

RADIUS ضيوفت :ثدحألا تارادصلإاو ASA 8.3 ةمئاق مادختساب VPN ىلإ لوصولل (ACS 5.x) ليزنتلل ةلباقلا (ACL) لوصولا يف مكحتلا ASDM نيوكت لاثم و CLI عم

تايوتحمل

[ةمدقملا](#)
[ةيساسألا تابلطتلا](#)
[تابلطتلا](#)
[ةمدختسمل تانوكملا](#)
[تاجالطصلا](#)
[ةيساسأ تامولعم](#)
[نيوكتلا](#)
[ةكبش ليل يطخ تلال مسرلا](#)
[\(IPsec\) دعب نع لوصولل VPN ةكبش نيوكت](#)
[CLI مادختساب ASA نيوكت](#)
[يدر فال مدختسمل ليل ليزنتلل ةلباقلا \(ACL\) لوصولا يف مكحتلا ةمئاقلا ACS نيوكت](#)
[ةومجمل ليل ليزنتلل ةلباقلا \(ACL\) لوصولا يف مكحتلا ةمئاقلا ACS نيوكت](#)
[ةكبشلا ةزهجأ ةومجمل ليزنتلل ةلباقلا \(ACL\) لوصولا يف مكحتلا ةمئاقلا ACS نيوكت](#)
[ني مدختسم ةومجمل IETF RADIUS تاداعا نيوكت](#)
[Cisco نم VPN ةكبش ليمع نيوكت](#)
[ةحصل نم ققحتلا](#)
[ريفش تلال رماو اراهظا](#)
[ةومجمل /مدختسمل ليل ليزنتلل ةلباقلا \(ACL\) لوصولا يف مكحتلا ةمئاق](#)
[ةيفصتلا لماع فرعمل \(ACL\) لوصولا يف مكحتلا ةمئاق](#)
[اهخالص او عاخذالا فاشكتسا](#)
[ةينمألا تانارتقالا حسم](#)
[اهخالص او عاخذالا فاشكتسا رماو](#)
[قلص تاذا تامولعم](#)

ةمدقملا

ىلإ لوصولل ني مدختسمل ةقداصل نامألا زاهج نيوكت ةيفيك دننتسمل اذه حضوي
يوتحي ال دننتسمل اذه نإف ،اي نمض RADIUS ضيوفت نيكمت كنكمي هنأل ارظنو .ةكبشلا
لوح تامولعم رفوي وهو .نامألا زاهج ىلع RADIUS ضيوفت نيوكت لوح تامولعم يأ ىلع
RADIUS مداوخ نم اهيقلت متي يتلا لوصولا ةمئاق تامولعمل نامألا زاهج ةجلاعم ةيفيك

لوصولا ةمئاق مسا وأ نامألا زاهج ىلإ لوصولا ةمئاق ليزنتل RADIUS مداخل نيوكت كنكمي
ةصخال لوصولا ةمئاق يف هب حومسم وه امب طقف مدختسملل حمسي .ةقداصل تقوي

م.دختسملاب

مداخ مادختسإ دنع ريوطتلل ةيلباق لئاسولا رثكأ يه ليزنتلل ةلباقلا لوصول مئاوق
م.دختسمل لك ةبسانملا لوصول مئاوق ريفوتل Cisco نم (ACS) نمآلا لوصول ي ف مكحتلا
عجرا، Cisco Secure ACS و ليزنتلل ةلباقلا لوصول ةمئاق تازيم لوح تامولعمل نم ديزمل
مئاوق و ليزنتلل ةلباقلا لوصول ي ف مكحتلا مئاوق لئاس رال RADIUS [مداخ نيوكت](#) يلا
ليزنتلل ةلباقلا IP يلا لوصول ي ف مكحتلا

[ةمئاق مادختساب ةكبشلا يلا لوصول رال RADIUS \(ACS\) ضيوفت: ASA/PIX 8.x](#) يلا عجرا
نيوكتلا ASDM نيوكت لاثم و CLI عم ليزنتلل ةلباقلا (ACL) لوصول ي ف مكحتلا
مدقألا تارادصإ او 8.2 تارادصإ عم Cisco ASA يلع قباطتملا

ةيساسألا تابلطتملا

تابلطتملا

متو لمالكلا ليغشتلا ديقي (ASA) فيكتلل لباقلا نامألا زاهج نأ دننتسمل اذه ضررت في
تاريغت ءارجاب Cisco نم CLI و ASDM) ةلدعمل نامألا ةزهجأ ري دمل حامسلل هنيوكت
نيوكتلا

ةطساوب دعب نع زاهجلا نيوكتب حامسلل [ASDM يلا HTTPS لوصول حامسل](#) يلا عجرا: ةطحالم
Secure Shell (SSH) و ASDM

ةمدختسمل تانوكمل

ةيولاتلا ةيدامل تانوكمل او جماربلا تارادصإ يلا دننتسمل اذه ي ف ةدراولا تامولعمل دننتست

- ثدحألا تارادصإ او Cisco نم 8.3 رادصإلا ASA جم انرب
- ثدحألا تارادصإ او 6.3 رادصإلا Cisco ASDM،
- ثدحألا تارادصإ او 5.x رادصإلا Cisco نم VPN ةكبش ليمع
- Cisco Secure ACS 5.x

ةصاخ ةي لمعم ةئيب ي ف ةدوجوملا ةزهجألا نم دننتسمل اذه ي ف ةدراولا تامولعمل ءاشنإ م
ت ناك اذا. (يضارتفا) حوسمم نيوكتب دننتسمل اذه ي ف ةمدختسمل ةزهجألا عيمج تادب
رمأ يال لمحتحمل ريثأتلل كمهف نم دكأتف، ةرشابم كتكبش

تاحالطصلا

[تاحالطصلا لوح تامولعمل نم ديزم يلع لوصول ةينقتلا Cisco تاحيملت تاحالطصا](#) عجار
[تادنتسمل](#)

ةيساسأ تامولعمل

نم تاعومجم ءاشنإ ليزنتلل ةلباقلا IP يلا لوصول ي ف مكحتلا مئاوق مادختسإ كنكمي

نم ديدعلال ىلع اهقبيبطت كنكمي يتلا (ACL) لوصولا يف مكحتلا ةمئاق تافيرعت
مكحتلا ةمئاق تافيرعت نم تاعومجمل هذه ىمست . ني مدختسمل تاعومجم وأ ني مدختسمل
(ACL) لوصولاب مكحتلا ةمئاق تافيرعت (ACL) لوصولاب

ةقيرطلا هذبه ليزننلل ةلباقلا IP ىلى (ACL) لوصولا يف مكحتلا ةمئاق لمعت

1. ةمئاق تناك اذا ام ددحي ACS نإف ، ةكبشلا ىلى لوصولا قح مدختسمل ACS حنمي ام دنع
ليوختلا فيرعت فلم ىلى اهنبيعت متي ليزننلل ةلباق IP ىلى لوصولا يف مكحتلا
جئاتنلا مسق يف

2. فلم ىلى اهنبيعت مت ليزننلل ةلباق IP ىلى لوصولا يف مكحت ةمئاق ACS ددح اذا
لوبق ةمزح يف ، مدختسمل لمع ةسلج نم ءزجك) ةمس لسري ACS نإف ، ليوختلا فيرعت
ةمئاق رادصاو ، ةامسمل ACL ىلى لوصولا يف مكحتلا ةمئاق ددحت (RADIUS ىلى لوصولا
ةامسمل (ACL) لوصولا يف مكحتلا

3. لوصولا يف مكحتلا ةمئاق نم يلاحلا رادصالا ىلع يوتحي ال هئاب AAA ليمع در اذا
وأ ديدج لوصولا يف مكحتلا ةمئاق نأ ي (أ) هب ةصاخلا تقوئل نيختلا ةركاذ يف (ACL)
ىلى (ةثدحم وأ ديدج) (ACL) لوصولا يف مكحتلا ةمئاق لسري ACS نإف ، (اهريغت مت
زاهجلا

يف مكحتلا ةمئاق نيوكتل ليدب يه ليزننلل ةلباقلا IP ىلى لوصولا يف مكحتلا ةمئاق
مدختسم ةومجم وأ مدختسم لكل RADIUS Cisco-AV-pair [26/9/1] ةمس يف (ACL) لوصولا
اهحنمو ، ةدحاو ةرم ليزننلل ةلباق IP ىلى (ACL) لوصولا يف مكحت ةمئاق ءاشن كنكمي
فيرعت فلم ي ىلى ليزننلل ةلباقلا IP ىلى لوصولا يف مكحتلا ةمئاق نيبيعت مت ، امسا
ةمس نيوكتب تمق اذا نم ةيلعاف رثكأ ةقيرطلا هذه نوكت . همس اعجاب تمق اذا ضيوفت
ليوختلا فيصوتل RADIUS Cisco-av-pair

مدختست ال ACS بيوهجاو يف (ACL) لوصولا يف مكحتلا ةمئاق تافيرعت لخدت ام دنع
ةمئاق رمأ ةغايص مدختسا ، ىرخال بنواجل عيمج يف ؛ مسالا وأ ةيساسالا ةملاكلا تالادخ
ةمئاق قبيبطت يونت يذلا AAA ليمعل ءامسالا ةيسايقلا (ACL) لوصولا يف مكحتلا
يف مكحتلا ةمئاق تافيرعت نمضتت . هيلع ليزننلل ةلباقلا IP ىلى لوصولا يف مكحتلا
لوصولا يف مكحتلا ةمئاق رم او نم رثكأ وأ دحاو رمأ ACS يف اهلخدت يتلا (ACL) لوصولا
لصفنم رطس ىلع (ACL) لوصولا يف مكحت ةمئاق رمأ لك نوكتي نأ بجي . (ACL)

ليزننلل ةلباقلا IP ىلى لوصولا يف مكحتلا ةمئاق نم ديدعلال ديدحت كنكمي ، ACS يف
دعاوق يف ةدراوال طورشلا ىلى اذانتسا . ةفلتخملا ليوختلا فيرعت تافل م يف مهمدختساو
ةمئاق ىلع يوتحت ةفلتخم ضيوفت فيرعت تافل لاسرا كنكمي ، لوصولا ةمدخ ضيوفت
نيفلتخم AAA ءالمع ىلى ليزننلل ةلباقلا IP ىلى لوصولا يف مكحتلا

يف (ACL) لوصولا يف مكحتلا ةمئاق تافيرعت بيترت ريغت كنكمي ، كلذ ىلع ةوالع
ةمئاق تافيرعت صحفب ACS موق ي . ليزننلل ةلباق IP ىلى (ACL) لوصولا يف مكحت ةمئاق
يف مكحتلا ةمئاق ليوحت لو ليزننلو ، لودجال ىلع نم ءدب ، (ACL) لوصولا يف مكحتلا
تمق اذا ماظنلا ةءافك نم دكأتلا كنكمي ، بيترتلا نيبيعت دنع . هيلع رثعي (ACL) لوصولا
ىلع وحن ىلع قبيبطتلا ةلباق رثكألا (ACL) لوصولا يف مكحتلا ةمئاق تافيرعت عضوب
ةمئاقلا يف

AAA ليمع ىلع ليزننلل ةلباق IP ىلى (ACL) لوصولا يف مكحت ةمئاق مادختسا لجأ نم
ةيلال دعاوقلاب AAA ليمع مزتلني نأ بجي ، ني مع

• قداصل ل RADIUS مادختسا

• ليزن تال لة لباقل ال IP ال (ACL) لوصول ال ف مكحتال مئوق معد

: ليزن تال لة لباقل ال IP ال لوصول ال ف مكحتال مئوق معدت ال Cisco ةزهجأ ال عة لثمأ هذ

• ASA

• ثدحال تارادصل ال او 12.3(8)T رادصل ال، IOS لغشت ال ال Cisco ةزهجأ

(ACL) لوصول ال ف مكحتال مئوق لادخال همادختسا كليلع بجي يذال قيسنن ال ال لاثم اذ
(ACL): لوصول ال ف مكحتال مئوق تافيرعت ع برم ال

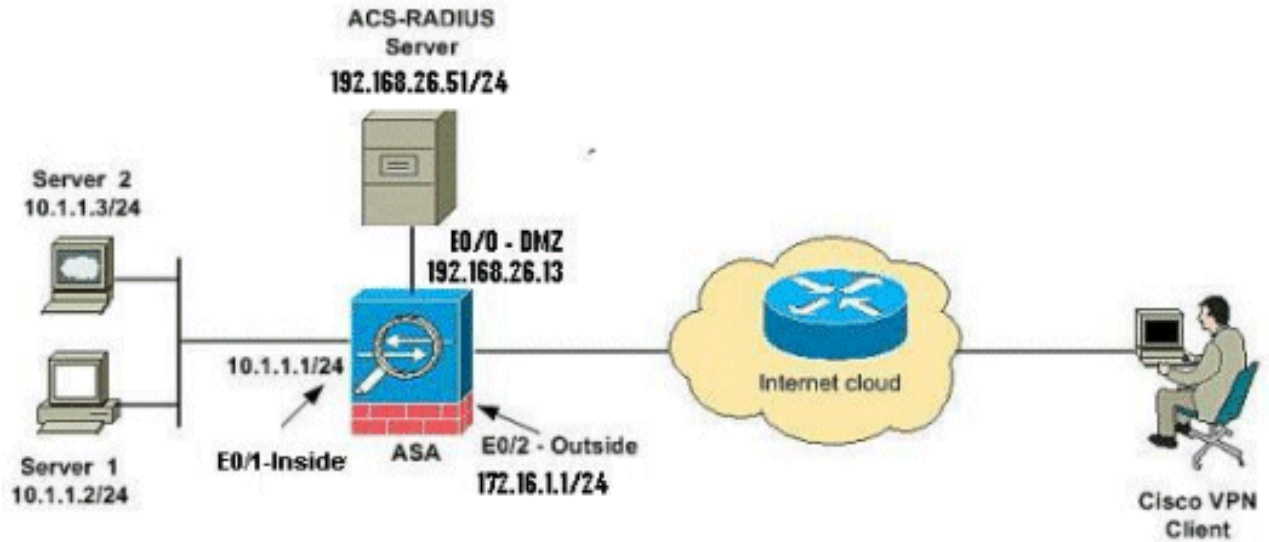
```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
    permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
    permit TCP any host 10.160.0.1 eq 80 log
    permit TCP any host 10.160.0.2 eq 23 log
    permit TCP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

نيوكتال

.دنتسما اذ ف ةحصولما تازيما نيوكت تامولعم كل مدقت، مسقلا اذ ف

ةكبش ل ال طي طختال مسرلا

: الال ةكبش ال دادع دننتسما اذ مدختسي



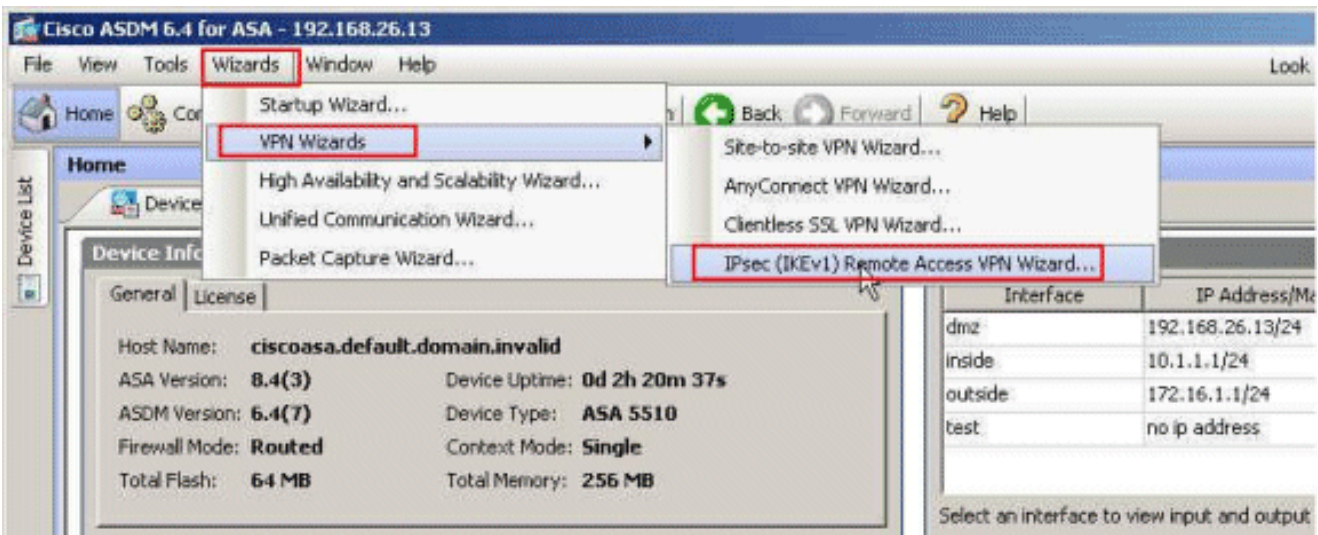
تنتزل اللى على routable ايجوز ليك شت اذه في لمعتسي ةطخ بطاخي سي ل ip ل: ةطخال م.
 ةئيب ربتخم في تلمعتسا ناك يا ناووع rfc 1918 مه

(IPsec) دع ب نع لوصولل VPN ةكبش نيوكت

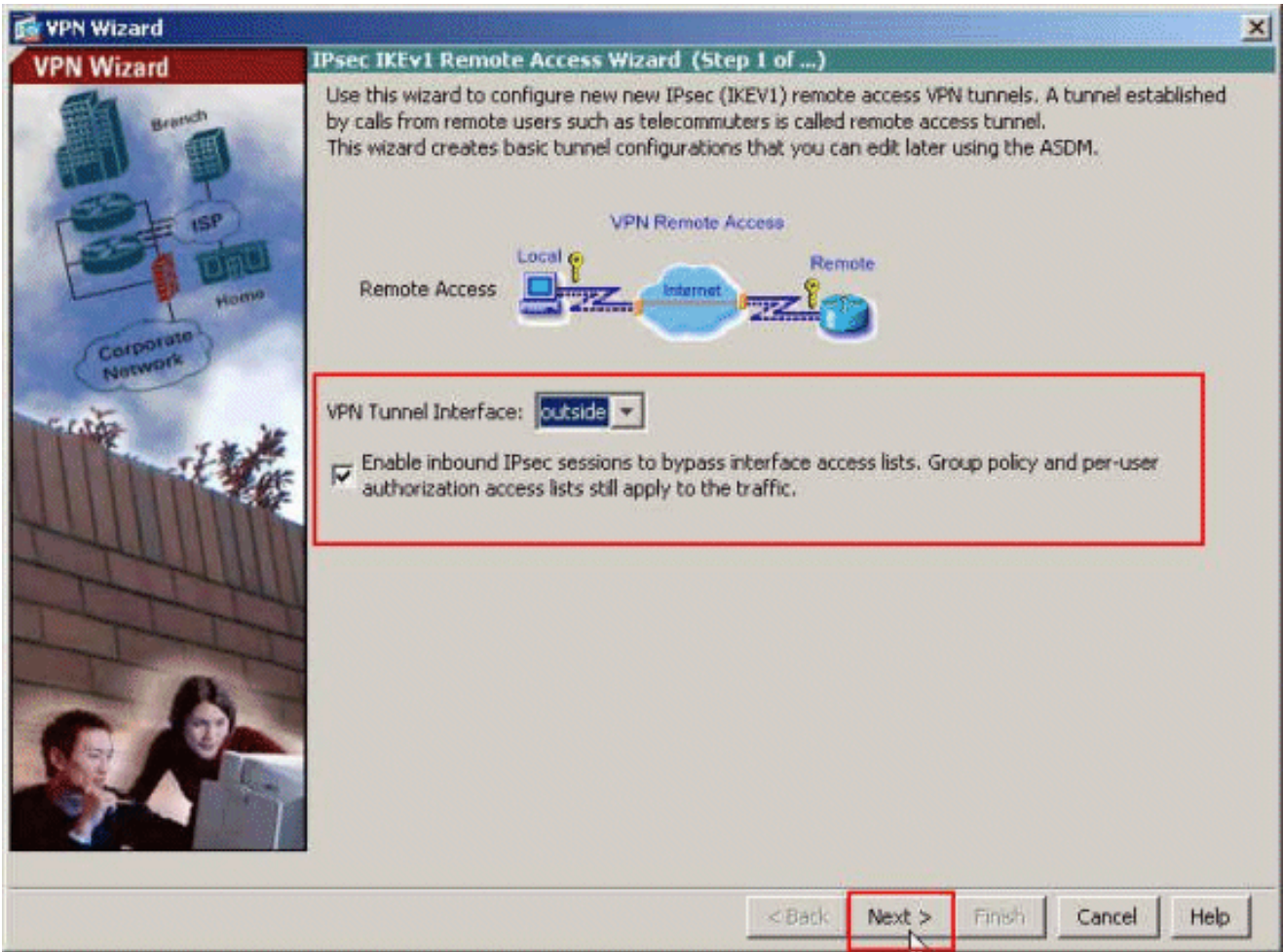
ASDM اءارء

VPN: دع ب نع لوصولل تلكش اذه تمأ

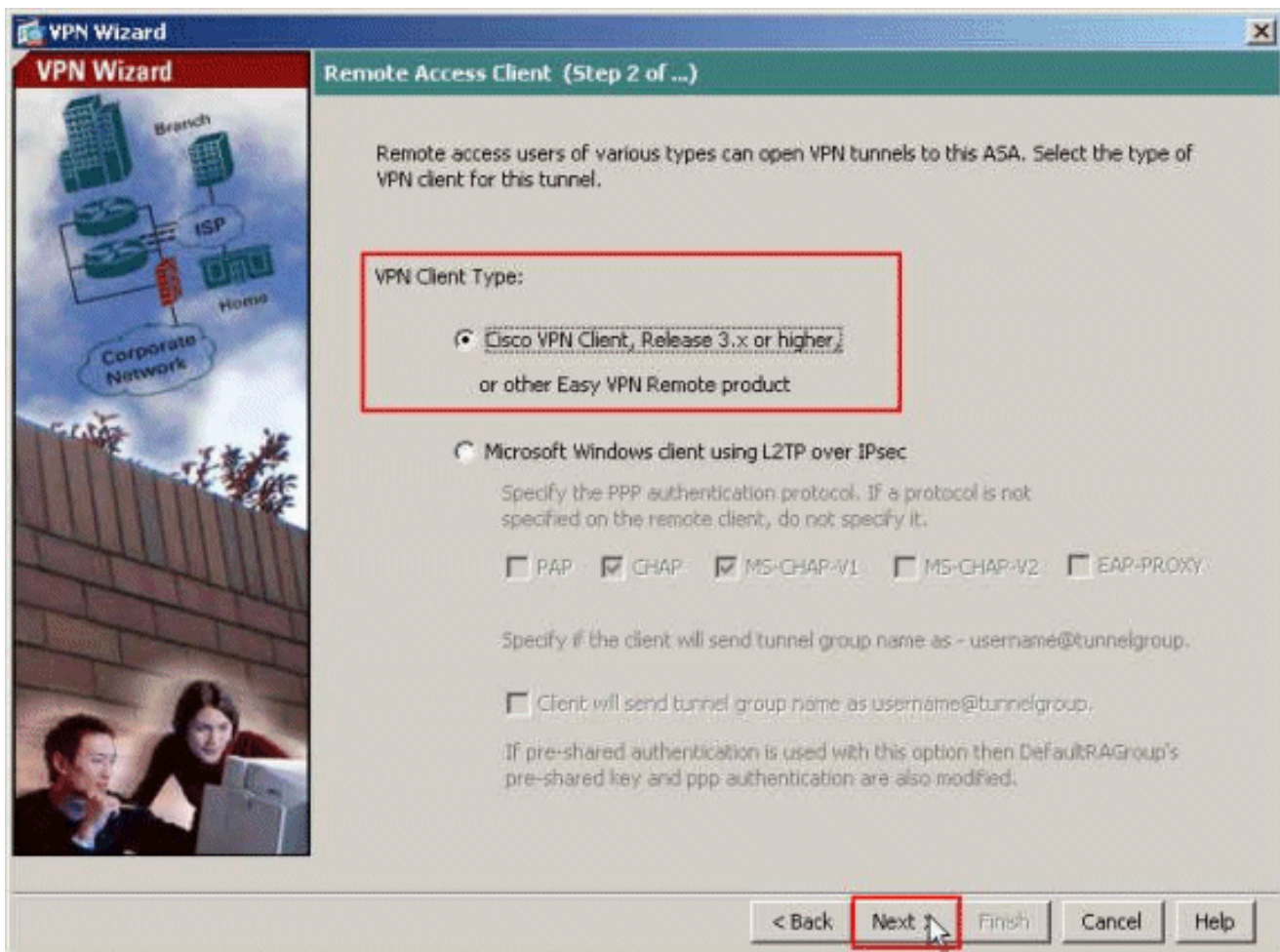
1. راطال نم دع ب نع لوصولل VPN ءلام (IPsec (IKEv1 > VPN ءلام > ءاعلام لادح
 .يسيرل



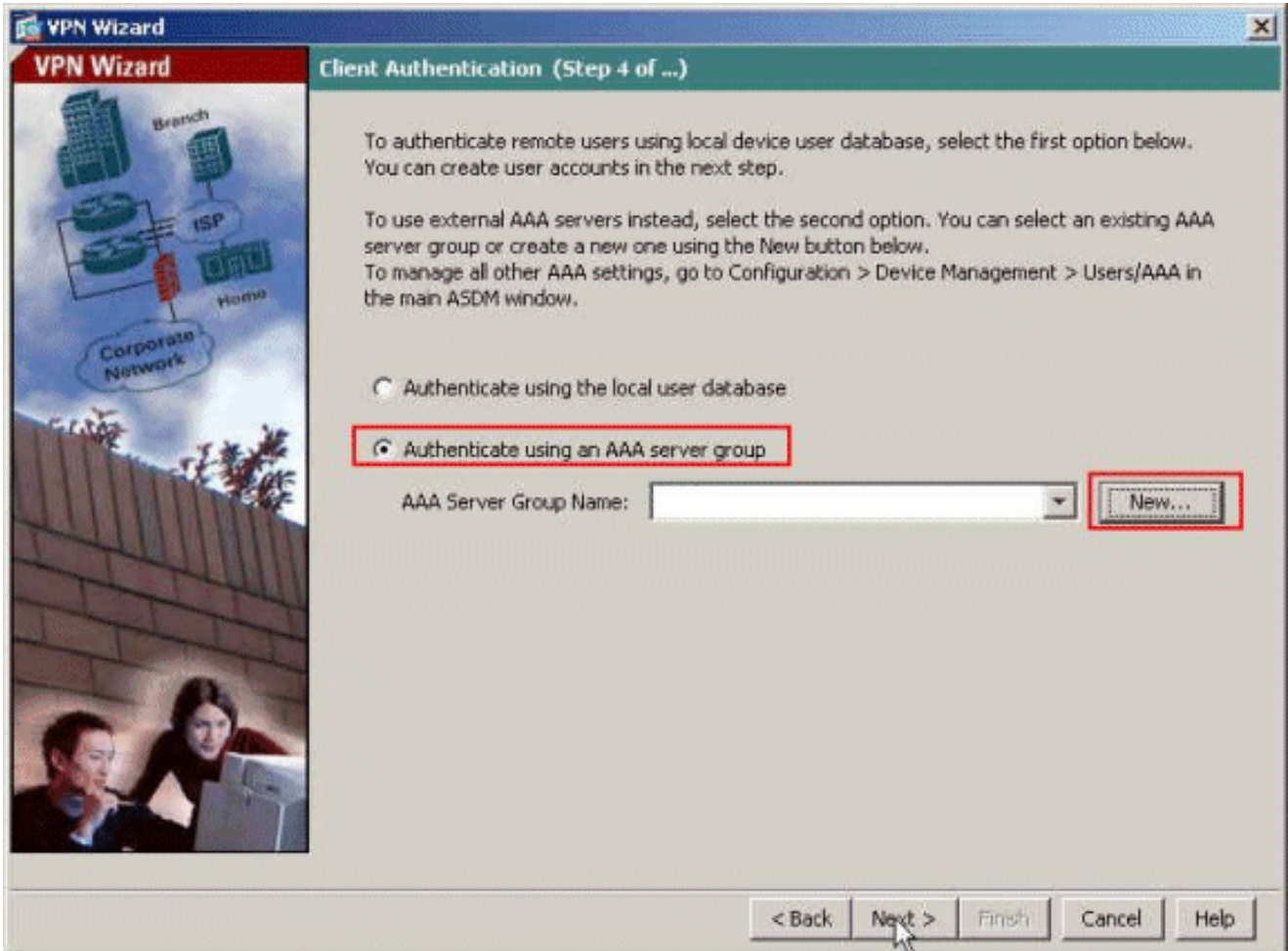
2. نأخ ديدحت نم اضيأ دكأتو، (لاثلما اذه يف، يجرأخ) بولطم وه امك VPN قفن ةهجاو ددح ةهجالا لىلا لوصولا مئاقوق زواجتل ةدراولال IPsec لمع تاسلج نيكمت ل ةرواجملا رايخالالا



3. Next3 قوف رقنا. لىلعأ وأ 3.x قالاطلا، نوبز VPN cisco نأ امب عون نوبز VPN لال تارتخأ (يلالالا).



4. يه انه ممدختسملا ةقداصملا ةقيرط . ةقداصملا تامولعم رفوو ةقداصملا بولسأ رتخأ . ةرفوتملا ةحاسملا يف قفنلا ةعومجم مسا ريفوتب اضيأ مق . اقبس م كرتشم حاتم ممدختسملا قفنلا ةعومجم مسا او Cisco123 وه انه ممدختسملا اقبس م كرتشملا حاتملا (يلالاتلا) Next قوف رقنا . Cisco-Tunnel وه انه



6. هة اول مس او مداخل ل IP ن اون عو ة قدا صم ل لوك و توربو مداخل ة عوم جم مس ا ري فوتب مق قفاوم رقاو ، ة رفوت م ل ة لبا ق م ل ا حاس م ل ا ي ف مداخل رس حات فمو .

New Authentication Server Group [X]

Create a new authentication server group containing one authentication server. To add more servers to the group or change other AAA server settings, go to Configuration > Device Management > Users/AAA > AAA Server Groups.

Server Group Name:

Authentication Protocol:

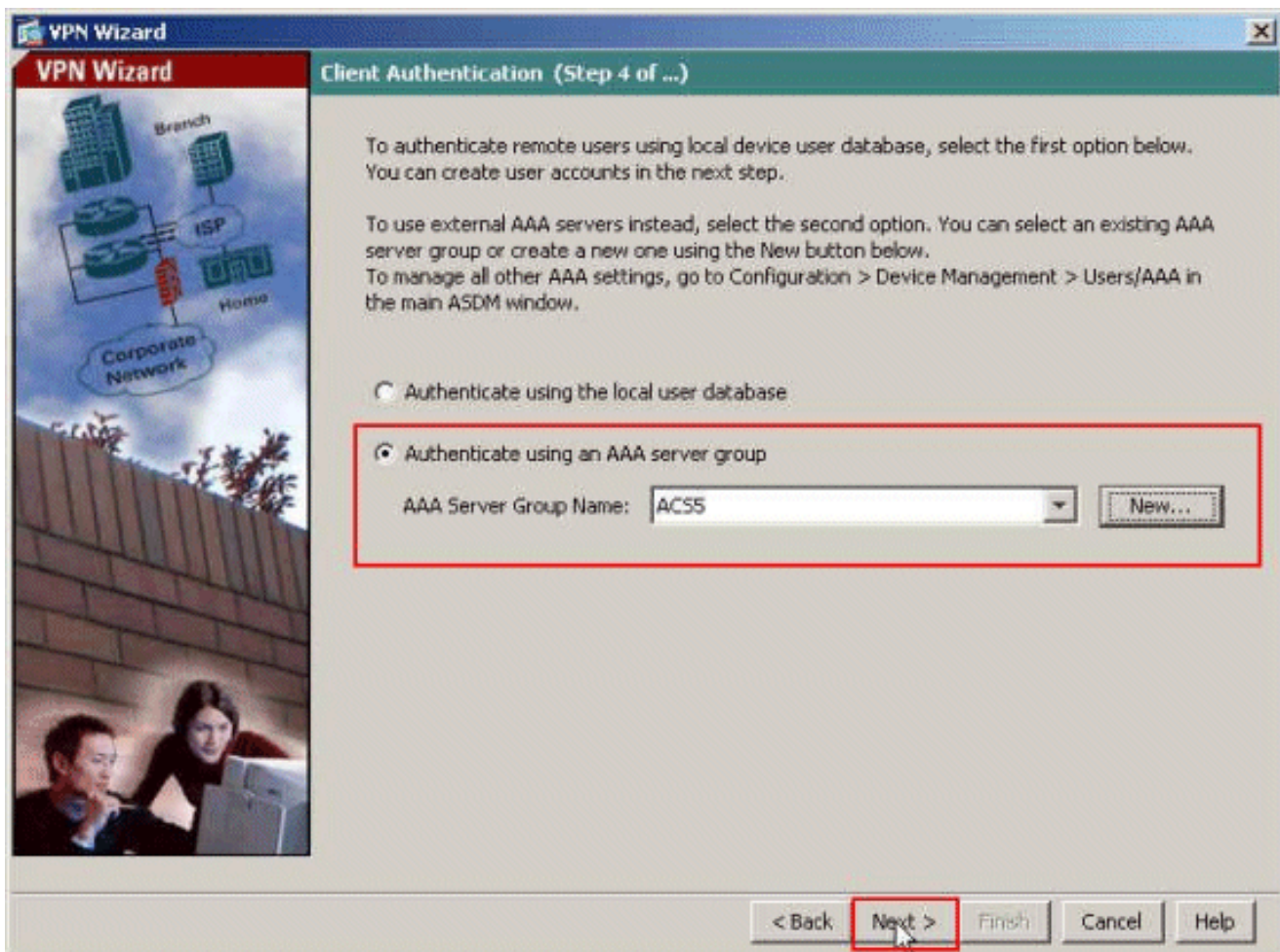
Server IP Address:

Interface:

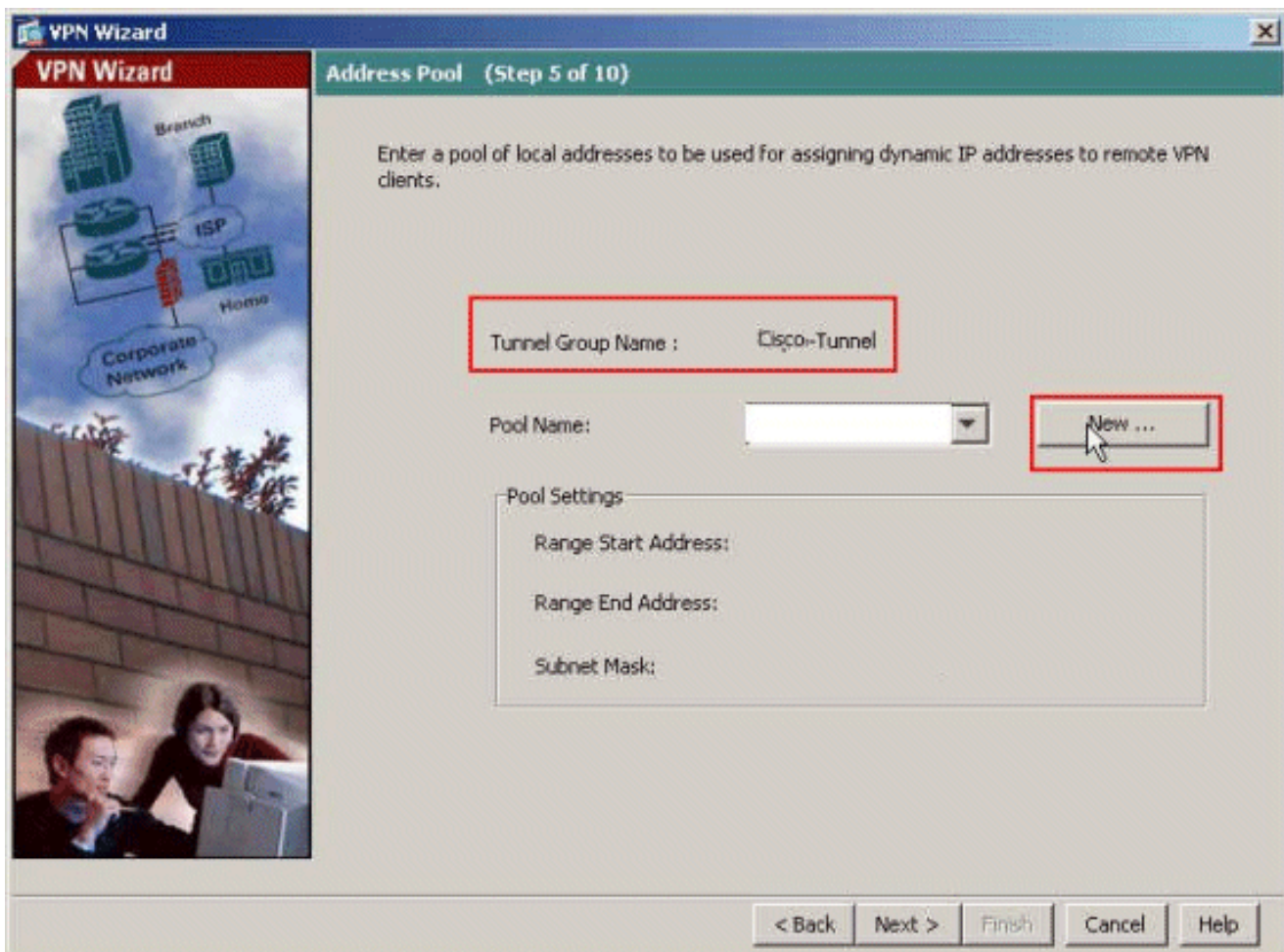
Server Secret Key:

Confirm Server Secret Key:

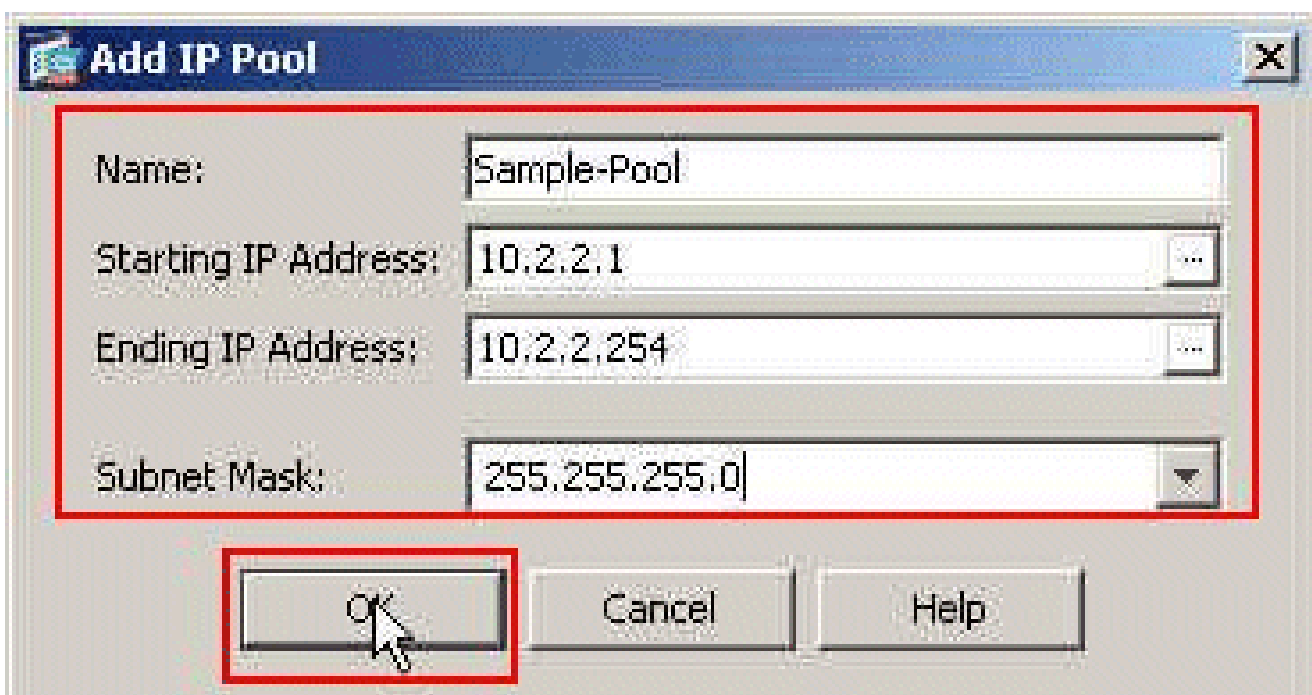
7. (يلاتلا) Next قوف رقنا



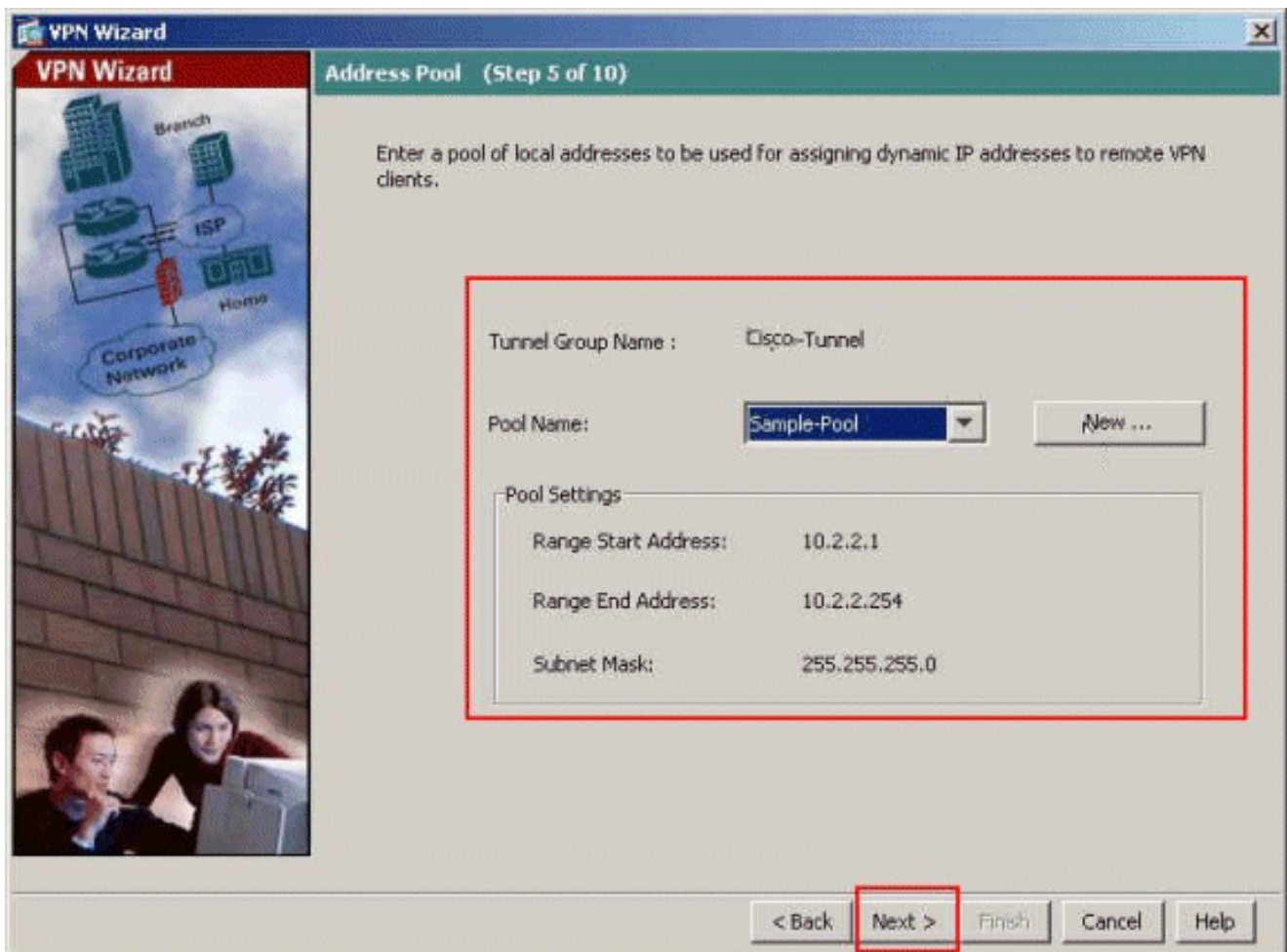
VPN8. تاكبشءالمعل ايكيمايديد اهنبيعت متيل لةلحمل لانيوانعل نم ةومجم دح
يلحم ناوع نم ةكرب ديدج تقلخ in order to ديدج تقلط. اهلصت ادنع ةديعل



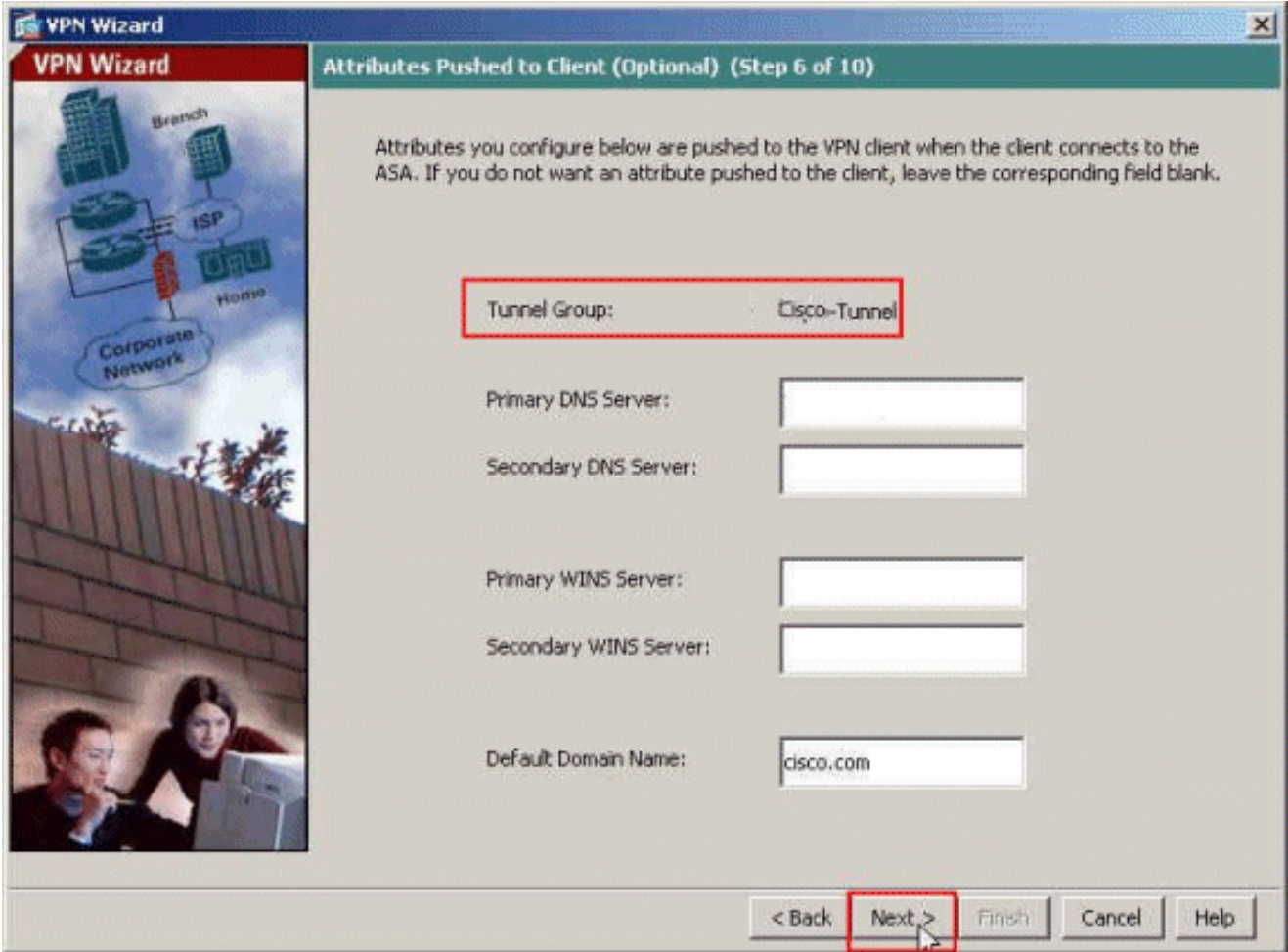
9. IP ناونع اهانو، IP ناونع ادبو، عمجتال مسا ريفوتب مق، IP عمجت ةفاض اذفان يف OK قوف رقناو. ةيعرفال ةكبشلال عانقو.



10. وه لاثملا اذهل عمجتال مسا .يلال رقناو، ةلدسنملا ةمئاقلا نم عمجتال مسا دح 9. ةوطخلال يف هؤاشنلا مت يذال عمجت جذومن.



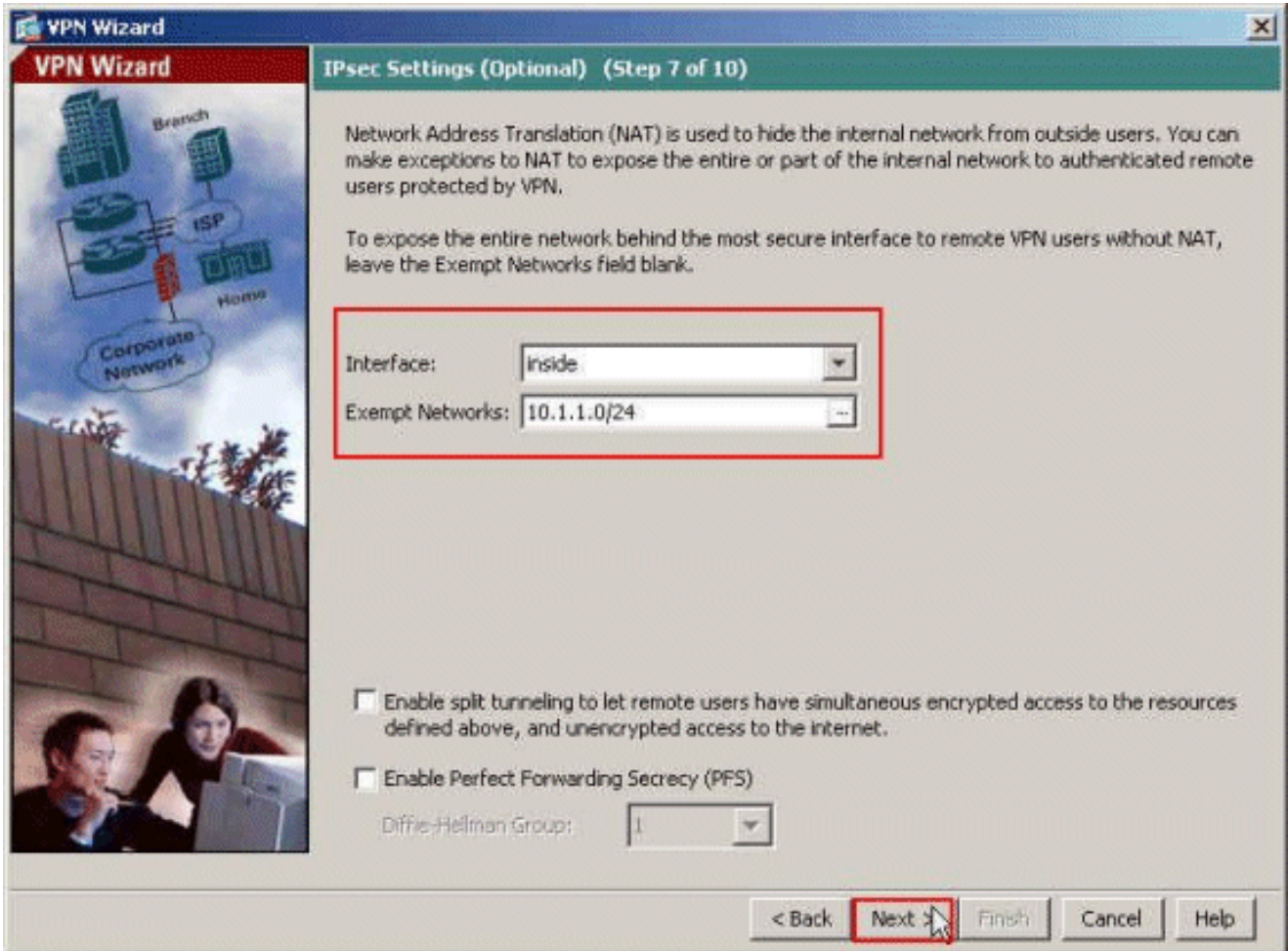
VPN11ءالمع ىل هعفد متيل يضا رتفا لاجم مساو WINS و DNS م داخ تامولعم دح :يراي تخا
ةديع ل



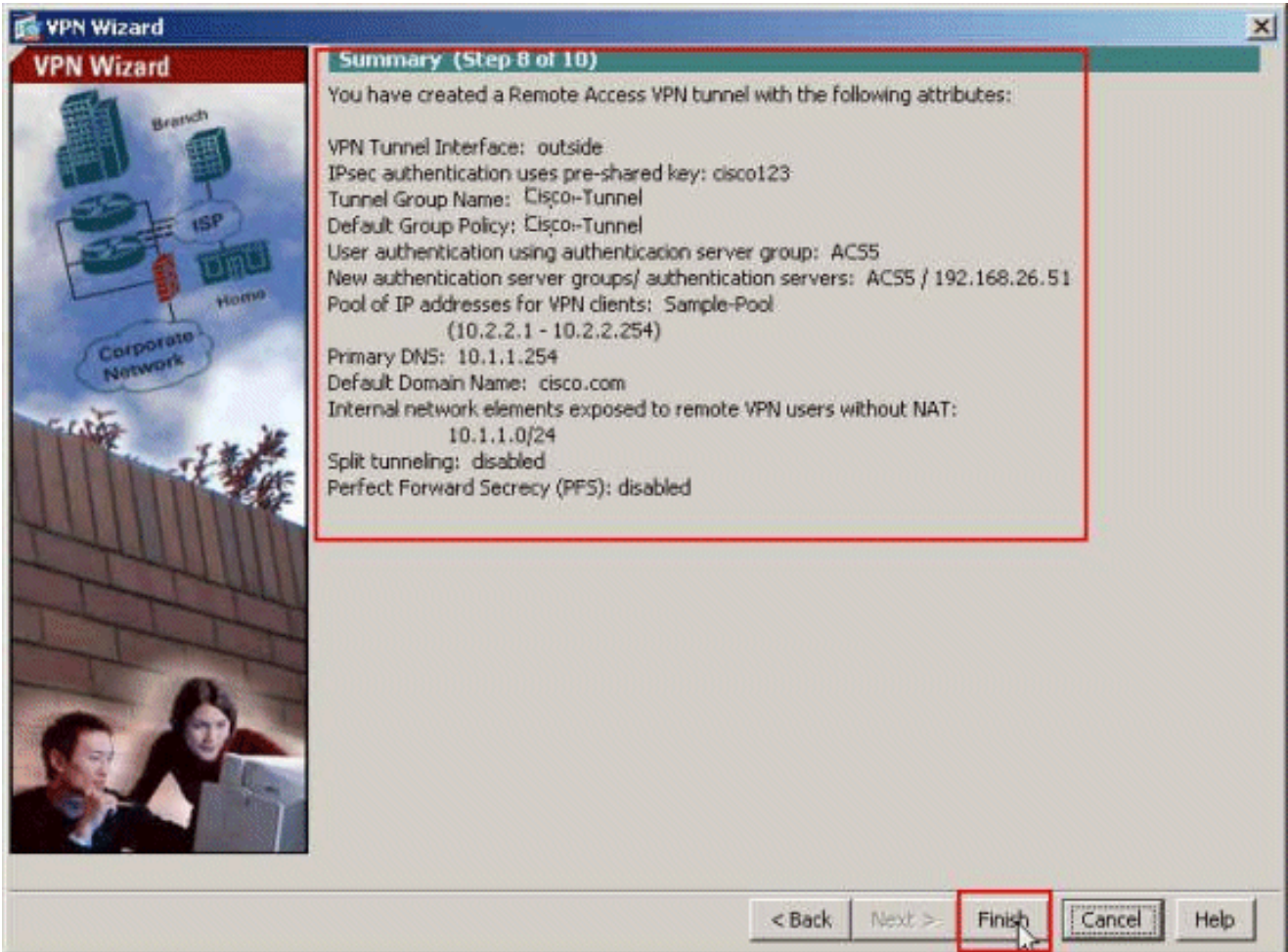
12. اه فيرعت متي نأ بجي ، تدجو نإ ، تاك بشلا وأ ةي لخادلا ة في ضملا تائي بل ا ي ا دح
 مسا نراقلا ريفوت دع ب كلذ دع ب تقطقط . ةديع بل VPN تاك بش ي مدختس مل
 لاجم ةك بش اناثتسالا ي ف تي نثتسا نو كي نأ تاك بشلاو

ةك بش لخاد لمالكلا ذفني نأ لمعتسم VPN دي عب حمسي وه ، غراف ةمئاق اذه تنأ كرتي نإ
 ل ASA نم

يقفنلا لاصتالا موقوي . ةذفان اذه يلع tunneling ماسقنا تنكم اضي ا عيطتسي تنأ
 اارجالا اذه ي ف اقبسم ةدحمل دراوملا يلا تانا ي بل رورم ةكرح ريفش ت مسقنملا
 ةكرحل تاونق عاشن ا مدع لالخنم ماع لكشب تنرتنالا يلا رفشم ريغ لوصو ريفوتو
 VPN دي عب نم رورم ةكرح لك ، نو كي tunneling ماسقنا نكمي ال نإ . هذه تانا ي بل رورم
 ا جلاع و ادج اضي رع ايدررت ا قاطن كلذ لكشي نأ نكمي . ل ASA ل ا قافنأ لمعتسم
 كيدل ةئيهتلا ةي لمع يلع انا ب كلذو ، افثكم



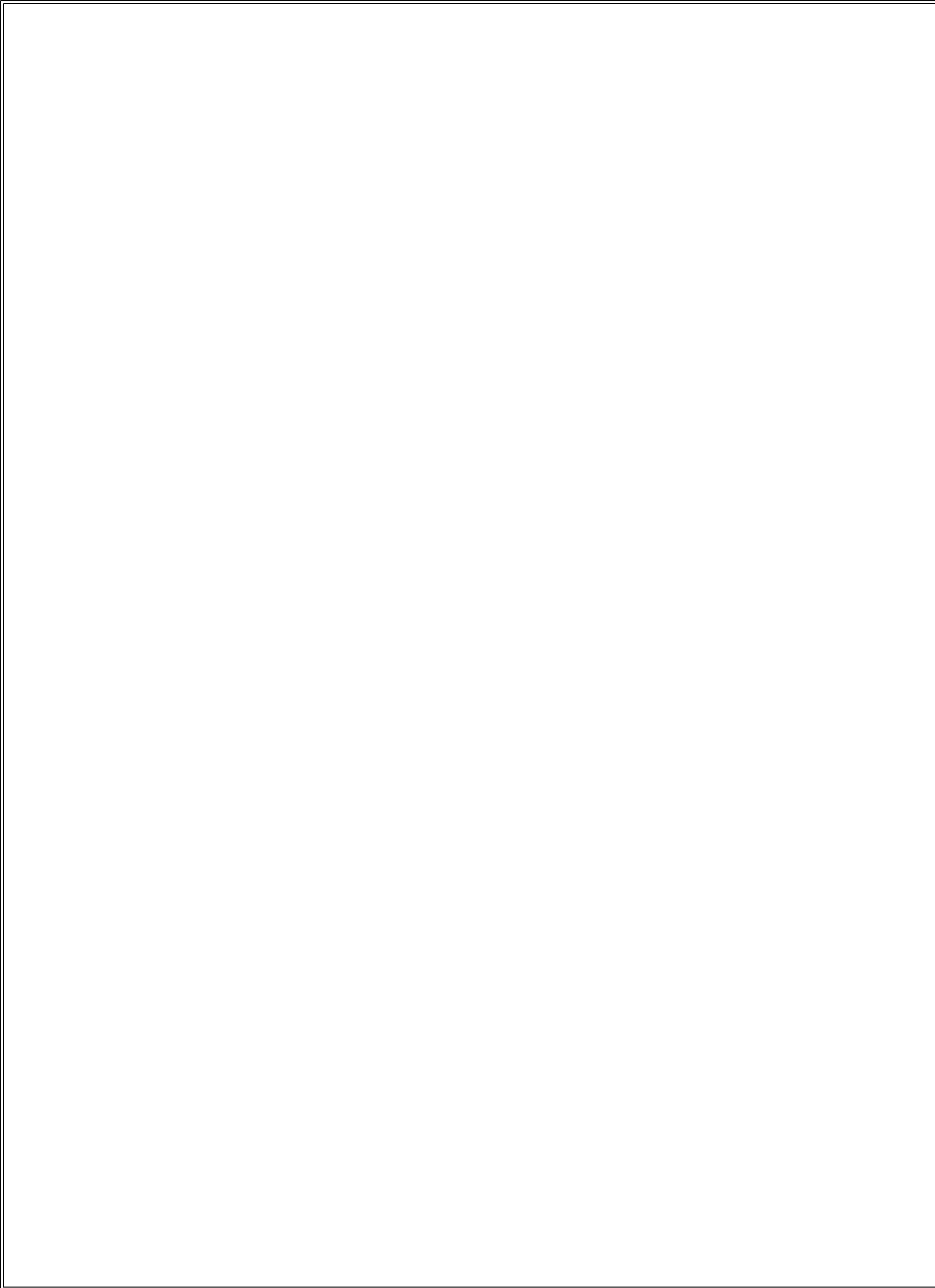
13. مع ايضار تنك اذا عاهن قوف رقنا. اهتذختا يتلا تاءارجال اصخلم ةذفانلا هذه ضرعت
كب صاخلا نيوكتلا



CLI مداخلت سبب ASA نيوكت

CLI نيوكت وه اذه

تمت



!--- Create the AAA server group "ACS5" and speci

!--- PHASE 2 CONFIGURATION ---! !---

!--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policies defined with all the perm

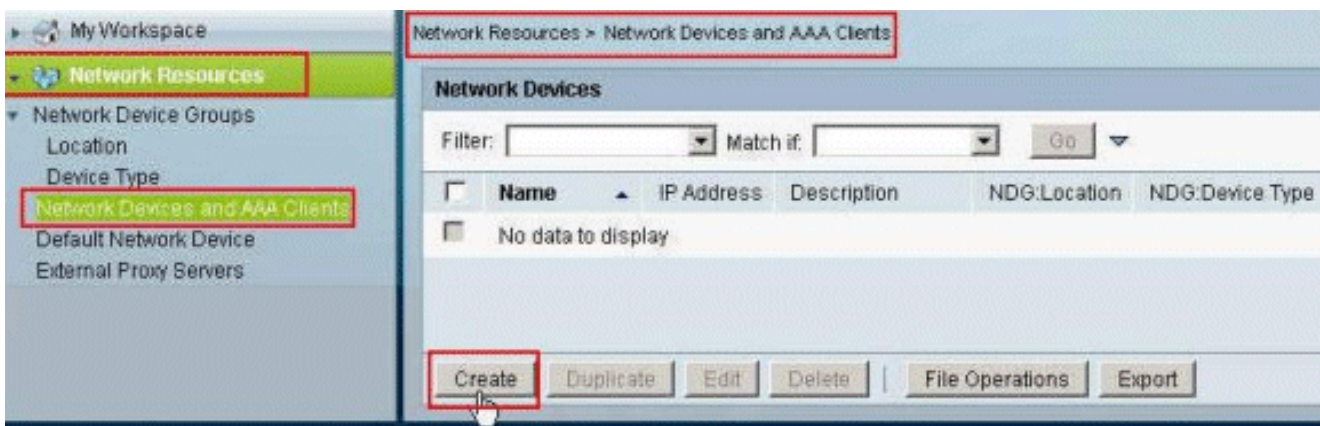
مدخستسملل ليزنللة لباقلال (ACL) لوصولال يف مكحتلال ةمئاقل ACS نيوكت يدرفال

تانوذا نئاكك Cisco Secure ACS 5.x لىل ليزنللة لباقلال لوصولال مئاقل نيوكت كنكمي نم جئاتنلال مسق يف هرايخا متيس يذلا ضيوفتلال فيرعت فلم لىل هنييعة مثة امسم لوصولال ةمدخ يف ةدعاقال

RADIUS مداخل لسريو، حاجنب IPsec ل VPN ةكبش مدخستسم ةقداصم متت، لاثمال اذه يف مداخل لوصولال "cisco" مدخستسملل نكمي. نامألا زاهج لىل ليزنللة لباقلال لوصولال ةمئاق (ACL)، لوصولال يف مكحتلال ةمئاق نم ققحتلل. رخأال لوصولال عيمج ضفريو طقف 10.1.1.2. [ةومجملال/مدخستسملل ليزنللة لباقلال \(ACL\) لوصولال يف مكحتلال ةمئاق](#) مسق عجار

ACS 5.x نمأي cisco يف نوبز RADIUS تلكش steps in order to اذه تمتأ

1. لال لخدم تفصأ in order to ققخي ةقطقو، نوبز AAA و ةادأ ةكبش > دروم ةكبش ترتخأ. تايطعم ةدعاق لدان RADIUS لال يف ASA.



192.168.26.132 تلخد كلذ دعب، (لاثلما اذه يف asa-ةنيع) لال ل مهم يلحم مسال تلخد RADIUS لال صحف يف ب مسق راخي ةقداصملا يف RADIUS ترتخأ. لاجم ناوئعلا يف لال سرا لىل رقنا. لاجم رس كراشي لال ل Cisco123 لخدأو قودنص قيقت

Network Resources > Network Devices and AAA Clients > Create

Name:
 Description:

Network Device Groups
 Location:
 Device Type:

IP Address
 Single IP Address IP Range(s) By Mask IP Range(s)
 IP:

Authentication Options
 TACACS+
 Shared Secret:
 Single Connect Device
 Legacy TACACS+ Single Connect Support
 TACACS+ Draft Compliant Single Connect Support

RADIUS
 Shared Secret:
 CoA port:
 Enable KeyWrap
 Key Encryption Key:
 Message Authenticator Code Key:
 Key Input Format ASCII HEX/DECIMAL

3. (ACS) RADIUS مداخل تاناي ب دةعاق ىل اءا بنب ASA ةفاضا م ت

Network Resources > Network Devices and AAA Clients

Network Devices

Filter: Match if:

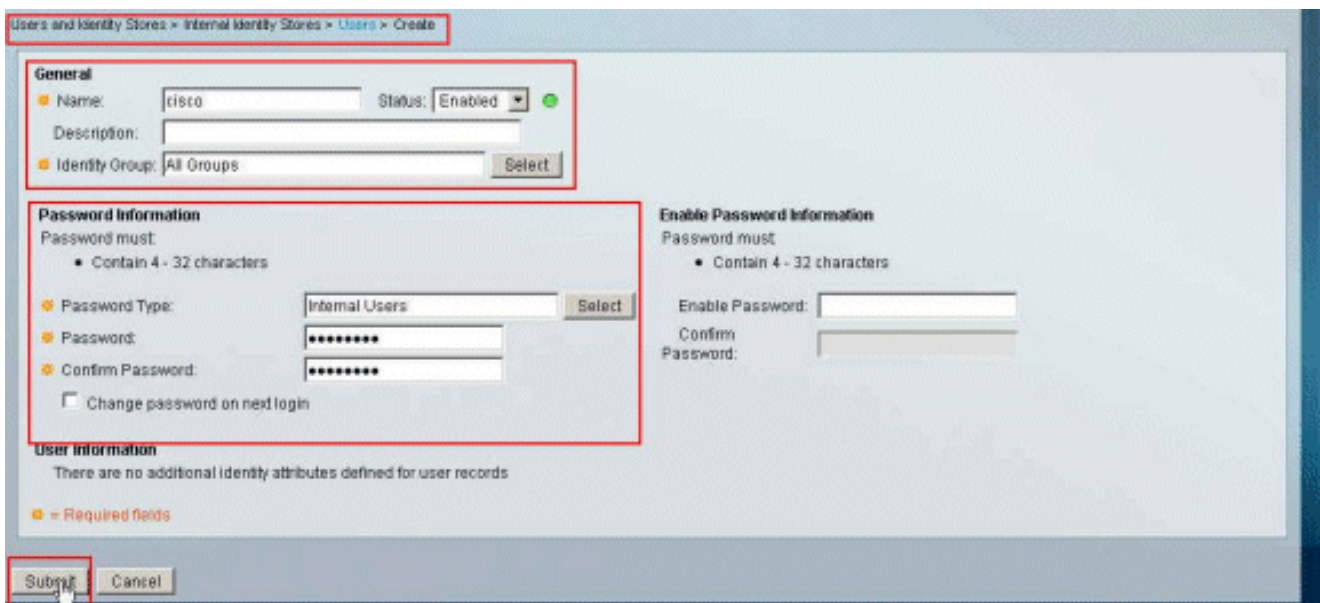
<input type="checkbox"/>	Name	IP Address	Description	NDG:Location	NDG:Device Type
<input checked="" type="checkbox"/>	<u>sample-asa</u>	192.168.26.13/32		All Locations	All Device Types

|

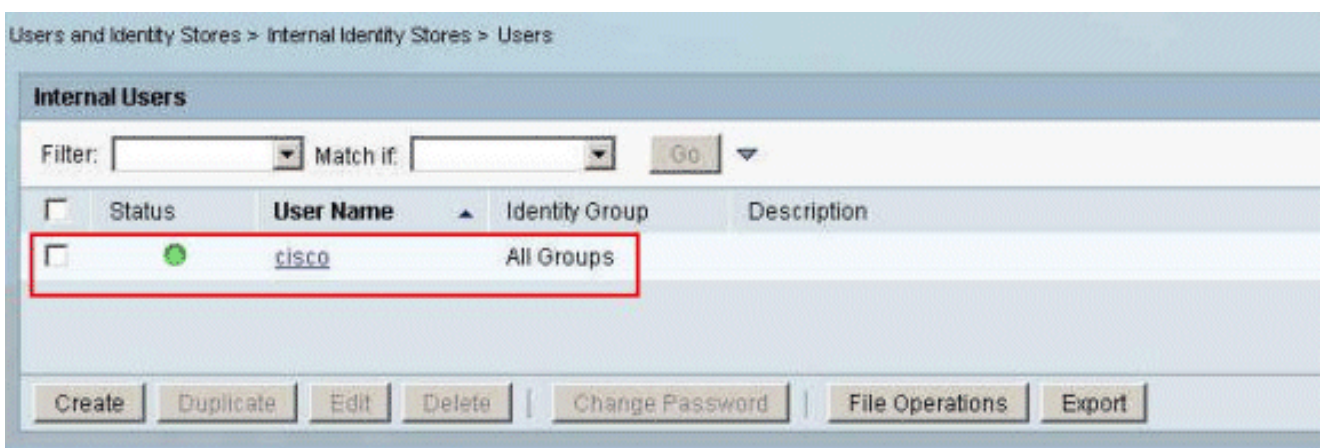
4. in order to ق لخي ة ق ط ق ط و ، لم ع ت س م > ن ن خ ي ة ي و ه ي ل خ ا د > ي و ه ن ز ا خ م و ل م ع ت س م ت ر ت خ ا ة ي و ه ة ح ص ل ACS ل VPN ل ا ن م ي ل ح م ت ا ي ط ع م ة د ع ا ق ل ا ي ف ل م ع ت س م ت ق ل خ



5. عم لك لخدأو، نني لخداد نني مدخت سمك رورملا عم لك عون دح. Cisco مدخت سملا مسا لخدأ لاسرا رقناو، رورملا عم لك ديك أتب مق. (لثمل اذه يف، Cisco123) رورملا

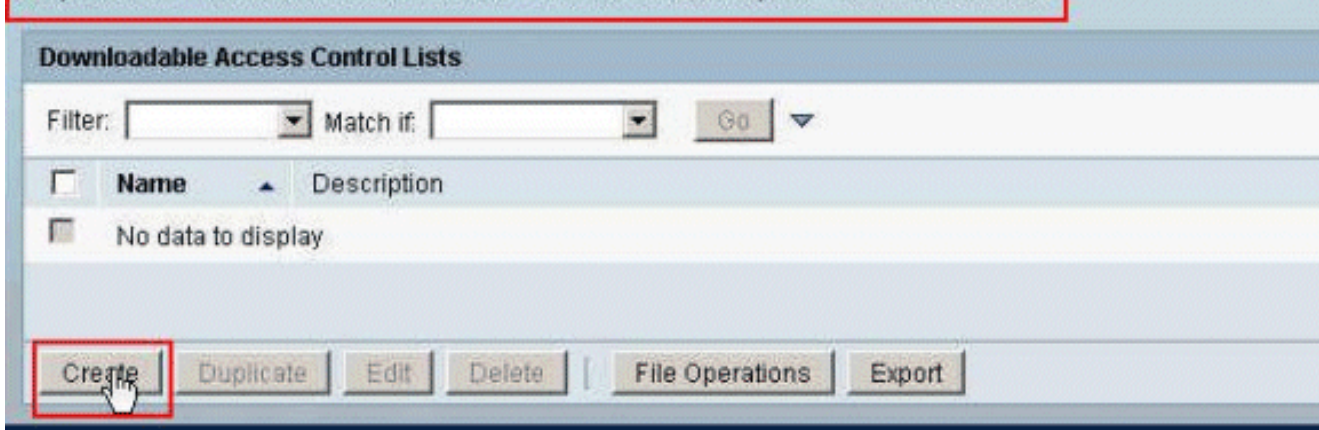


6. حاجن ب cisco مدخت سملا عاشنإ مت



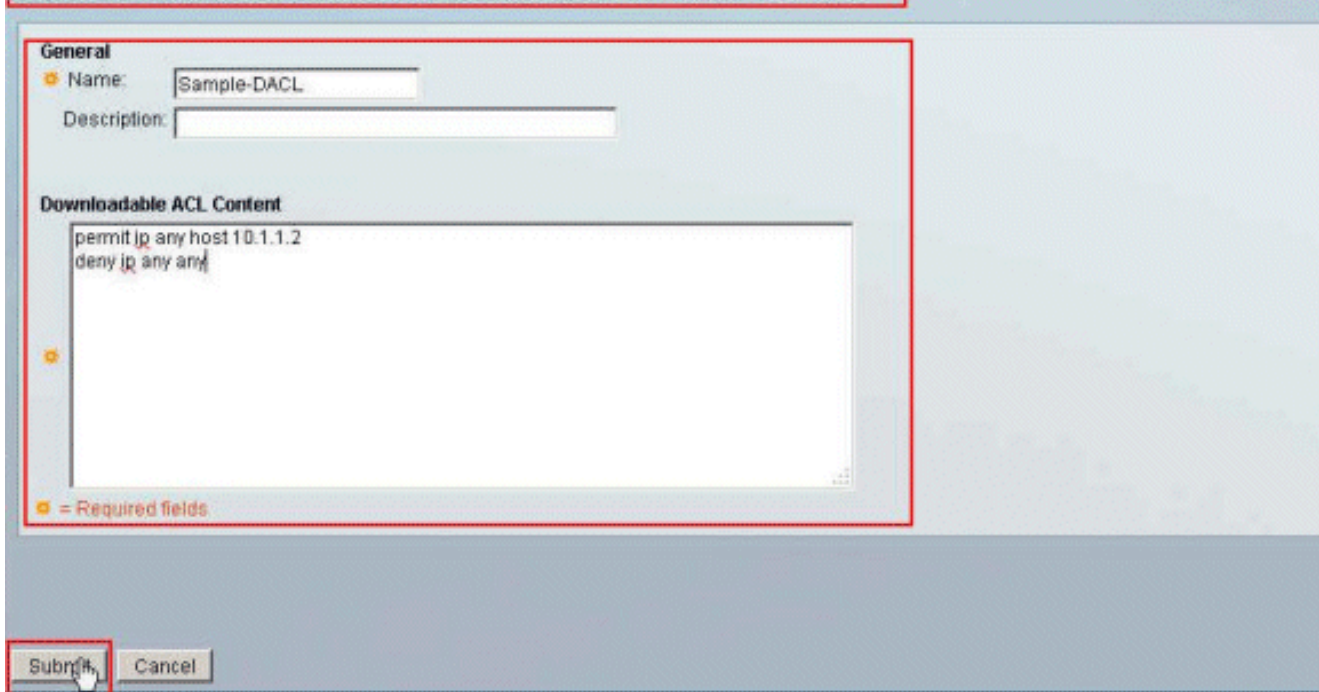
7. > جهنلا رصانع رتخأ، ليزنتلل ةلباق (ACL) لوصولا يف مكحت ةمئاق عاشنإل (ACL) لوصولا يف مكحتلا مئاق > ةام سملا تانوذال تانئاك > تانوذال او ضيوفتلا عاشنإ قوف رقناو، ليزنتلل ةلباقلا

Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs



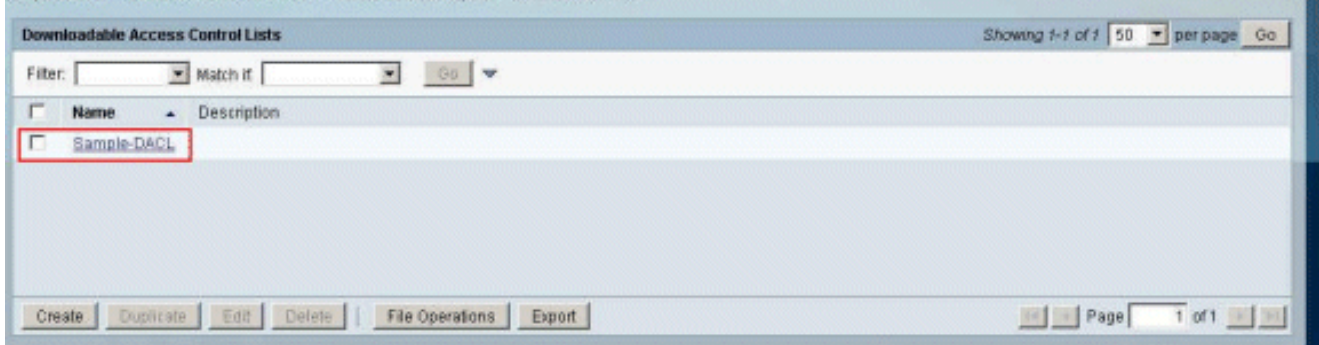
8. إلى إضافة إلاب ، لي زنت لل ةلباق ال (ACL) لوصول ا في مكحت ال ةمئاق مس ا ريفوت ل. اسرا لى لى رقنا . (ACL) لوصول ا في مكحت ال ةمئاق يوتحم

Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs > Create



9. ا جانب DACL ا ذومن لى زنت لل ةلباق ال (ACL) لوصول ا في مكحت ال ةمئاق عاشنا م تي

Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs



10. ا ذفنا م ةسايس ا ذفنا م ، ةي وه ةحص Access-Policy for VPN ا لكش in order to ا ترتخ ا اذ ف RADIUS لوكوتورب لى ا مدخت ةمدخ ةمدخ ا ا تدحو ، ةدعاق ا دي دحت ةمدخ ةمدخ ا م دخ

يضارت فالإلة كبشلال إلى لوصولي بلللسو، RADIUS عم 1 ةءاقلال قباطت، لالالم
RADIUS بلط

Access Policies > Access Services > Service Selection Rules

Single result selection Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	Status	Name	Protocol	Conditions	Results	Hit Count
1	<input type="checkbox"/>	Rule-1	match Radius		Default Network Access	0
2	<input type="checkbox"/>	Rule-2	match Tacacs		Default Device Admin	0

Default If no rules defined or no enabled rule matches. DenyAccess 0

Create... Duplicate... Edit Delete Move to... Customize Hit Count

Save Changes Discard Changes

11. لوصولو ماءءلسإ مءي، لالالم اءه ي ف 10 ةوطءلال نم ةءءءم لوصولو ةمءء رءءأ
نم ءكأءو، اءب ءومسمل الوكوءوربل ال بوبءلال ةمالع رءءأ. ةكبشلال إلى يضارت فالإ
للسرل قوف رقنل. MS-CHAPv2 ب ءامسلالو PAP/ASCII ب ءامسلال ءيءء

General **Allowed Protocols**

Process Host Lookup

Authentication Protocols

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow LEAP

Allow PEAP

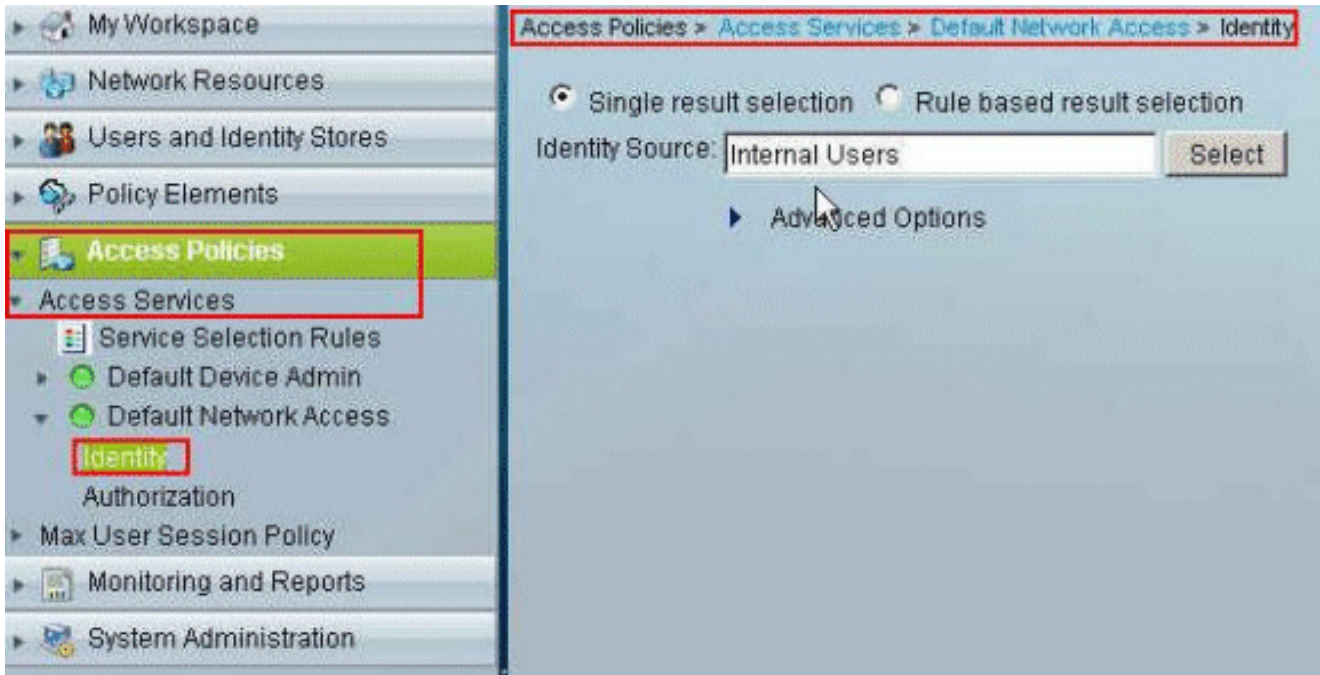
Allow EAP-FAST

Preferred EAP protocol LEAP

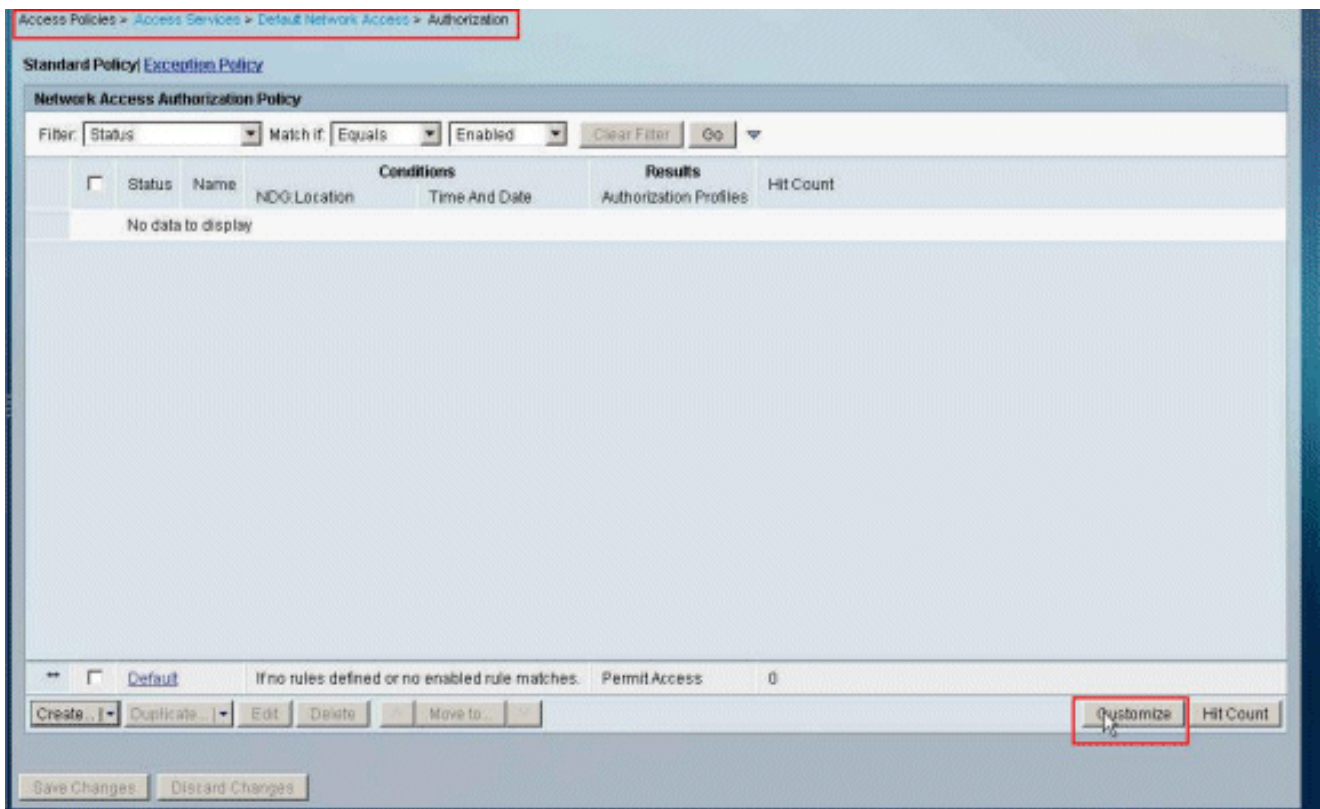
Submit

Cancel

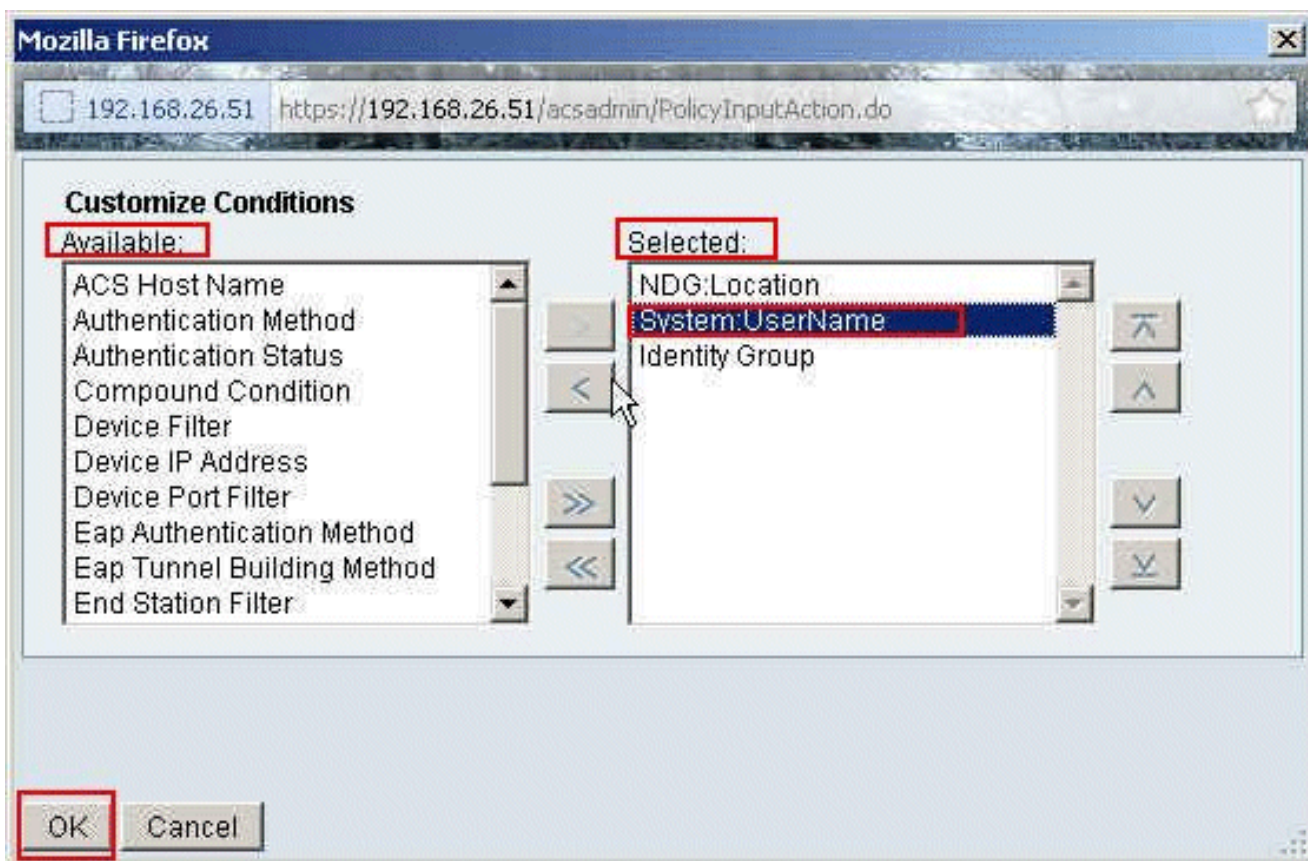
12. نبي لخال ادا نبي مدخت سمل ادي دحت نم دكأتو، Access تامدخ يف ةيوهال مسق قوف رقنا ةكبشلل يضارتهال لوصول انذخأ، لاثمل اذه يف ةيوه ردصمك.



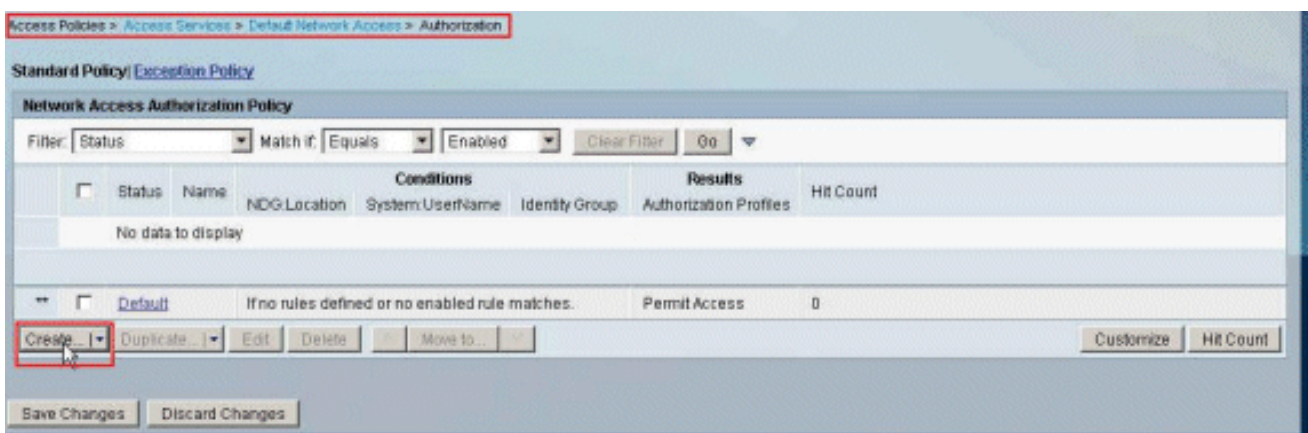
13. ضيوف التلا > ةكپشلل يضارت فالال لوصولال > لوصولال تامدخ > لوصولال تاسايس رتخأ صي صخت قوف رقناو.



14. OK. قوف رقناو، ددحمالادومعلالال رفوتمالادومعلال نم System:UserName لقون




15. ةديج ةدعاق عاشنإل عاشنإ قوف رقنا





16. ةمئاقلا نم يواسي رتخاو ، System:UserName ل ةرواجملا رايئتخال ةناخ ديحت نم دكأت Cisco مءختسملا مسا لخدأو ، ةلدس نملا

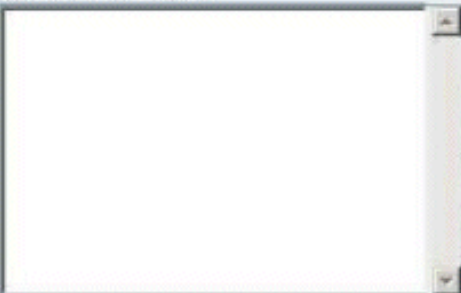


Cisco Secure ACS - Mozilla Firefox

192.168.26.51 https://192.168.26.51/acsadmin/PolicyInputAction.do

General
Name: Rule-2 Status: Enabled 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

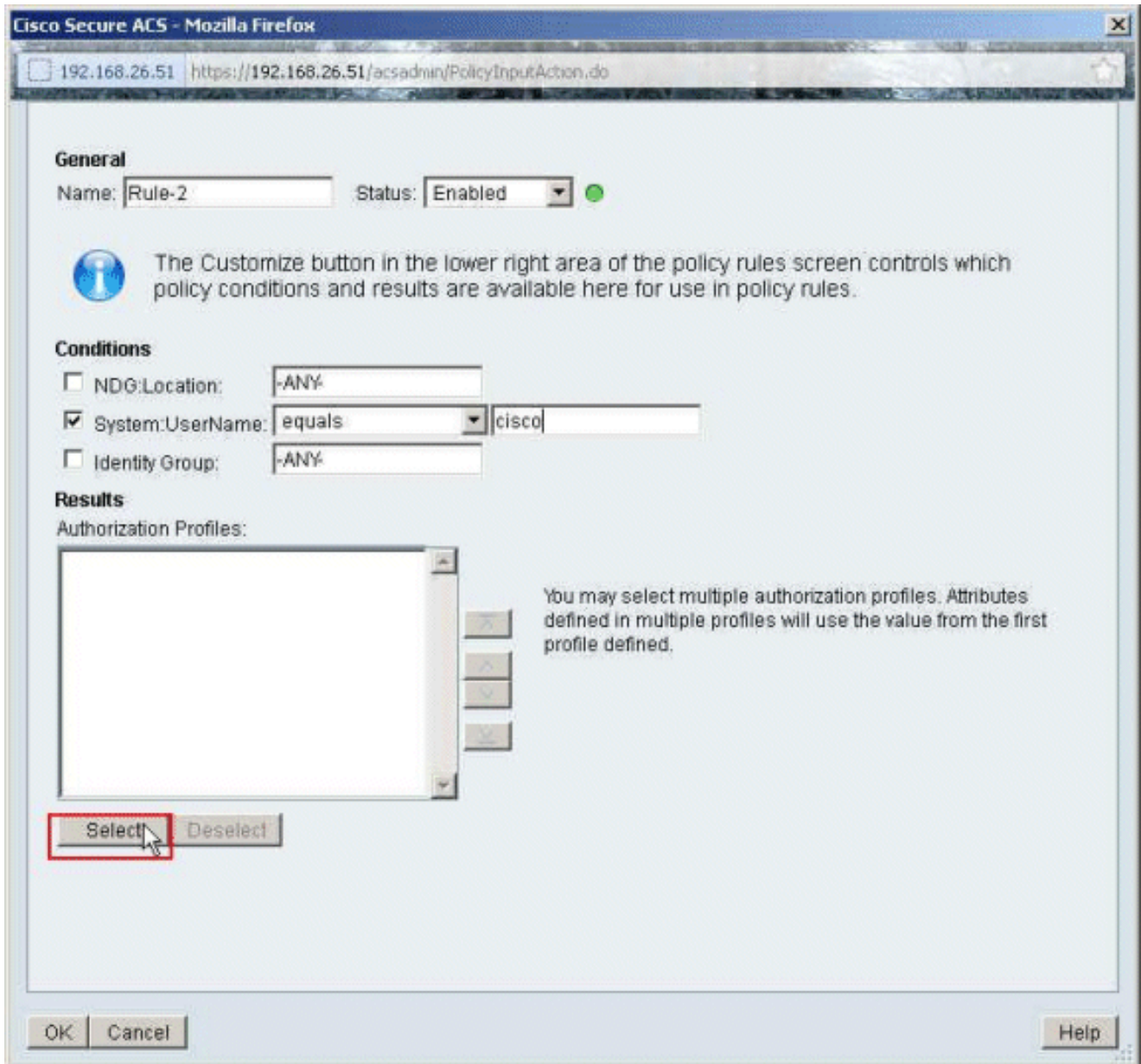
Conditions
 NDG:Location: -ANY
 System:UserName: equals  cisco
 Identity Group: -ANY

Results
Authorization Profiles:

 

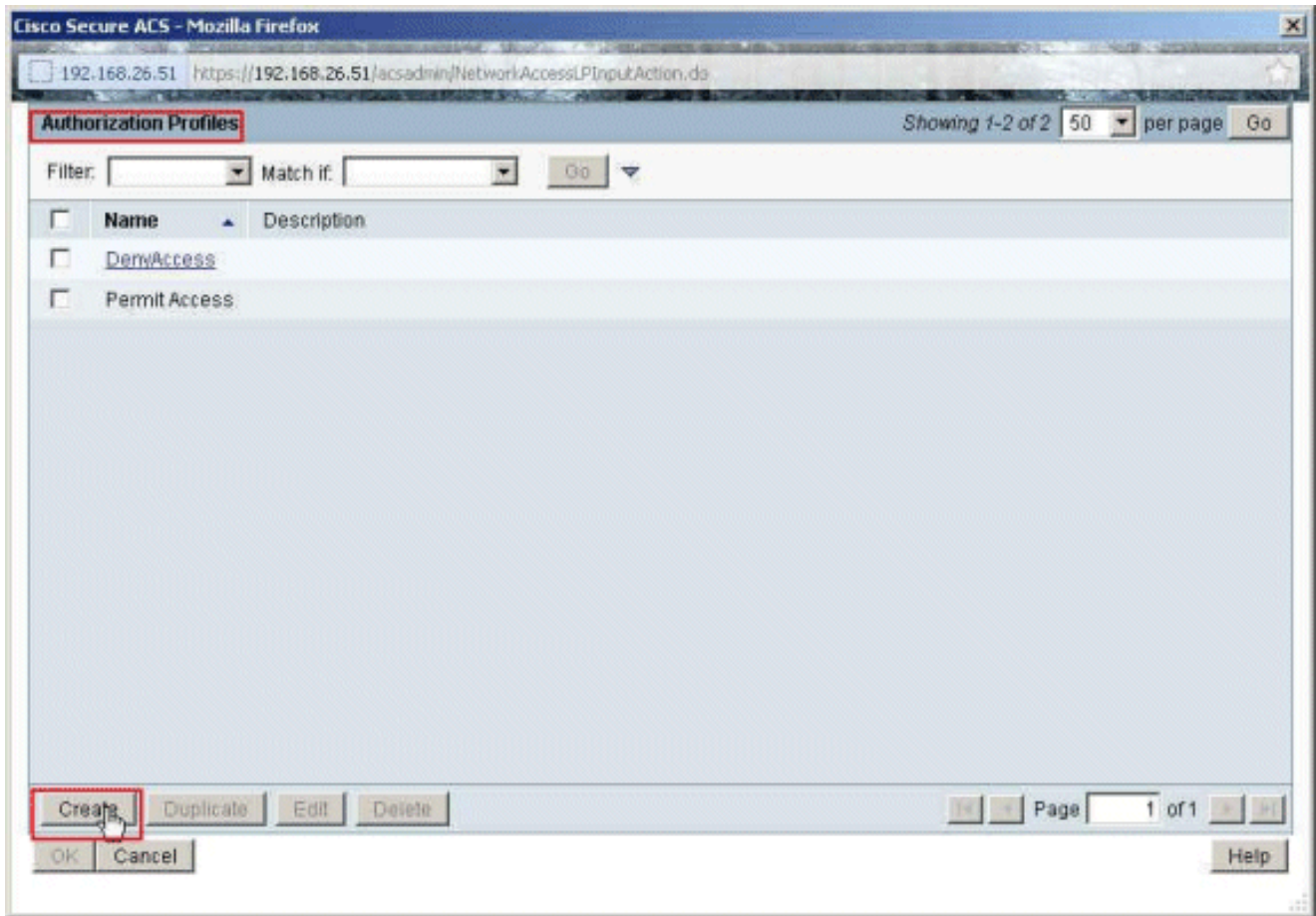
You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

OK Cancel Help

17. ديدحت قوف رقنا



18. دېدج لېوخت فيرعت فلم عاشن ال عاشن اىل ع رقنا



19. اذہ یف فی رعیت لال فلم چزوم ن مادختسا متی . لی وخت لال فی رعیت فل مل مسا ری فوت ب مق لال .

Cisco Secure ACS - Mozilla Firefox

192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do

General Common Tasks RADIUS Attributes

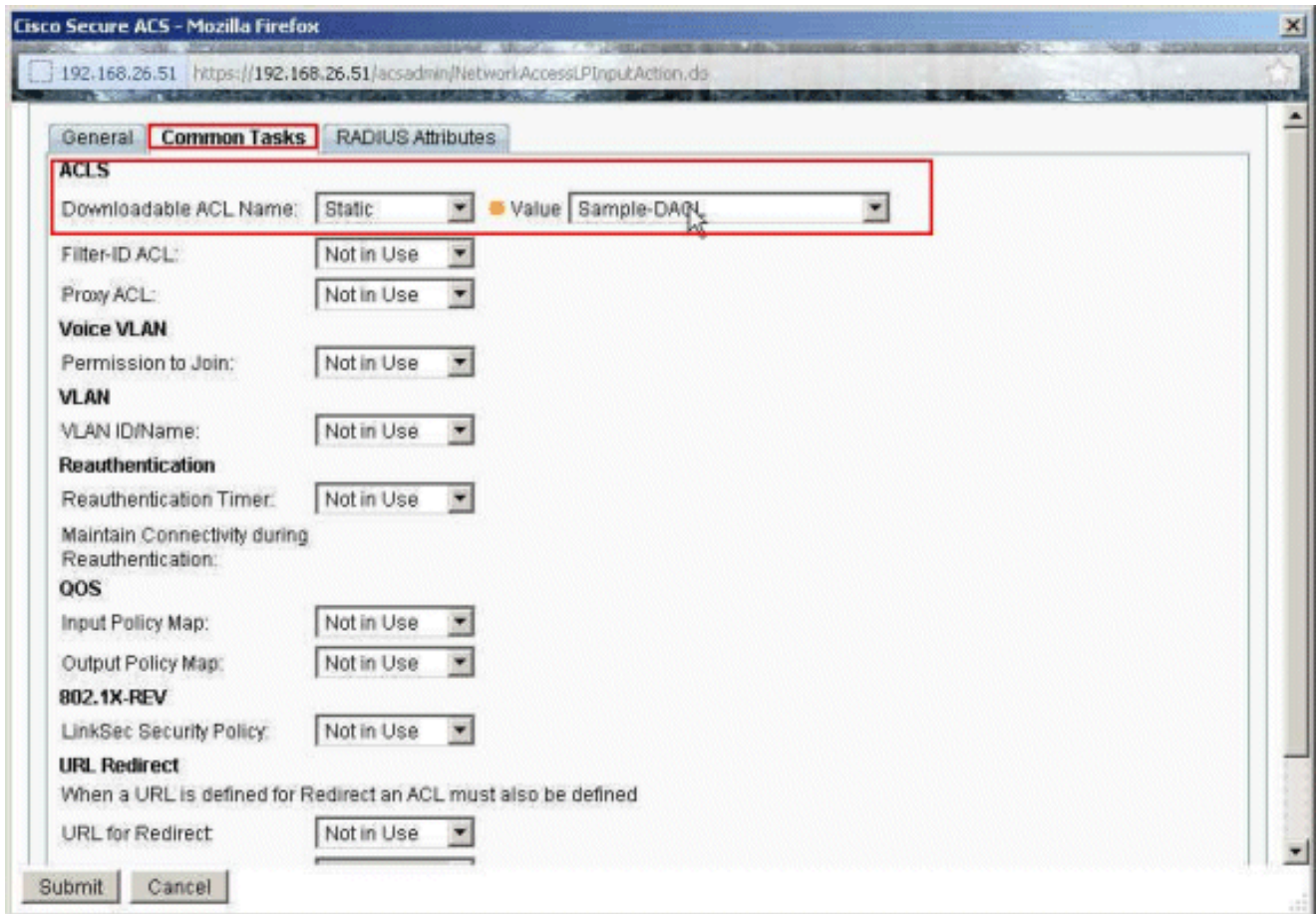
Name: Sample-Profile

Description:

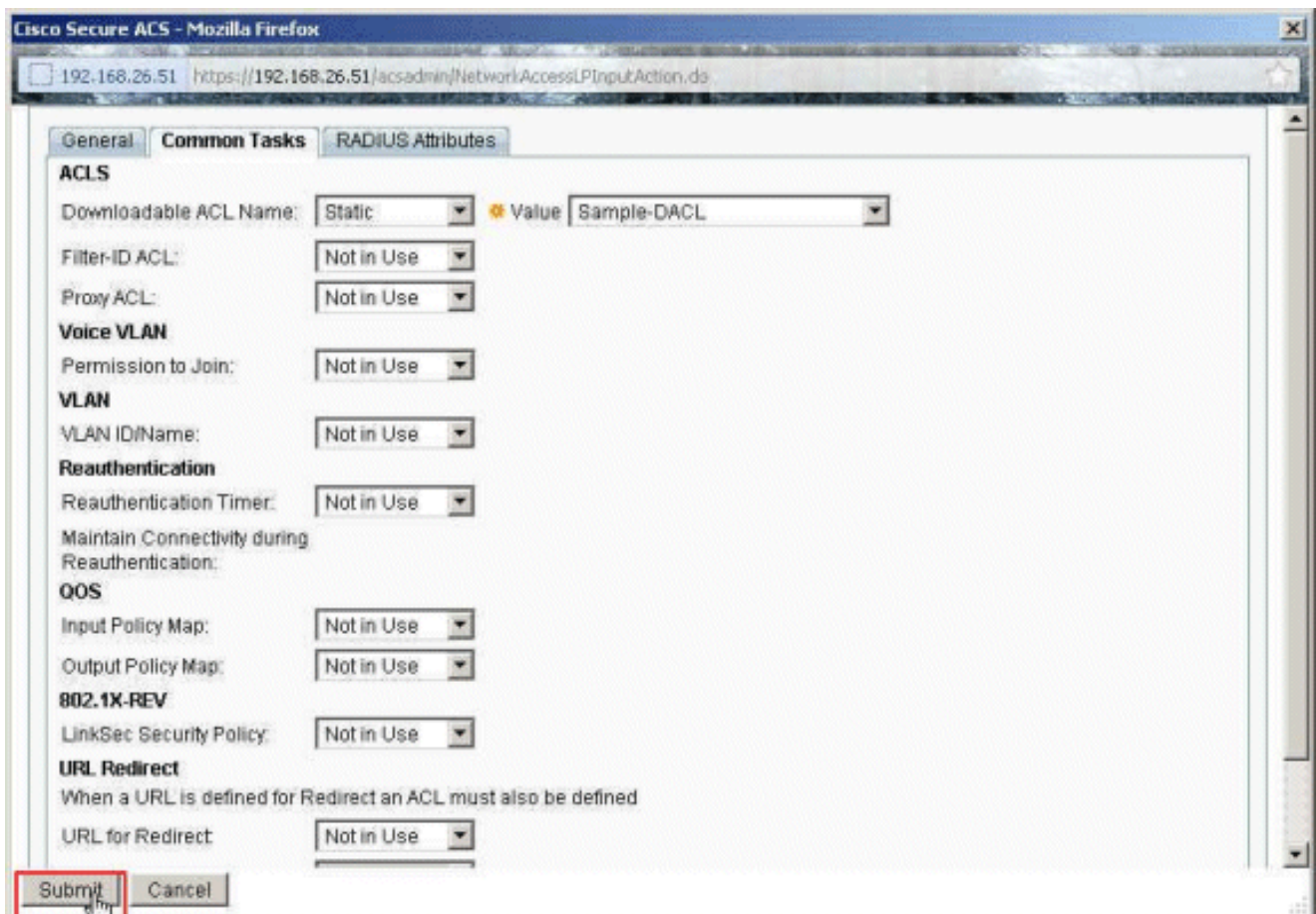
= Required fields

Submit Cancel

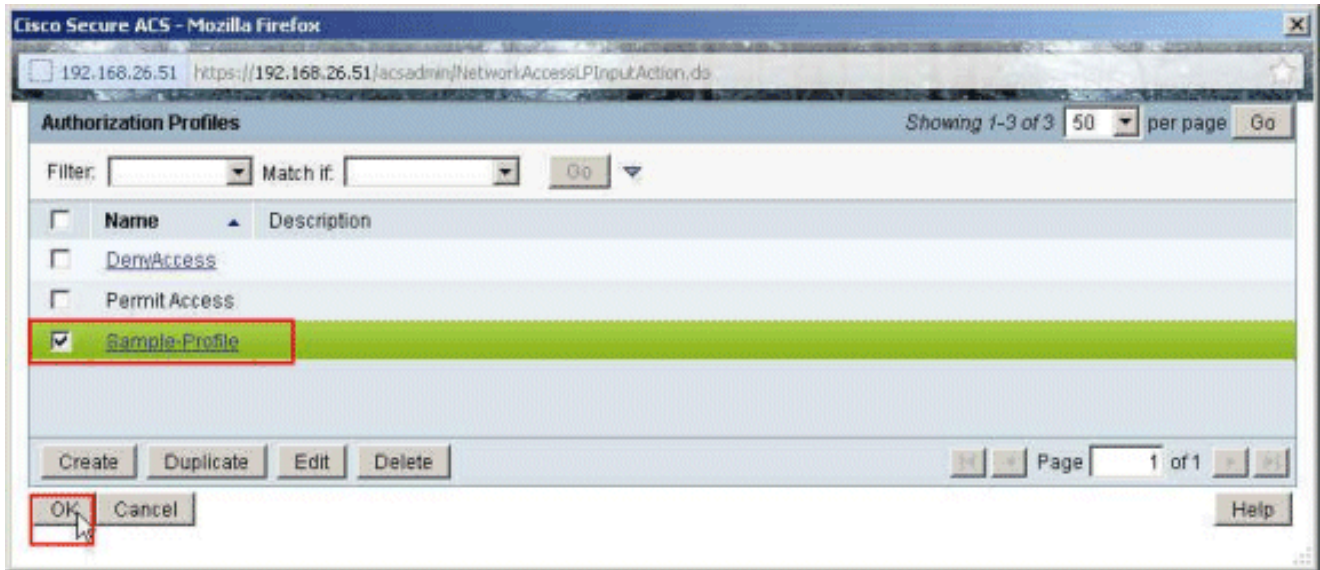
20. عمى اق مسال ةلدس نم لى عمى اق لى نم تابا ددو ، ةكرشم ما هم بى وب لى عمى اق رى ا
