor meer informatie over het oplossen van problemen bij externe toegang IPsec VPN de meest gebruikelijke oplossingen voor probleemoplossing in L2L en Remote Access IPsec VPN.

Beveiligingsassociaties wissen

Wanneer u problemen oplossen, zorg er dan voor dat bestaande SA's worden gewist nadat u een wijziging hebt aangebracht. In de bevoorrechte modus van de PIX, gebruik deze opdrachten:

- **Schakel [crypto] ipsec sa** - Verwijdert de actieve IPsec SA's. Het sleutelwoord crypto is optioneel.
- **helder [crypto] isakmp sa** - verwijdert de actieve IKE SA's. Het sleutelwoord crypto is optioneel.

Opdrachten voor probleemoplossing

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug crypto ipsec 7** - Hiermee worden de IPsec-onderhandelingen van fase 2 weergegeven.
- **debug crypto isakmp 7** - Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

Gerelateerde informatie

- Cisco ASA 5500 Series ondersteuningspagina voor adaptieve security applicaties
- Cisco ASA 5500 Series Opdrachten voor adaptieve security applicaties
- Cisco adaptieve security apparaatbeheer
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- Cisco VPN-clientondersteuningspagina
- Cisco Secure Access Control-systeem
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems