ASA 8.3 e mais atrasado: Autorização RADIUS (ACS 5.x) para a utilização do acesso VPN ACL baixável com CLI e exemplo da configuração ASDM

Índice

Introdução

Este documento descreve como configurar o mecanismo de segurança para autenticar usuários para o acesso de rede. Desde que você pode implicitamente permitir autorizações RADIUS, este original não contém nenhuma informação sobre a configuração da autorização RADIUS na ferramenta de segurança. Ela fornece informações sobre como o mecanismo de segurança lida com as informações da lista de acesso recebidas dos servidores RADIUS.

Você pode configurar um servidor Radius para transferir uma lista de acessos à ferramenta de

segurança ou um nome da lista de acessos na altura da autenticação. O usuário é autorizado fazer somente o que é permitido na lista de acessos USER-específica.

As Listas de acesso carregável são os meios os mais escaláveis quando você usa o Serviço de controle de acesso Cisco Secure (ACS) para fornecer as Listas de acesso apropriadas para cada usuário. Para obter mais informações sobre dos recursos de lista de acesso carregável e do Cisco Secure ACS, refira configurar um servidor Radius para enviar as listas de controle de acesso carregável e IP carregável ACL.

Refira ASA/PIX 8.x: Autorização RADIUS (ACS) para a utilização do acesso de rede ACL baixável com CLI e exemplo da configuração ASDM para a configuração idêntica em Cisco ASA com versões 8.2 e anterior.

Pré-requisitos

Requisitos

Este original supõe que a ferramenta de segurança adaptável (ASA) é plenamente operacional e configurada para permitir que o Cisco Adaptive Security Device Manager (ASDM) ou o CLI façam alterações de configuração.

Nota: Refira permitir o acesso HTTPS para o ASDM a fim permitir que o dispositivo seja configurado remotamente pelo ASDM ou pelo Shell Seguro (ssh).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de software 8.3 de Cisco ASA e mais atrasado
- Versão ASDM Cisco 6.3 e mais atrasado
- Versão Cliente VPN Cisco 5.x e mais tarde
- Cisco Secure ACS 5.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Você pode usar IP carregável ACL a fim criar grupos de definições de ACL que você pode aplicar a muitos usuários ou grupos de usuário. Estes grupos de definições de ACL são chamados índices ACL.

O IP carregável ACL opera esta maneira:

1. Quando ACS concede um acesso de usuário à rede, ACS determina se um IP carregável ACL está atribuído ao perfil da autorização na seção do resultado.
2. Se ACS encontra um IP carregável ACL que esteja atribuído ao perfil da autorização, ACS envia um atributo (como parte da sessão do usuário, no pacote de aceitação acesso do RAIO) que especifica o ACL nomeado, e a versão do ACL nomeado.
3. Se o cliente de AAA responde que não tem a versão atual do ACL em seu esconderijo (isto é, o ACL é novo ou mudou), ACS envia o ACL (novo ou actualizado) ao dispositivo.

O IP carregável ACL é uma alternativa à configuração dos ACL no atributo [26/9/1] do Cisco-av-pair de Cisco do RAIO de cada usuário ou grupo de usuário. Você pode criar um IP carregável ACL uma vez, dá-lhe um nome, e atribui-o então o IP carregável ACL a todo o perfil da autorização se você provê seu nome. Este método é mais eficiente do que se você configura o atributo do Cisco-av-pair de Cisco do RAIO para o perfil da autorização.

Quando você incorpora as definições de ACL à interface da WEB ACS, não use a palavra-chave ou as entradas de nome; em todos respeitos restantes, sintaxe e semântica padrão de comando acl do uso para o cliente de AAA em que você pretende aplicar o IP carregável ACL. As definições de ACL que você incorpora em ACS compreendem uns ou vários comandos acl. Cada comando acl deve estar em uma linha separada.

Em ACS, você pode definir IP carregável múltiplo ACL e usá-lo em perfis diferentes da autorização. Baseado nas condições nas regras da autorização do serviço do acesso, você pode enviar os perfis diferentes da autorização que contêm IP carregável ACL aos clientes de AAA diferentes.

Mais, você pode mudar a ordem dos índices ACL em um IP carregável ACL. ACS examina os índices ACL, partindo da parte superior da tabela, e transfere o primeiro índice ACL que encontra. Quando você ajusta a ordem, você pode assegurar a eficiência de sistema se você posiciona o mais extensamente os índices aplicáveis ACL mais altamente sobre a lista.

A fim usar um IP carregável ACL em um cliente de AAA particular, o cliente de AAA deve aderir a estas regras:

- Use o RAIO para a autenticação
- Apoie IP carregável ACL

Estes são exemplos dos dispositivos Cisco que apoiam IP carregável ACL:

- ASA
- Dispositivos Cisco que executam a Versão do IOS 12.3(8)T e mais tarde

Este é um exemplo do formato que você deve usar a fim incorporar ASA ACL à caixa das definições de 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
```

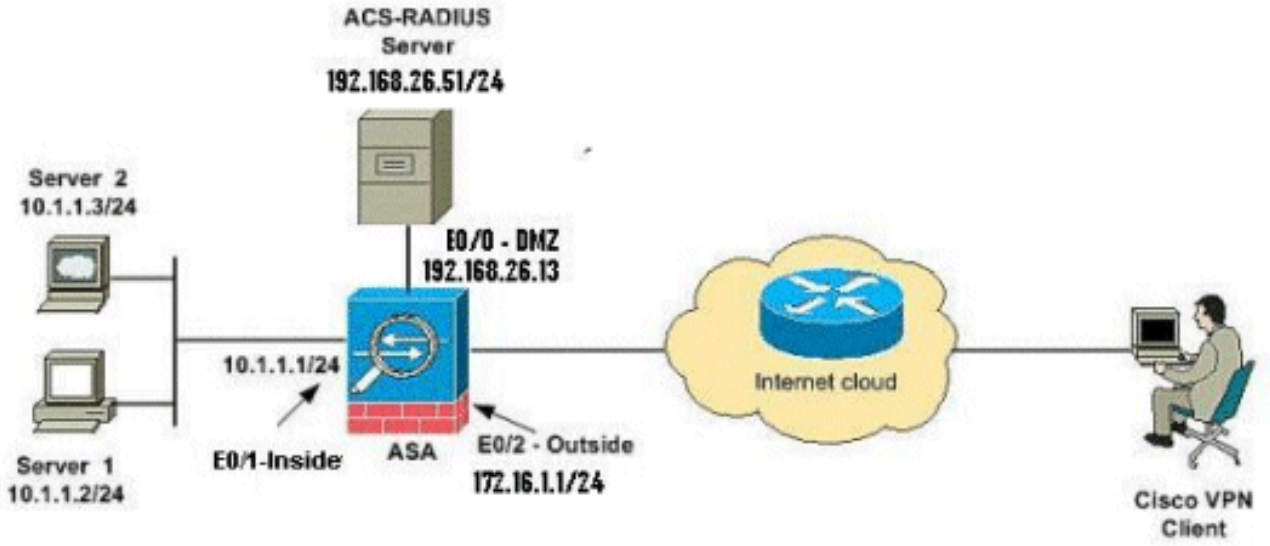
```
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



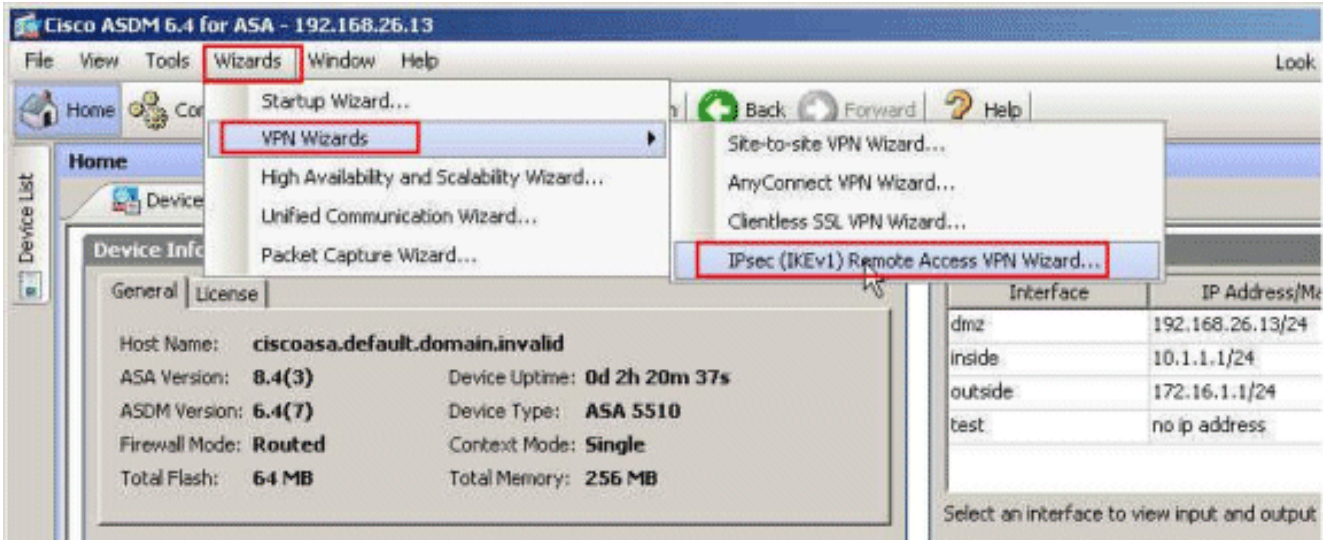
Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Configurar o acesso remoto VPN (IPsec)

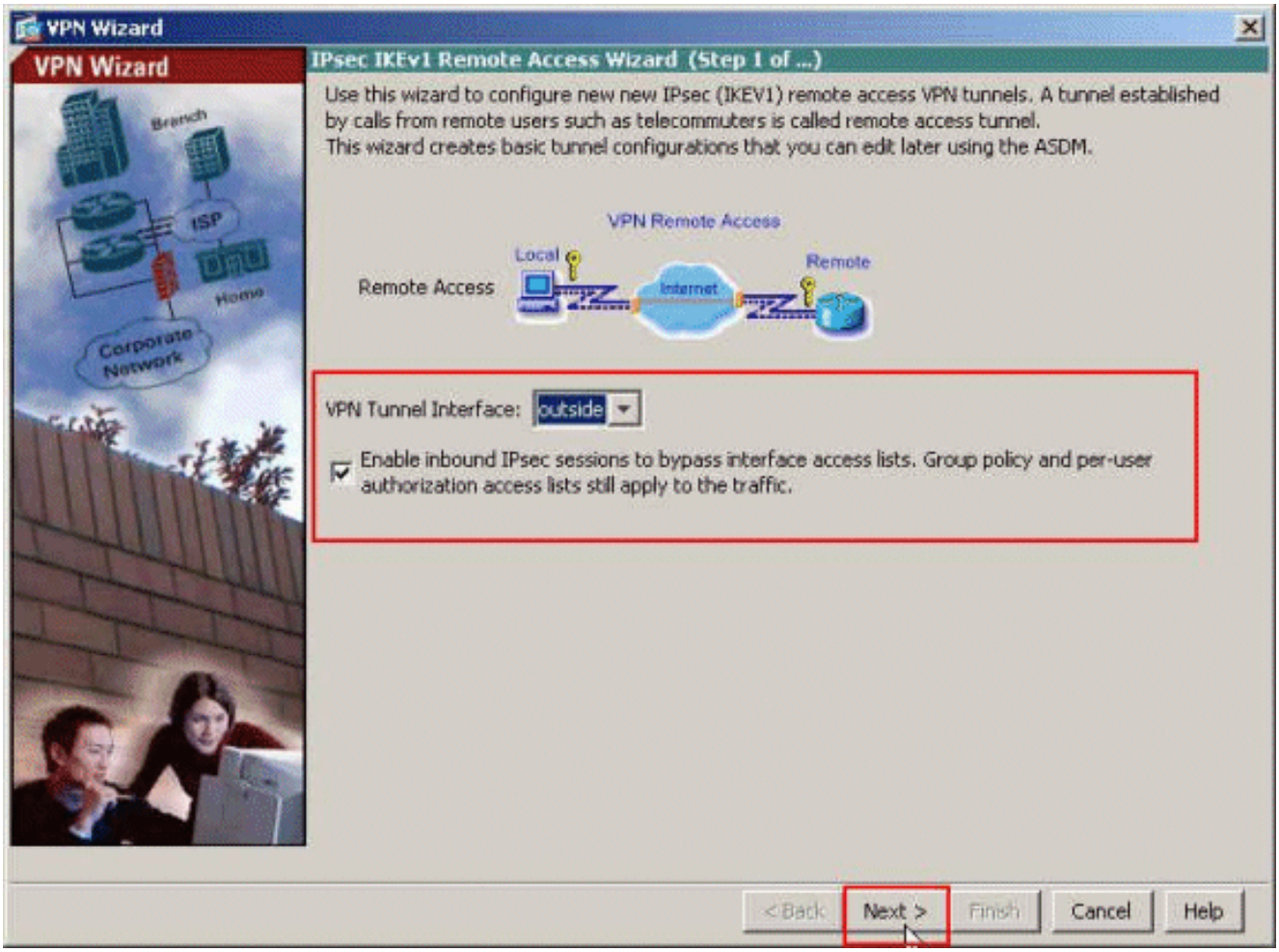
Procedimento ASDM

Termine estas etapas a fim configurar o acesso remoto VPN:

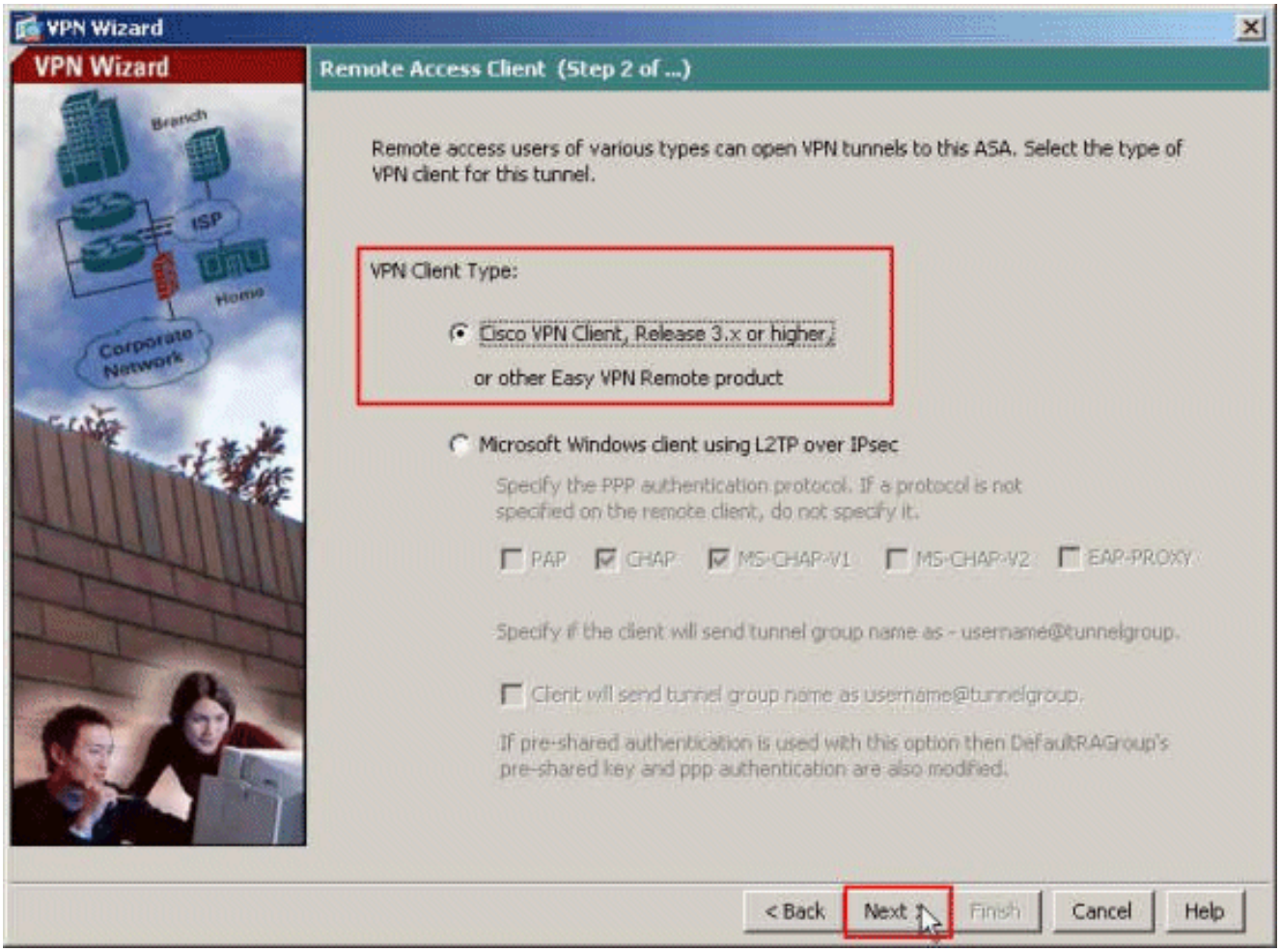
1. Selecione **assistentes > wizard VPN > IPsec(IKEv1) assistente do acesso remoto VPN do** indicador
   home.



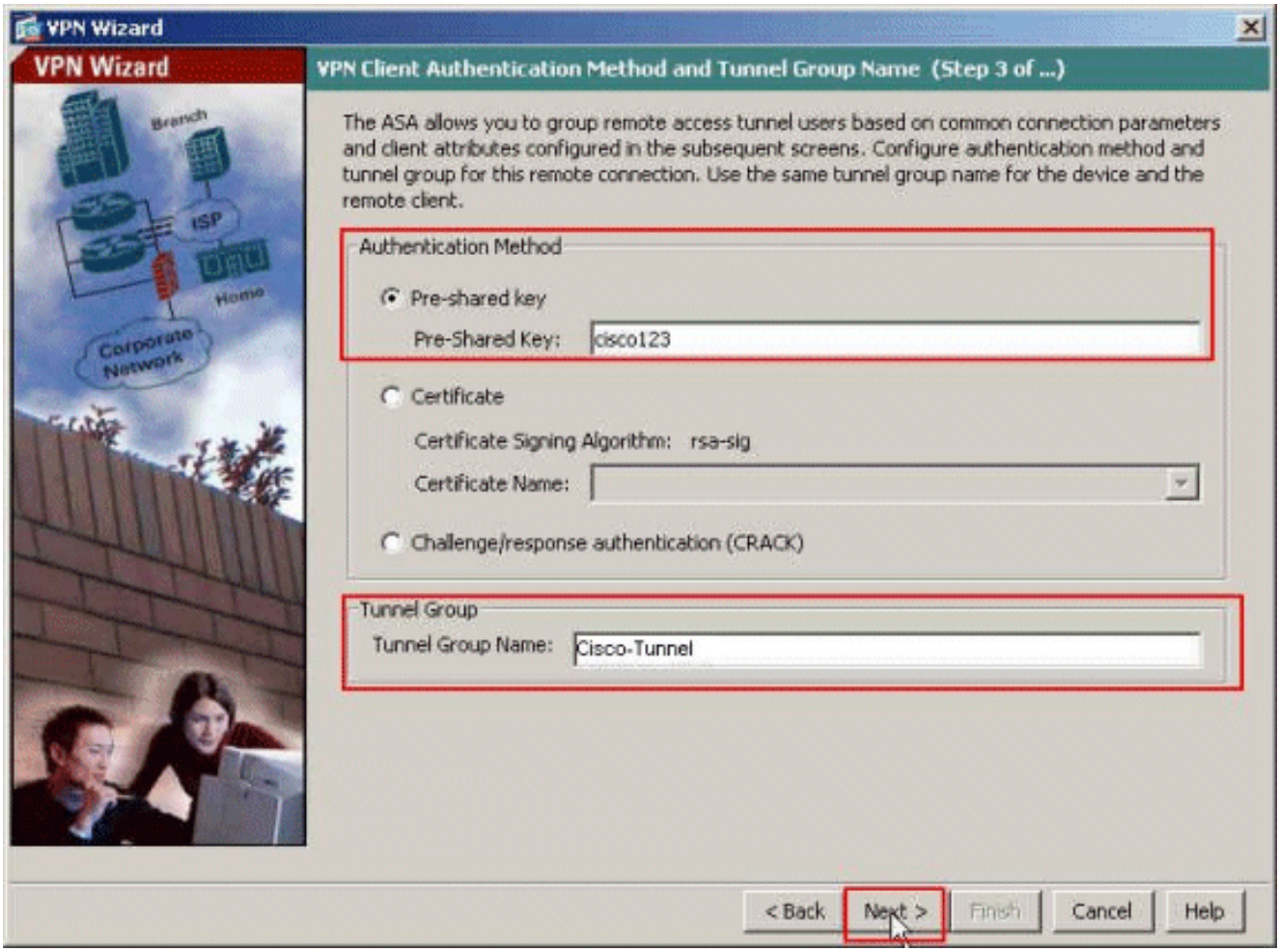
2. Selecione a **interface de túnel VPN** como necessário (**fora**, neste exemplo), e igualmente certifique-se de que a caixa de seleção ao lado do **permite sessões do IPSec de entrada contornear Listas de acesso da relação** está verificada.



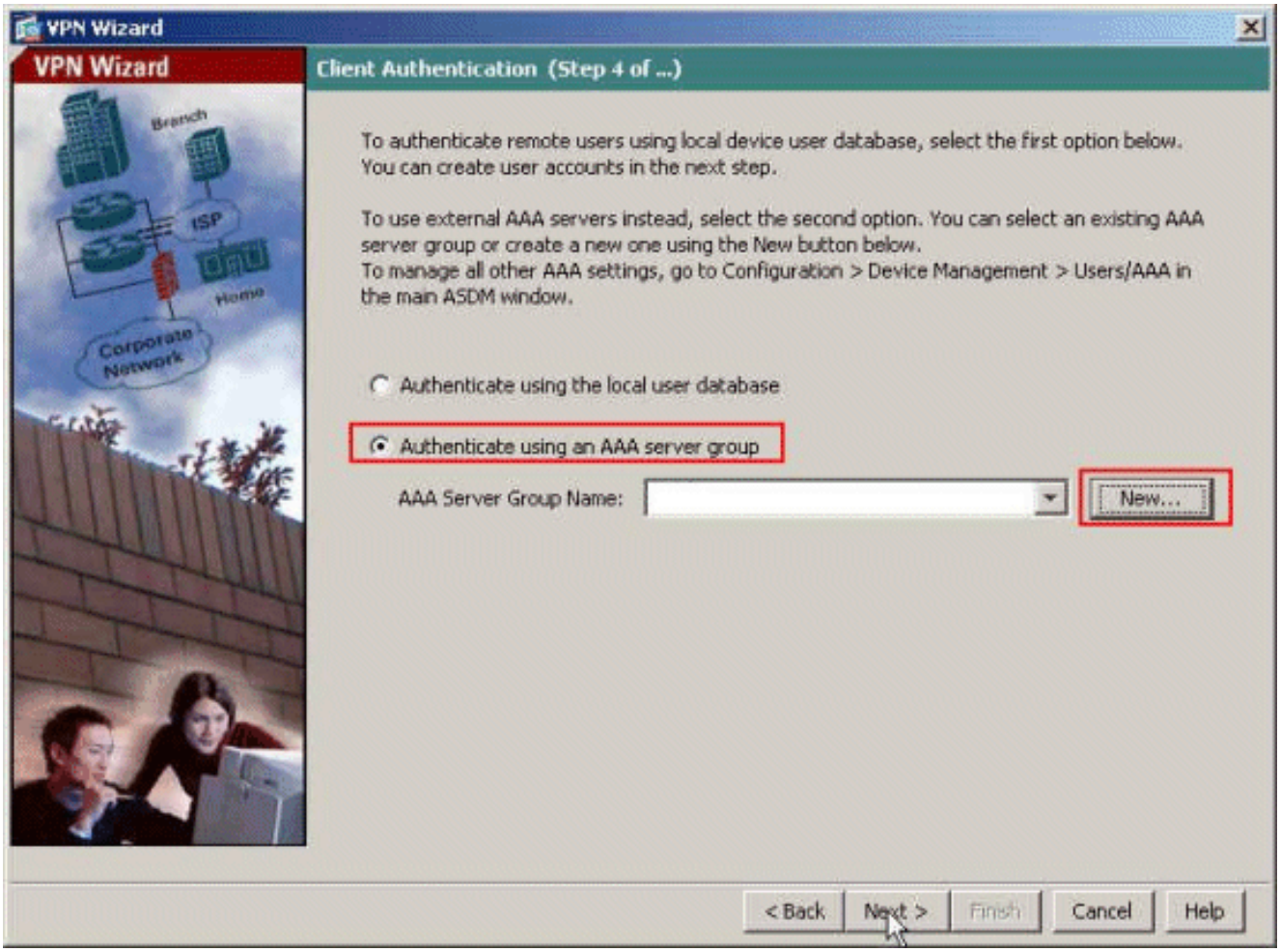
3. Escolha o tipo do cliente VPN como o **Cisco VPN Client, a liberação 3.x ou mais altamente**. Clique em Next.



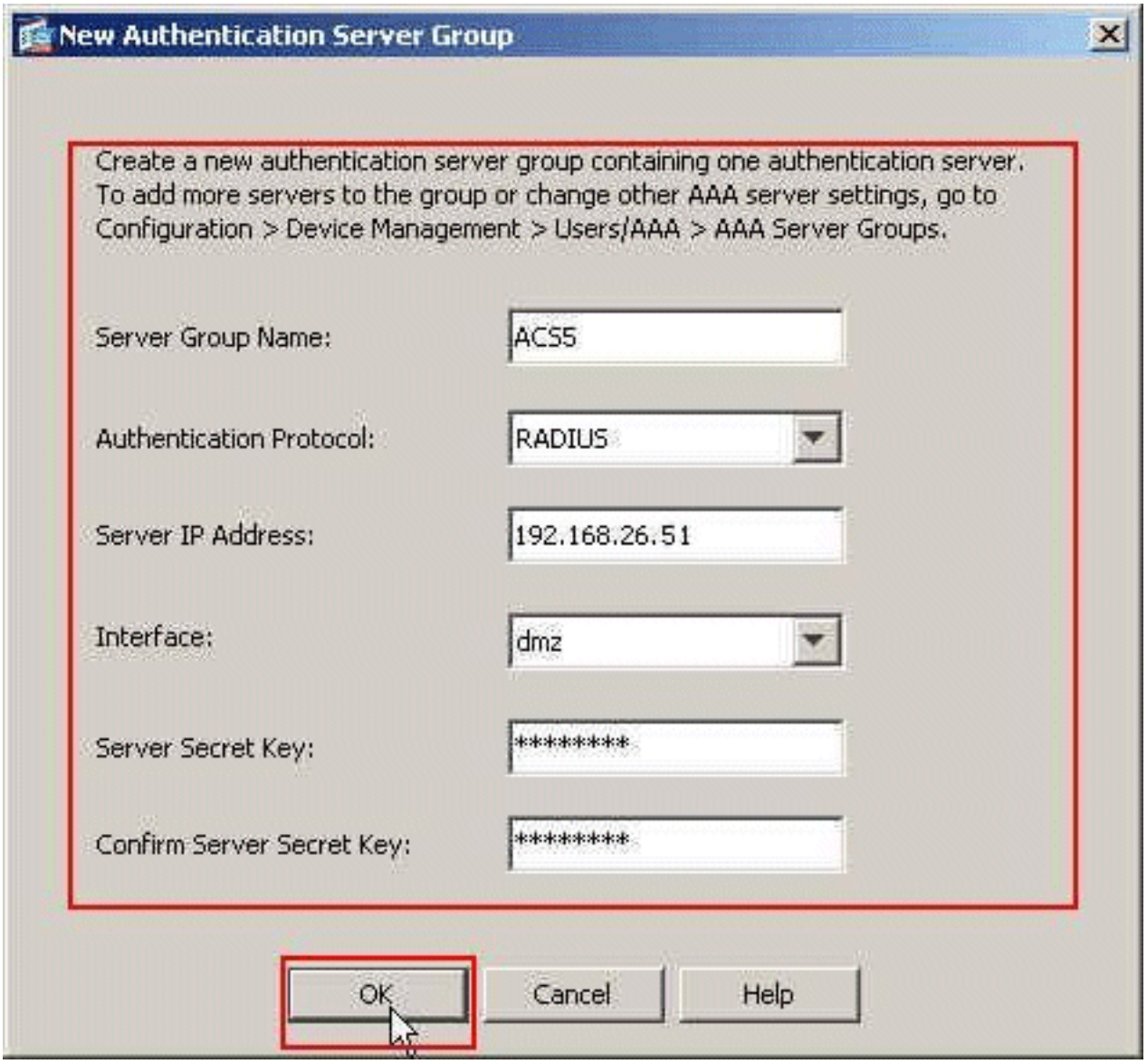
4. Escolha o **método de autenticação** e forneça a informação da autenticação. O método de autenticação usado aqui é **chave pré-compartilhada**. Também, forneça um nome de **grupo de túneis no** espaço fornecido. **A chave pré-compartilhada** usada aqui é **cisco123** e o **nome de grupo de túneis** usado aqui é Cisco-**túnel**. Clique em
Next.



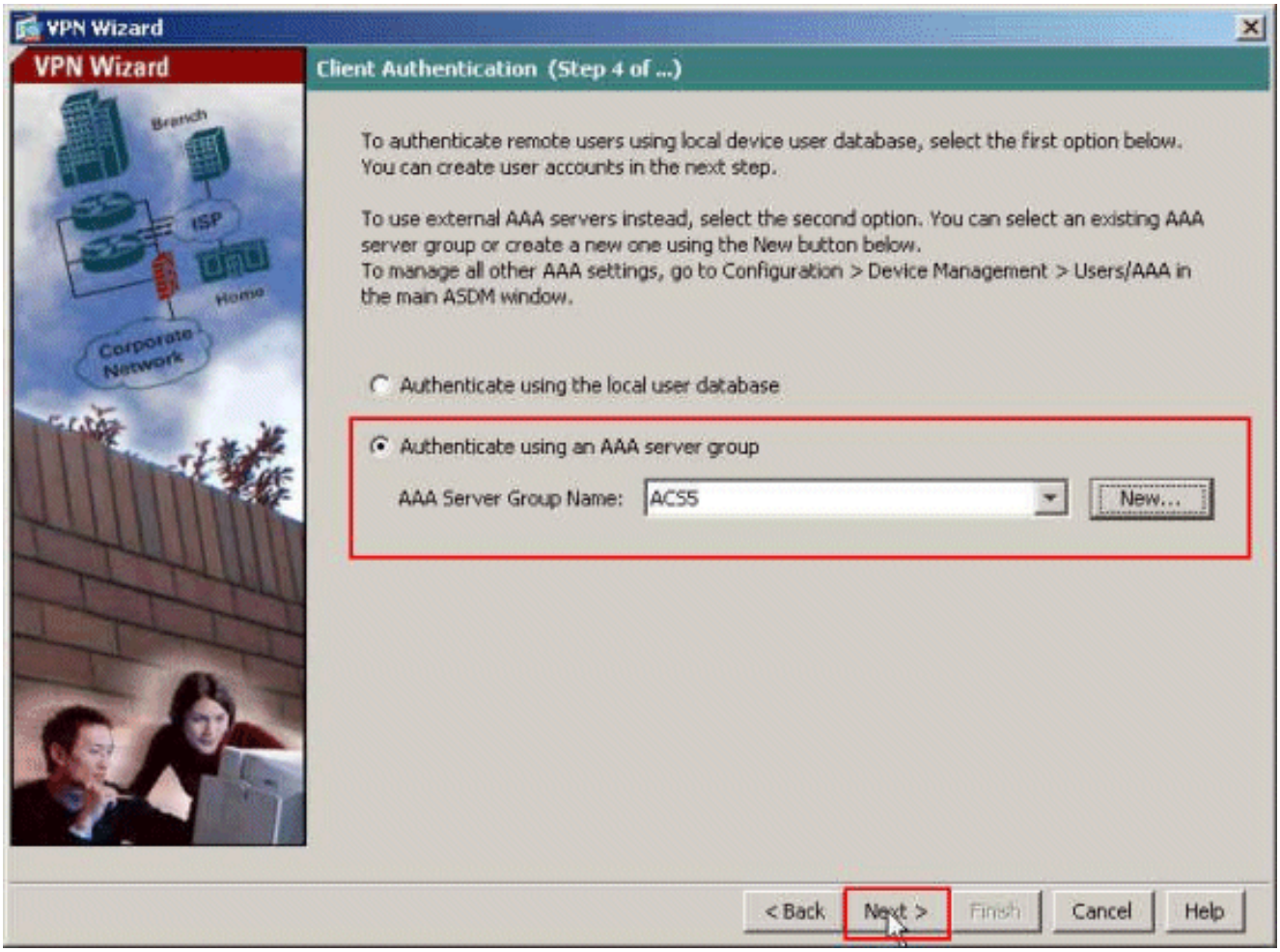
5. Escolha se você quer usuários remotos ser autenticado à base de dados de usuário local ou a um Grupo de servidores AAA externo. Aqui, nós escolhemos **autenticamos usando um Grupo de servidores AAA**. Clique **novo** ao lado do campo de nome do Grupo de servidores AAA a fim criar um nome de Grupo de servidores AAA
novo.



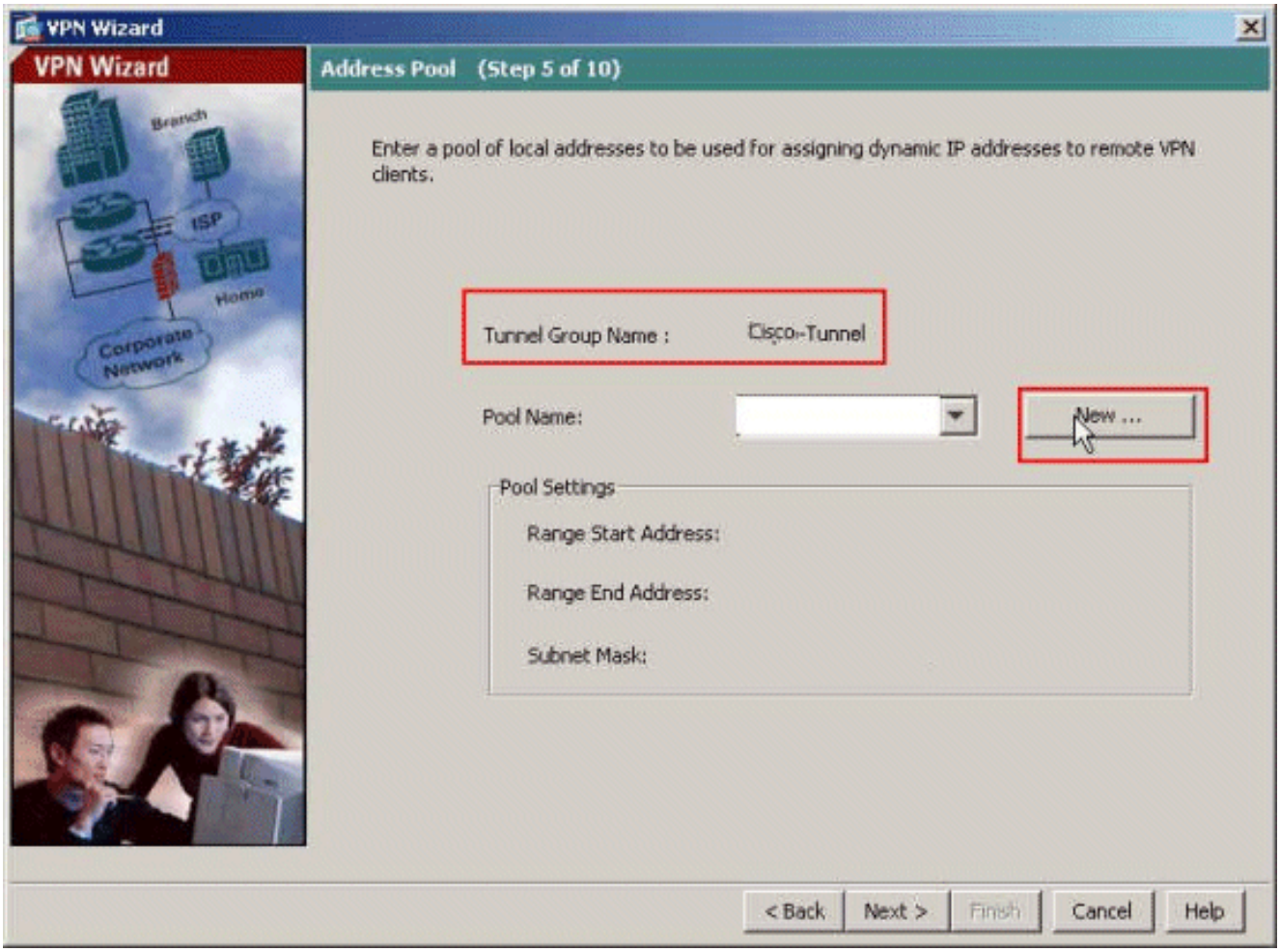
6. Forneça o nome de grupo de servidor, o nome do protocolo de autenticação, do endereço IP do servidor, da relação, e a chave do segredo de servidor nos espaços respectivos fornecidos, e na **APROVAÇÃO do**
clique.



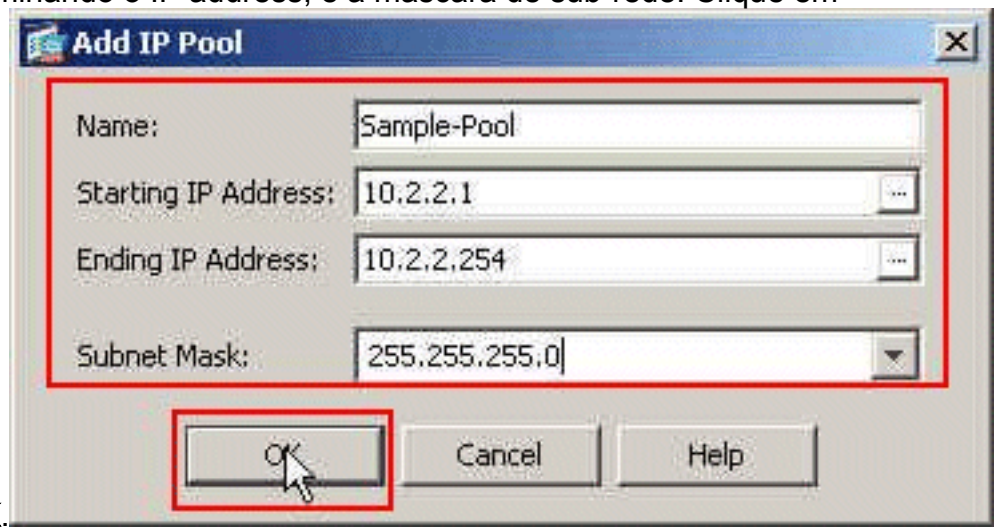
7. Clique em Next.



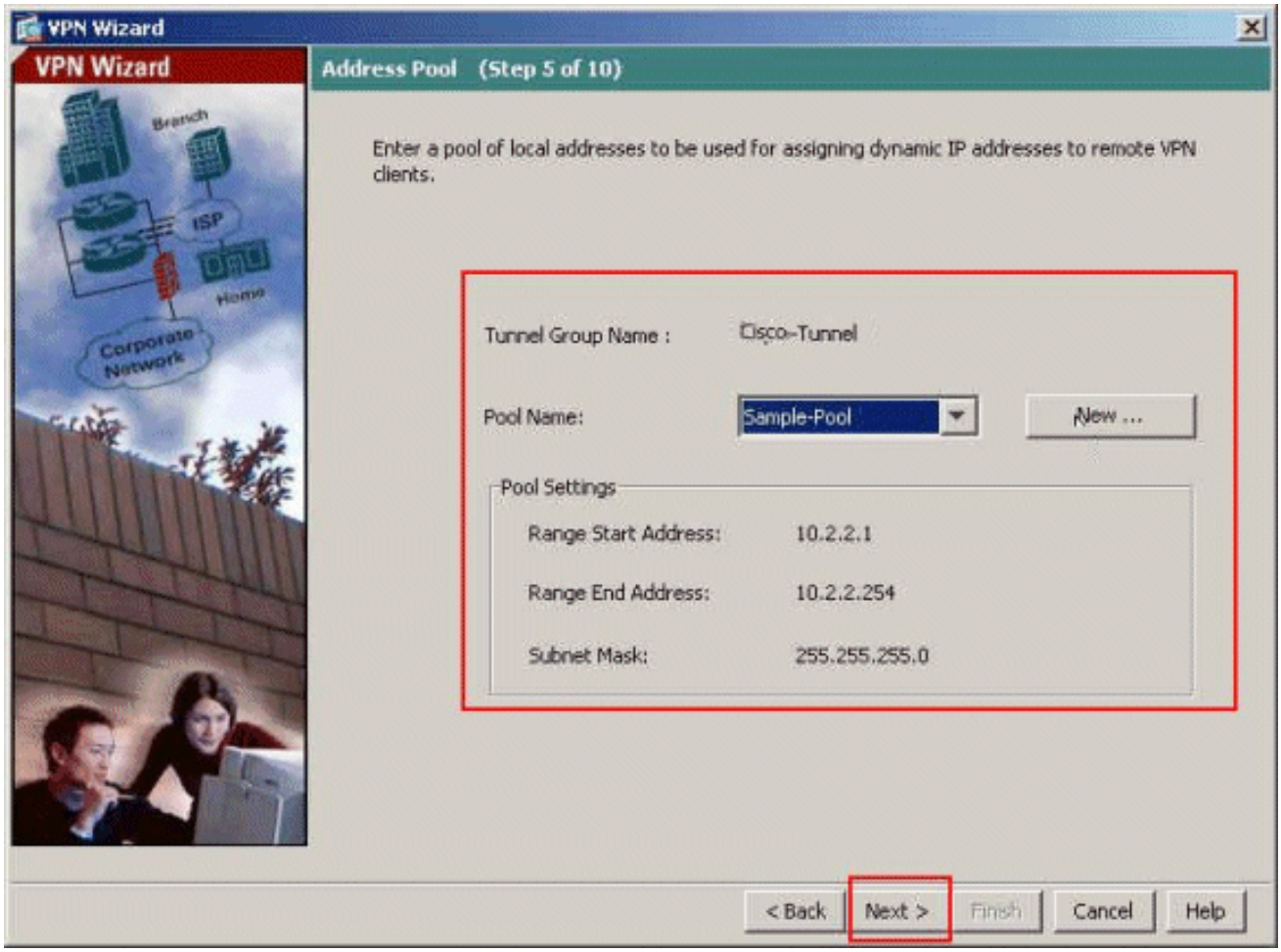
8. Defina um pool dos endereços locais a ser atribuídos dinamicamente aos clientes VPN remotos quando conectam. Clique **novo** a fim criar um pool novo do endereço local.



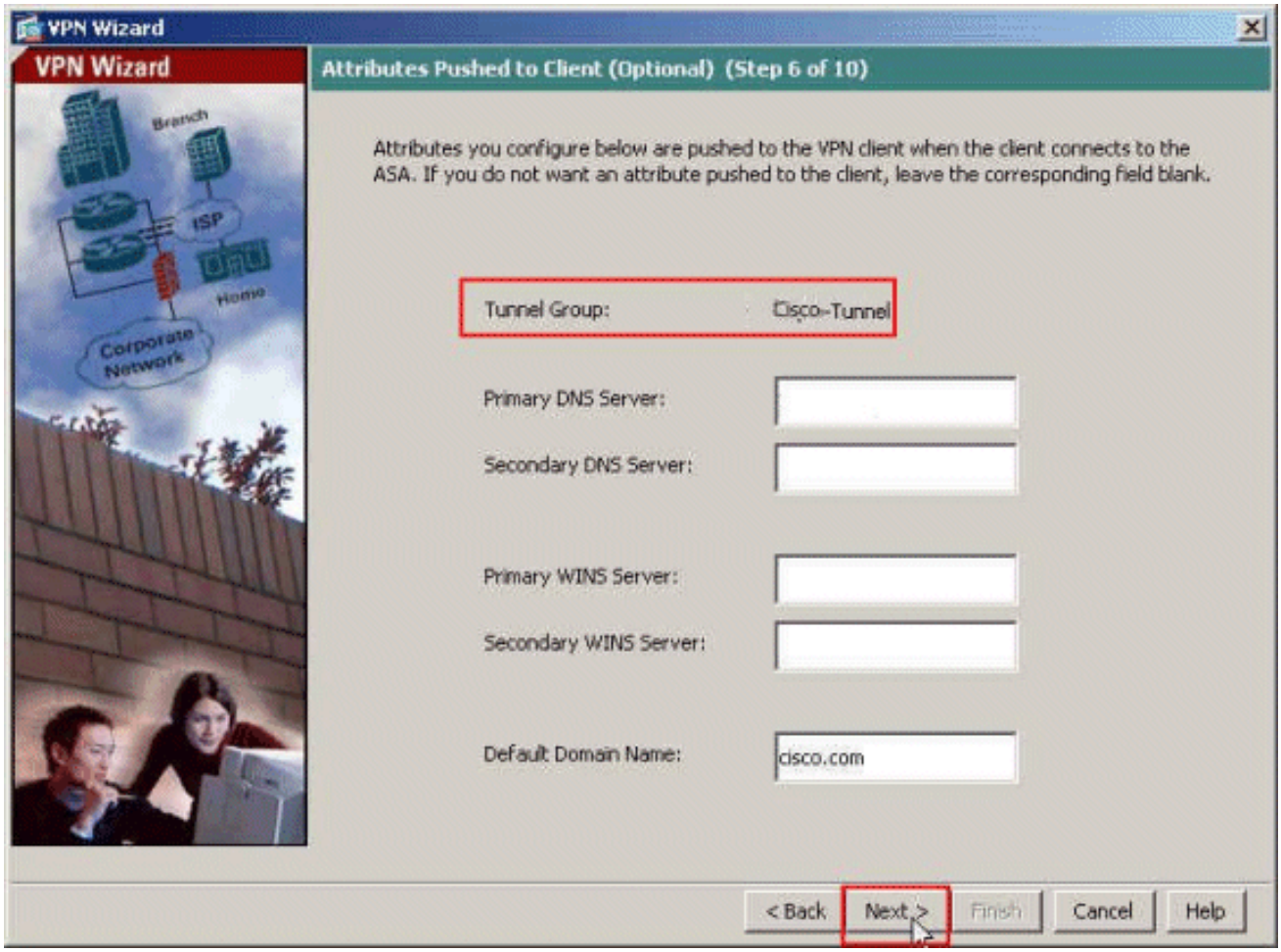
9. No indicador do IP pool adicionar, forneça o nome do pool, começando o IP address, terminando o IP address, e a máscara de sub-rede. Clique em **OK**.



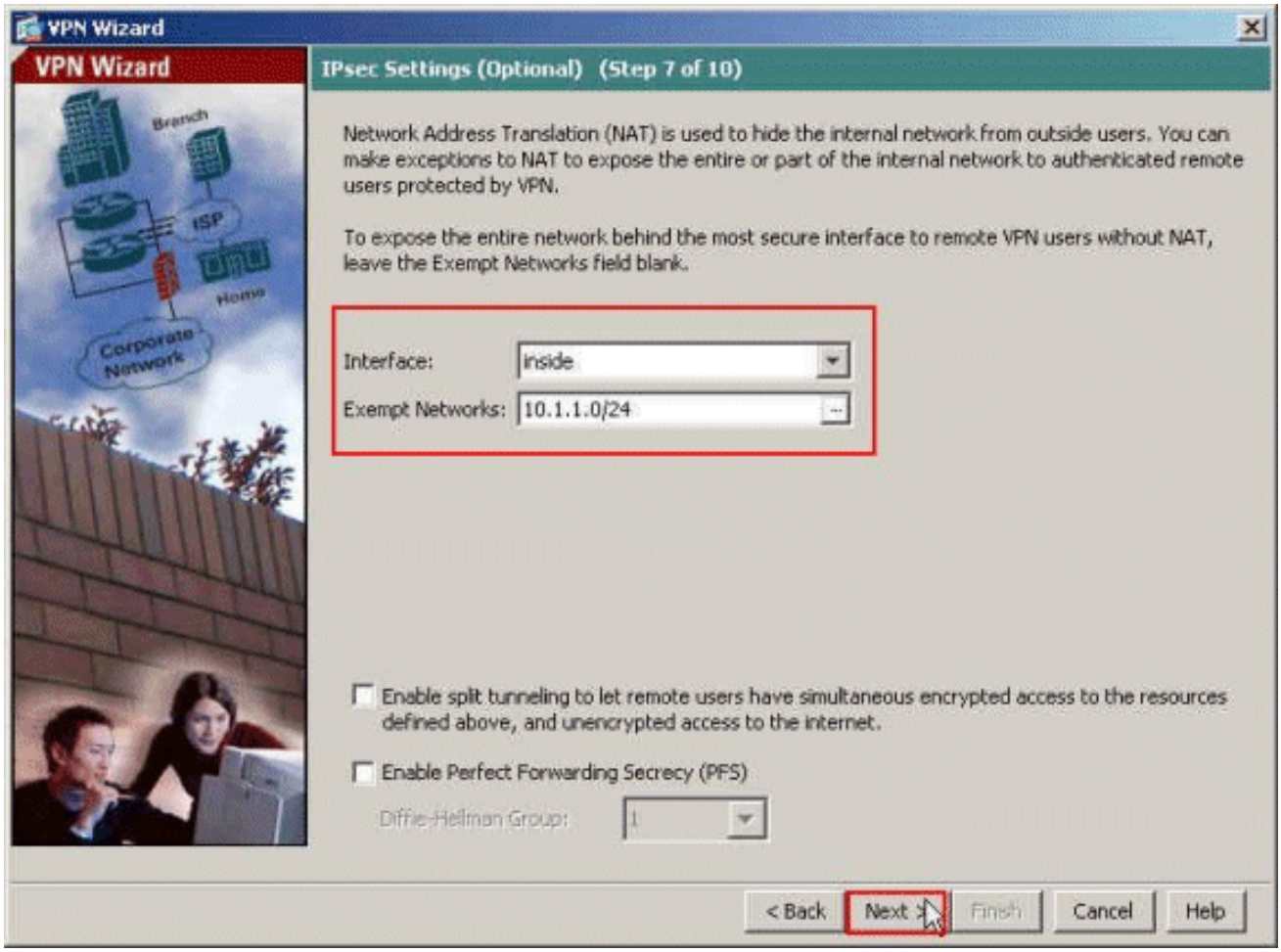
10. Selecione o nome do pool da lista de drop-down, e clique-o **em seguida**. O nome do pool para este exemplo é Amostra-**pool** que foi criado na etapa 9.



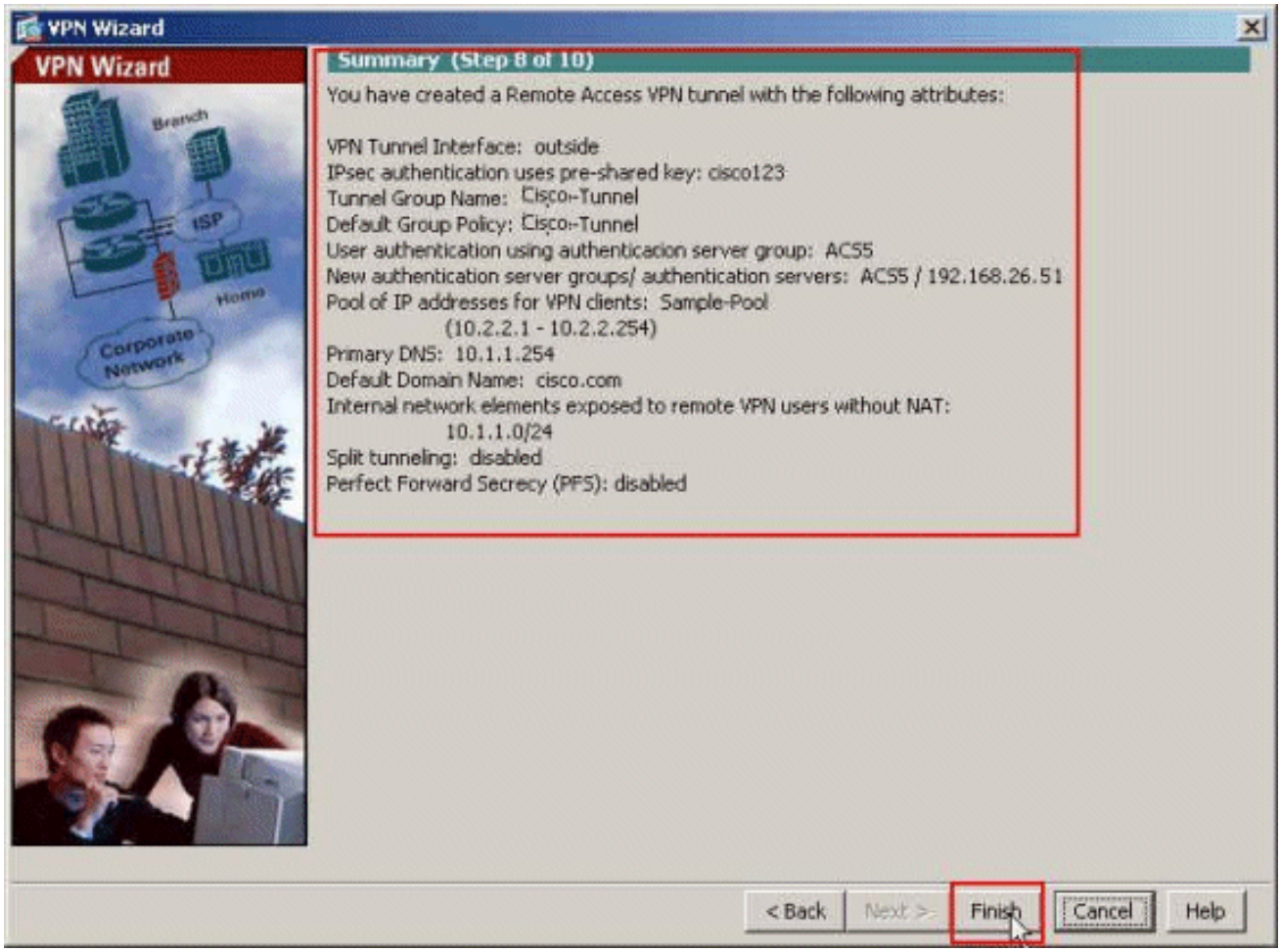
11. *Opcional:* Especifique o DNS e GANHE a informação do server e um Domain Name do padrão a ser empurrado para clientes VPN remotos.



12. Especifique qual, eventualmente, os host internos ou as redes devem ser expostos aos usuários remotos VPN. Clique **em seguida** após ter fornecido o nome da relação e as redes a ser isentadas nas redes isentas colocam.Se você deixa esta lista vazia, permite que os usuários remotos VPN alcancem a rede interna inteira do ASA.Você pode igualmente permitir o Split Tunneling neste indicador. O Split Tunneling cifra o tráfego aos recursos definidos mais cedo neste procedimento e fornece acesso unencrypted ao Internet em grande não escavando um túnel esse tráfego. Se o Split Tunneling não é permitido, todo o tráfego dos usuários remotos VPN está escavado um túnel ao ASA. Esta pode transformar-se muito largura de banda e utilização de processador, com base em sua configuração.



13. Este indicador mostra um sumário das ações que você tomou. Clique o **revestimento** se você é satisfeito com sua configuração.



Configurar o ASA com CLI

Esta é a configuração de CLI:

Configuração running no 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#
```

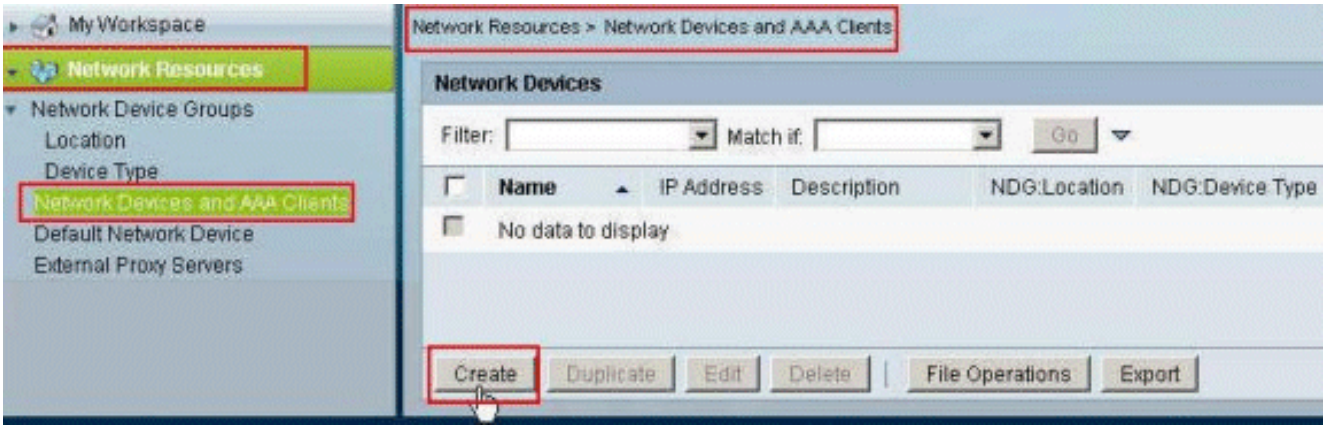
Configurar ACS para ACL baixável para o usuário individual

Você pode configurar Listas de acesso carregável no Cisco Secure ACS 5.x porque umas Permissões Nomeados Objeto e o atribui então a um perfil da autorização que seja escolhido na seção do resultado da regra no Acesso-serviço.

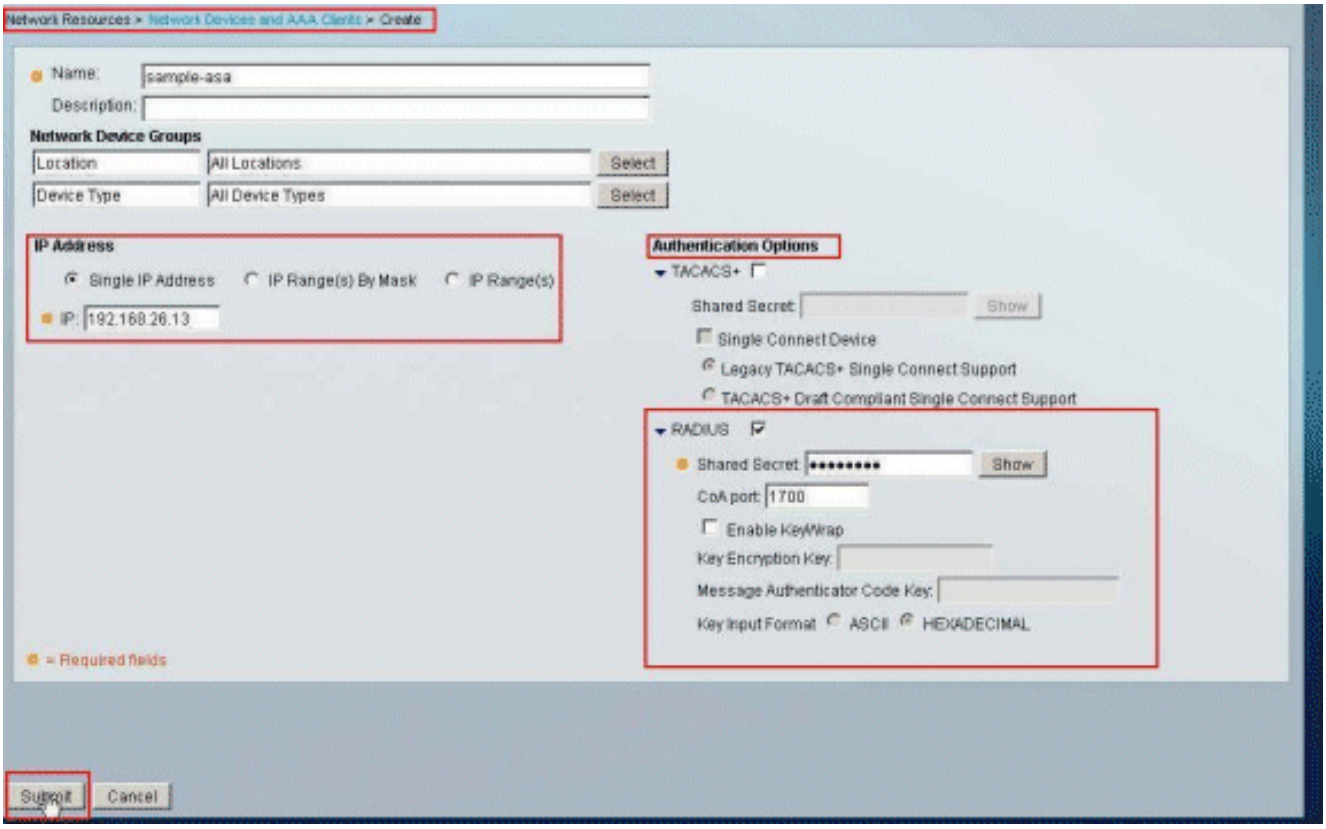
Neste exemplo, o usuário **Cisco do** IPSec VPN autentica com sucesso, e o servidor Radius envia uma lista de acessos carregável à ferramenta de segurança. O usuário “Cisco” pode alcançar somente o server de 10.1.1.2 e nega todo acesso restante. A fim verificar o ACL, veja o ACL baixável para o usuário/seção de grupo.

Termine estas etapas a fim configurar o cliente RADIUS em um Cisco Secure ACS 5.x:

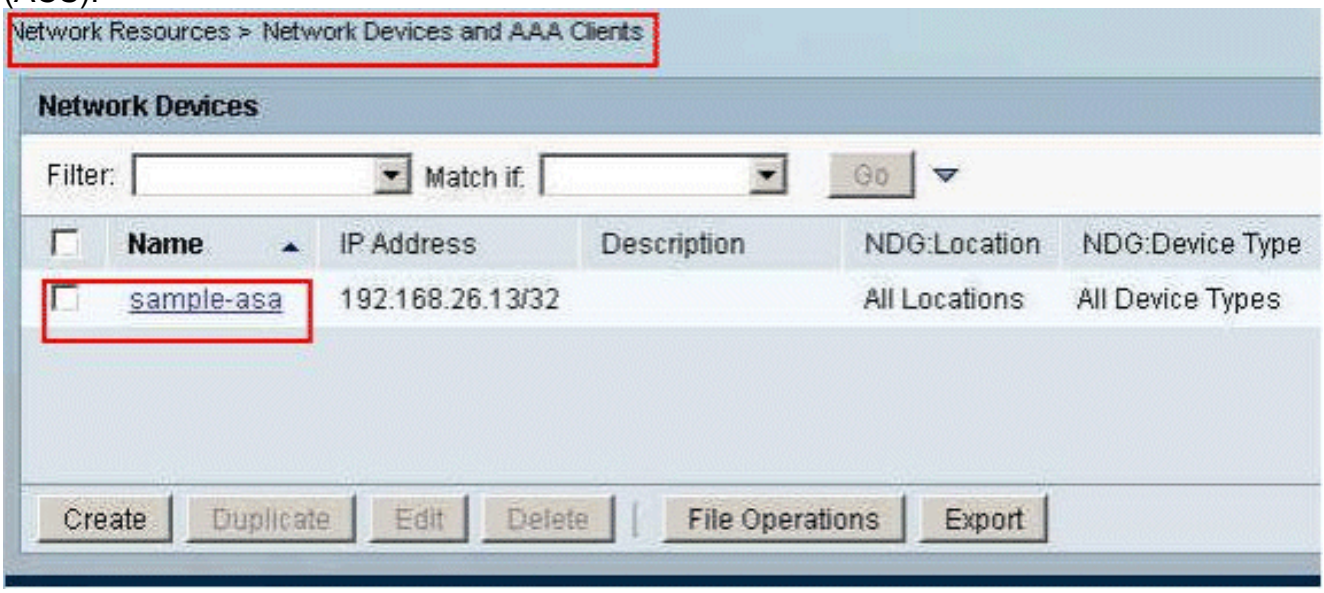
1. Escolha **recursos de rede > dispositivos de rede e clientes de AAA**, e o clique **cria** a fim adicionar uma entrada para o ASA na base de dados do servidor radius.



2. Dê entrada com o nome significativo a localmente - para o ASA (amostra-**ASA**, neste exemplo), a seguir inscreva **192.168.26.13 no** campo do IP address. Escolha o **RAIO na** seção das opções de autenticação verificando a caixa de seleção do **RAIO** e entre no **cisco123** para o campo secreto compartilhado. Clique em Submit.

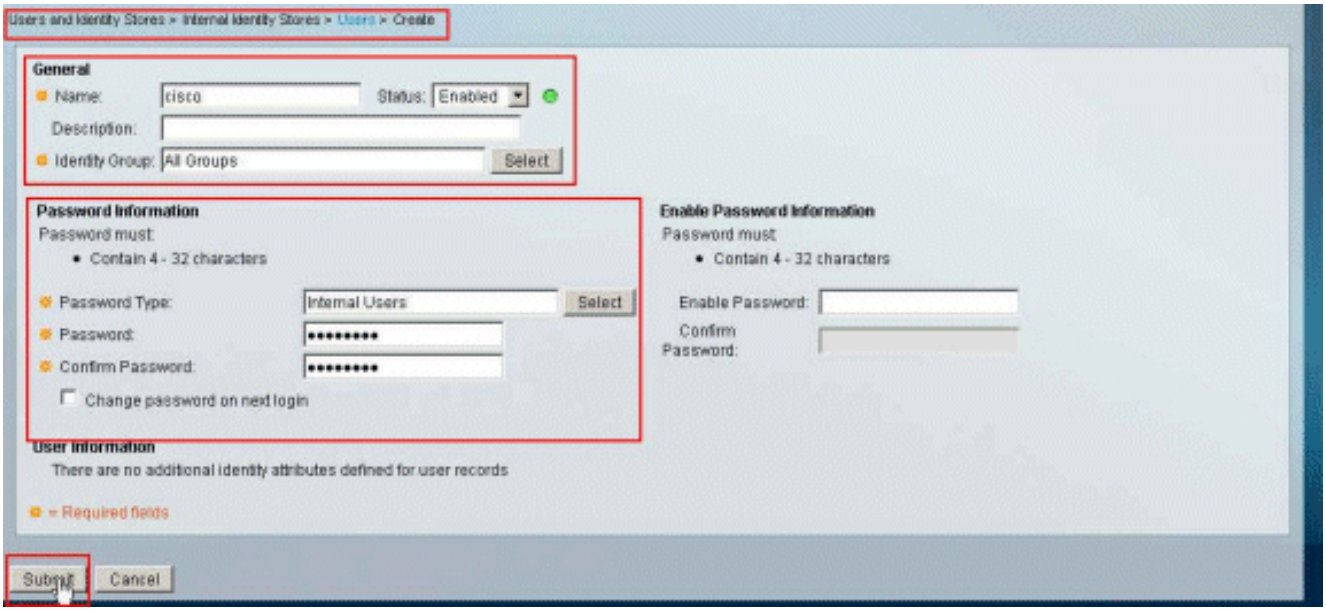


3. O ASA é adicionado com sucesso ao base de dados do servidor Radius (ACS).

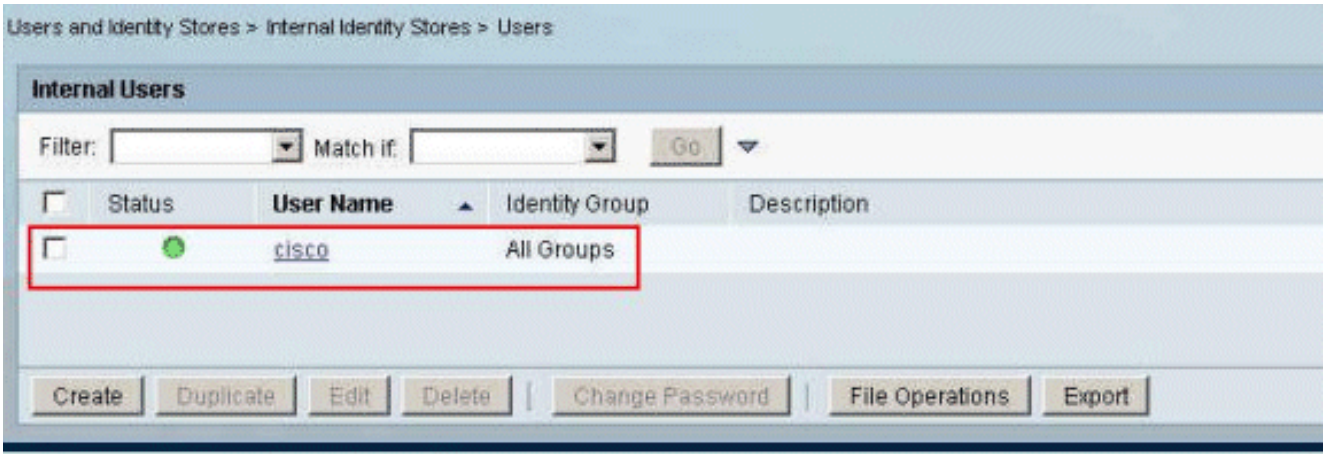


4. Escolha **usuários e a identidade armazena > identidade interna armazena > usuários**, e o clique **cria** a fim criar um usuário no base de dados local do ACS para a autenticação VPN.

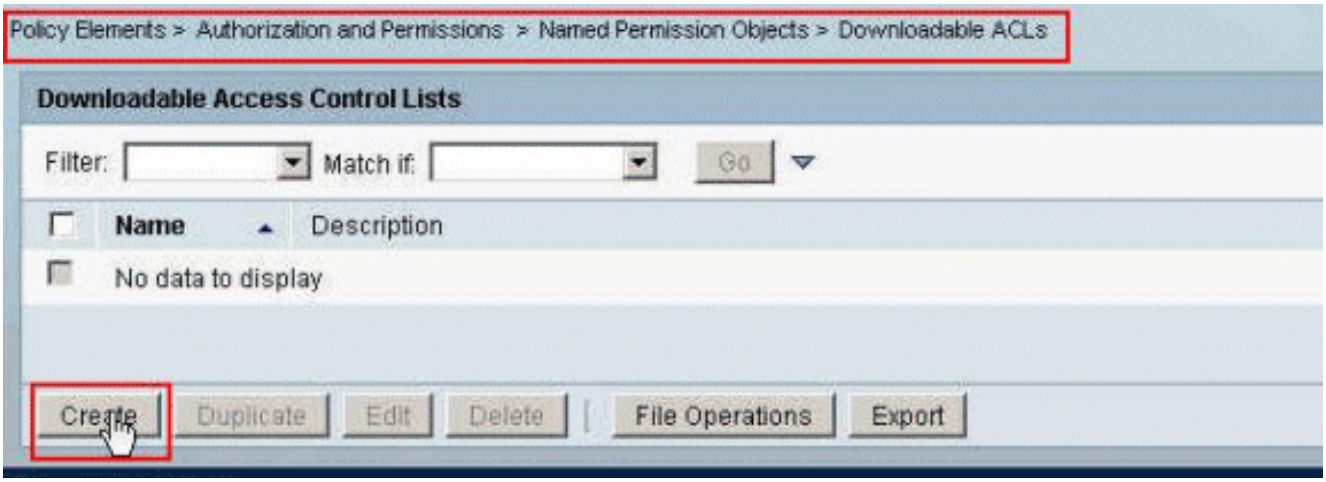
5. Incorpore o username **Cisco**. Selecione o tipo de senha como **usuários internos**, e incorpore a senha (**cisco123**, neste exemplo). Confirme a senha, e o clique **submete-se**.



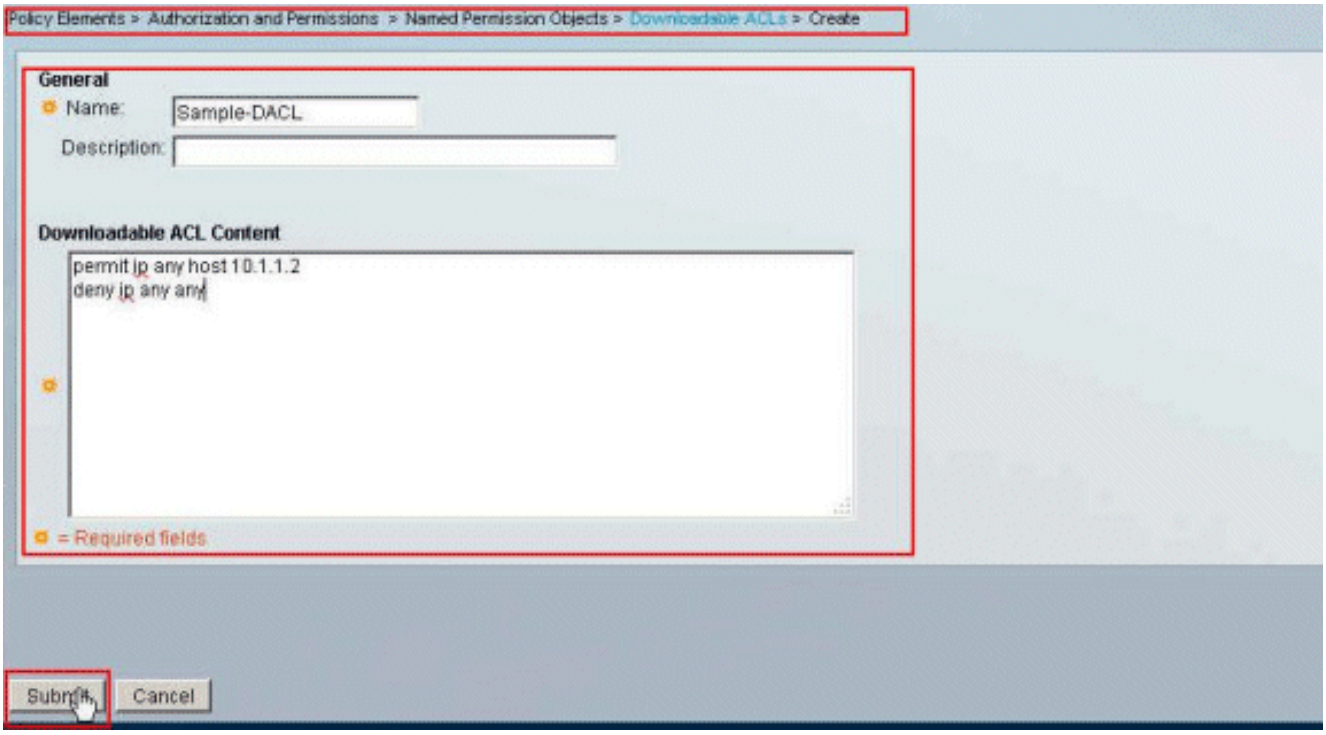
6. O usuário **Cisco** é criado com sucesso.



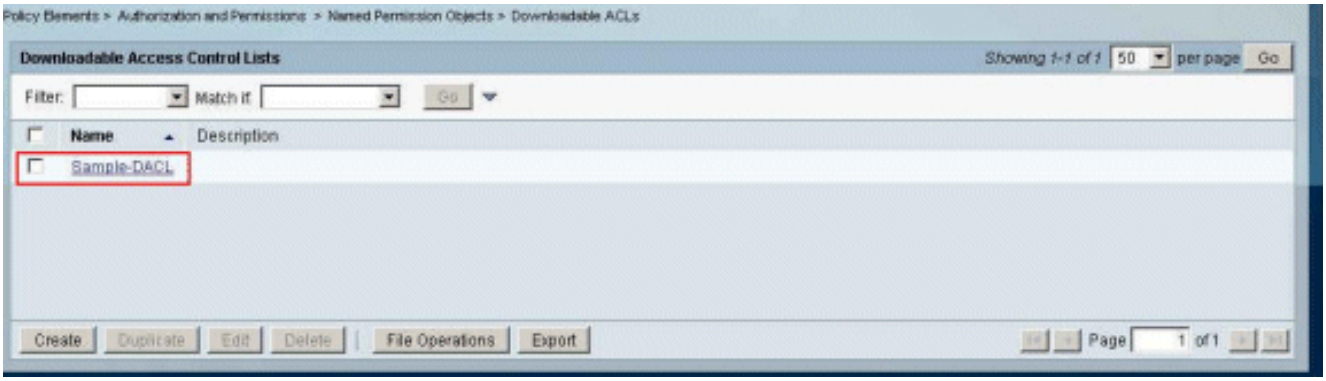
7. A fim criar um ACL baixável, para escolher **elementos da política > autorização e permissões > nomeou Permissão Objeto > ACL carregável**, e o clique **cria**.



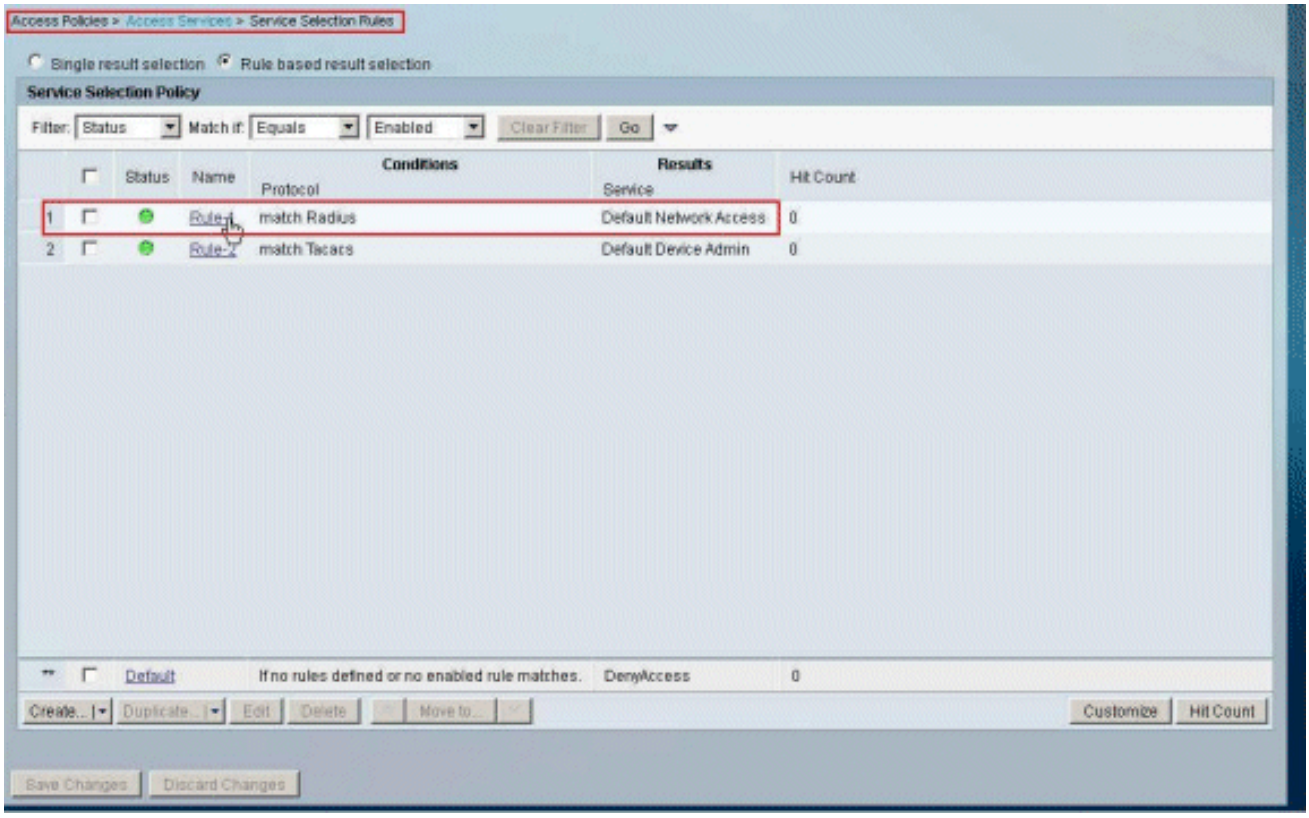
8. Forneça o **nome** para o **índice** ACL baixável, assim como **ACL**. Clique em Submit.



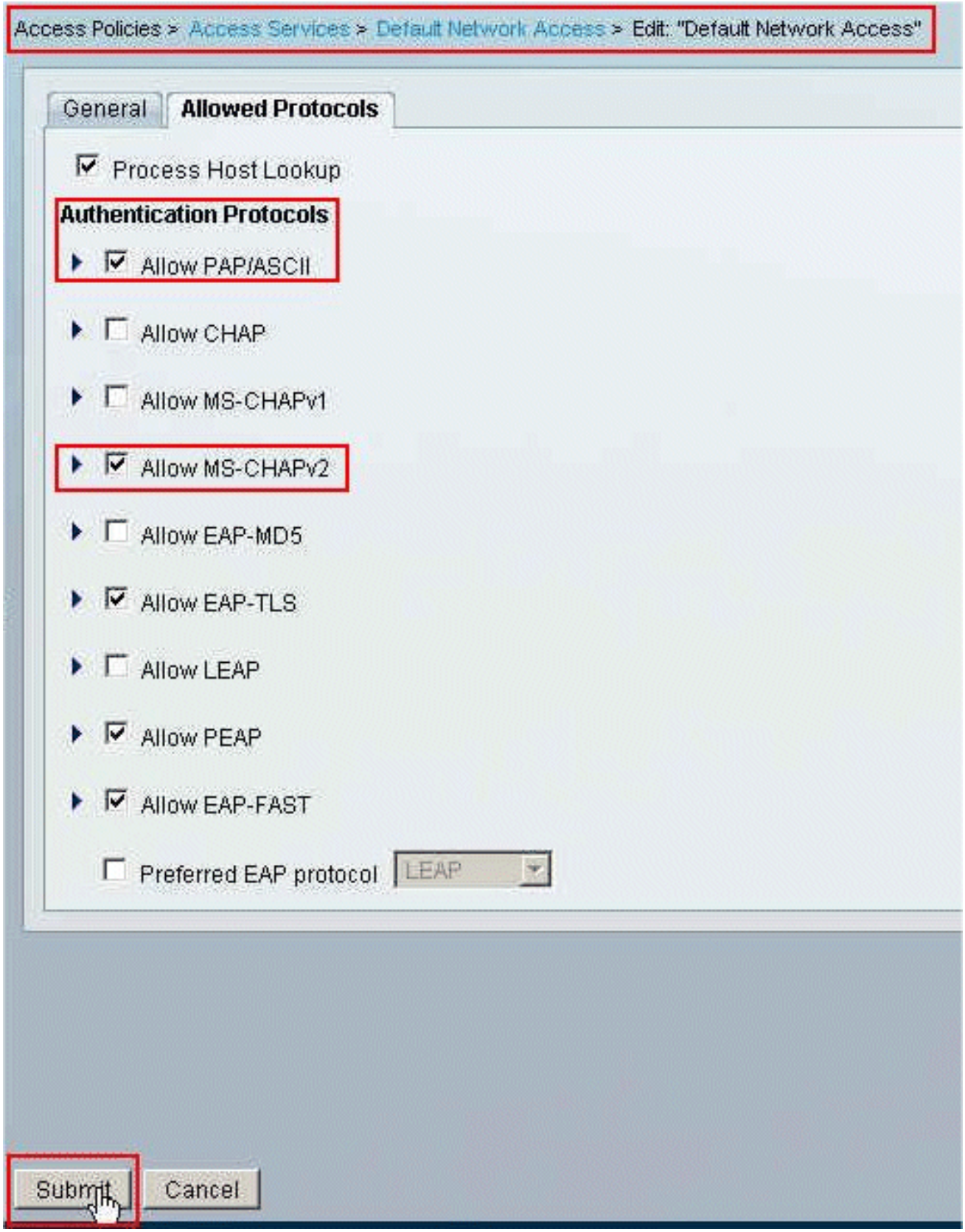
9. **A amostra-DACL** ACL baixável é criada com sucesso.



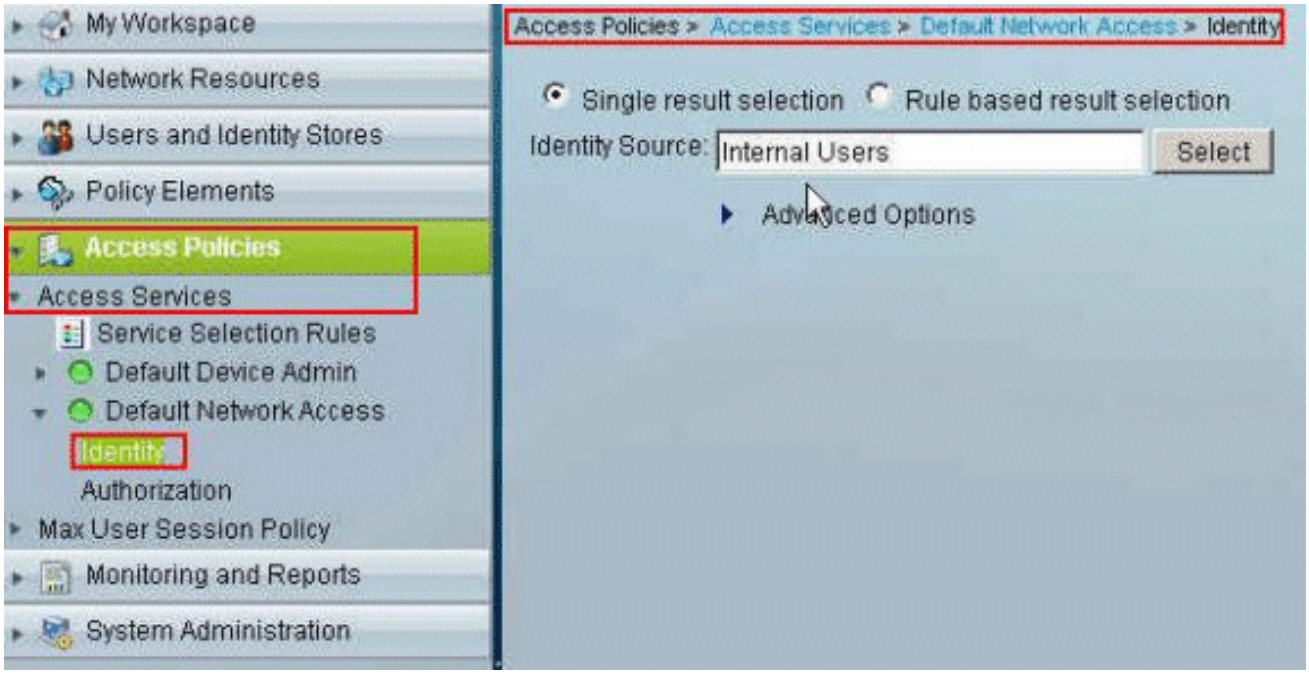
10. A fim configurar as políticas de acesso para a autenticação VPN, escolha **políticas de acesso > acesso presta serviços de manutenção > regras de seleção do serviço**, e determinam que serviço está abastecendo ao protocolo de raio. Neste exemplo, **ordene 1 RAIO dos** fósforos, e o acesso de rede padrão abastecerá à requisição RADIUS.



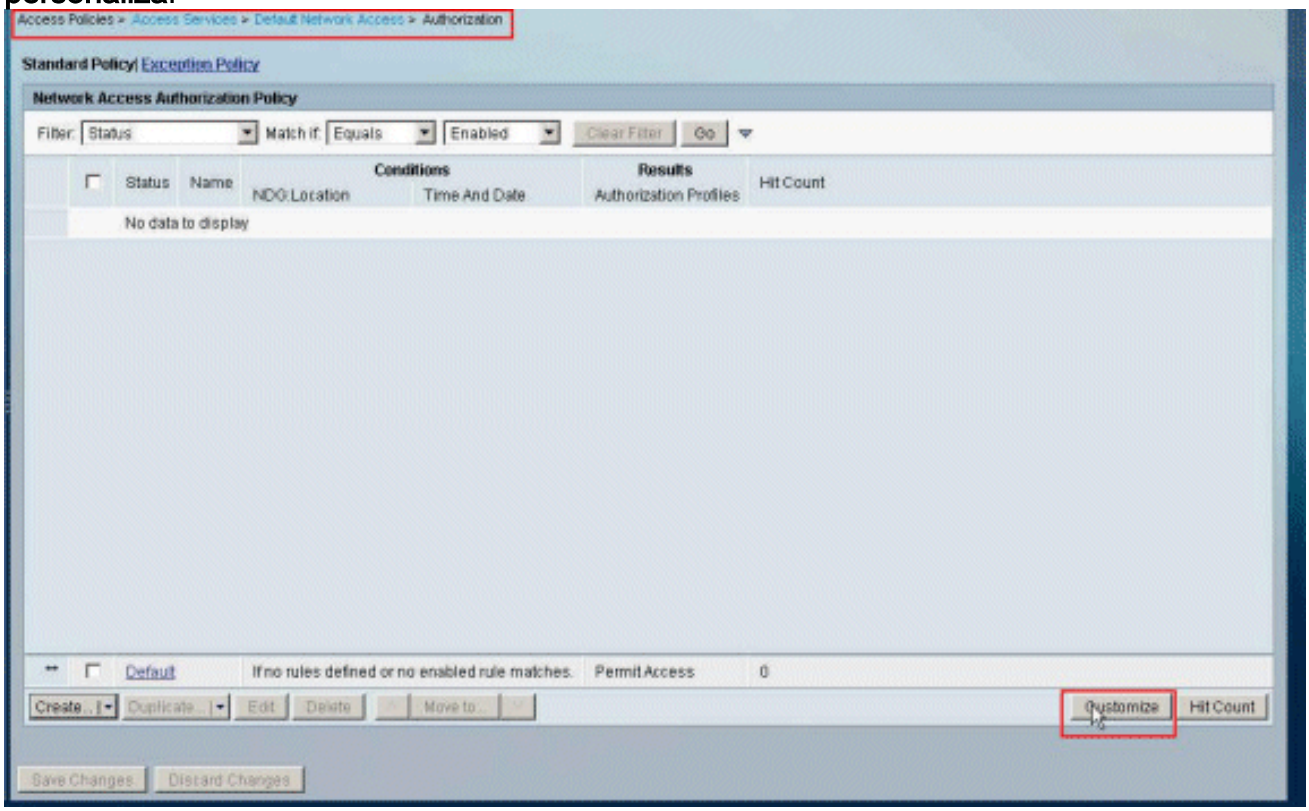
11. Escolha o **serviço do acesso** determinado da etapa 10. Neste exemplo, o **acesso de rede padrão** é usado. Escolha a aba **permitida dos protocolos**, e certifique-se de que **permita PAP/ASCII** e **permita MS-CHAPv2** estão selecionados. Clique em Submit.



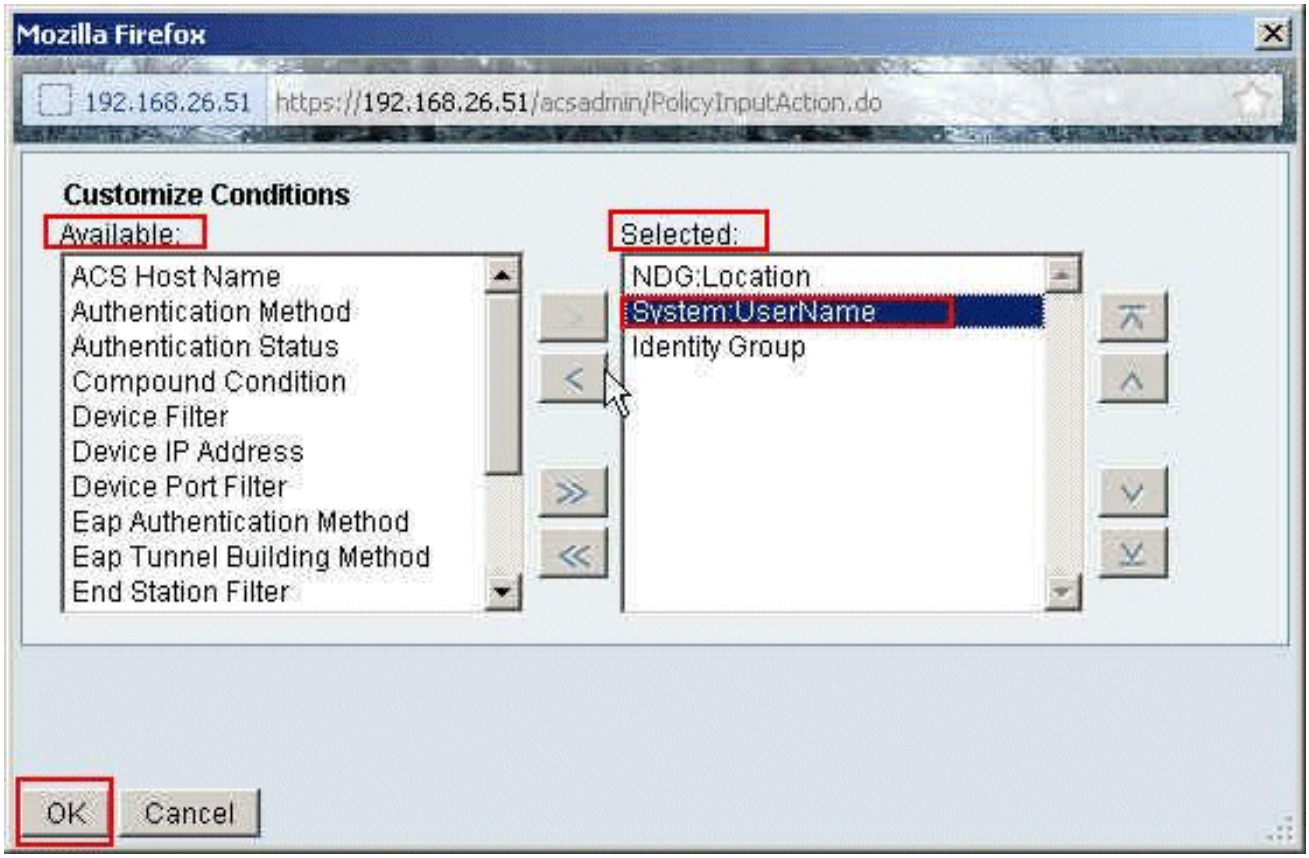
12. Clique sobre a **seção da identidade dos serviços do acesso**, e certifique-se de que os **usuários internos** estão selecionados como a fonte da identidade. Neste exemplo, nós tomamos o acesso de rede
padrão.



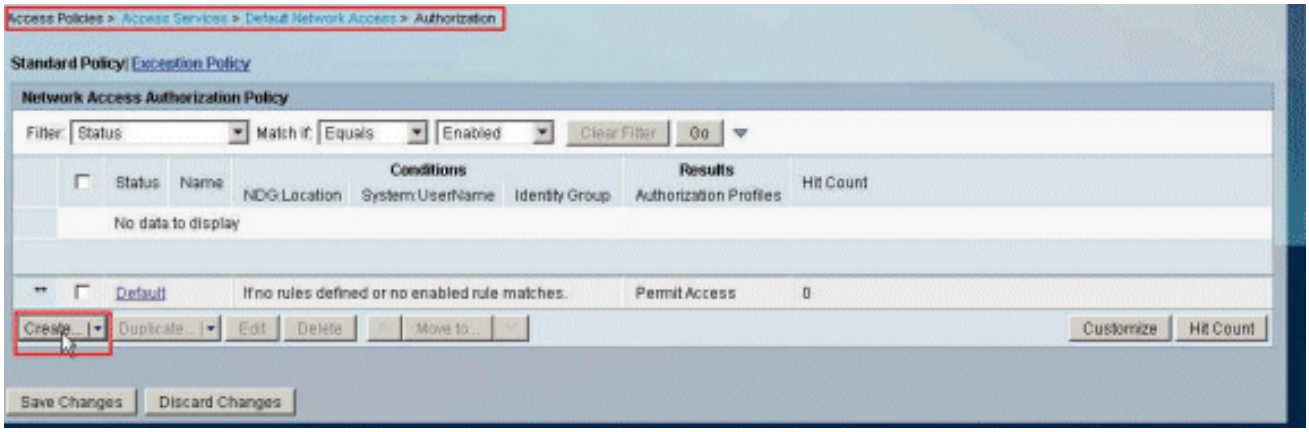
13. Escolha **políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão**, e o clique **personaliza**.



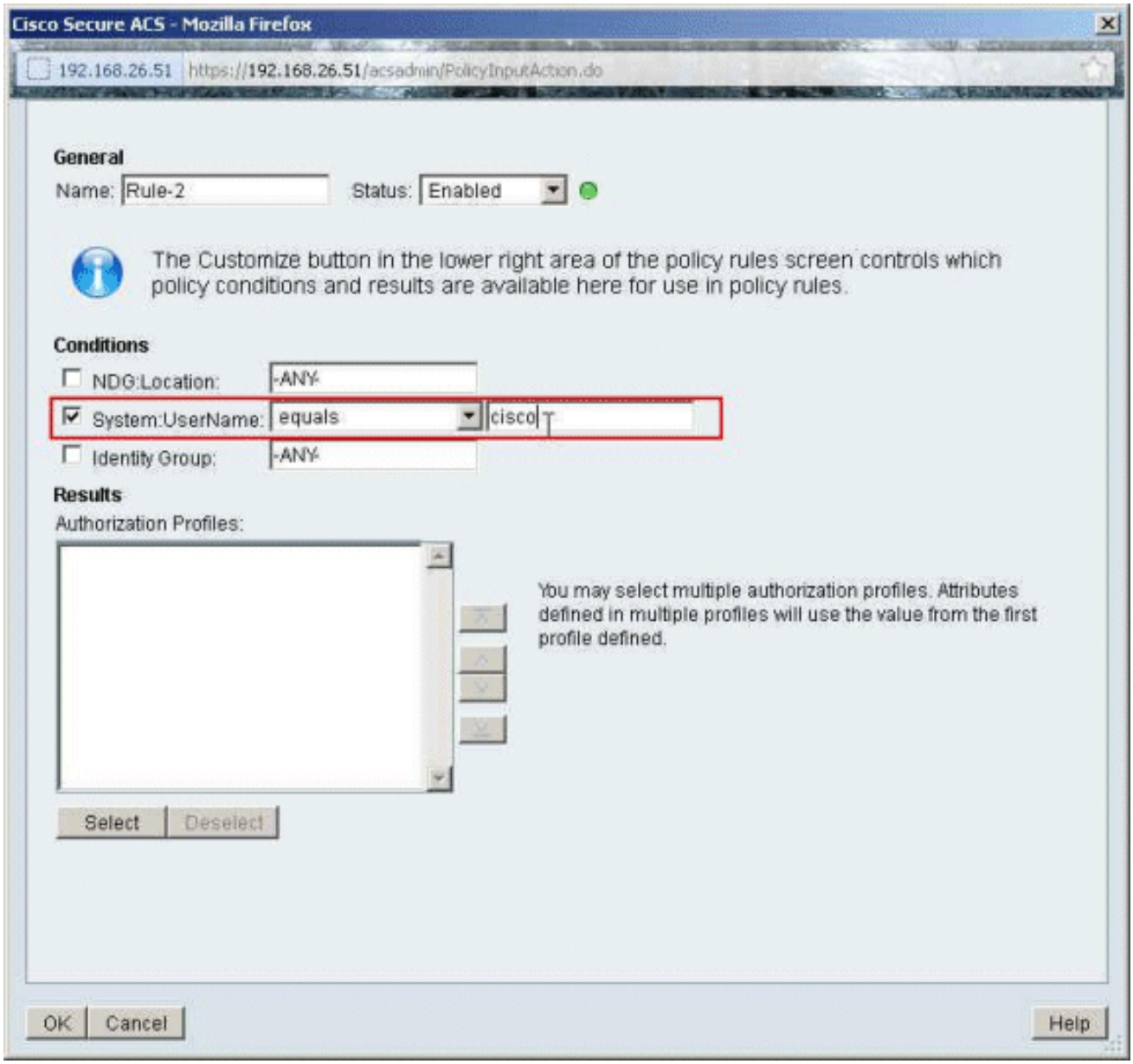
14. **Sistema do** movimento: **Username da** coluna **disponível à** coluna **selecionada**, e **APROVAÇÃO do** clique.



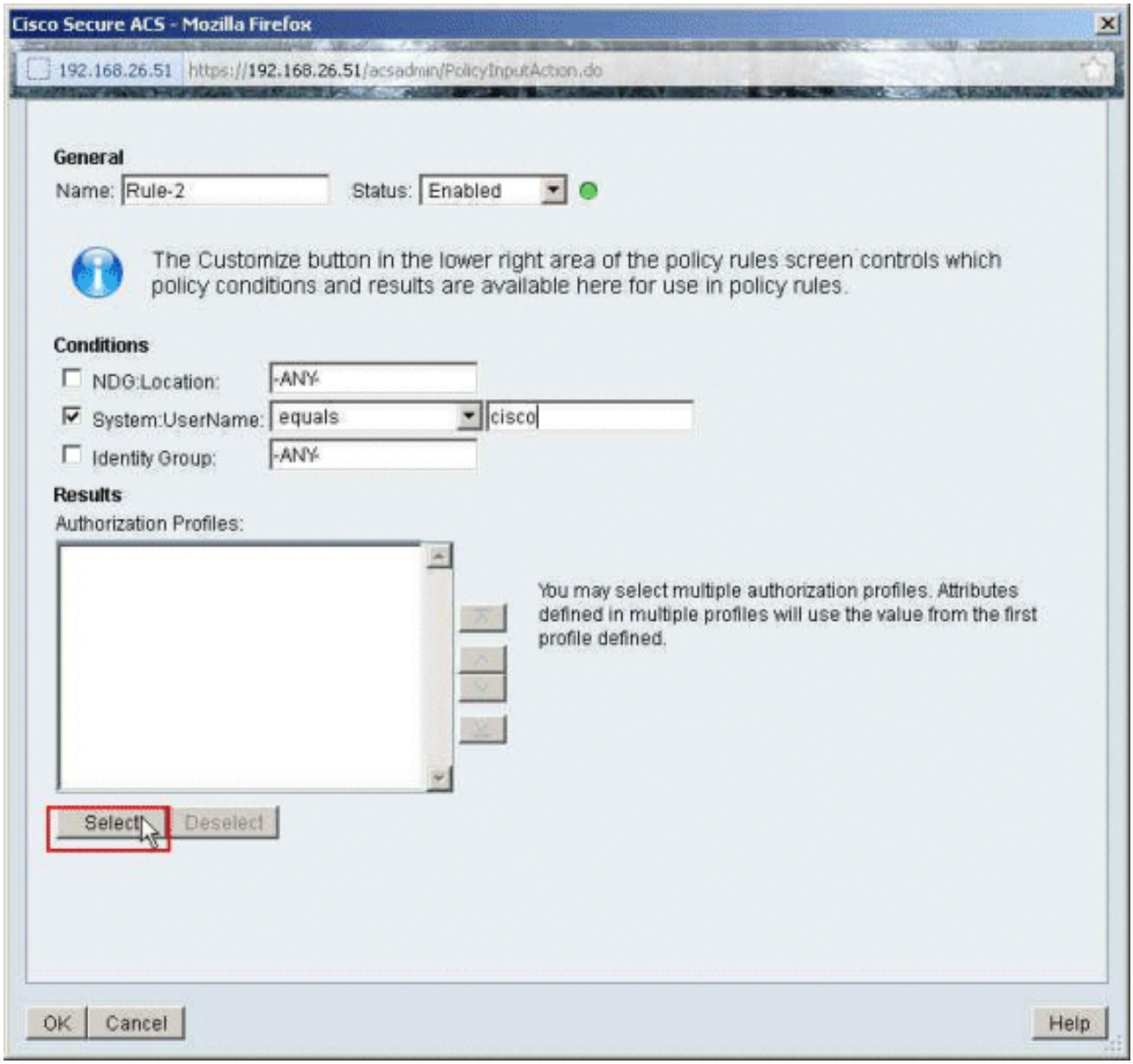
15. O clique **cria** a fim criar uma regra nova.



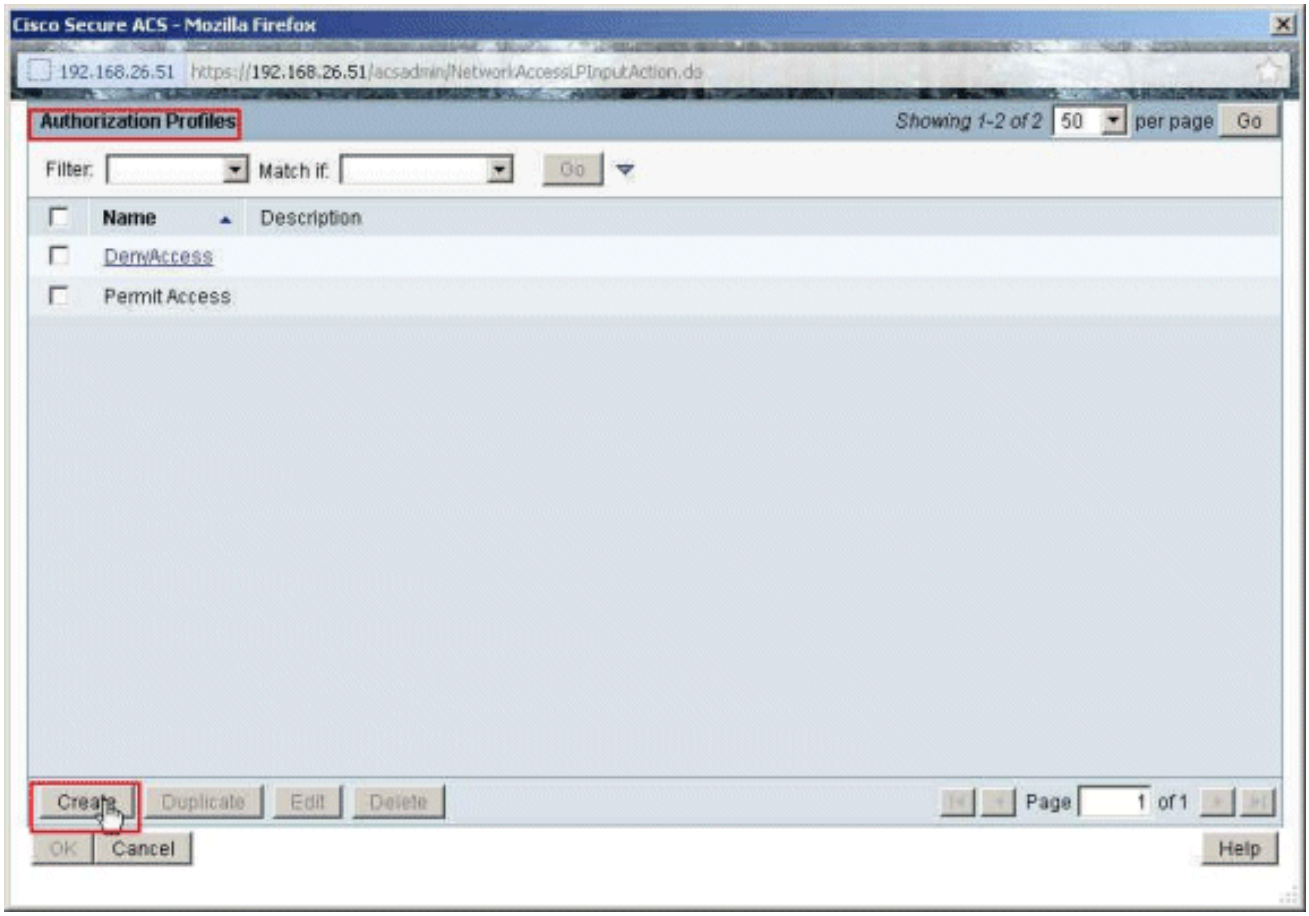
16. Certifique-se de que a caixa de seleção ao lado do **sistema: O username** é selecionado, escolhe **iguais da** lista de drop-down, e incorpora o username **Cisco**.



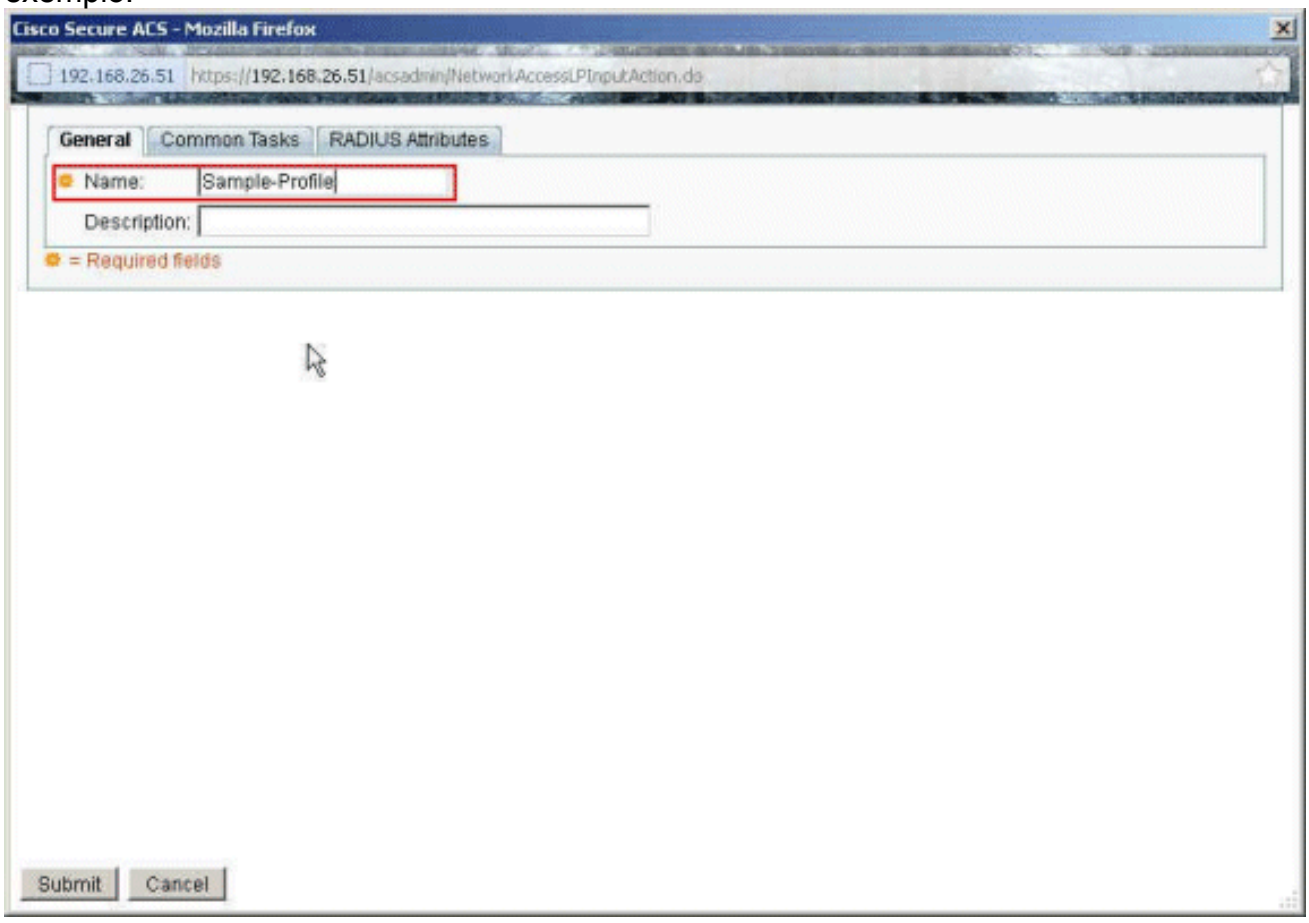
17. Clique **seleto**.



18. O clique **cria** a fim criar um perfil novo da autorização.

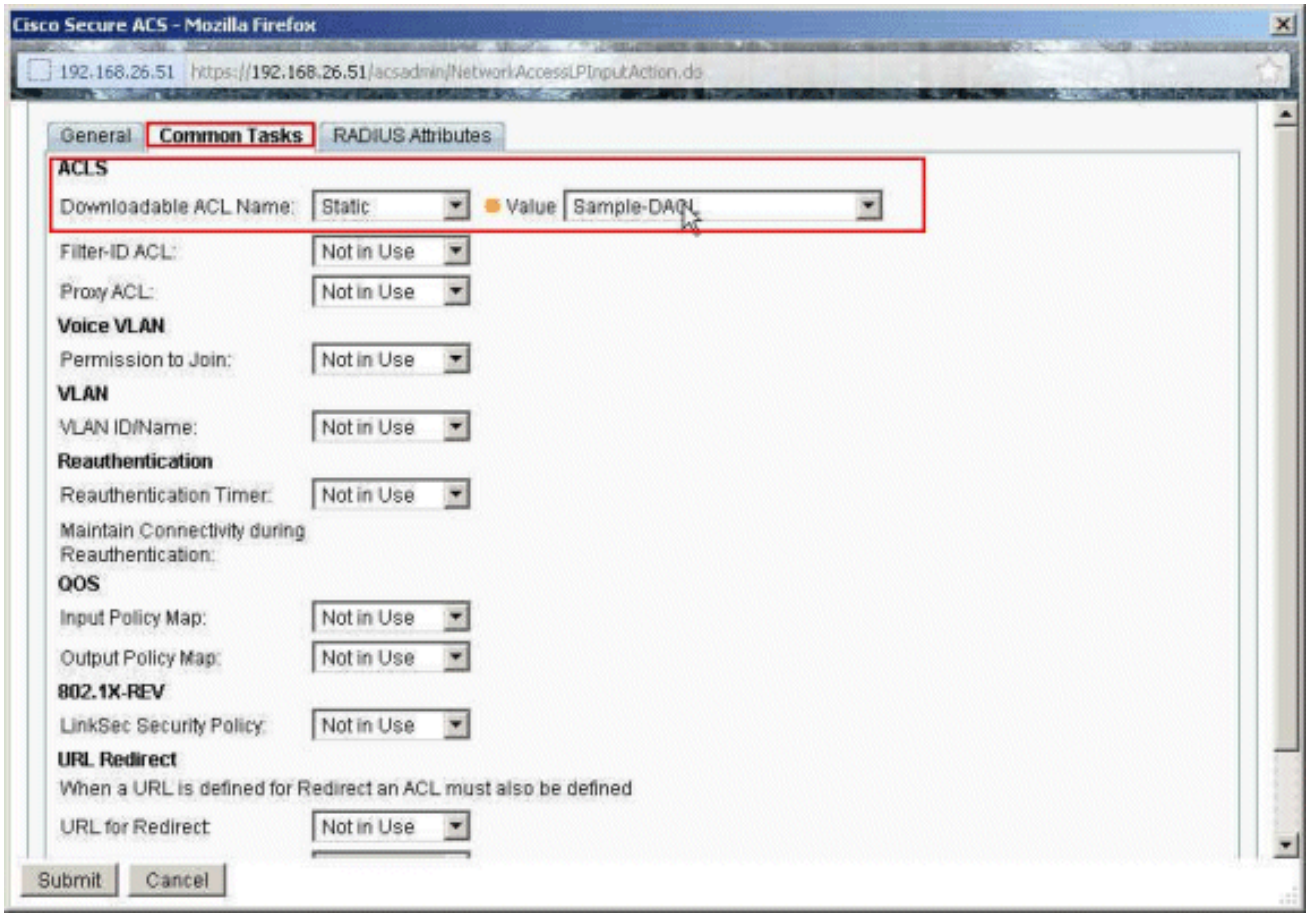


19. Forneça um nome para o **perfil da autorização**. **O exemplo de perfil** é usado neste exemplo.

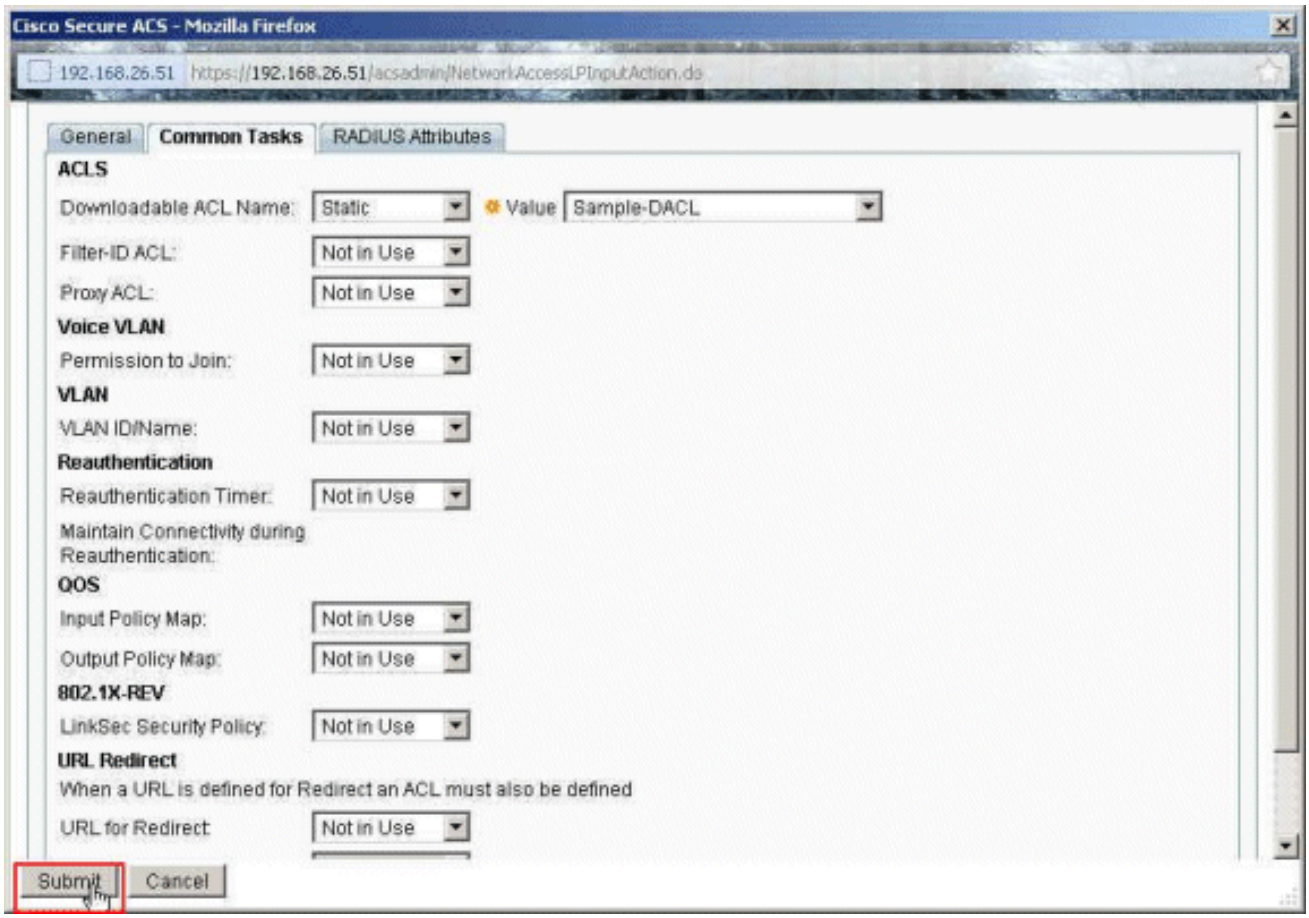


20. Escolha a aba **comum das tarefas**, e selecione a **estática da** lista de drop-down para o **nome ACL baixável**. Escolha o **DACL** recém-criado **(a amostra - DACL) da** lista de drop-down de

valor.

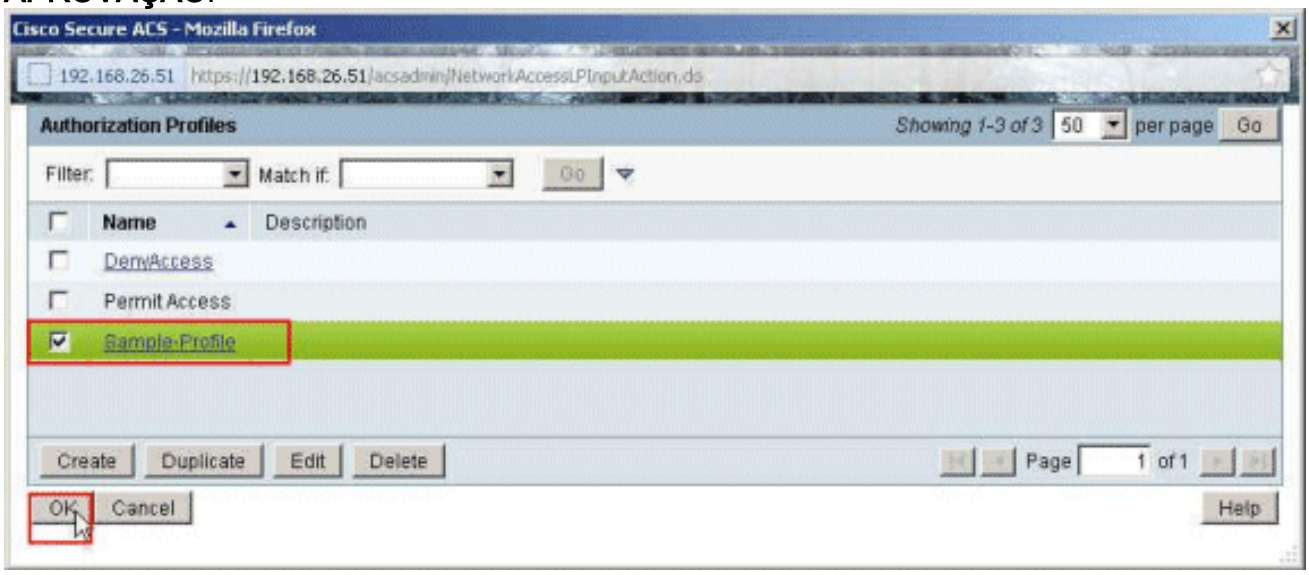


21. Clique em Submit.

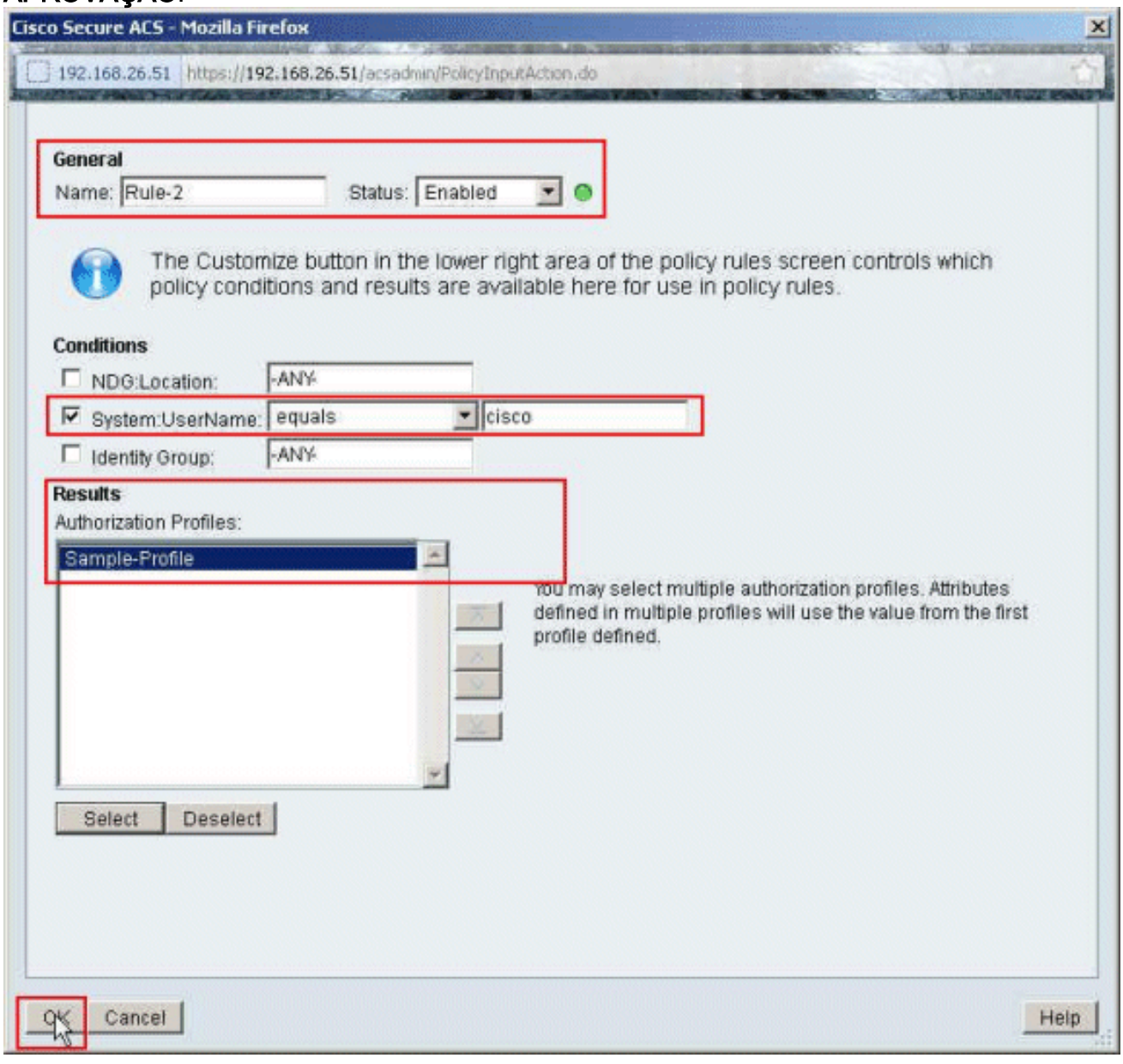


22. Certifique-se de que a caixa de seleção ao lado do **exemplo de perfil** (o perfil recém-criado da autorização) está verificada, e clique-se a

APROVAÇÃO.

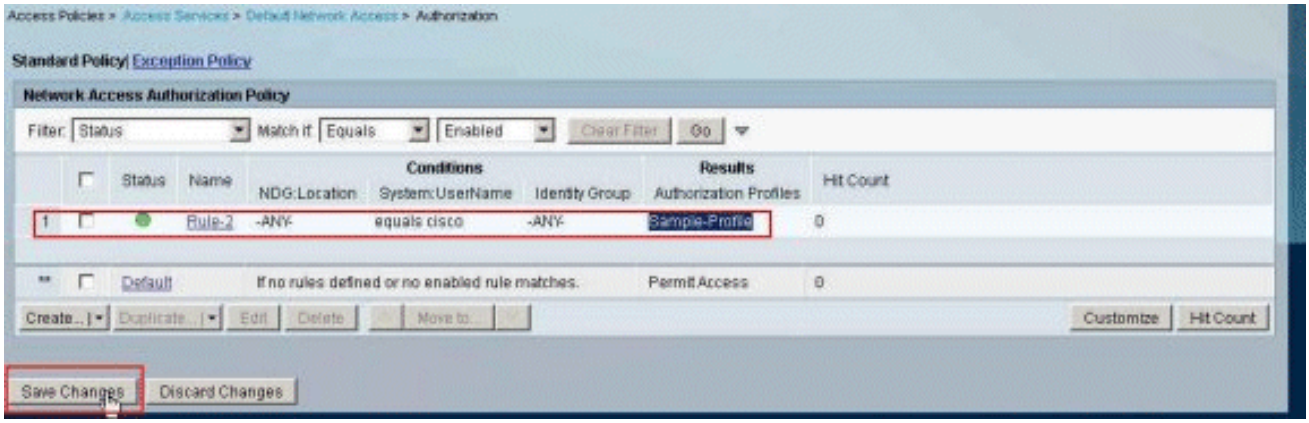


23. Uma vez que você verificou que o **exemplo de perfil** recém-criado está selecionado no campo dos **perfis da autorização**, clique a APROVAÇÃO.



24. Verifique que a regra nova (**Rule-2**) está criada com o sistema: O username **iguala** condições e **exemplo de perfil de Cisco** como o resultado. **Mudanças da salvaguarda do**

clique. A regra 2 é criada com sucesso.



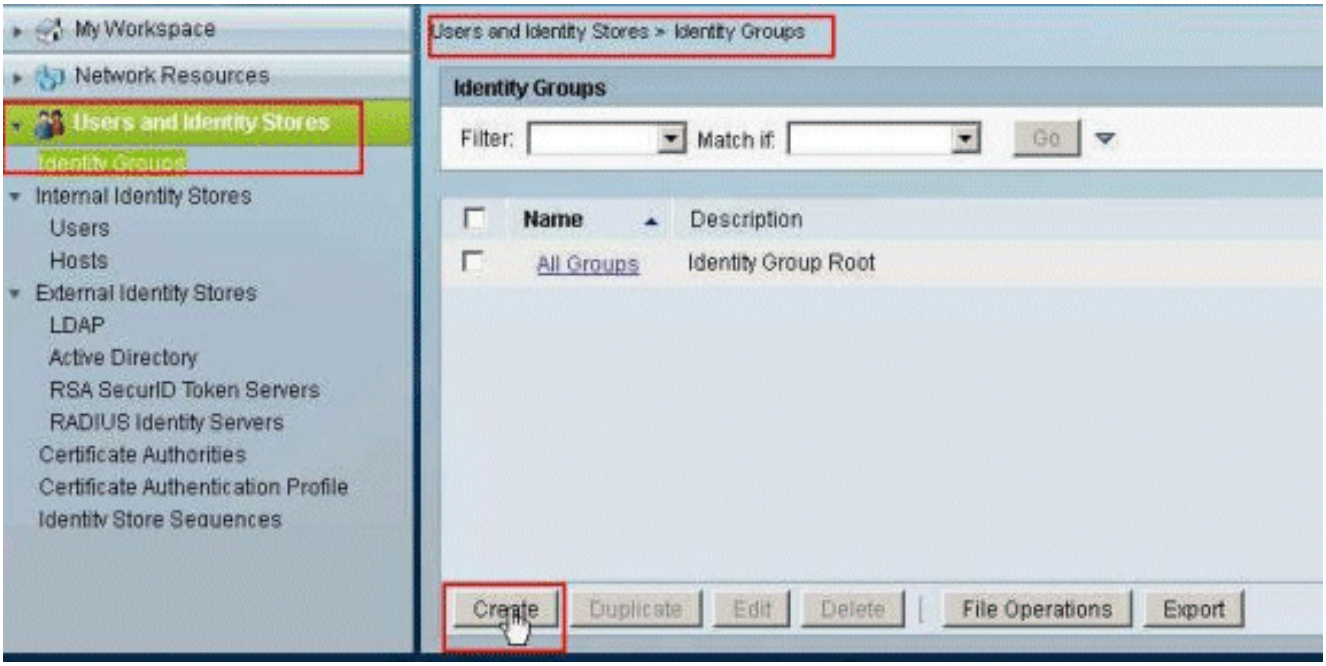
Configurar ACS para ACL baixável para o grupo

Termine etapas 1 a 12 configurar ACS para ACL baixável para o usuário individual e execute estas etapas a fim configurar ACL baixável para o grupo em um Cisco Secure ACS.

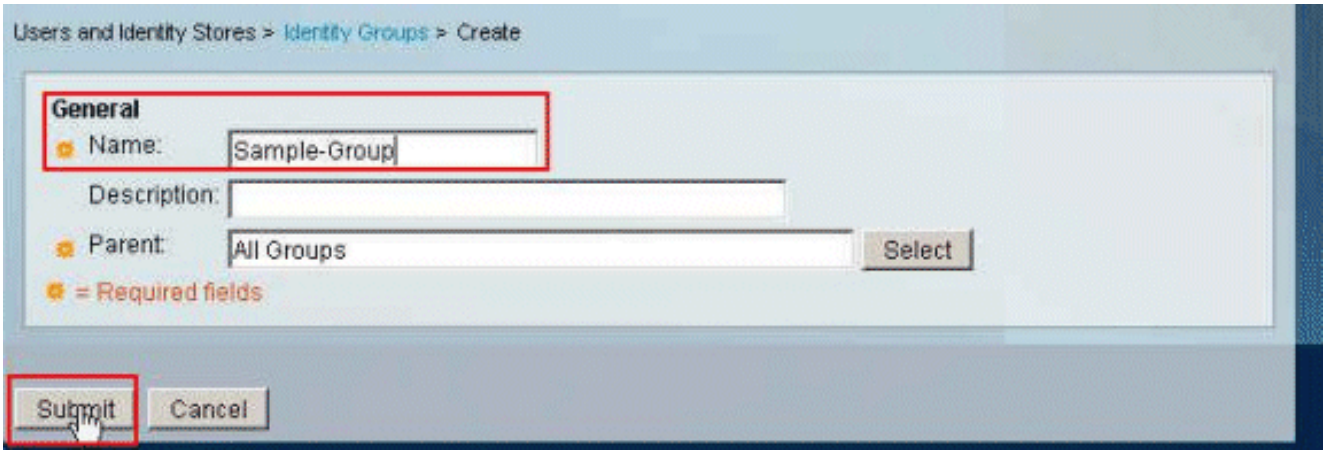
Neste exemplo, o usuário “Cisco” do IPSec VPN pertence ao Amostra-**grupo**.

O usuário **Cisco do Amostra-grupo** autentica com sucesso, e o servidor Radius envia uma lista de acessos carregável à ferramenta de segurança. O usuário “Cisco” pode alcançar somente o server de 10.1.1.2 e nega todo acesso restante. A fim verificar o ACL, refira o ACL baixável para o usuário/seção de grupo.

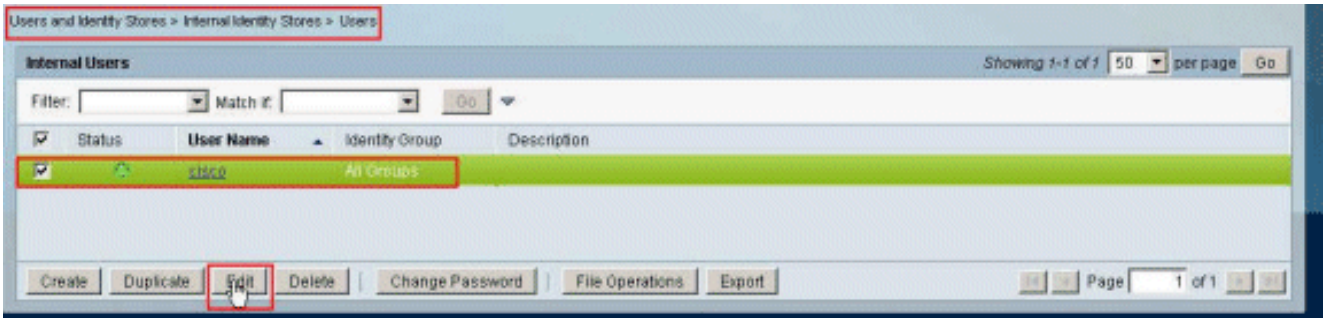
1. Na barra de navegação, clique **usuários e a identidade armazena > grupos da identidade**, e o clique **cria** a fim criar um grupo novo.



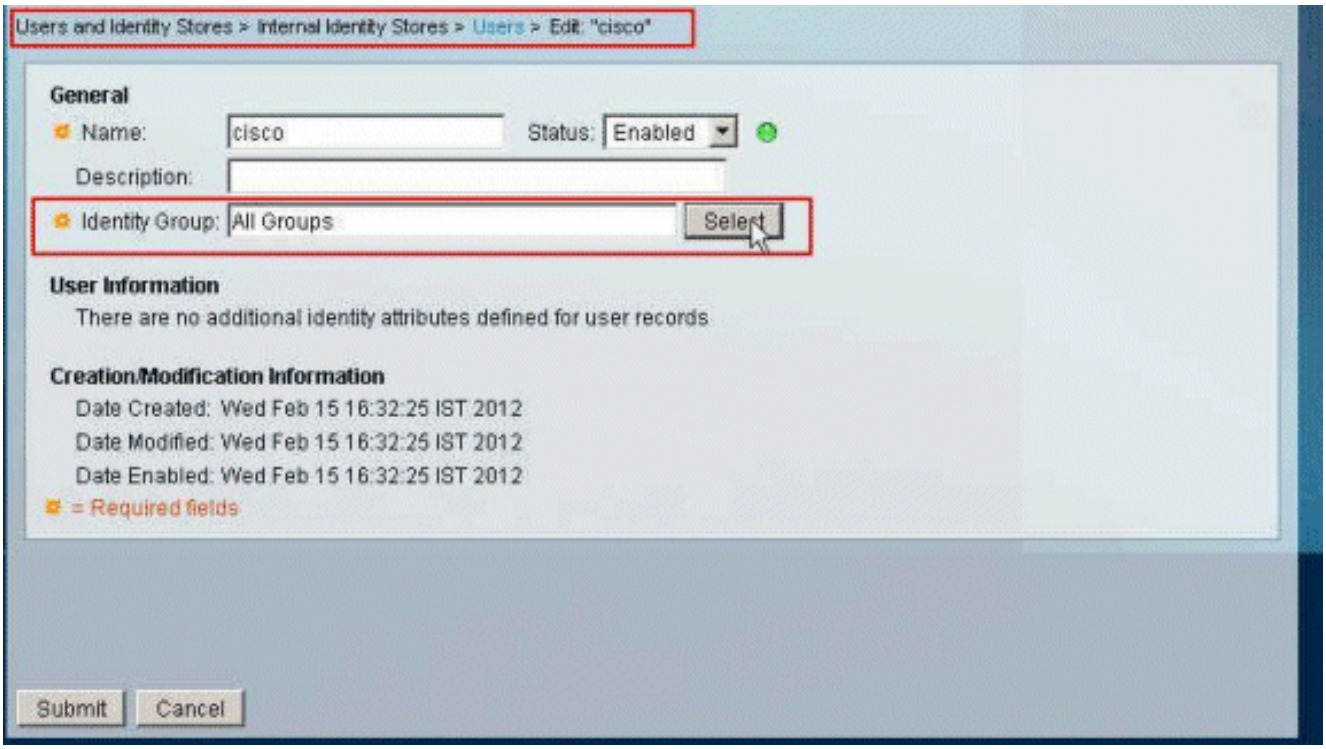
2. Forneça um nome do grupo (Amostra-**grupo**), e o clique **submete-se**.



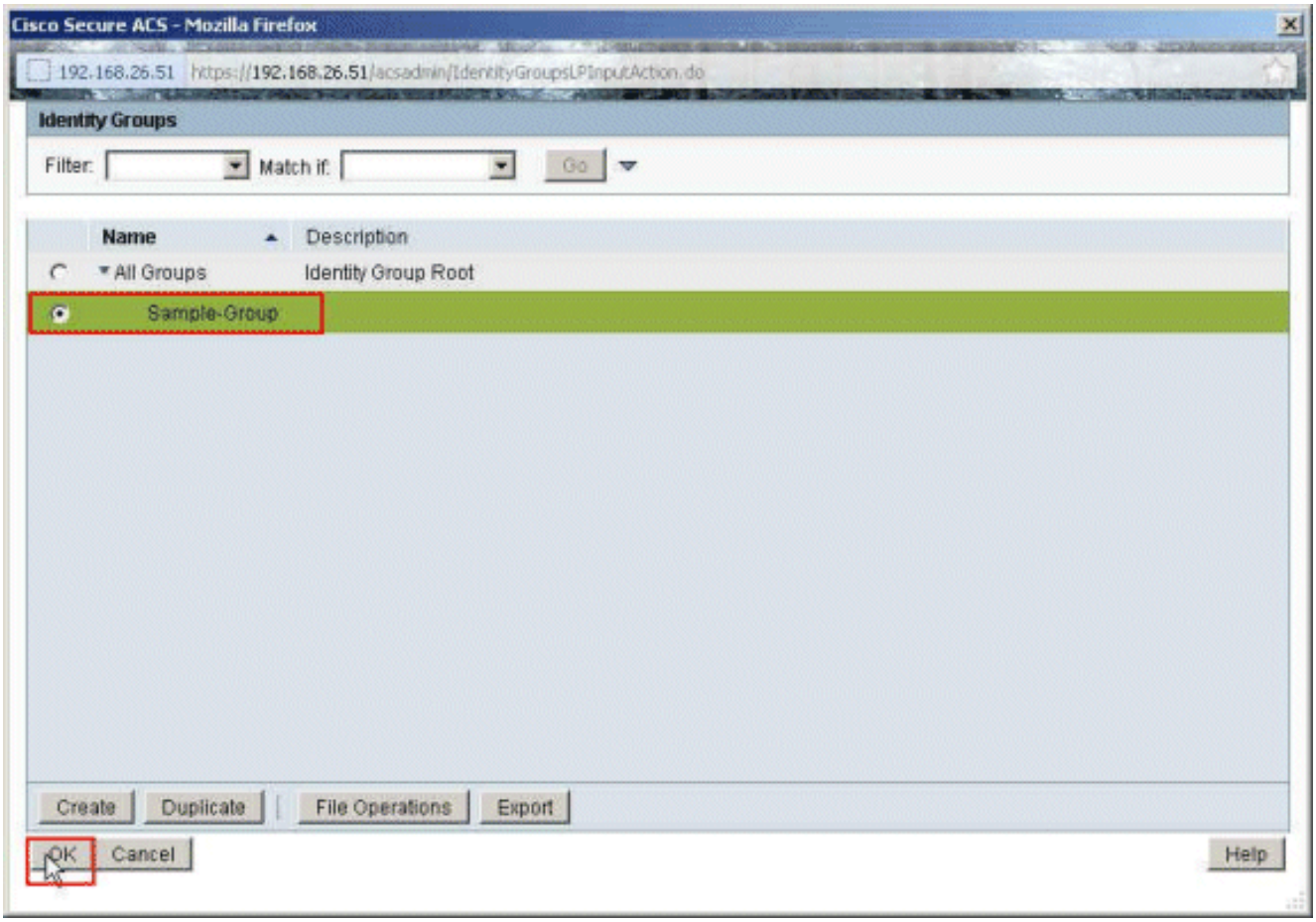
3. Escolha **lojas da identidade do usuário > identidade interna armazena > usuários**, e selecionam o usuário **Cisco**. O clique **edita** a fim mudar a membrasia do clube deste usuário.



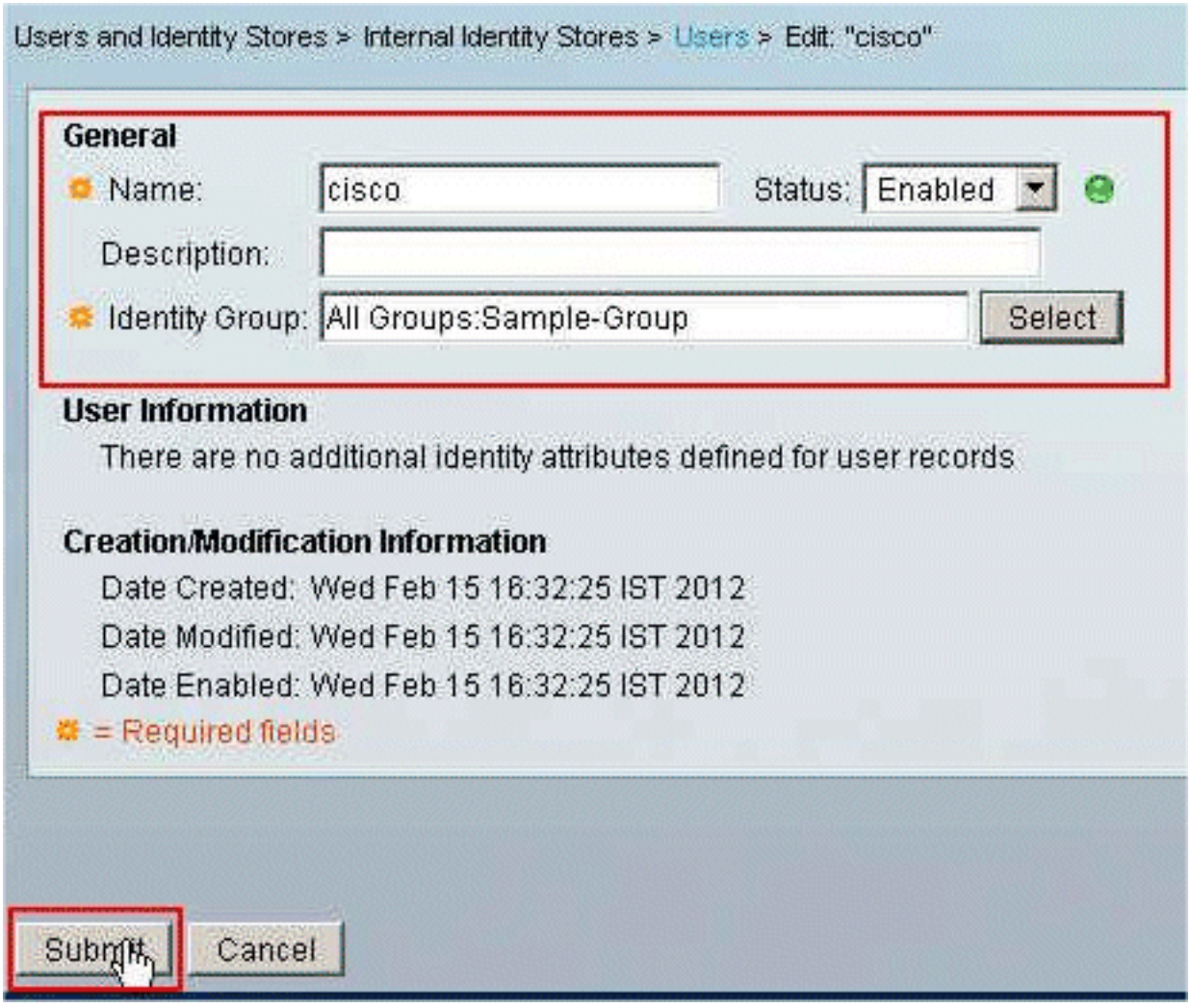
4. Clique **seleto** ao lado do grupo da identidade.



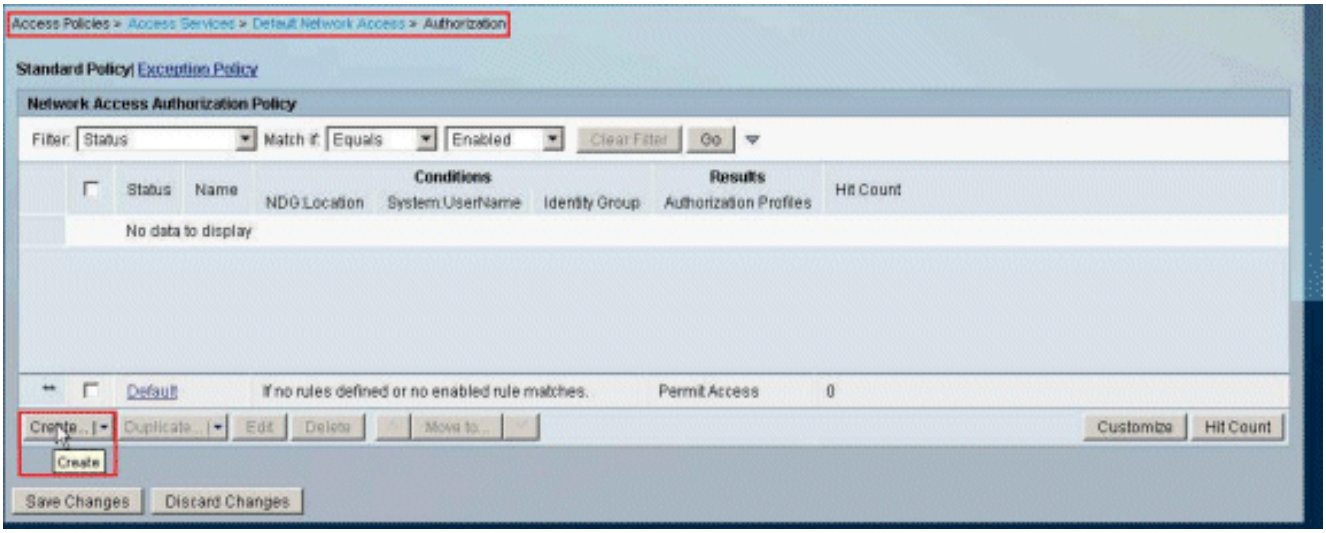
5. Selecione o grupo recém-criado (isto é, Amostra-**grupo**), e clique a **APROVAÇÃO**.



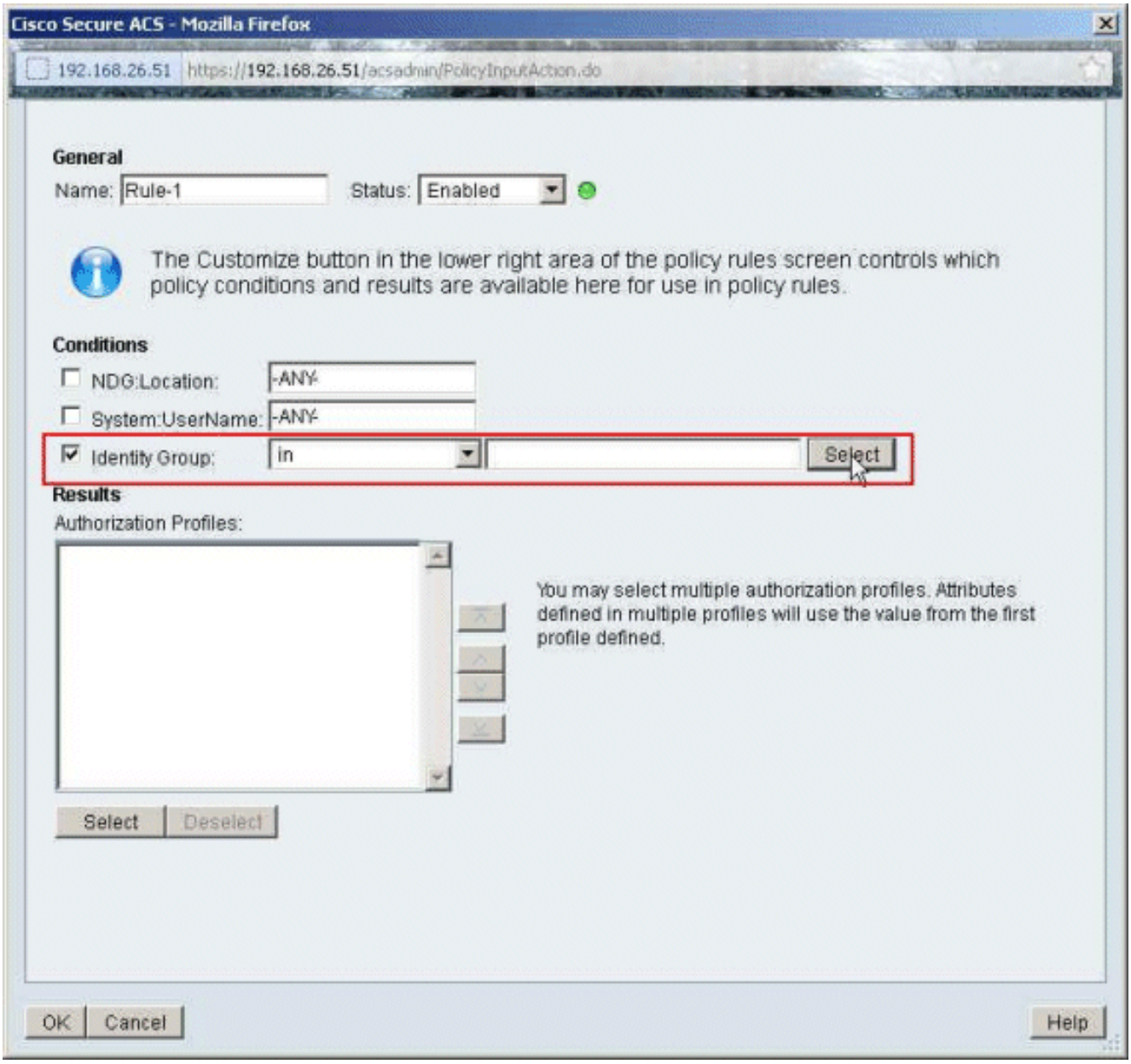
6. Clique em Submit.



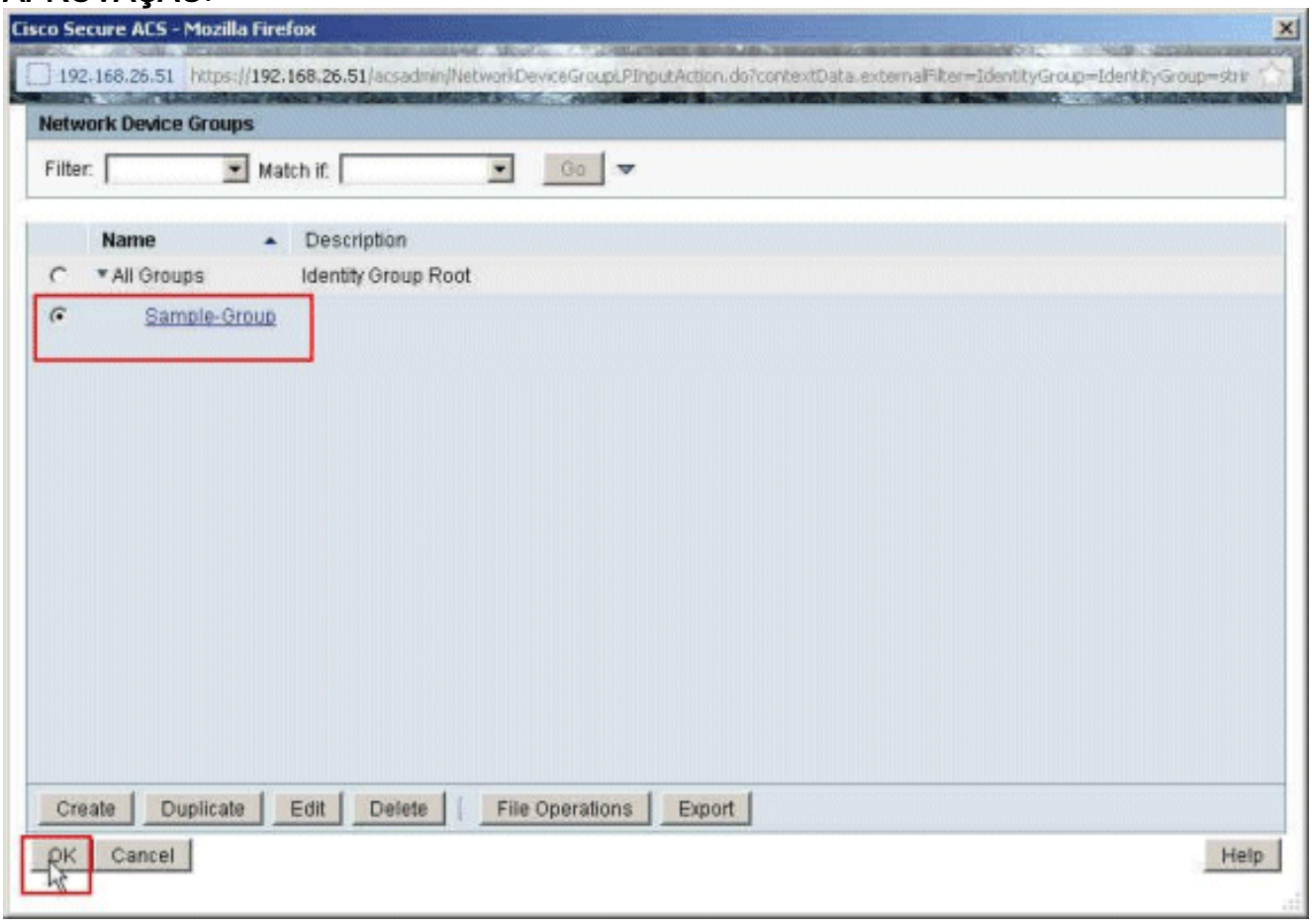
7. Escolha **políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão**, e o clique **cria** a fim criar uma regra nova.



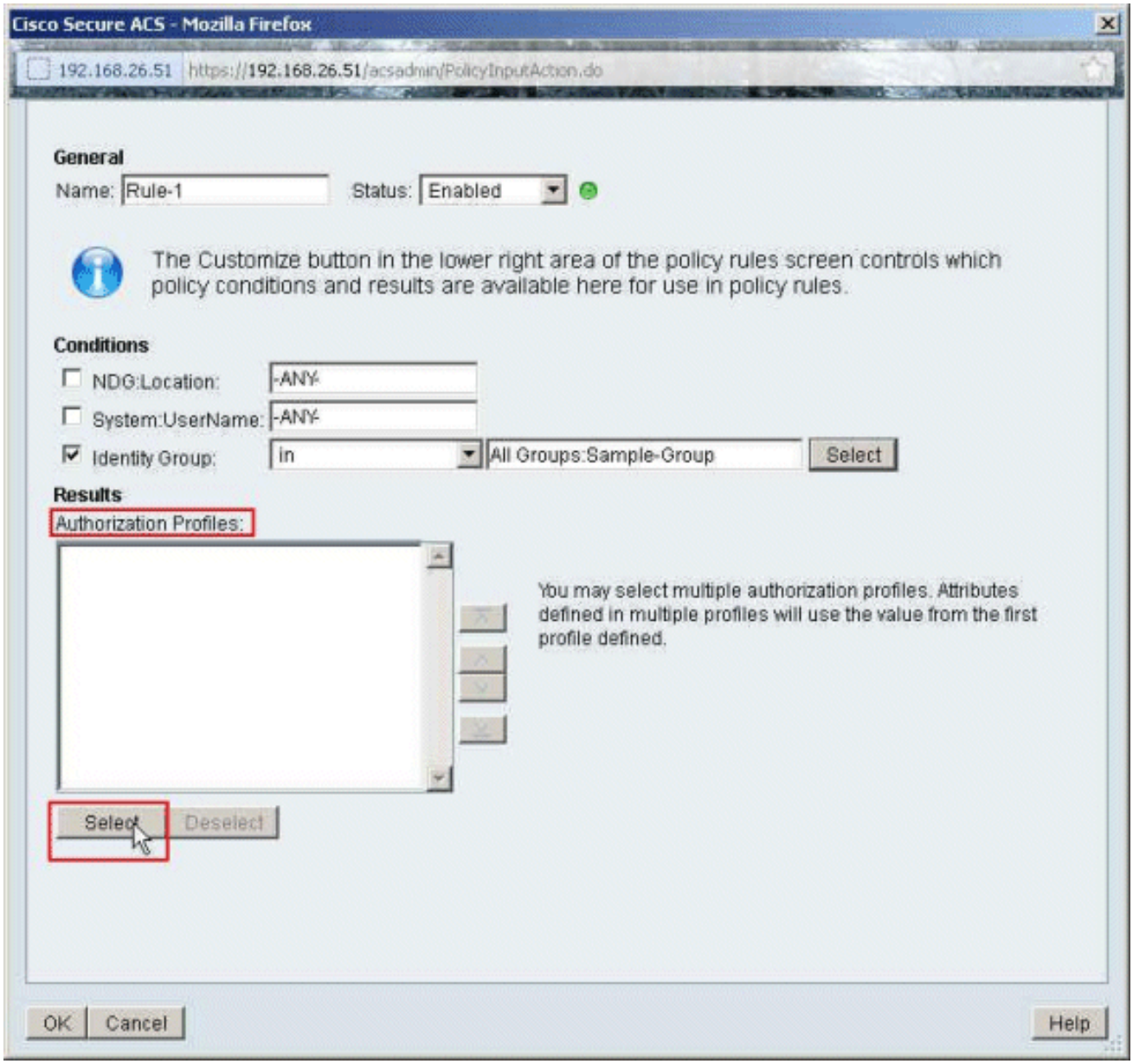
8. Certifique-se de que a caixa de seleção ao lado do **grupo da identidade** está verificada, e clique-se **seleto**.



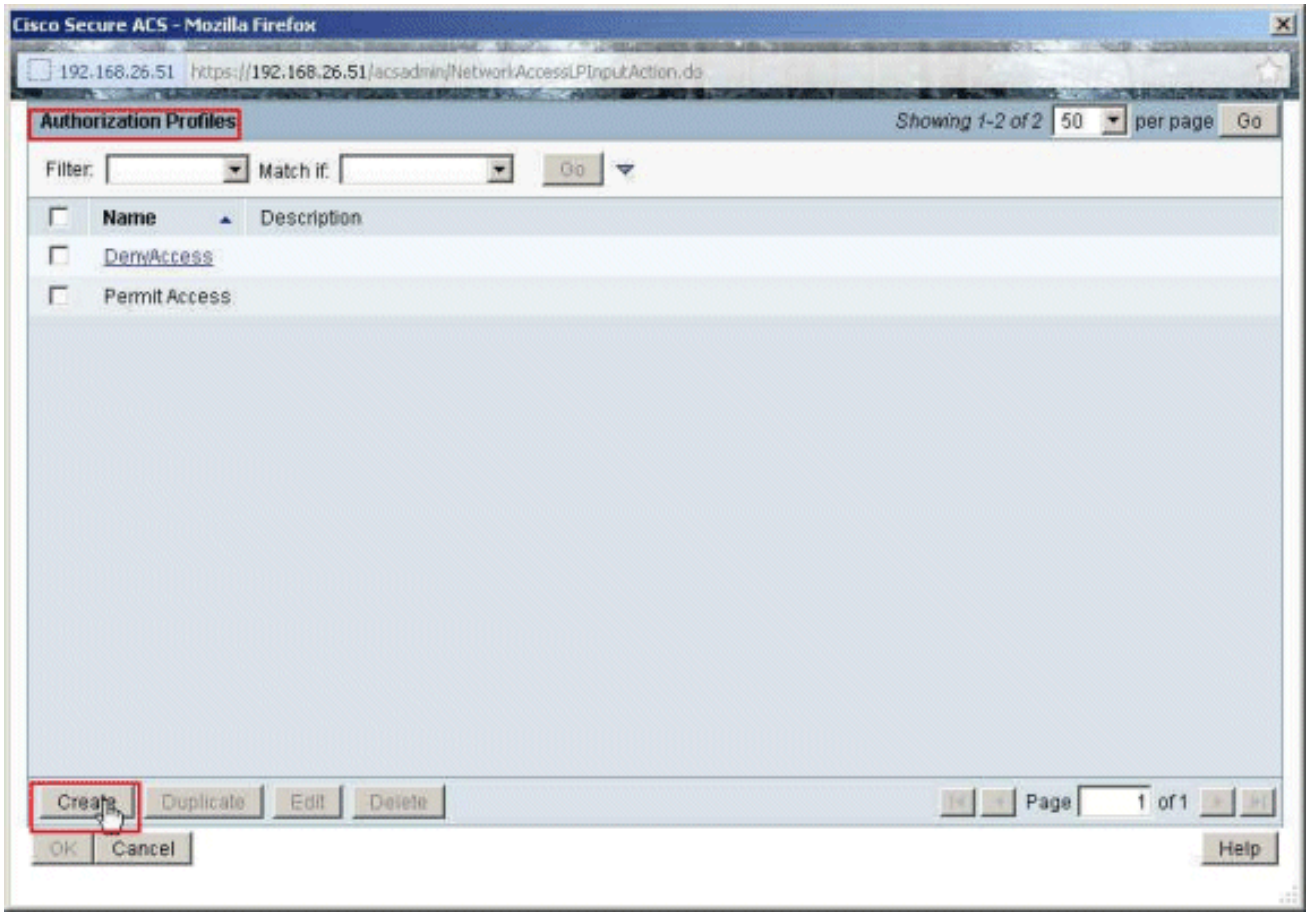
9. Escolha o Amostra-**grupo**, e clique a **APROVAÇÃO**.



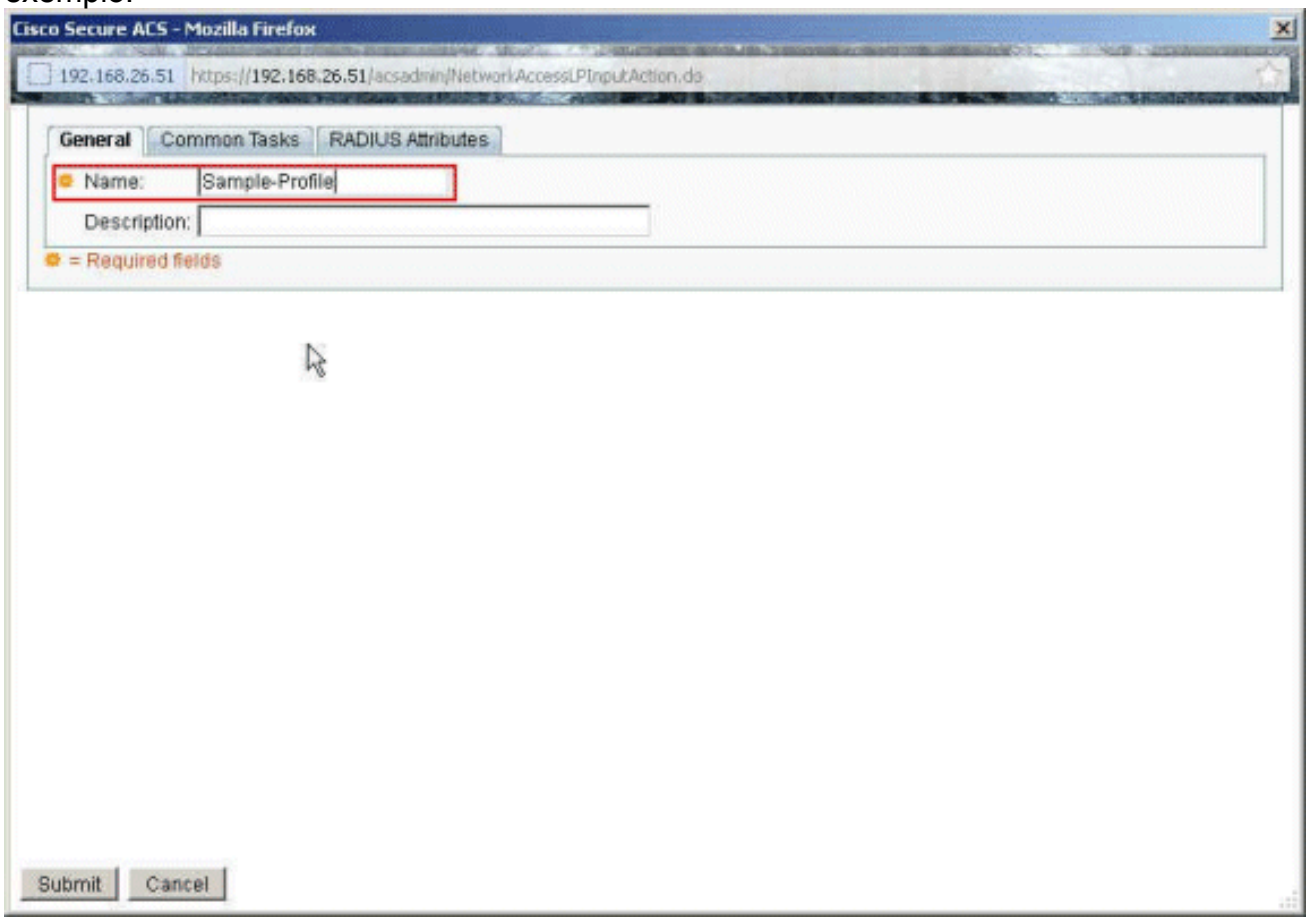
10. Clique **seleto**, na seção dos perfis da autorização.



11. O clique **cria** a fim criar um perfil novo da autorização.

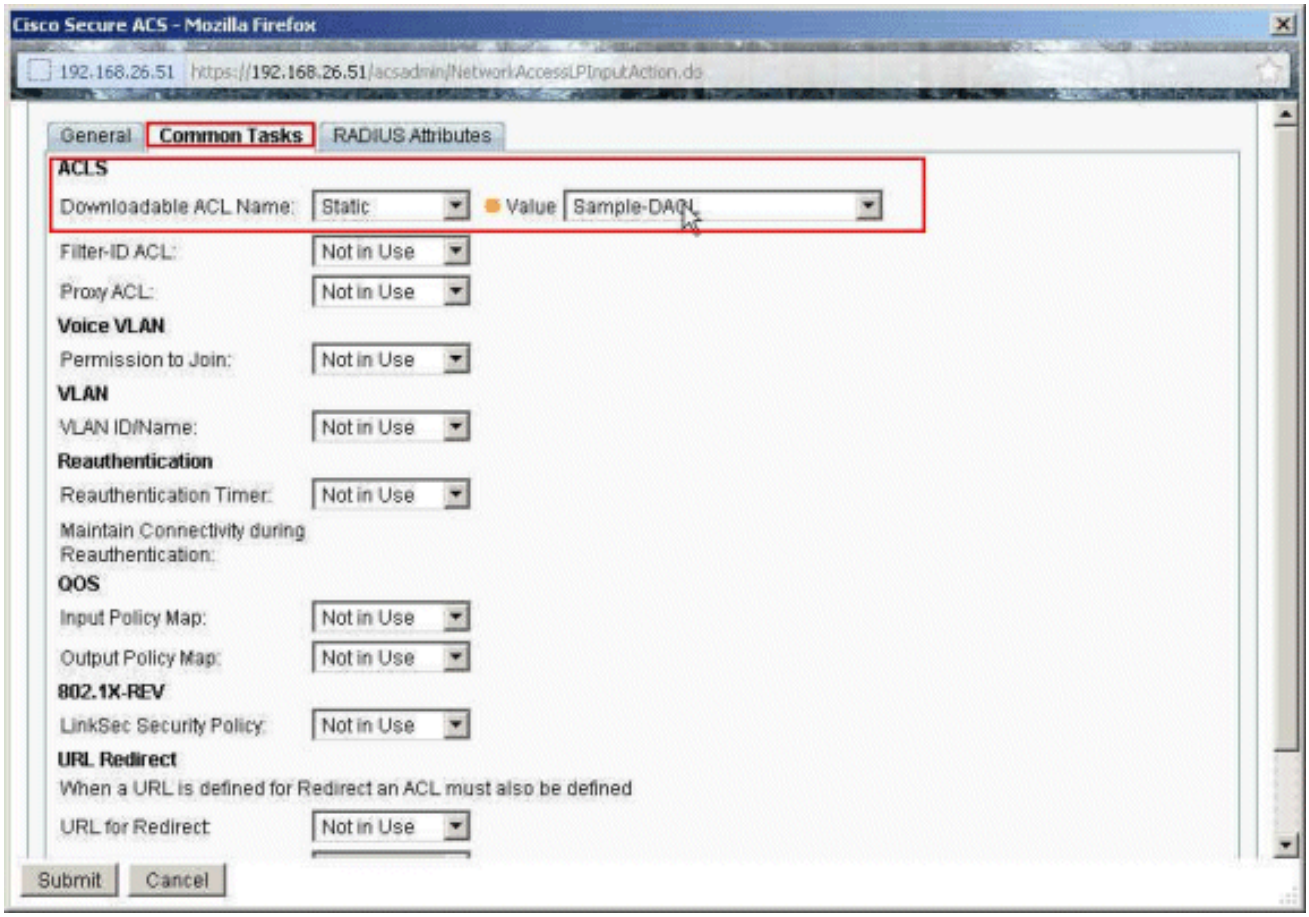


12. Forneça um nome para o **perfil da autorização**. **O exemplo de perfil** é o nome usado neste exemplo.

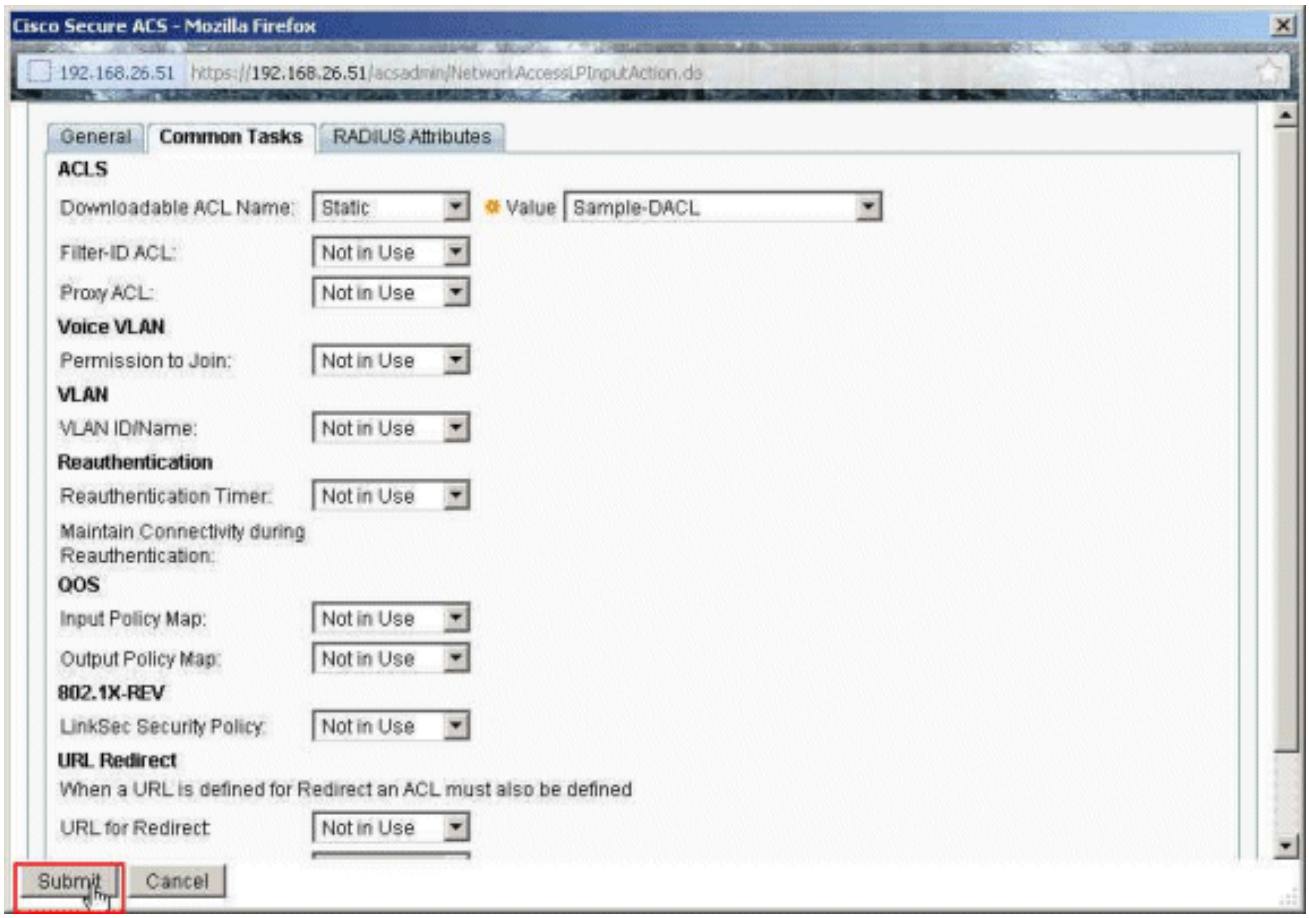


13. Escolha a aba **comum das tarefas**, e selecione a **estática da** lista de drop-down para o **nome ACL baixável**. Escolha o **DACL** recém-criado **(a amostra - DACL) da** lista de drop-down de

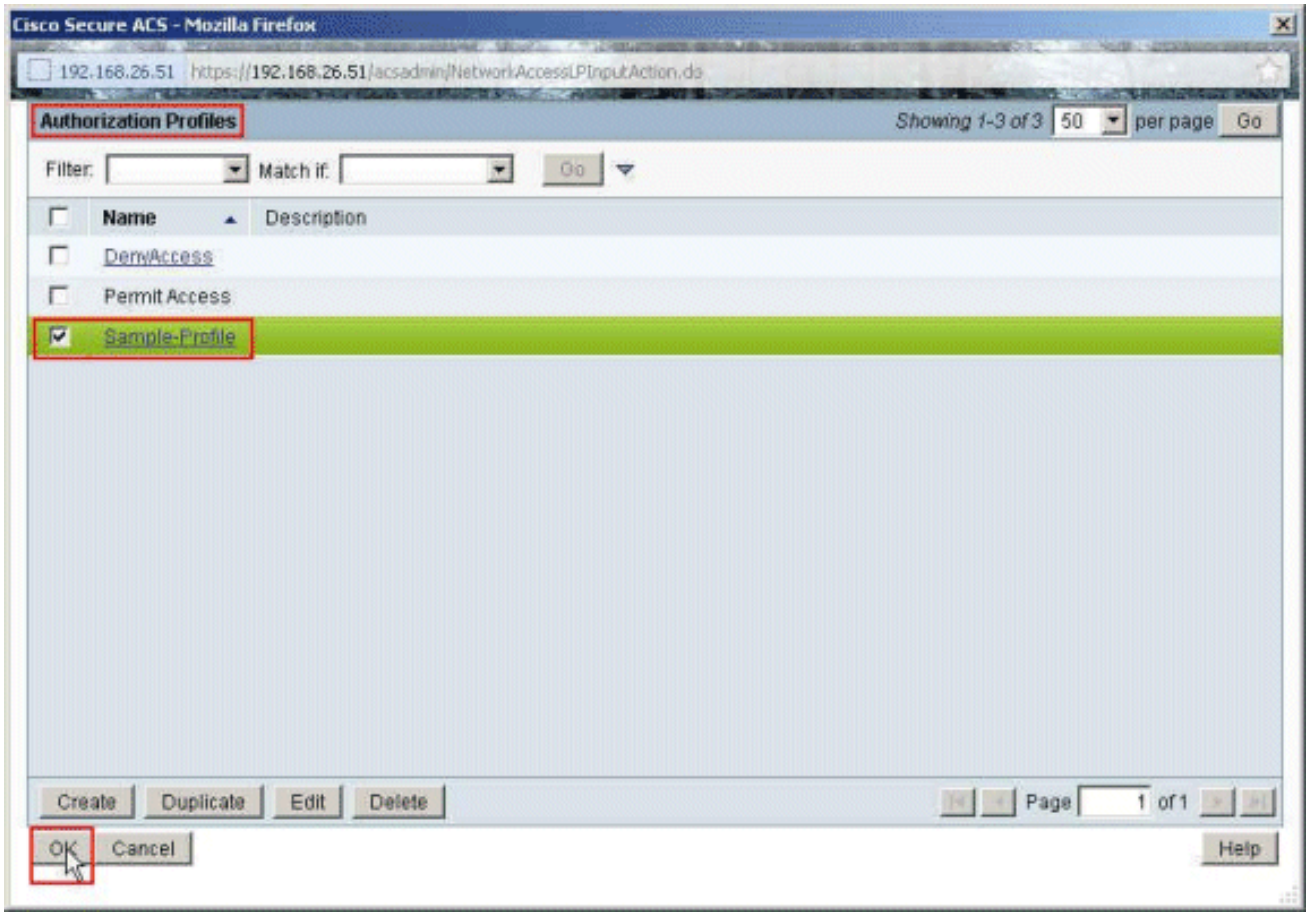
valor.



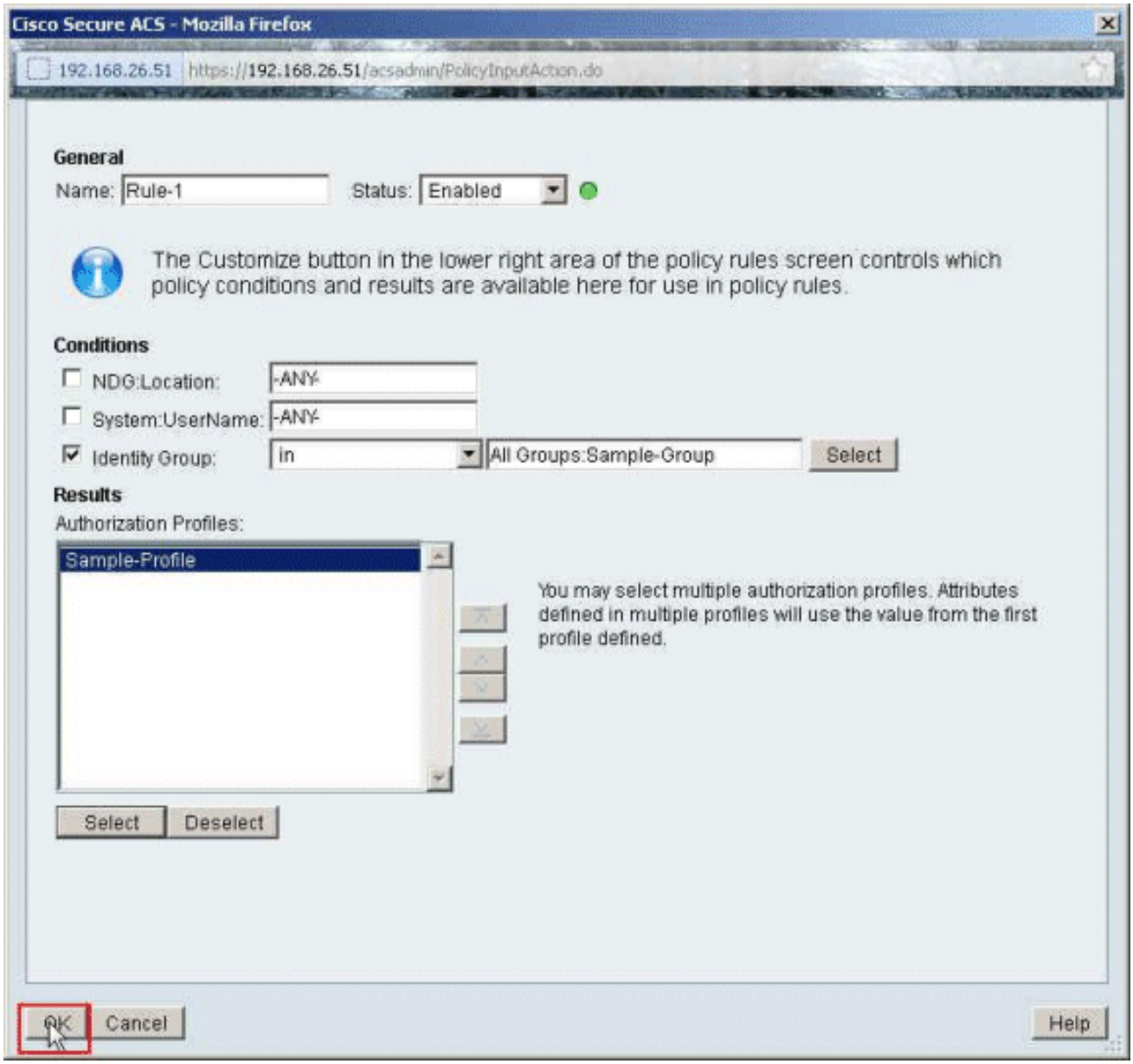
14. Clique em Submit.



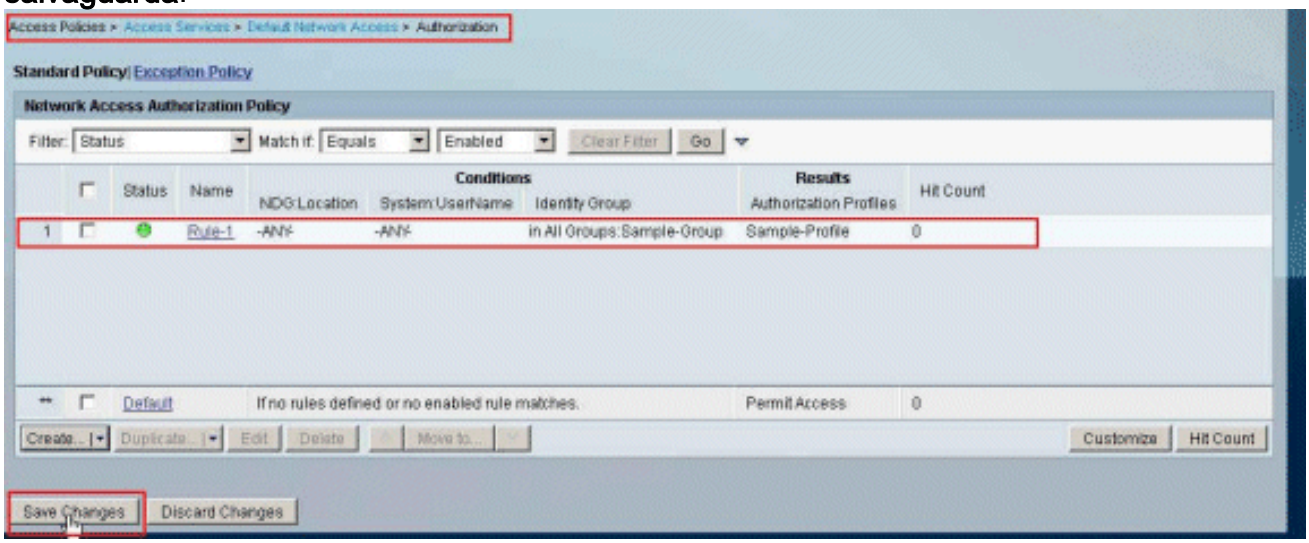
15. Escolha o **exemplo de perfil do** perfil da autorização criado mais cedo, e clique a **APROVAÇÃO**.



16. Clique em **OK**.



17. Verifique que **Rule-1** está criado com o Amostra-**grupo do** grupo da identidade como a circunstância e o **exemplo de perfil** como o resultado. Clique **mudanças da salvaguarda**.



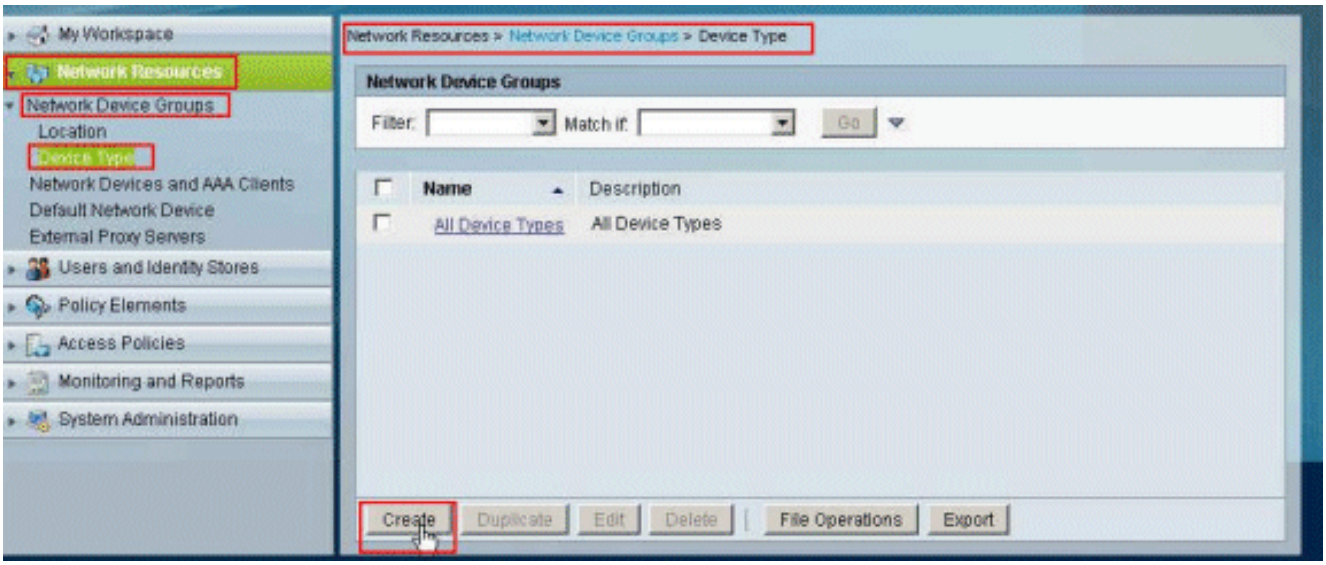
Configurar ACS para ACL baixável para um grupo de dispositivo de rede

Termine etapas 1 a 12 configurar ACS para ACL baixável para o usuário individual e execute

estas etapas a fim configurar ACL baixável para um grupo de dispositivo de rede em um Cisco Secure ACS.

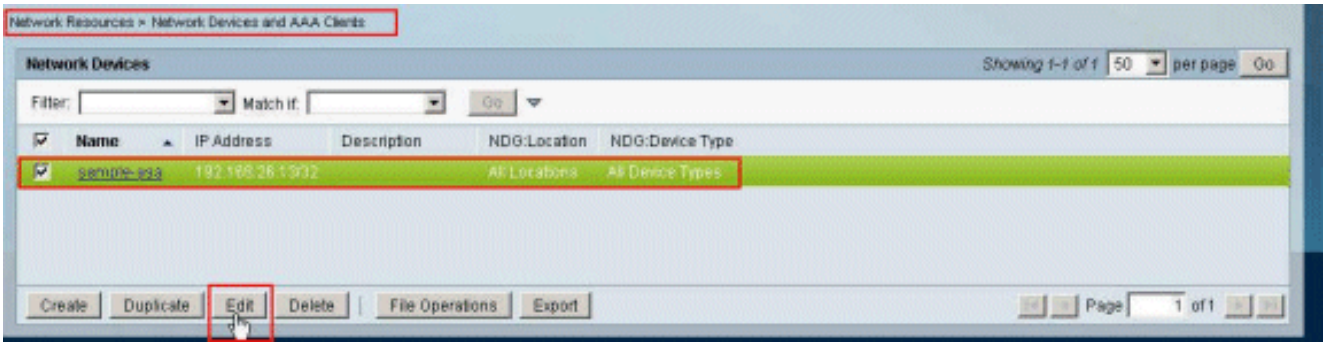
Neste exemplo, o cliente RADIUS (ASA) pertence ao grupo de dispositivo de rede o pedido de autenticação VPN-Gateways.The VPN que que vem do ASA para o usuário “Cisco” autentica com sucesso, e o servidor Radius envia uma lista de acessos carregável à ferramenta de segurança. O usuário “Cisco” pode alcançar somente o server de 10.1.1.2 e nega todo acesso restante. A fim verificar o ACL, refira o ACL baixável para o usuário/seção de grupo.

1. Escolha **recursos de rede > grupos de dispositivo de rede > tipo de dispositivo**, e o clique **cria** a fim criar um grupo de dispositivo de rede novo.

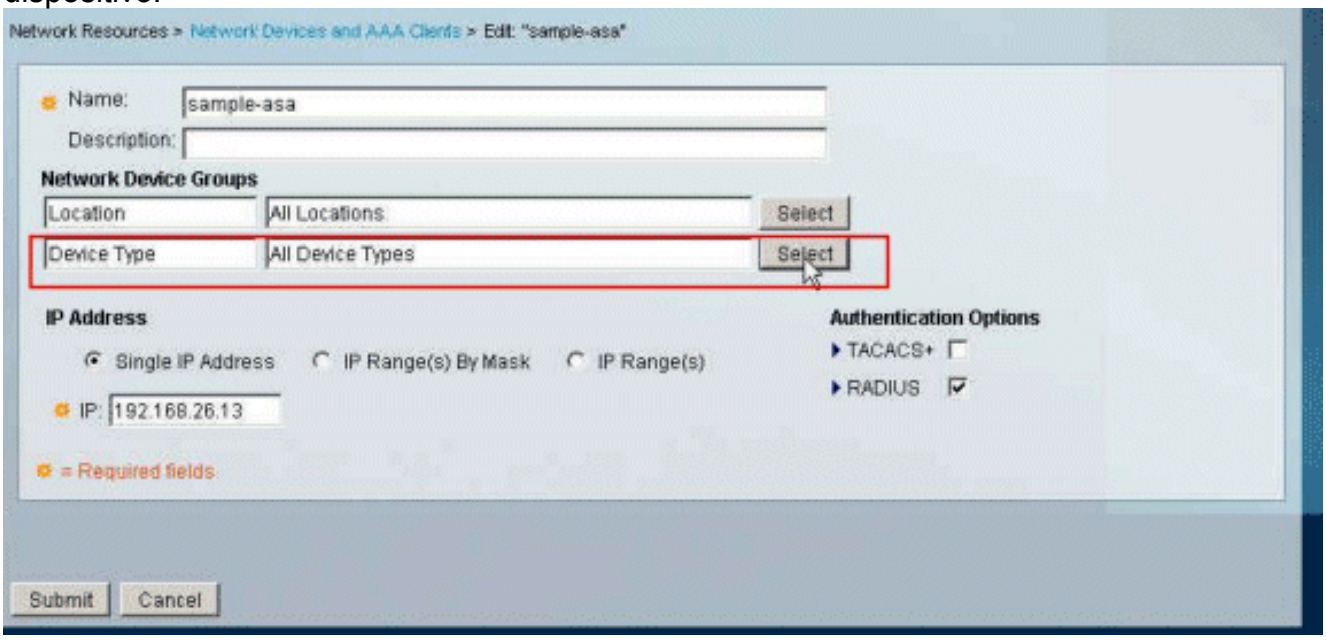


2. Forneça um nome de **grupo de dispositivo de rede** (**gateways de VPN** neste exemplo), e o clique **submete-se**.

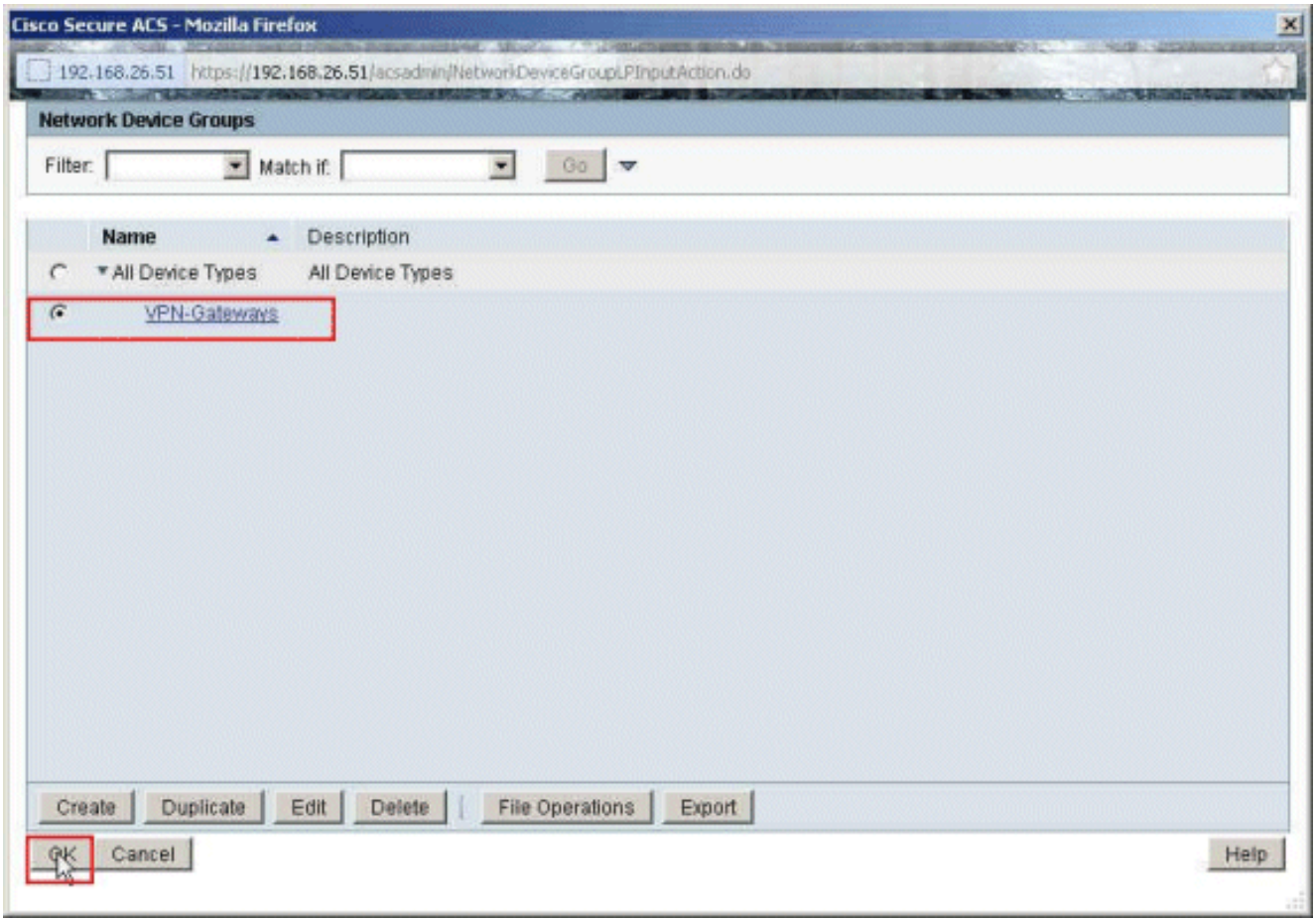
3. Escolha **recursos de rede > dispositivos de rede e clientes de AAA**, e selecione o **cliente RADIUS amostra-ASA** criado mais cedo. O clique **edita** a fim mudar a sociedade de **grupo de dispositivo de rede** deste cliente RADIUS (asa).



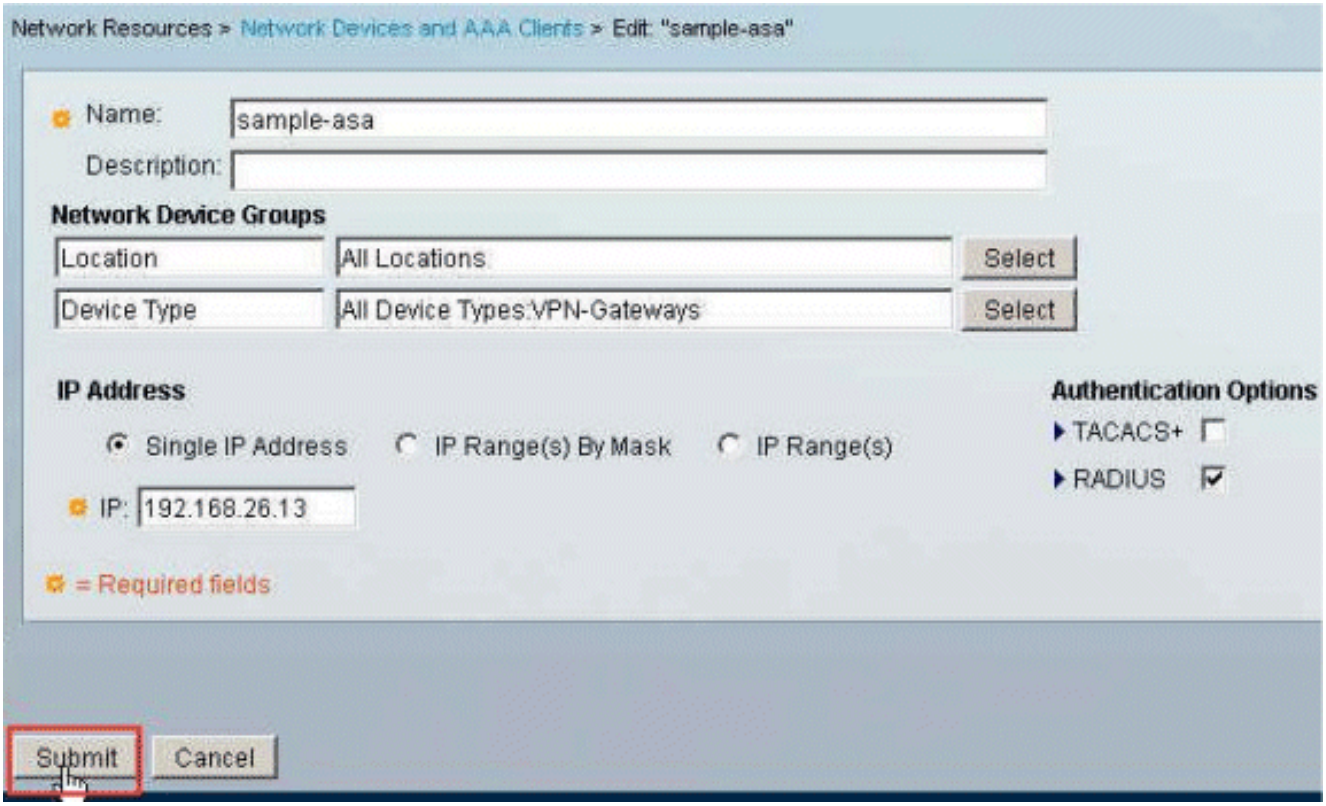
4. Clique **seleto** ao lado do tipo de dispositivo.



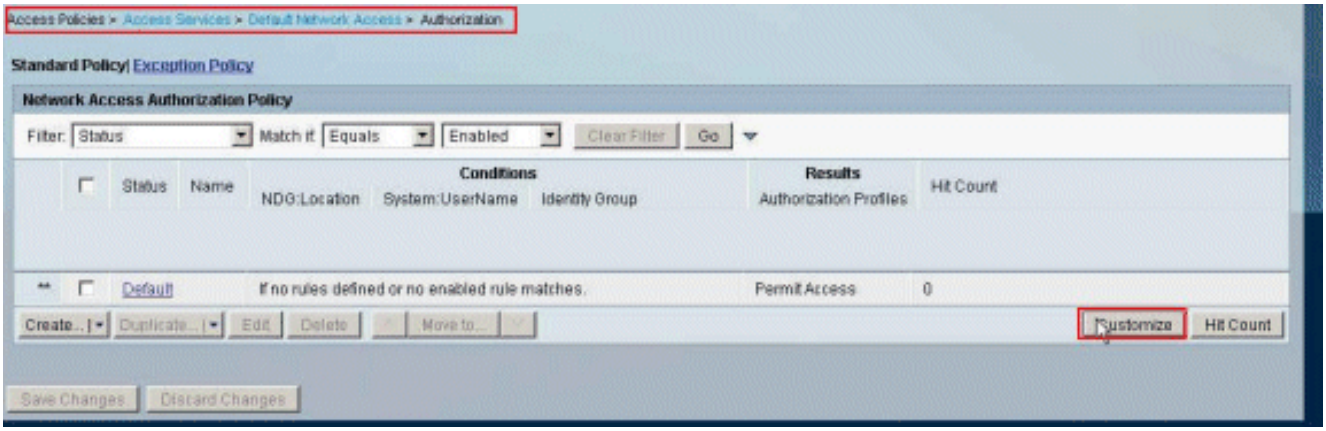
5. Selecione o grupo de dispositivo de rede recém-criado (que é **gateways de VPN**), e clique a **APROVAÇÃO**.



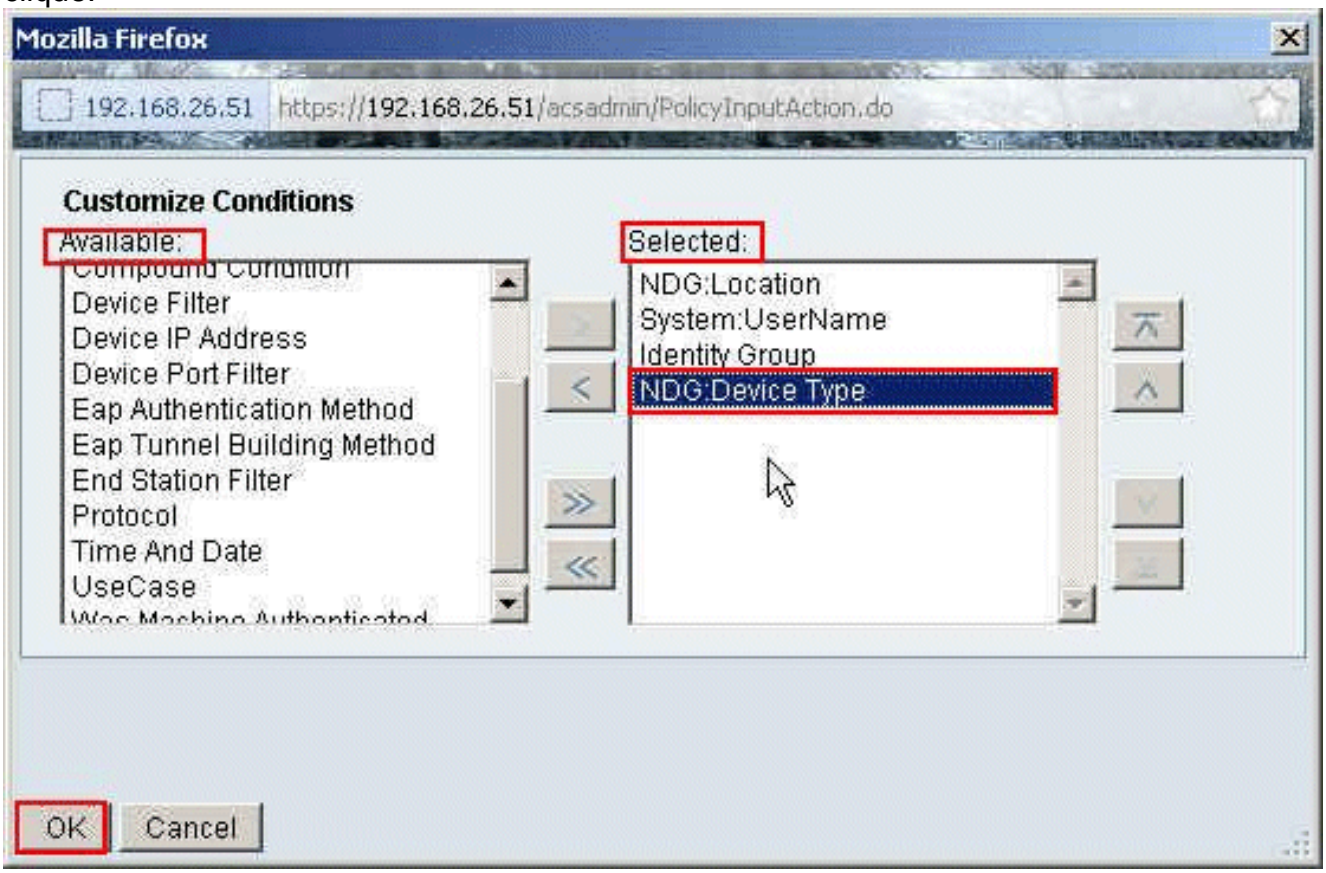
6. Clique em Submit.



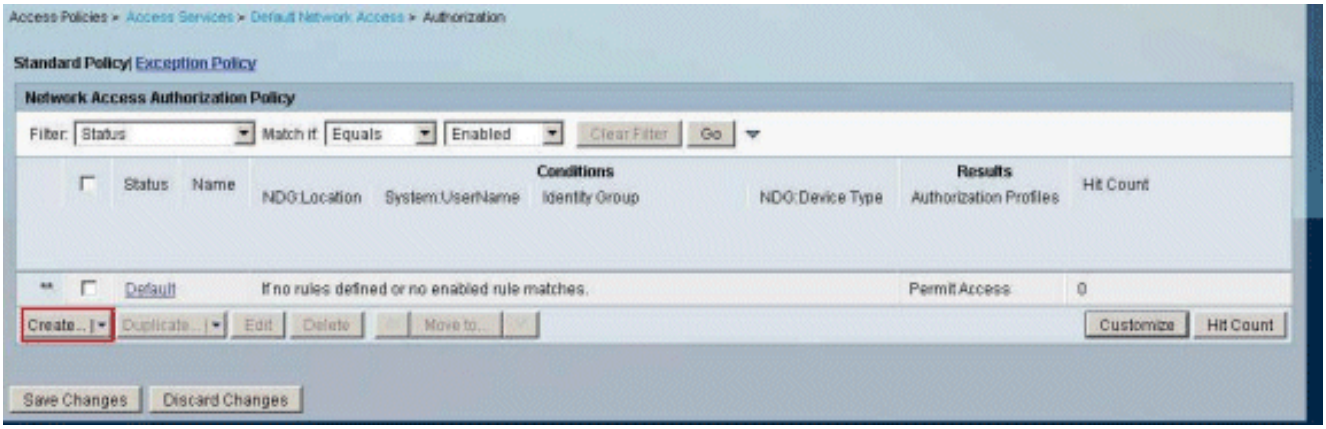
7. Escolha **políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão**, e o clique **personaliza**.



8. Movimento **NDG: Tipo de dispositivo da** seção **disponível à seção selecionada**, e **APROVAÇÃO do**
clique.

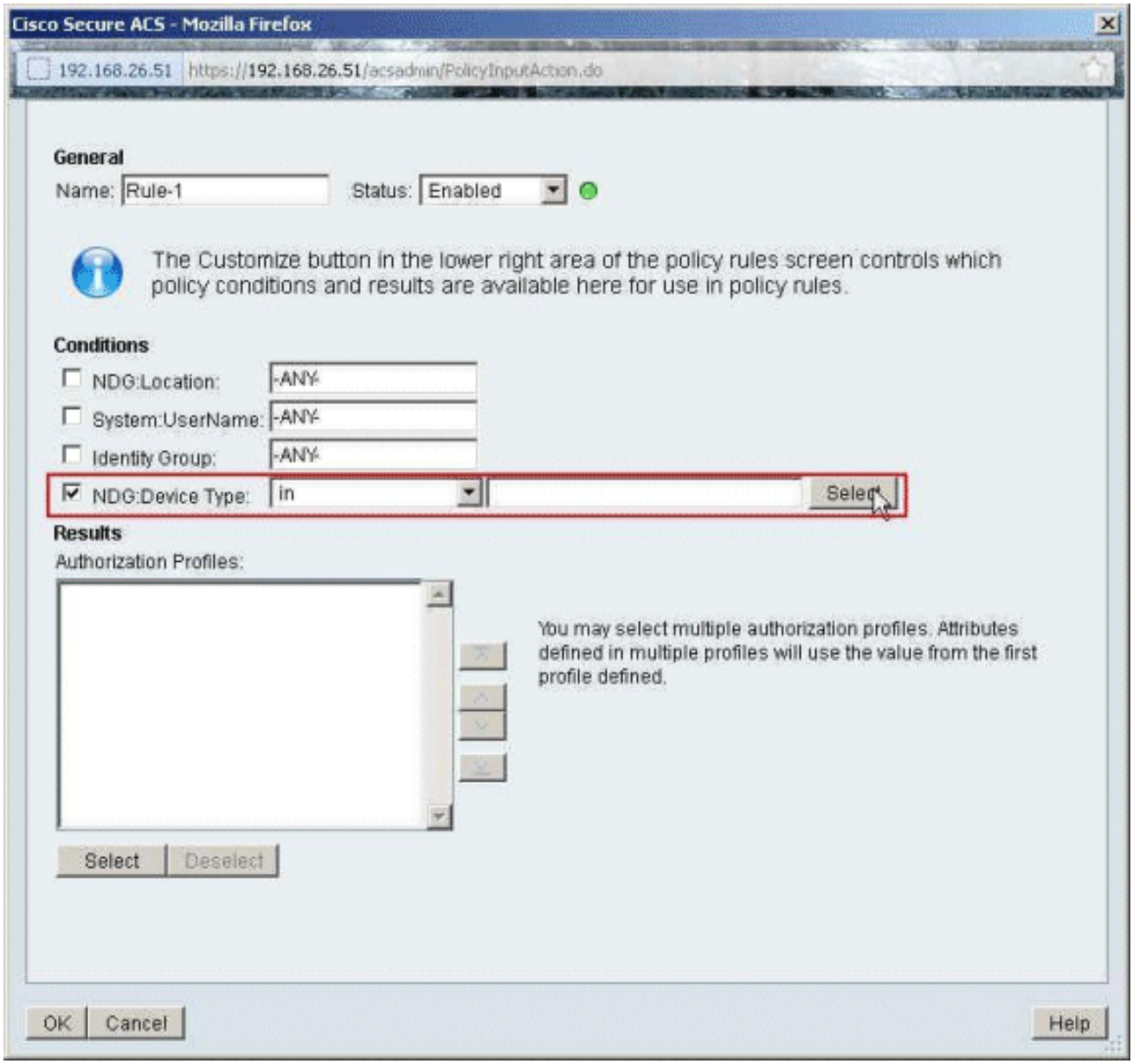


9. O clique **cria** a fim criar uma regra
nova.

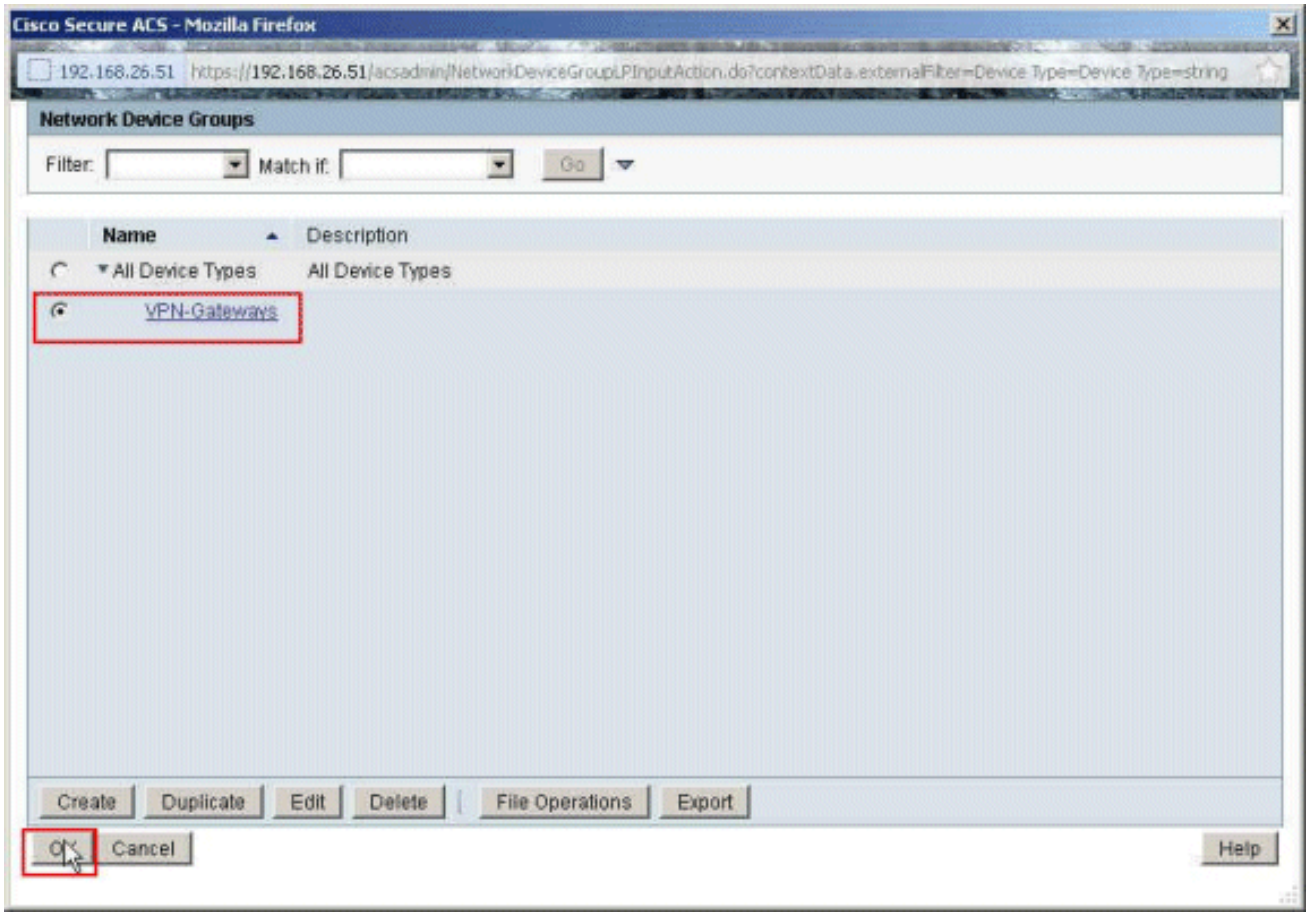


10. Certifique-se de que a caixa de seleção ao lado de **NDG: O tipo de dispositivo** é selecionado e escolhe **dentro da** lista de drop-down. Clique

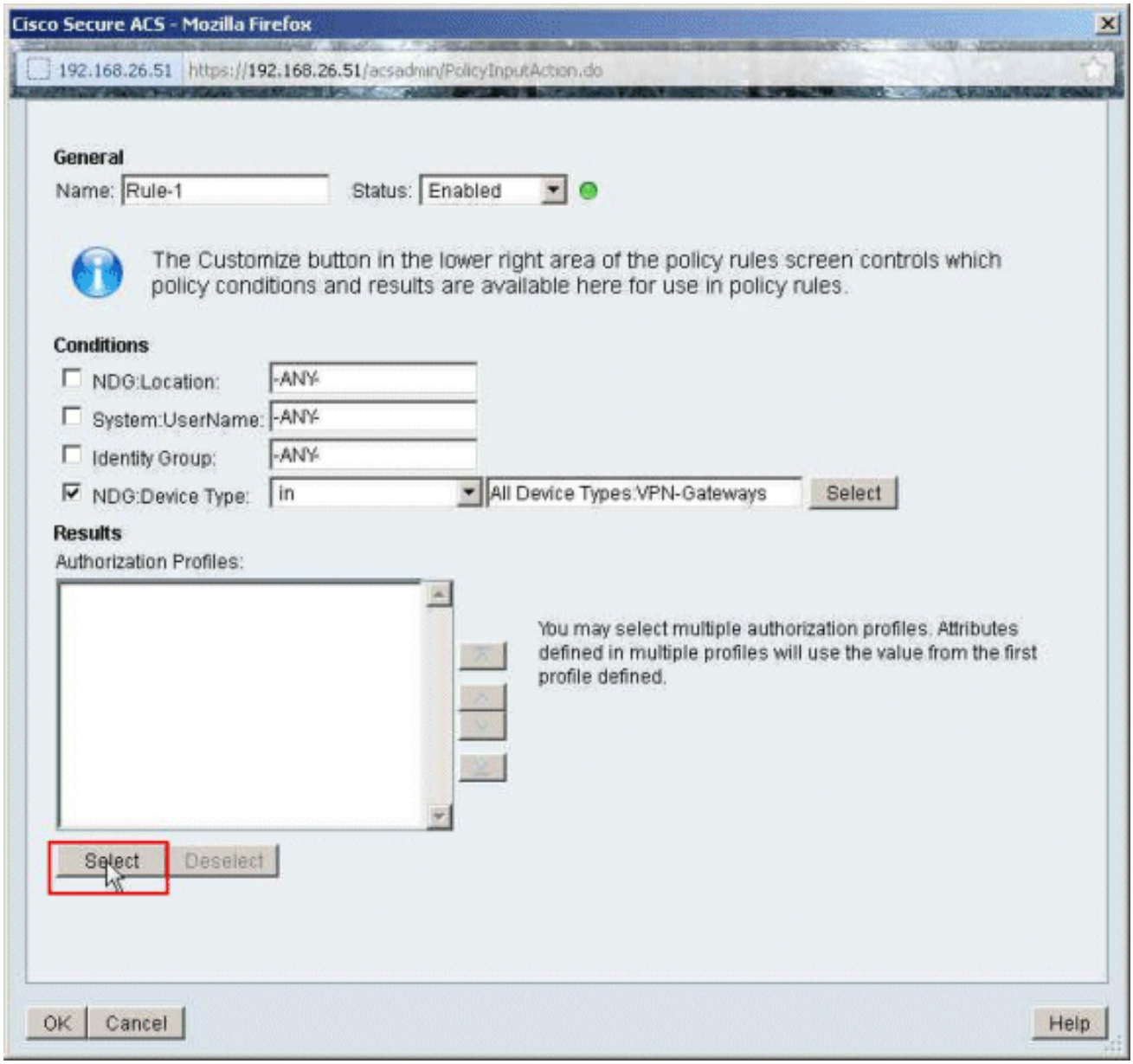
seleto.



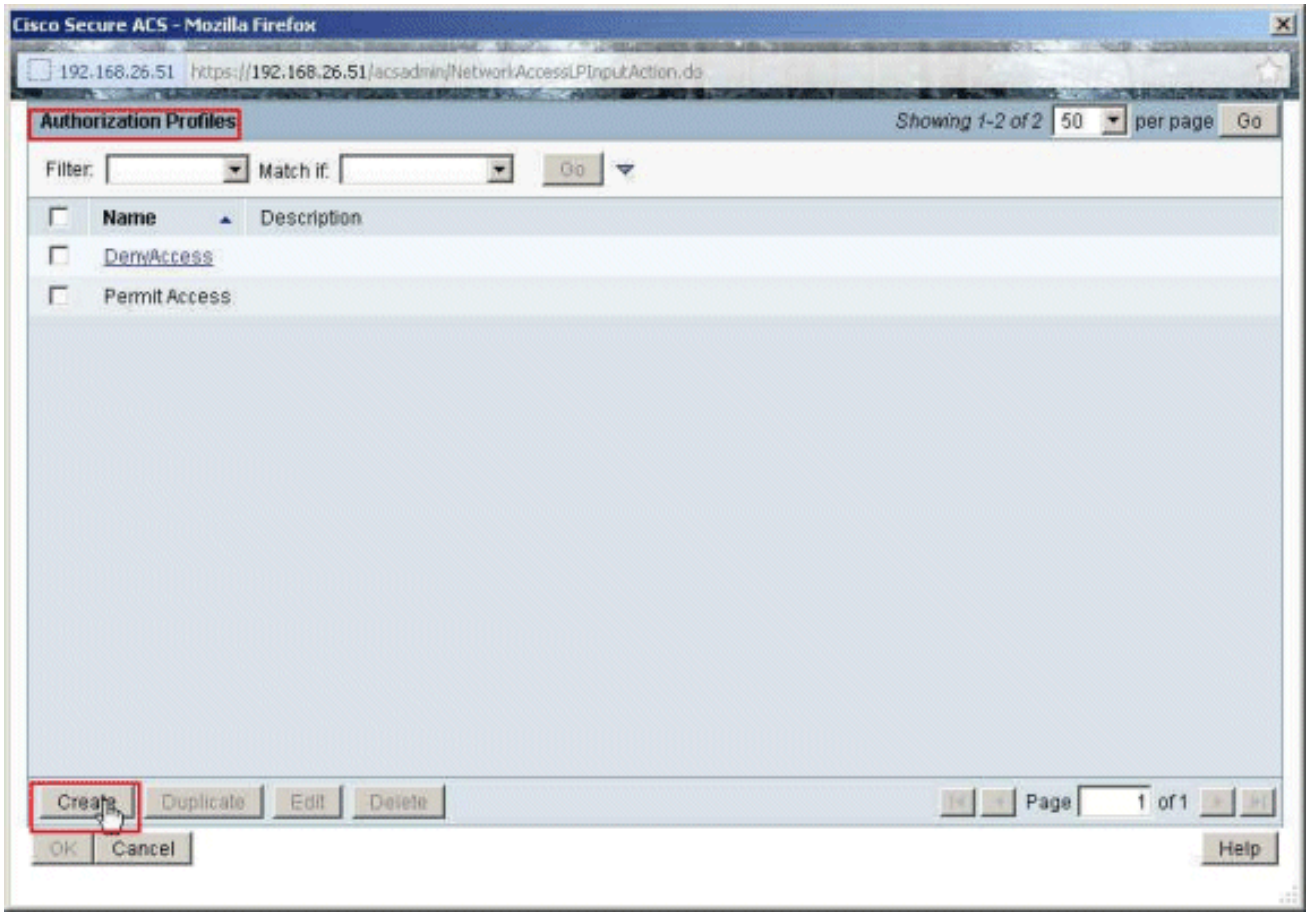
11. Escolha os **gateways de VPN do** grupo de dispositivo de rede criados mais cedo, e clique a **APROVAÇÃO**.



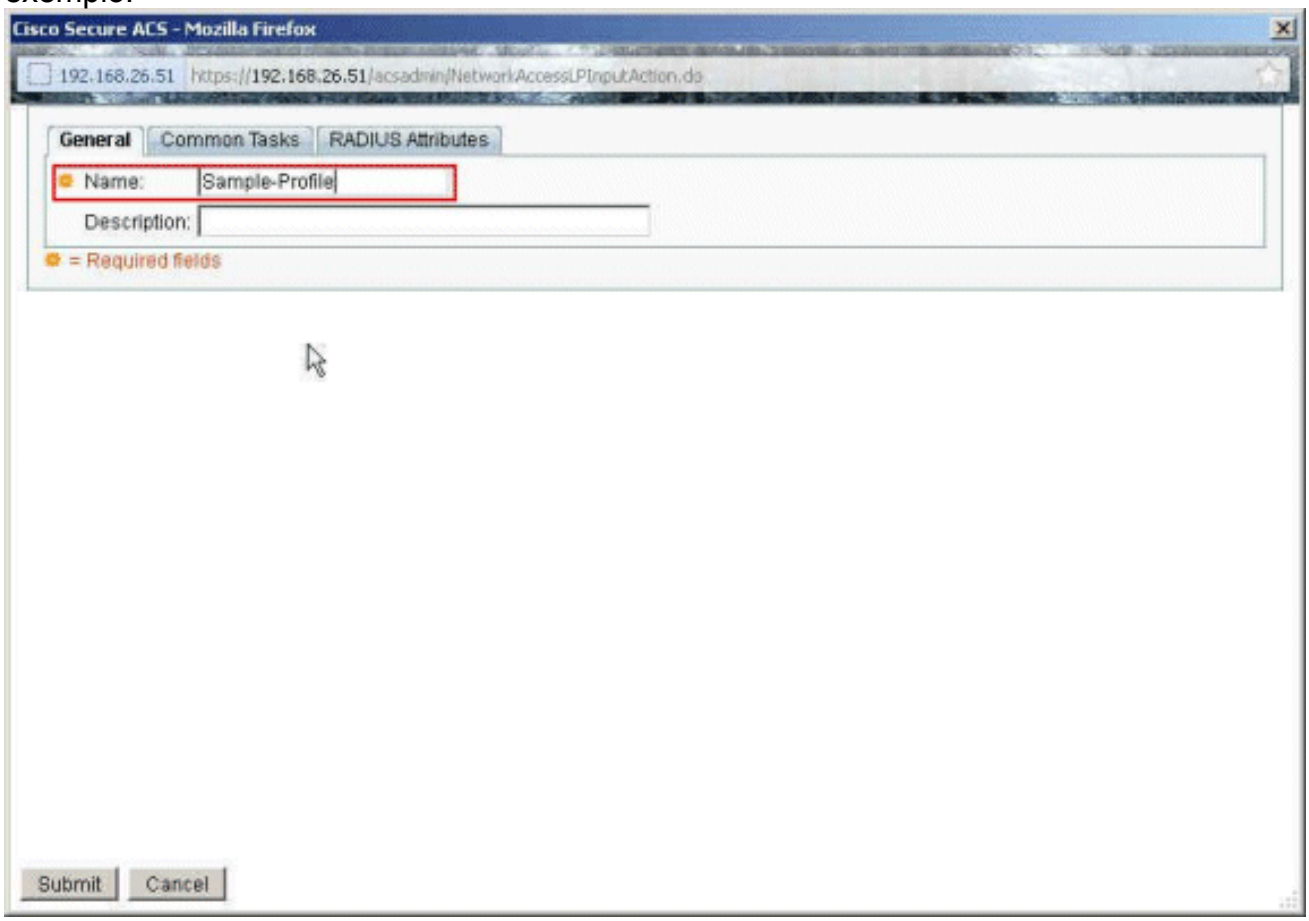
12. Clique **seleto**.



13. O clique **cria** a fim criar um perfil novo da autorização.

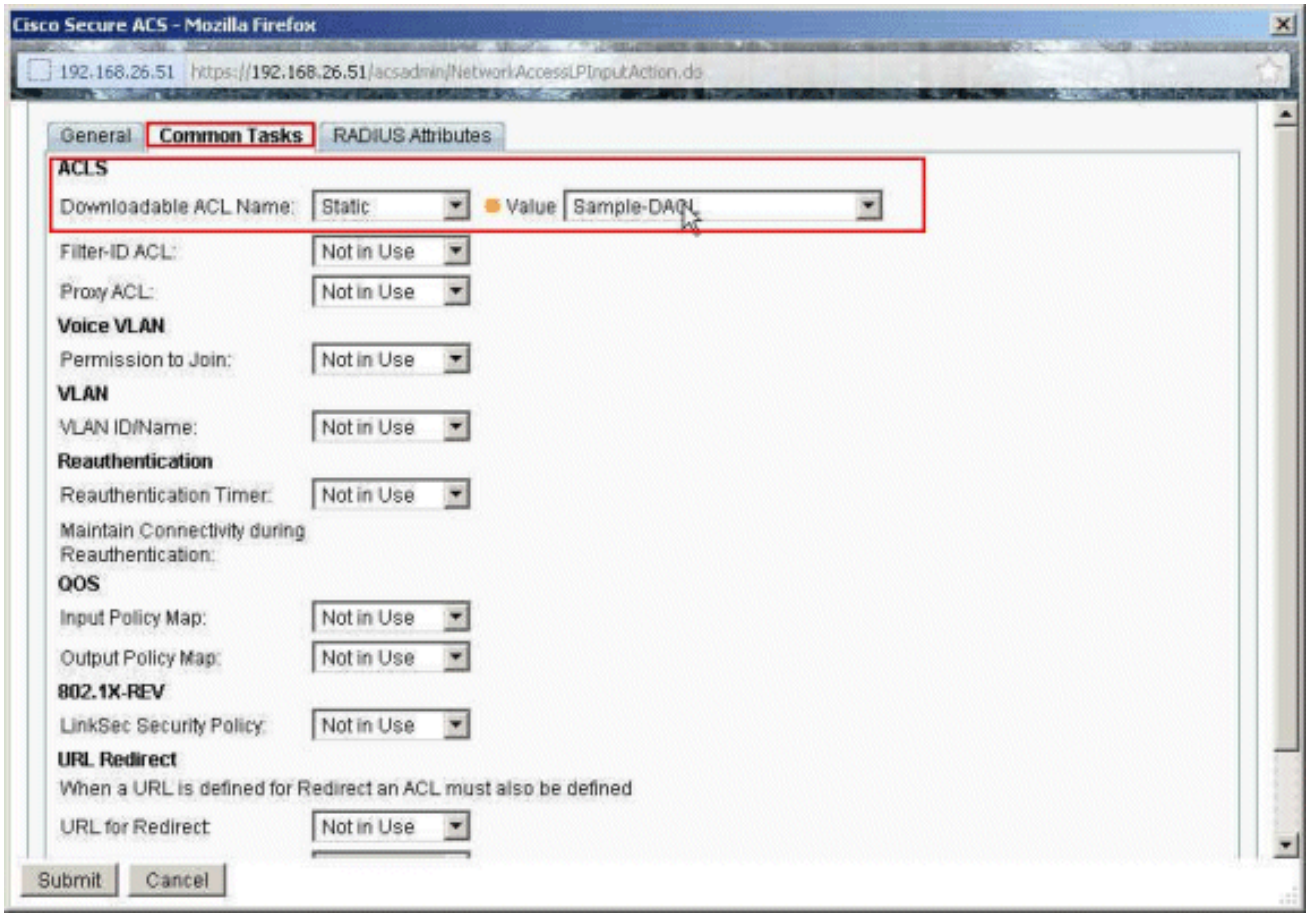


14. Forneça um nome para o **perfil da autorização**. **O exemplo de perfil** é o nome usado neste exemplo.

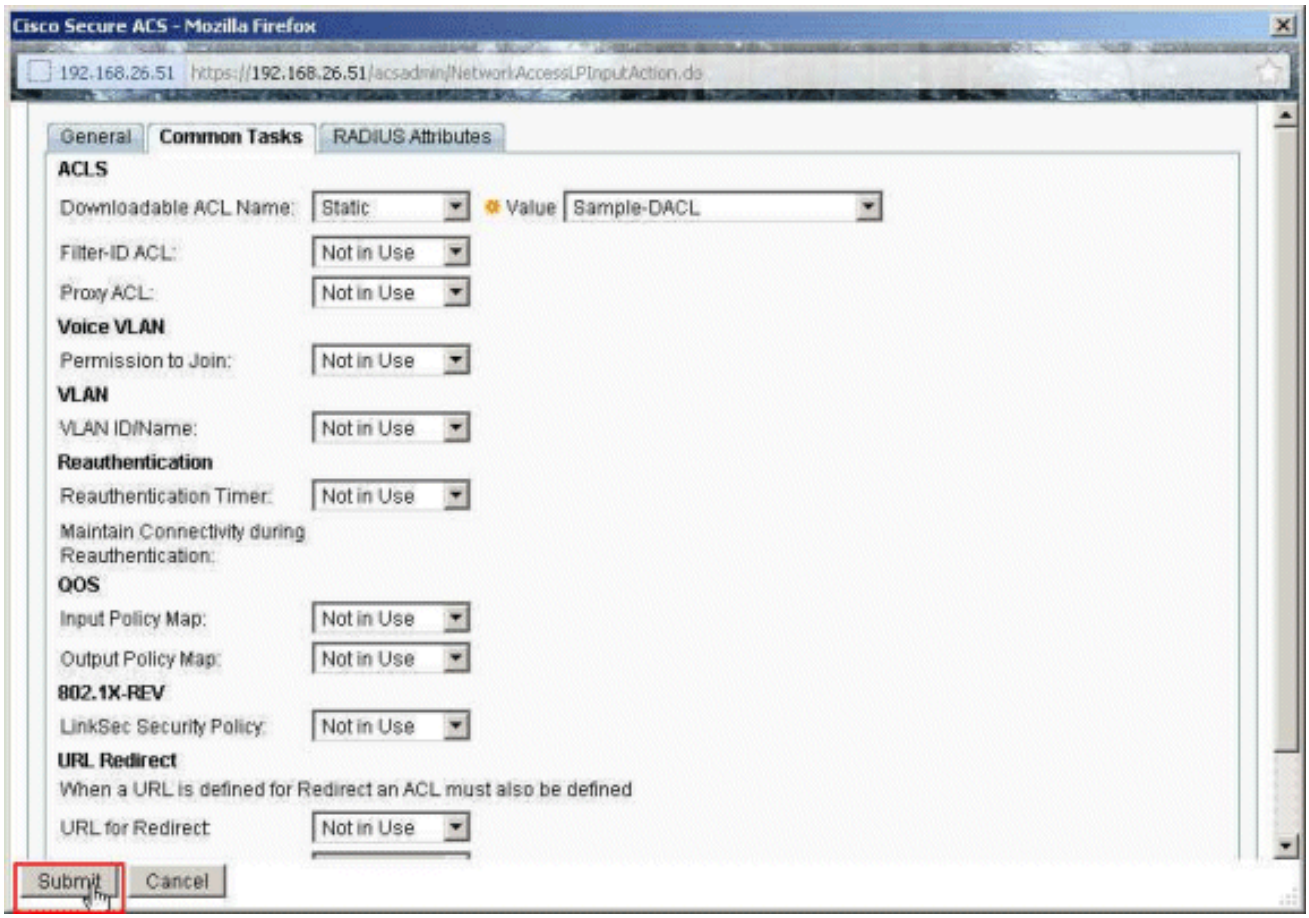


15. Escolha a aba **comum das tarefas**, e selecione a **estática da** lista de drop-down para o nome ACL baixável. Escolha o **DACL** recém-criado **(amostra-DACL) da** lista de drop-down de

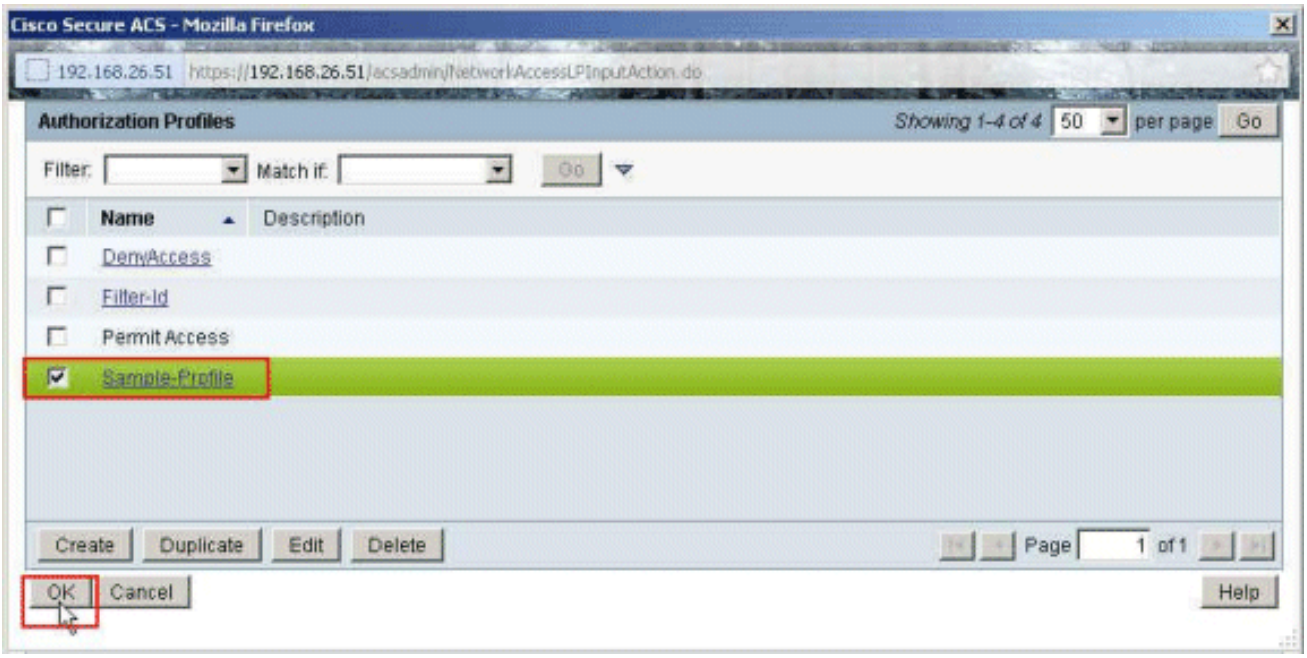
valor.



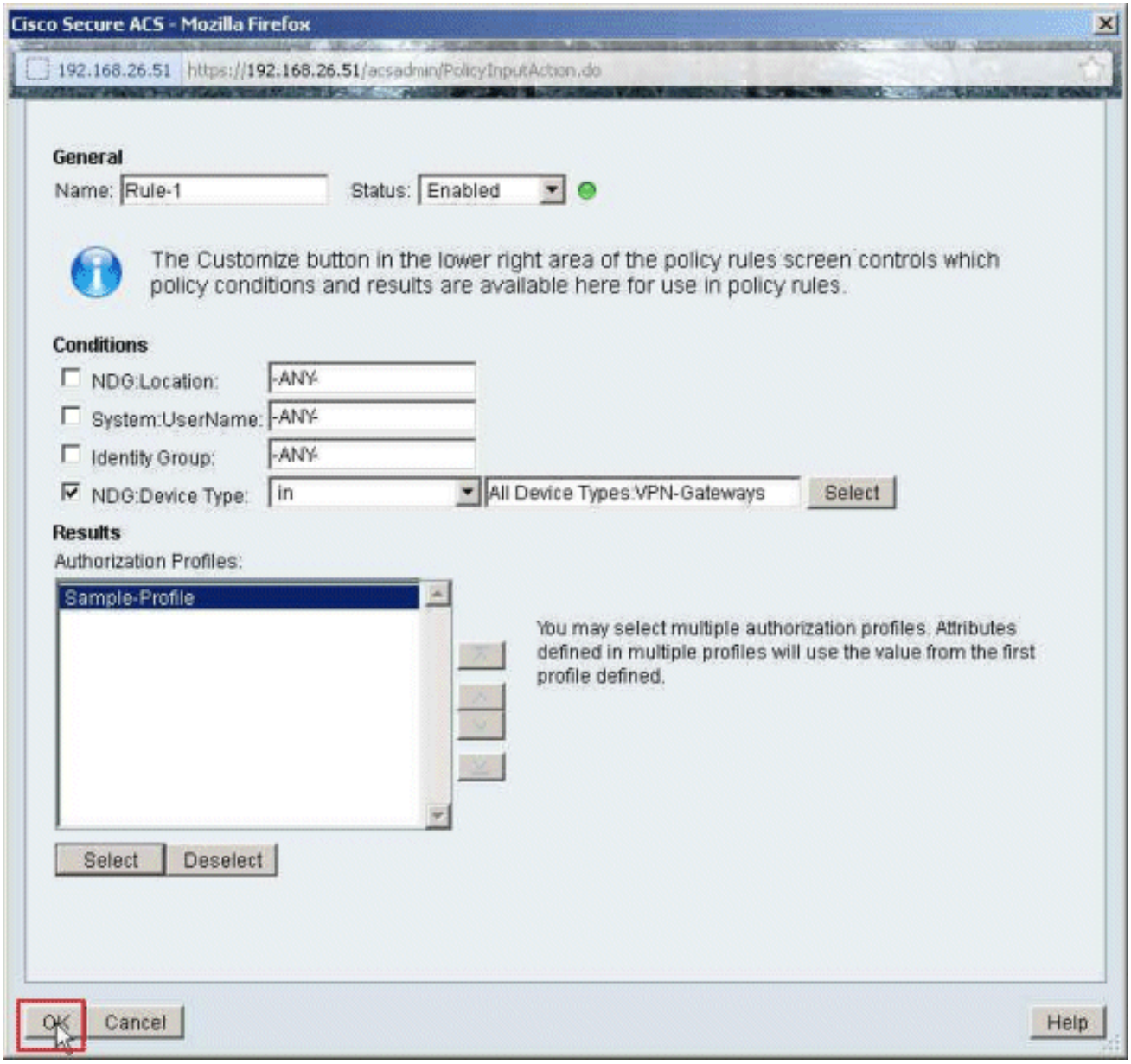
16. Clique em Submit.



17. Selecione o **exemplo de perfil** criado mais cedo, e clique a **APROVAÇÃO**.

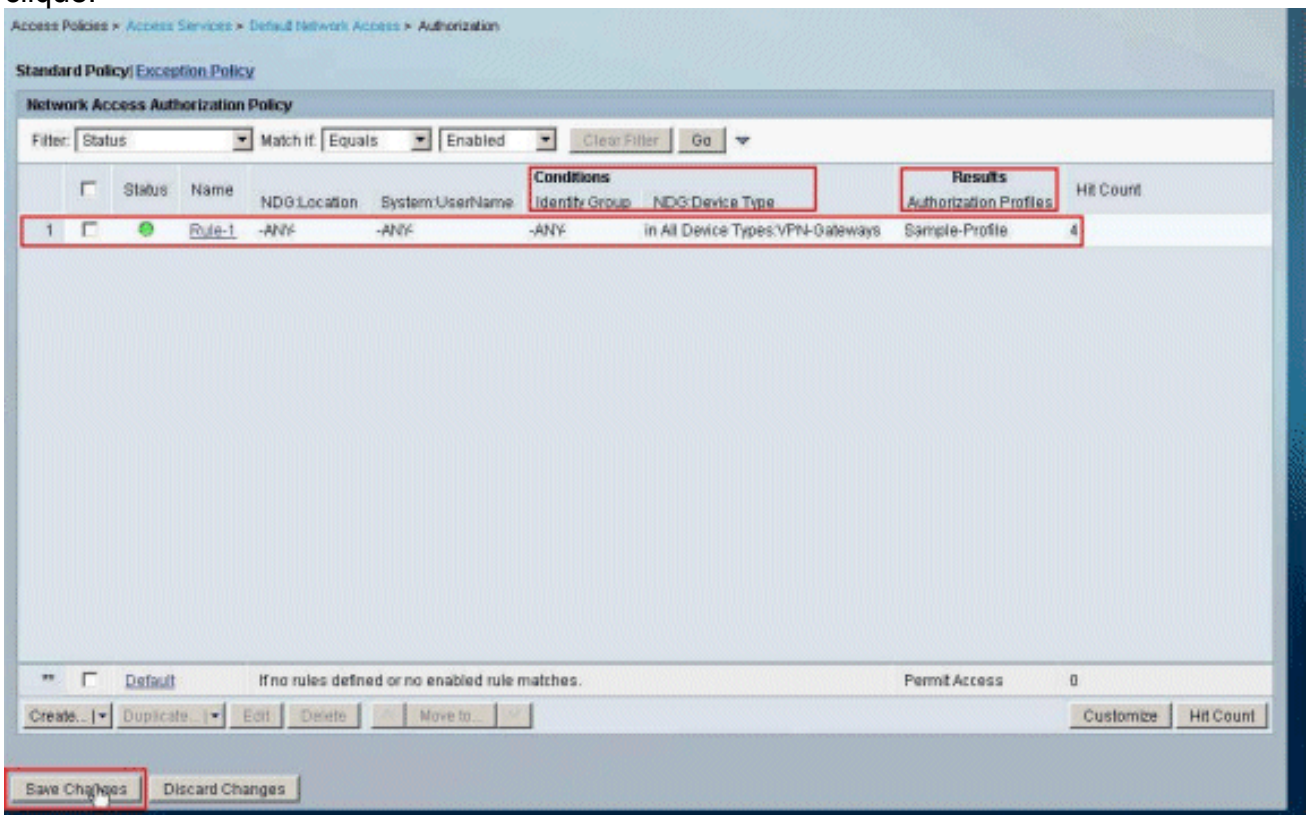


18. Clique em **OK**.



19. Verifique que **Rule-1** está criado com os **gateways de VPN** como NDG: Tipo de dispositivo como a circunstância, e **exemplo de perfil** como o resultado. **Mudanças da salvaguarda do**

clique.



Configurar ajustes do RADIUS IETF para um grupo de usuário

A fim transferir um nome para uma lista de acessos que você já crie na ferramenta de segurança do servidor Radius quando um usuário autentica, configurar o atributo do ID de filtro do RADIUS IETF (número de atributo 11):

```
filter-id=acl_name
```

O usercisco do Amostra-grupo autentica com sucesso, e o servidor Radius transfere um nome ACL (novo) para uma lista de acessos que você já crie na ferramenta de segurança. O usuário “Cisco” pode alcançar todos os dispositivos que são dentro da rede do ASA **exceto o** server de 10.1.1.2. A fim verificar o ACL, veja a seção ACL do ID de filtro.

Conforme o exemplo, o **novo** nomeado ACL é configurado filtrando no ASA:

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

Estes parâmetros aparecem somente quando estes são verdadeiros. Você configurou:

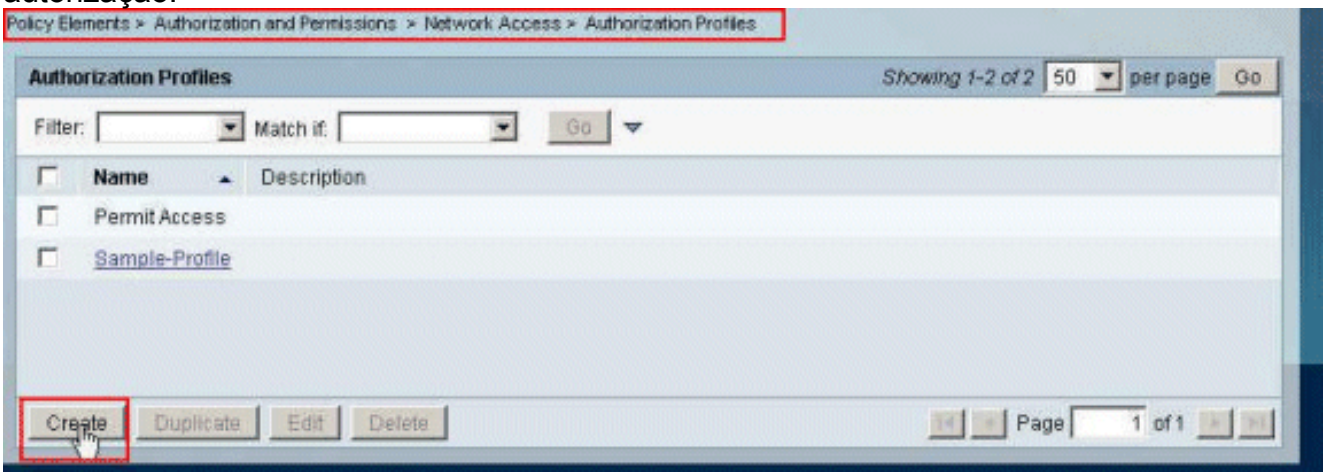
- Cliente de AAA para usar um dos protocolos de raio na configuração de rede
- Um perfil da autorização com o ID de filtro do RAIO (IETF) é selecionado sob a seção do resultado da regra no Acesso-serviço.

Os atributos RADIUS são enviados como um perfil para cada usuário de ACS ao cliente de AAA de pedido.

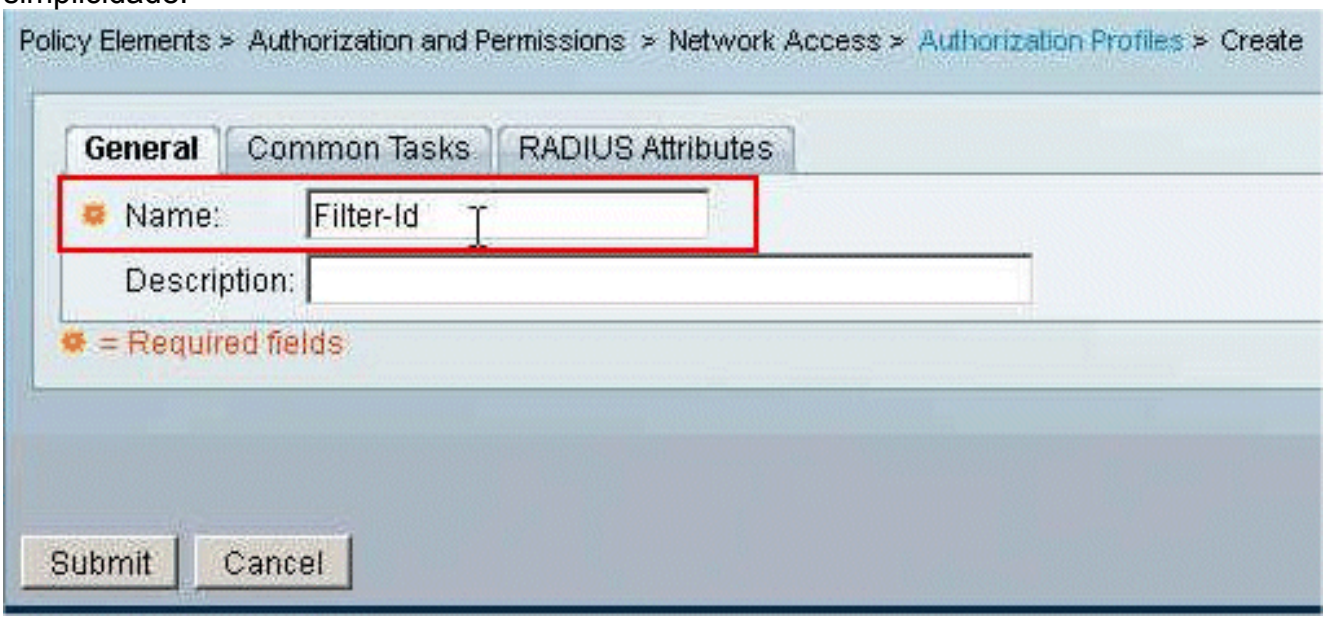
Termine etapas 1 com 6 e 10 com 12 configurar ACS para ACL baixável para o usuário individual, seguido por etapas 1 com 6 configurar ACS para ACL baixável para o grupo, e execute estas etapas nesta seção a fim configurar o ID de filtro no Cisco Secure ACS.

A fim configurar ajustes do **atributo de raio de IETF** para aplicar-se como no perfil da autorização, execute estas etapas:

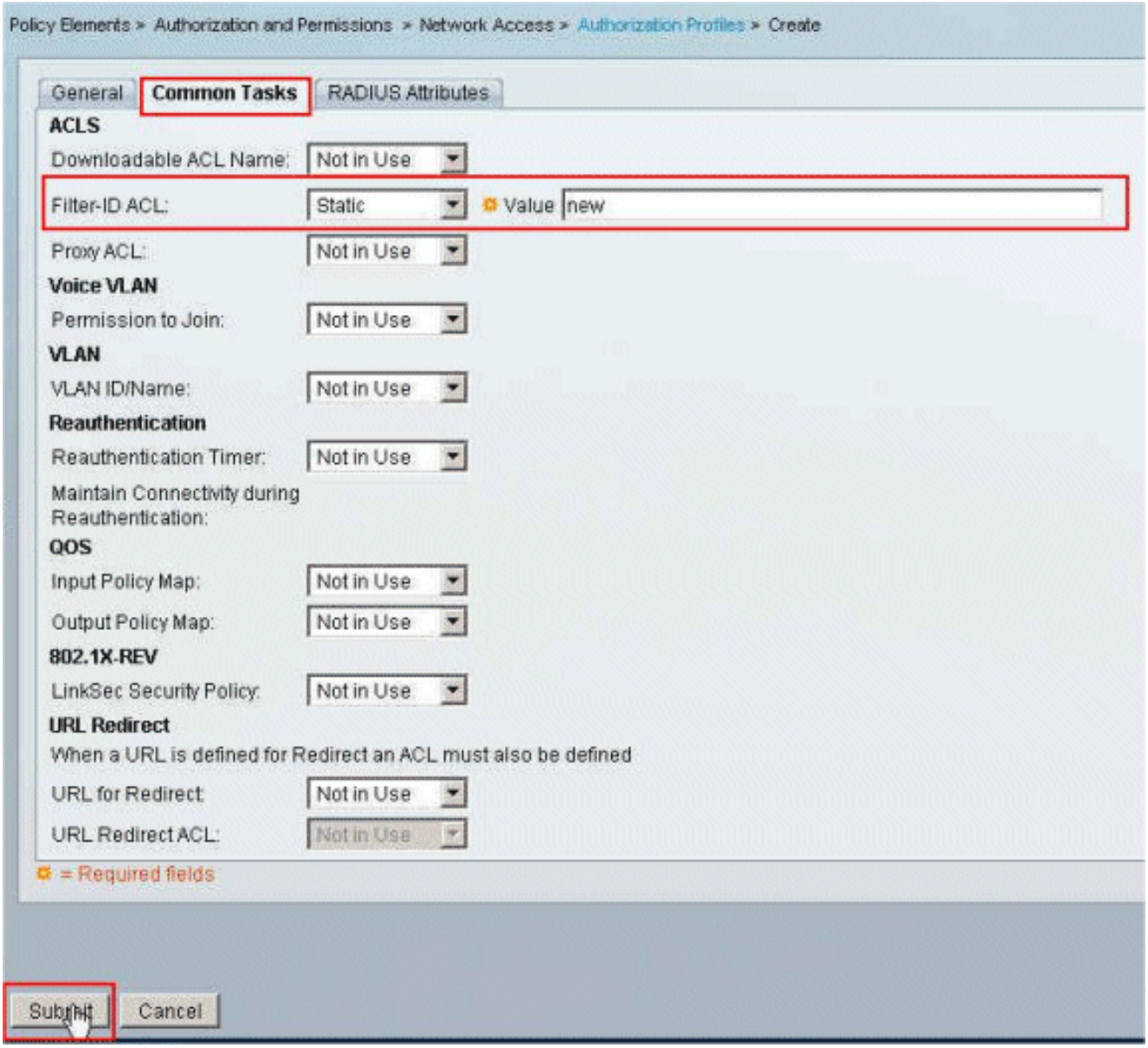
1. Escolha **elementos da política > autorização e permissões > perfis do acesso de rede >** da **autorização**, e o clique **cria** a fim criar um perfil novo da autorização.



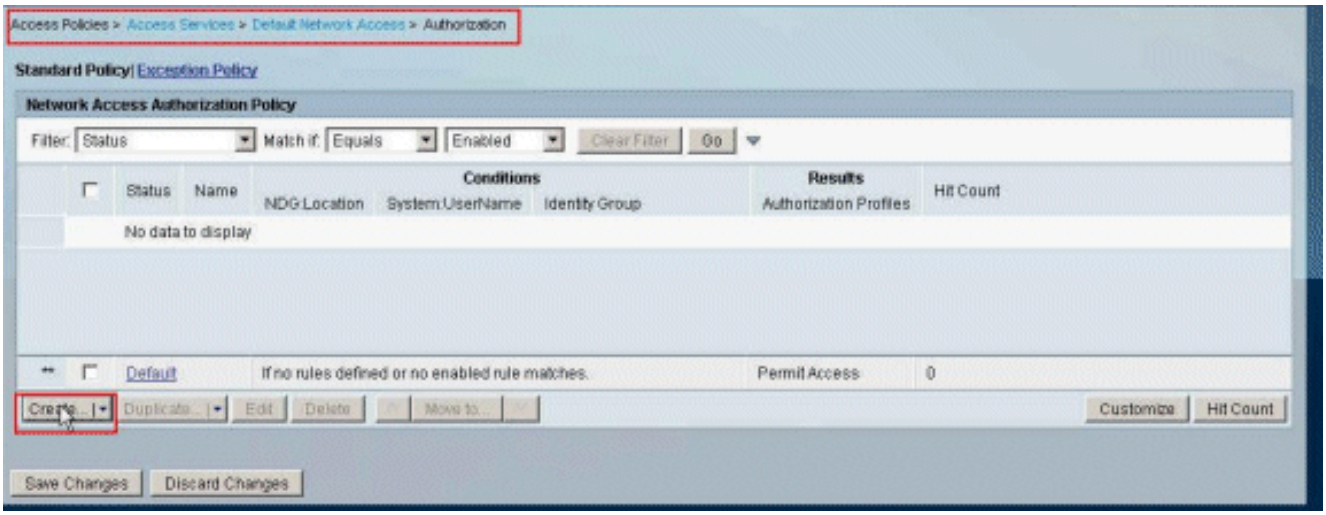
2. Forneça um nome para o **perfil da autorização**. **O ID de filtro** é o nome de perfil da autorização escolhido neste exemplo para a simplicidade.



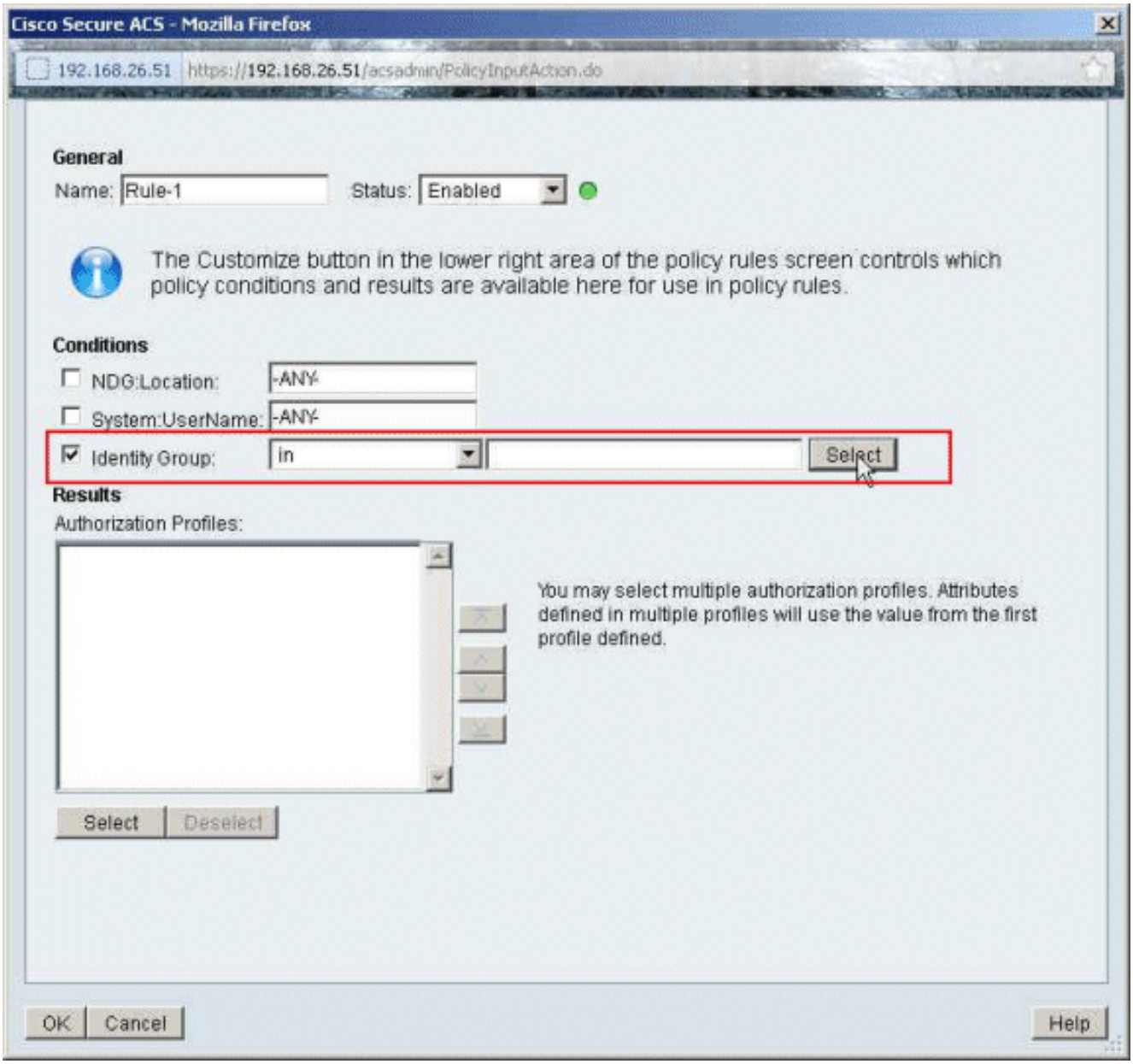
3. Clique a aba **comum das tarefas**, e escolha a **estática da** lista de drop-down para o **ID de filtro ACL**. Dê entrada com o nome da lista de acessos como **novo no** campo de valor, e o clique **submete-se**.



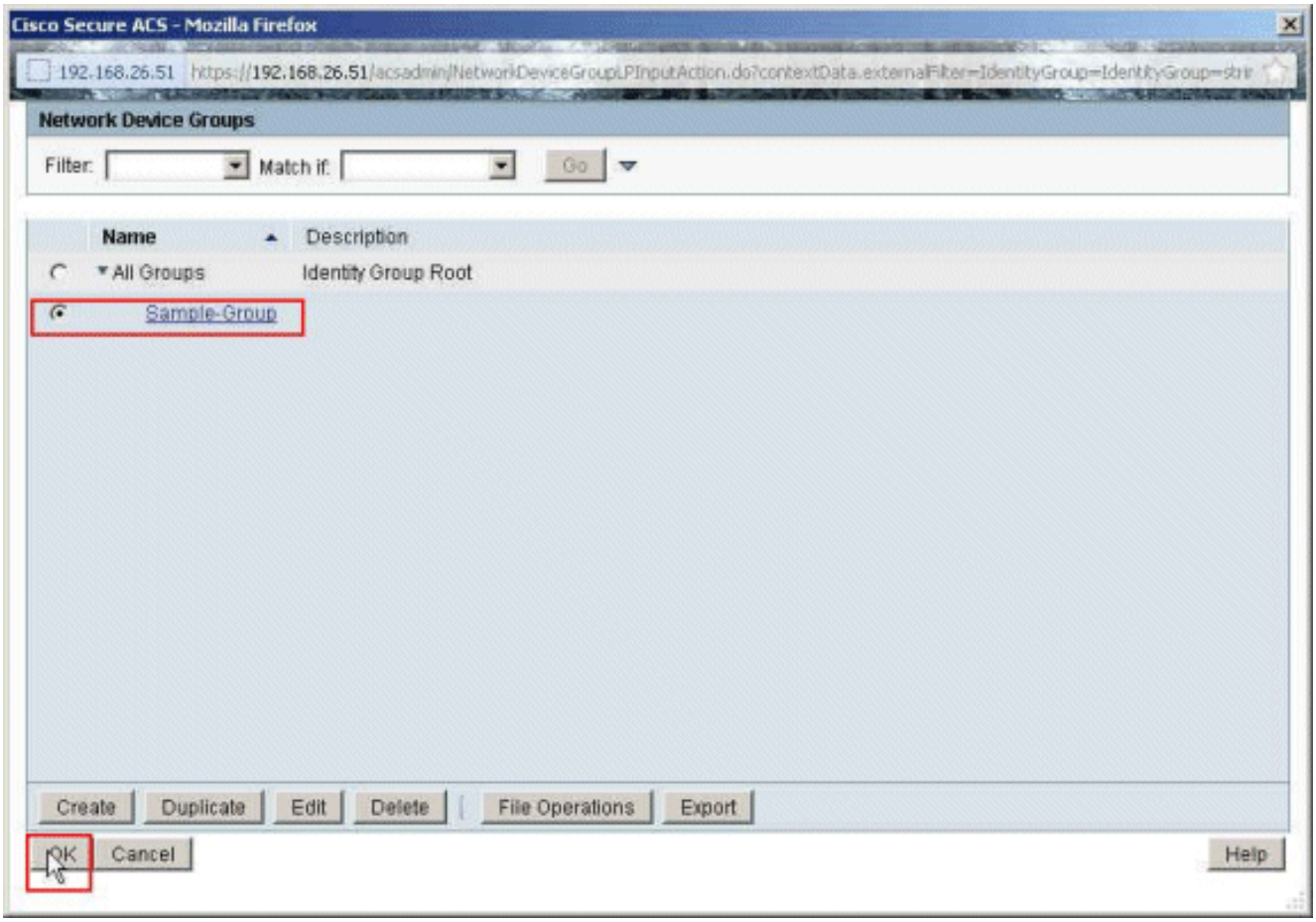
4. Escolha **políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão**, e o clique **cria** a fim criar uma regra nova.



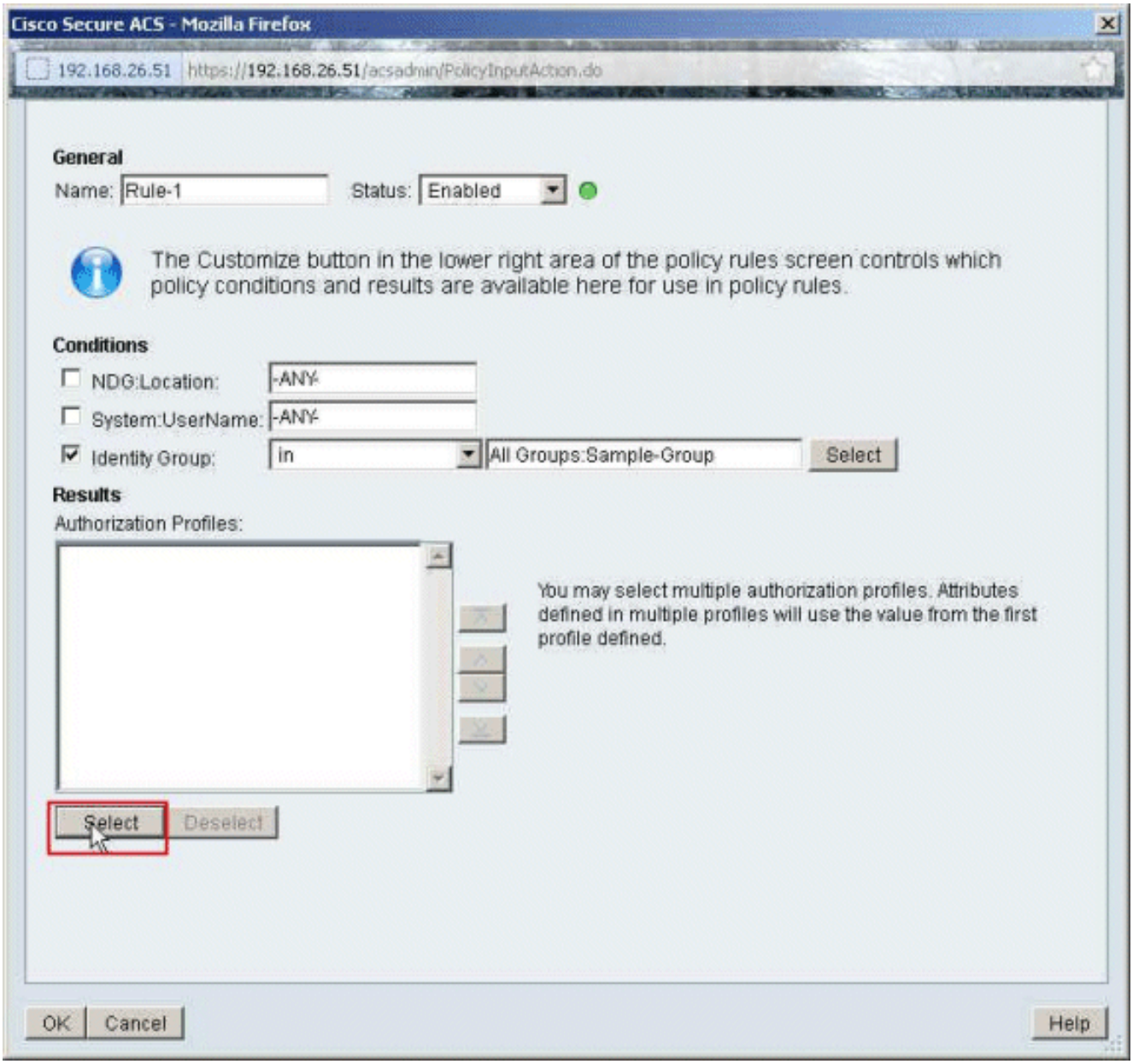
5. Certifique-se de que a caixa de seleção ao lado do **grupo da identidade** está verificada, e clique-se **seleto**.



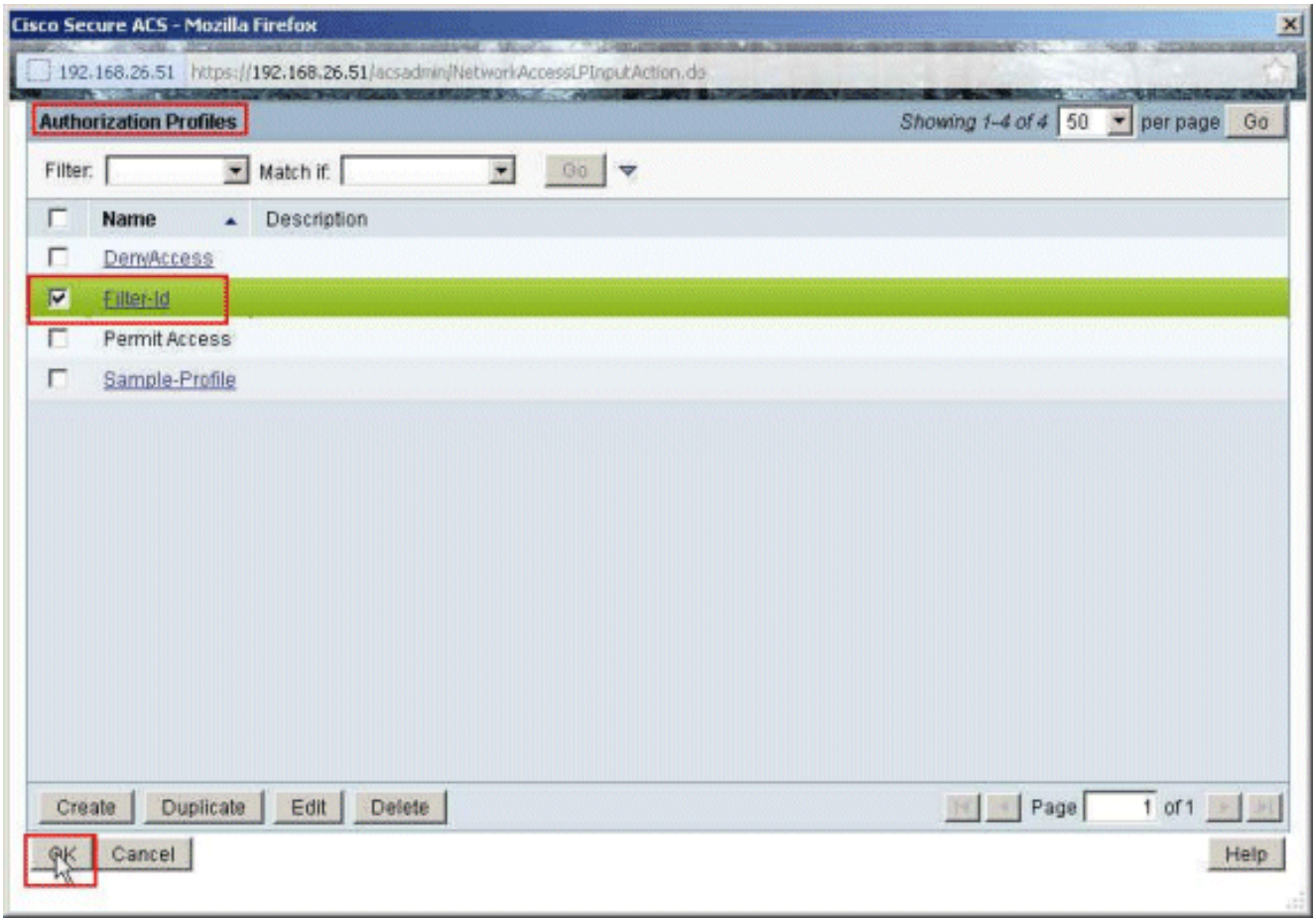
6. Escolha o Amostra-**grupo**, e clique a **APROVAÇÃO**.



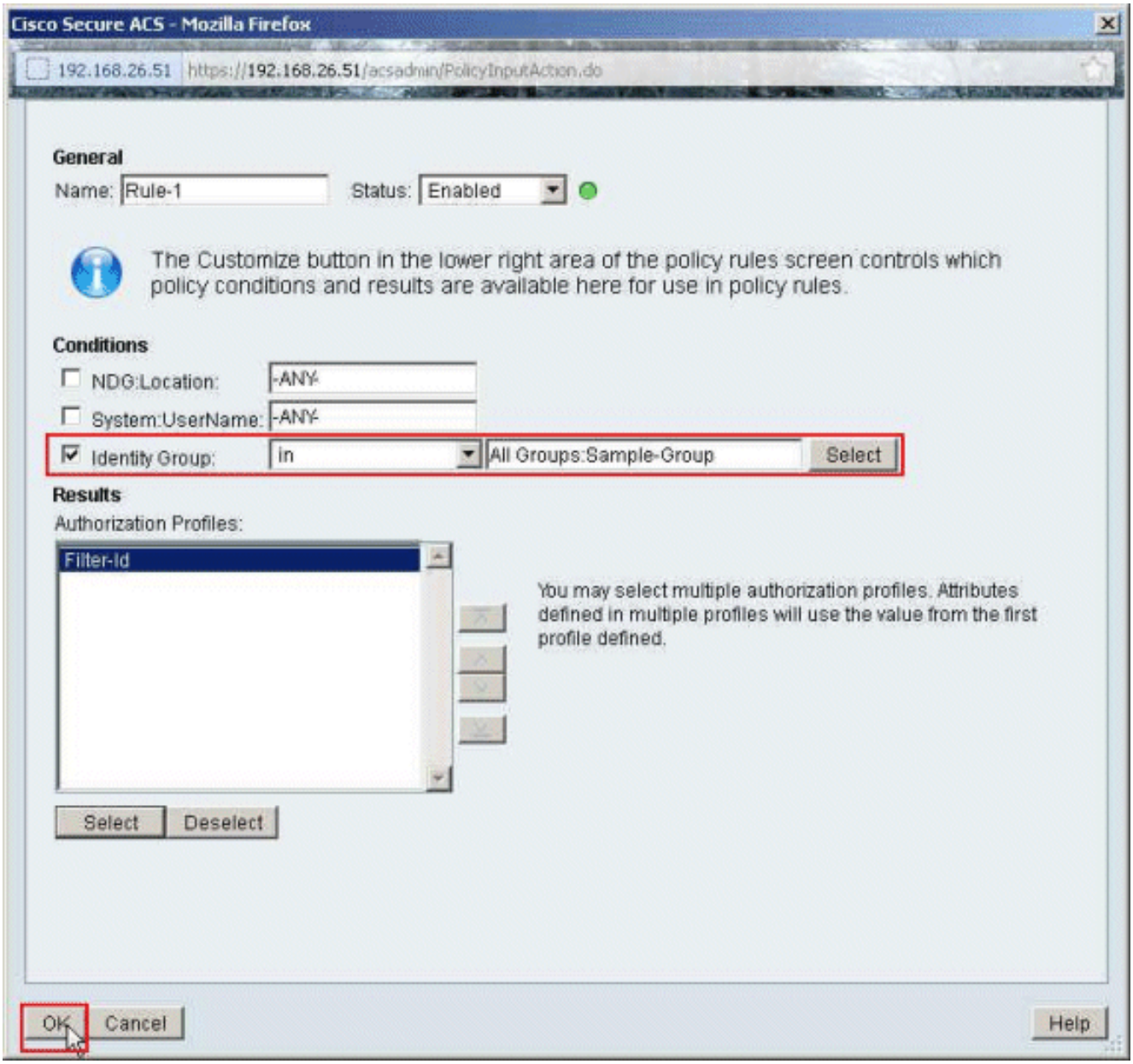
7. Clique **seleto na** seção dos perfis da autorização.



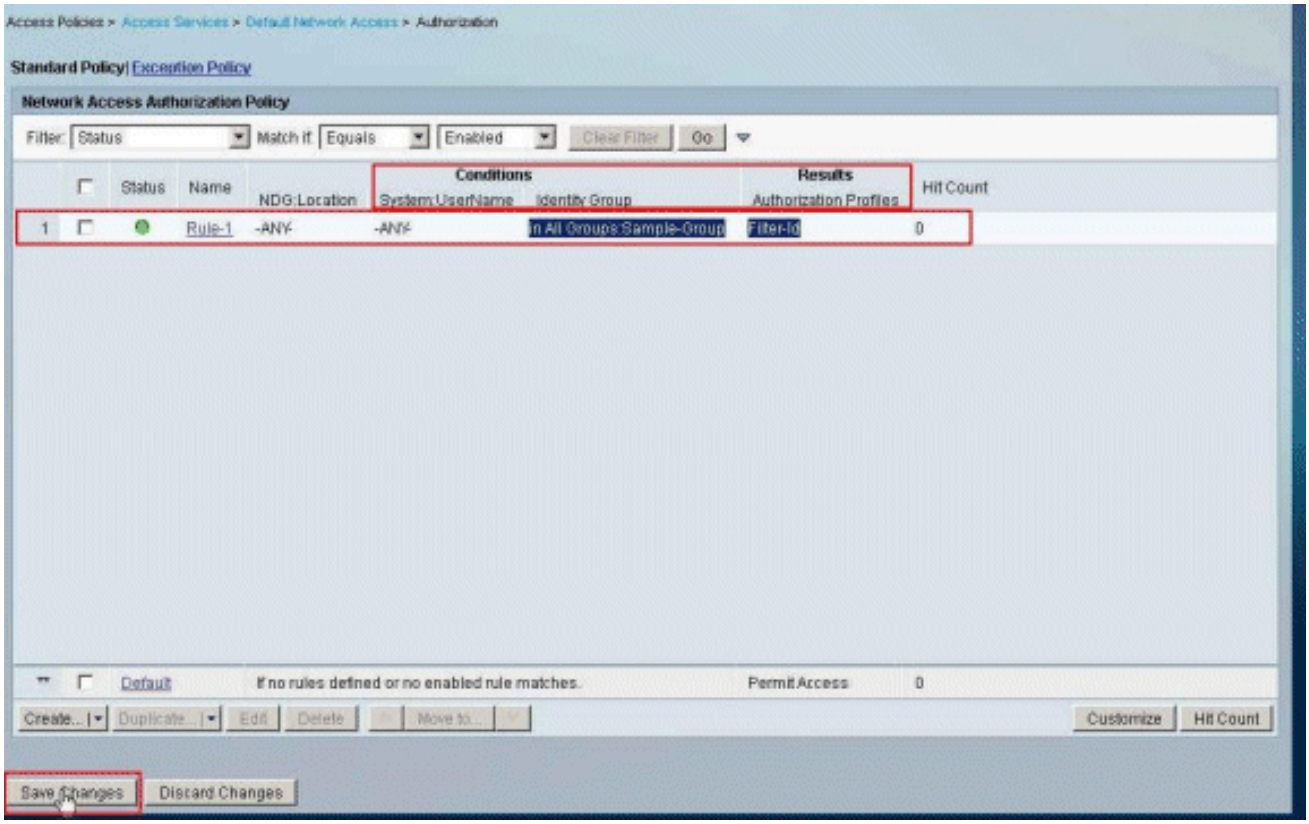
8. Escolha o **ID de filtro do** perfil da autorização criado mais cedo, e clique a **APROVAÇÃO**.



9. Clique em **OK**.



10. Verifique que **Rule-1** está criado com o Amostra-**grupo do** grupo da identidade como a circunstância e o **ID de filtro** como o resultado. Clique **mudanças da salvaguarda**.

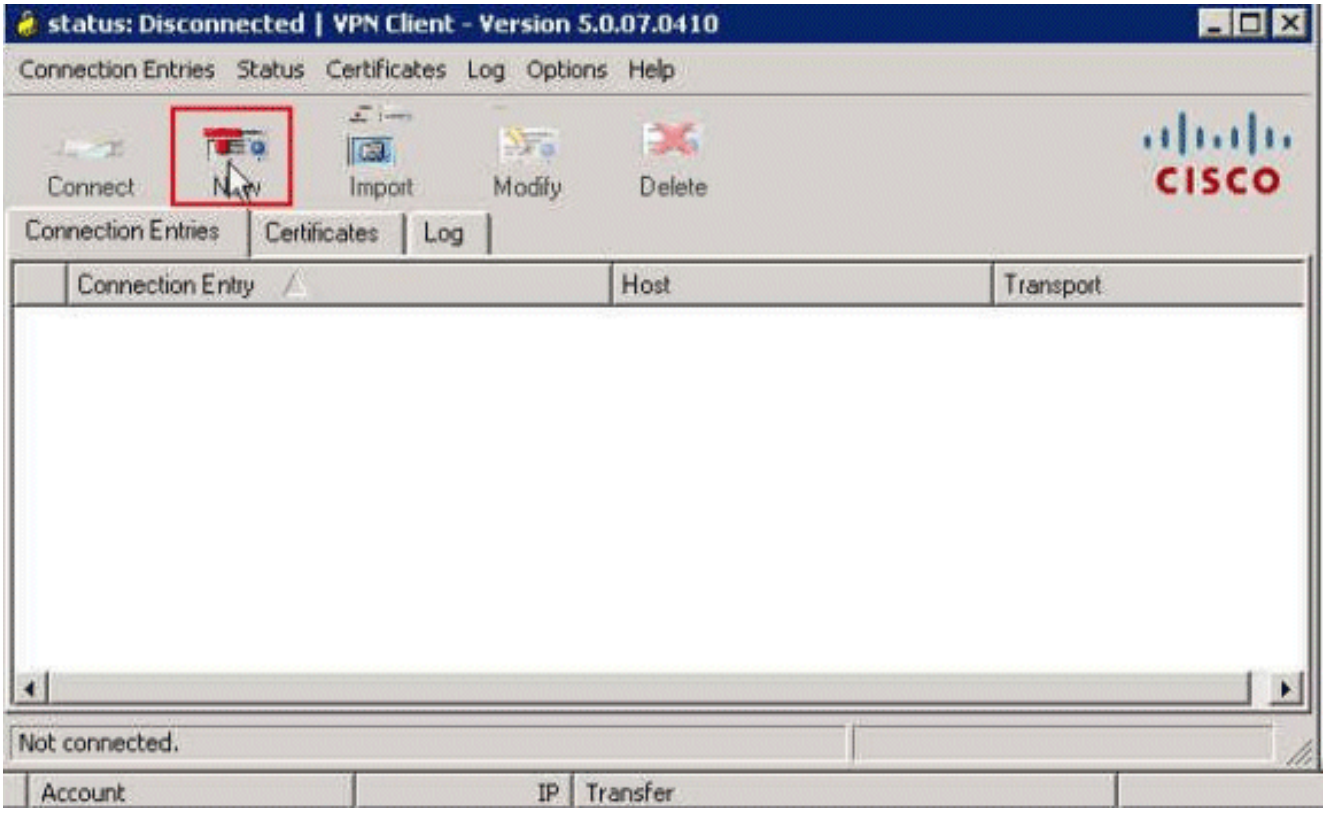


Configuração de Cisco VPN Client

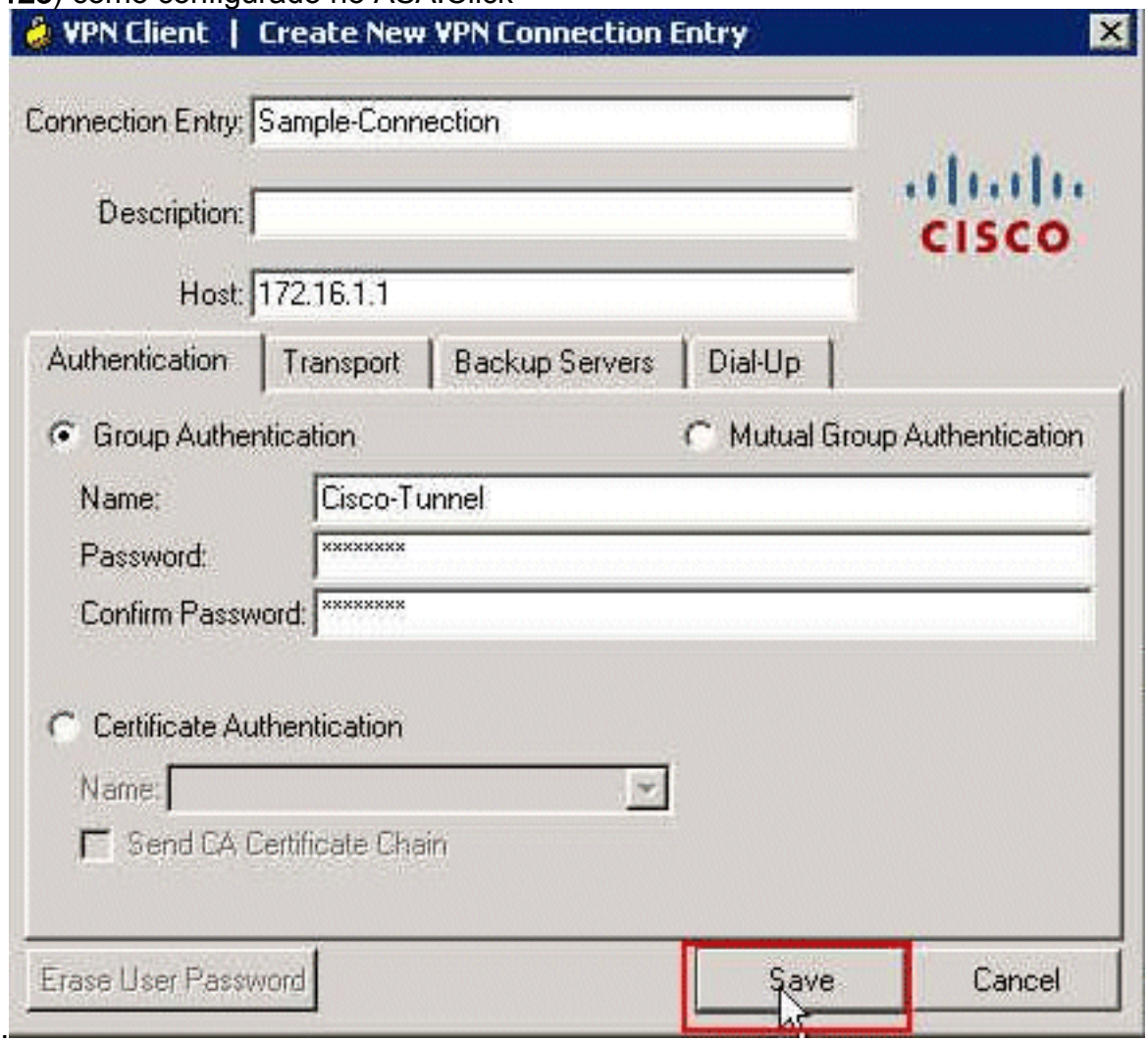
Conecte a Cisco ASA com o Cisco VPN Client a fim verificar que o ASA está configurado com sucesso.

Conclua estes passos:

1. Escolha o **Start > Programs** > o **cliente VPN de Cisco Systems** > o **cliente VPN**.
2. Clique **novo** a fim lançar a janela de entrada nova da conexão de VPN da criação.

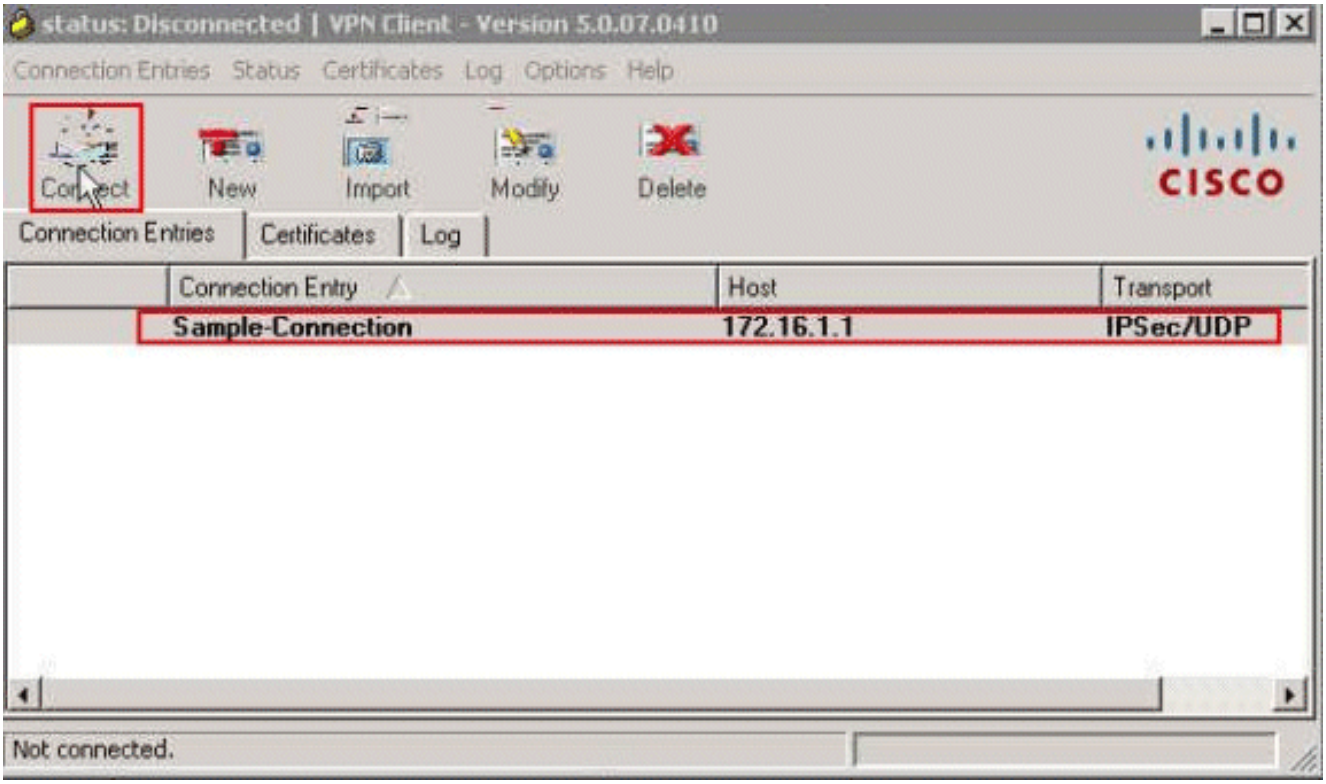


3. Preencha os detalhes de sua nova conexão:Dê entrada com o nome da entrada de conexão junto com uma descrição.Incorpore o **endereço IP externo do ASA à** caixa do host.Incorpore o nome de grupo de túneis VPN (Cisco-**túnel**) e a senha (chave pré-compartilhada - **cisco123**) como configurado no ASA.Click



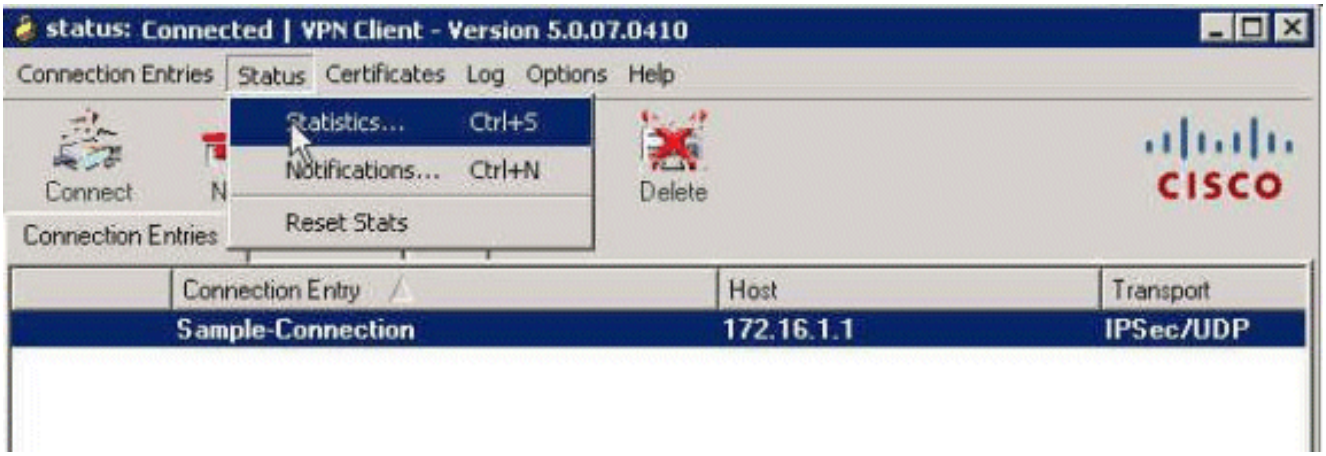
Save.

4. Clique a conexão que você quer usar, e o clique **conecta da** janela principal do cliente VPN.



5. Quando alertado, entre no **cisco123** username **Cisco** e da senha como configurado no ASA para a autenticação, e clique a **APROVAÇÃO** a fim conectar à rede remota.

6. Uma vez que a conexão é estabelecida com sucesso, escolha **estatísticas do** menu de status a fim verificar os detalhes do túnel.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Comandos show crypto

- show crypto isakmp sa – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.

```
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#
```

- **mostre ipsec cripto sa** - Mostra os ajustes usados pelo SAs atual.

```
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 baixável para o usuário/grupo

Verifique o ACL baixável para o usuário Cisco. Os ACL são transferidos do 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
```

ID de filtro ACL

O ID de filtro [011] aplicou-se para o grupo - o Amostra-grupo, e os usuários do grupo são filtrados conforme o ACL (novo) definido no 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
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração. O exemplo de debug é mostrado igualmente.

Nota: Para obter mais informações sobre do IPSec VPN do Acesso remoto do Troubleshooting, refira a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções.

Cancele associações de segurança

Quando você pesquisa defeitos, certifique-se cancelar o SAs existente depois que você faz uma mudança. No modo privilegiado do PIX, use estes comandos:

- **clear [crypto] ipsec sa** - Suprime do IPSec ativo SAs. As palavras-chave crypto são opcionais.
- **clear [crypto] isakmp sa** - Suprime do IKE ativo SAs. As palavras-chave crypto são opcionais.

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **ipsec 7 do debug crypto** - Indica as negociações de IPSEC de fase 2.
- **isakmp 7 do debug crypto** - Indica as negociações de ISAKMP de fase 1.

Informações Relacionadas

- Página de Suporte dos Cisco ASA 5500 Series Adaptive Security Appliances
- Referências de comandos do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Cisco Adaptive Security Device Manager
- Página de suporte da Negociação IPSec/Protocolos IKE
- Página de suporte do Cisco VPN Client
- Cisco Secure Access Control System
- Request for comments (RFC)
- Suporte Técnico e Documentação - Cisco Systems