- جومن) اى دى هؤاشن ا م تى ذلى DACL رى ا . لى زن لى لى اق لى (ACL) لوصول ا فى مكح لى
عمى قل لى ةلدس نم لى عمى اق لى نم (DACL)



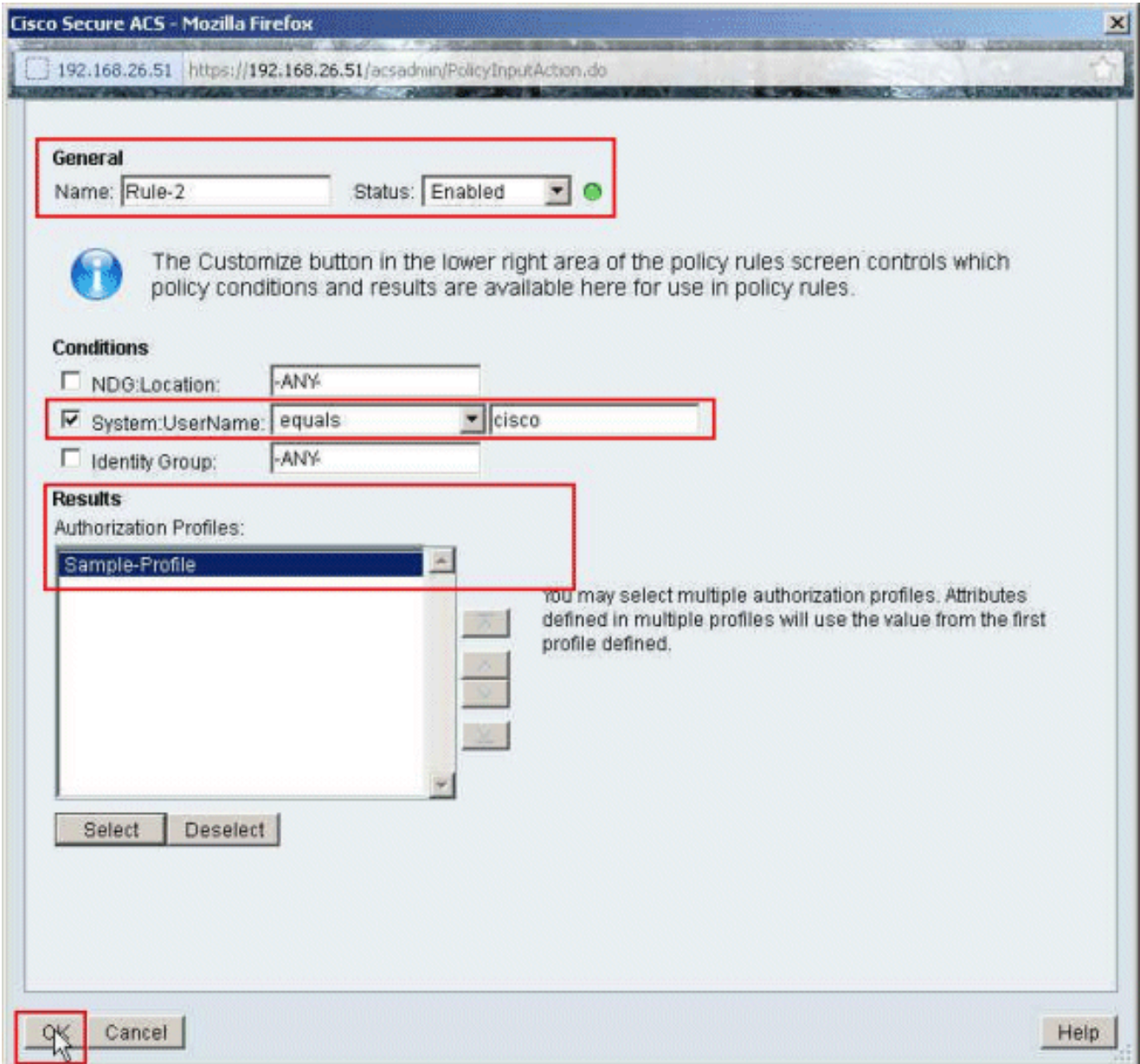
21. لاس را دلع رقنا



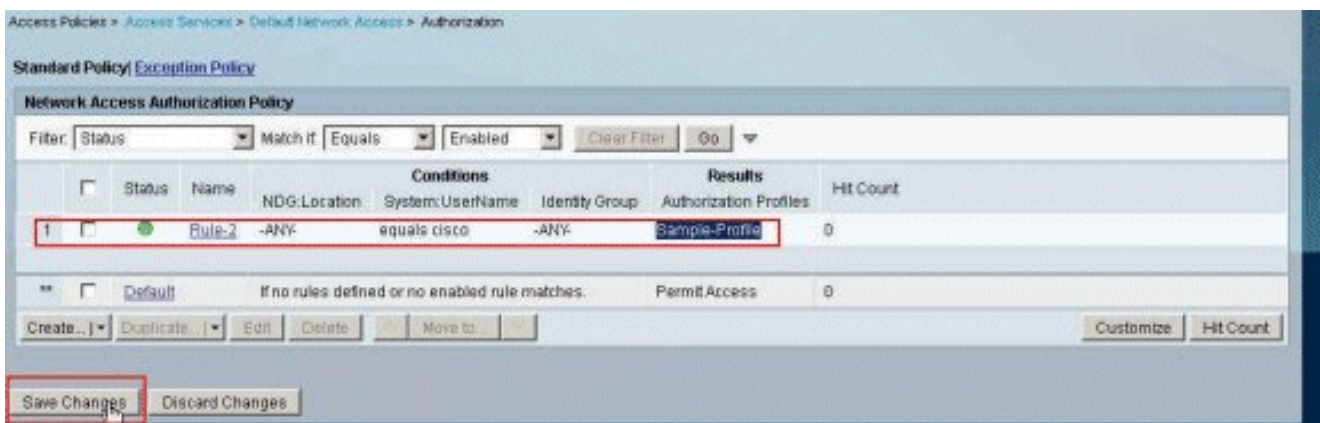
22. مت يذلا لي وختلا في رعت فلم) في رعتلا فلم ج ذومن ل ة رواج م ل ا راي ت خال ا ة ن ا ن م دك ا ت ق ف ا و م ر ق ن ا و ، ة د د ح م (ا ث ي د ح ه و ا ش ن ا



23. ا ت ا ف ي ص و ت ل ق ح ي ف ا ث ي د ح ه و ا ش ن ا م ت ي ذ ل ا ف ي ص و ت ل ا ج ذ و م ن د ي د ح ت ن م ق ق ح ت ل ا د ر ج م ب ق ف ا و م ر ق ن ا ، ل ي و خ ت ل ا



24. يواسي System:UserName مادختساب (2-ةدعاقلا) ةديدل ةدعاقلا عاشن نم ققحت عاشن مت. تاريغتلا ظفح قوف رونا. كلذل ةجيتنك Cisco و Sample-Profile طورش. حاجنب 2 ةدعاقلا



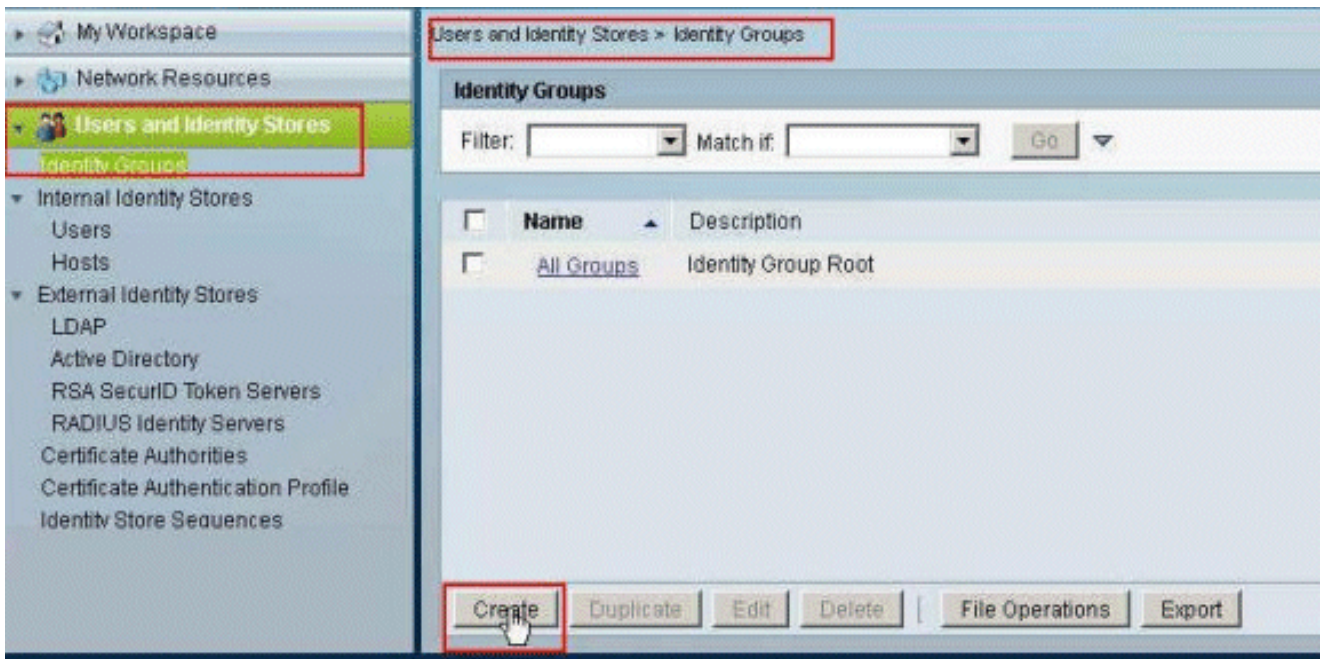
ةوعومجلل ليزنلل ةلباقلا (ACL) لوصولي مكحتلا ةمئاقلا ACS نيوكت

قالب اقل (ACL) لوصول في مكحتل اعمئاق ACS نيوكت نم 12 الى 1 نم تاوطلخا لمكأ
(ACL) لوصول في مكحتل اعمئاق نيوكتل تاوطلخا هذه ىرجأو يدرفل امدختس ملل لي زنتلل
نم آل Cisco ACS في ةومجملل لي زنتلل قالب اقل

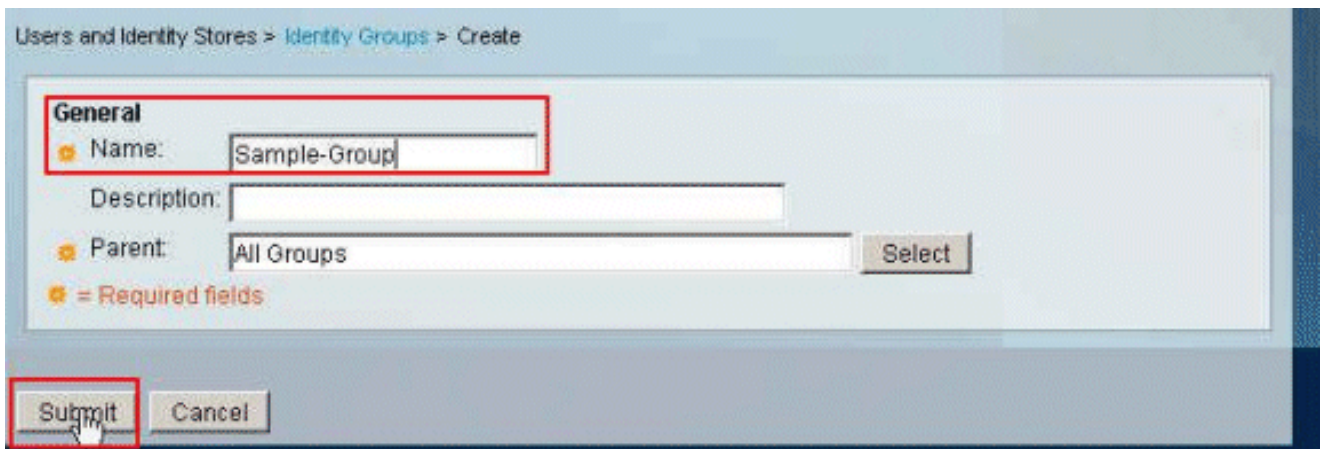
ةني ةومجمل الى "cisco" IPsec VPN م دختسم في متني ، ل اثلما اذ في

لوصول اعمئاق RADIUS م داخ لسريو ، حاجنب ةقداصل ملاب Cisco ةني ةومجمل م دختسم موقى
طقف 10.1.1.2 م داخ الى لوصول "cisco" م دختسم ملل نكمي . نام آل زاخ الى لي زنتلل قالب
مسق الى عجرا ، (ACL) لوصول في مكحتل اعمئاق نم ققحتلل . رخ آل لوصول عي مجض فرىو
ةومجمل / م دختسم ملل لي زنتلل قالب اقل (ACL) لوصول في مكحتل اعمئاق

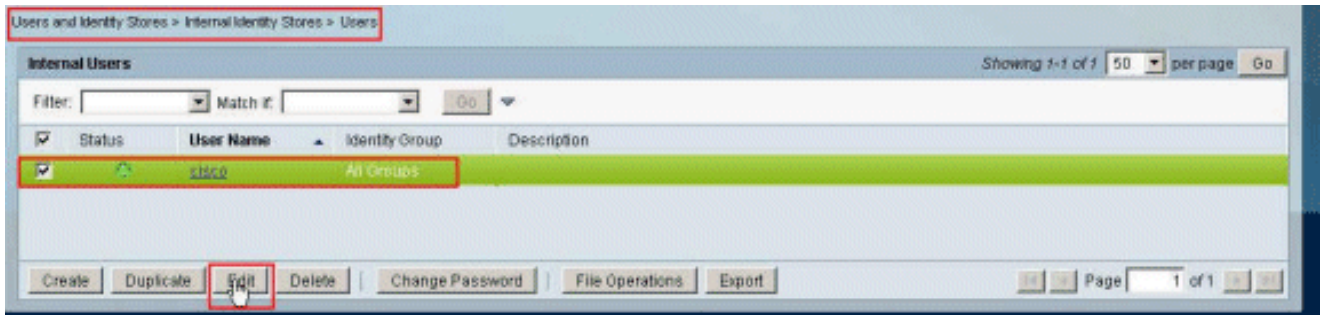
1. رقناو ، ةي وهلا تاومجمل > ةي وهلا نزاخمو ني م دختسم لاقوف رقنا ، لقنتلا طيرش في
ةديج ةومجمل عاشنال عاشن ااقوف



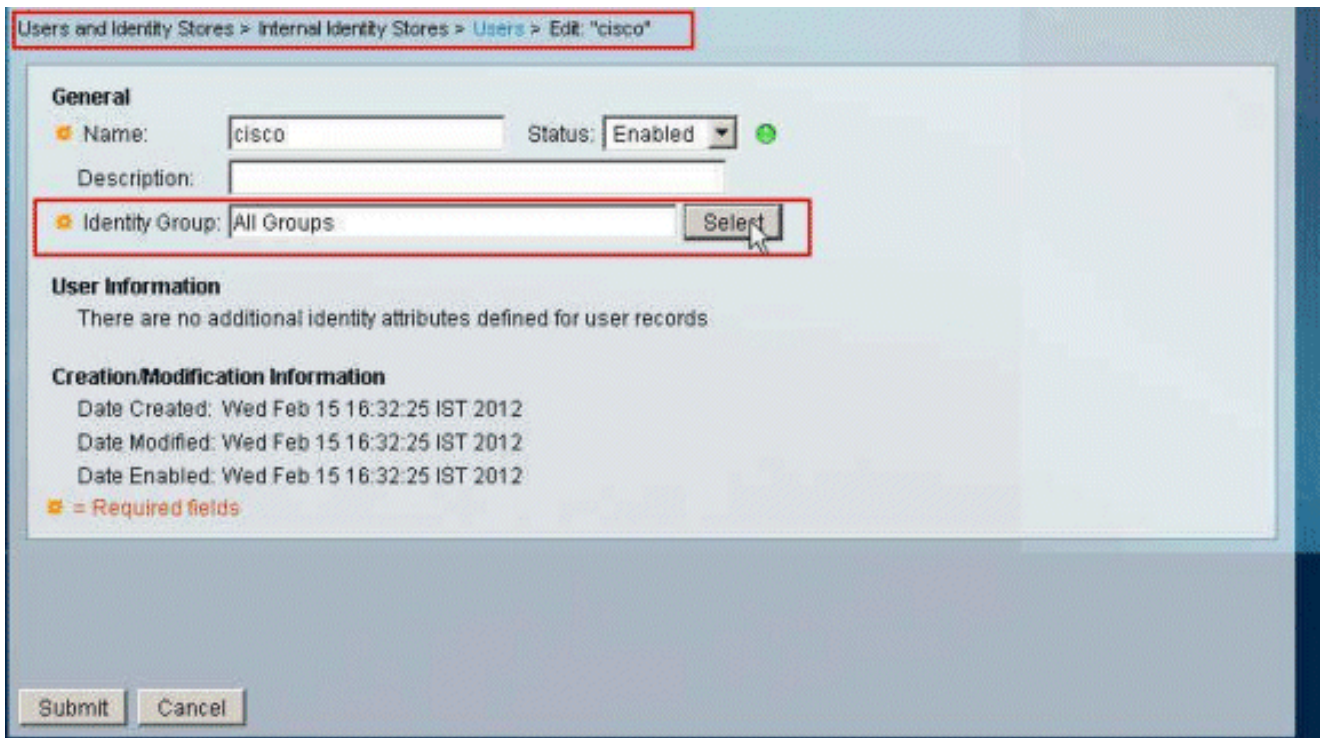
2. لاسرا رقناو ، (ةومجمل جذومن) ةومجمل مسا ريفوتب مق



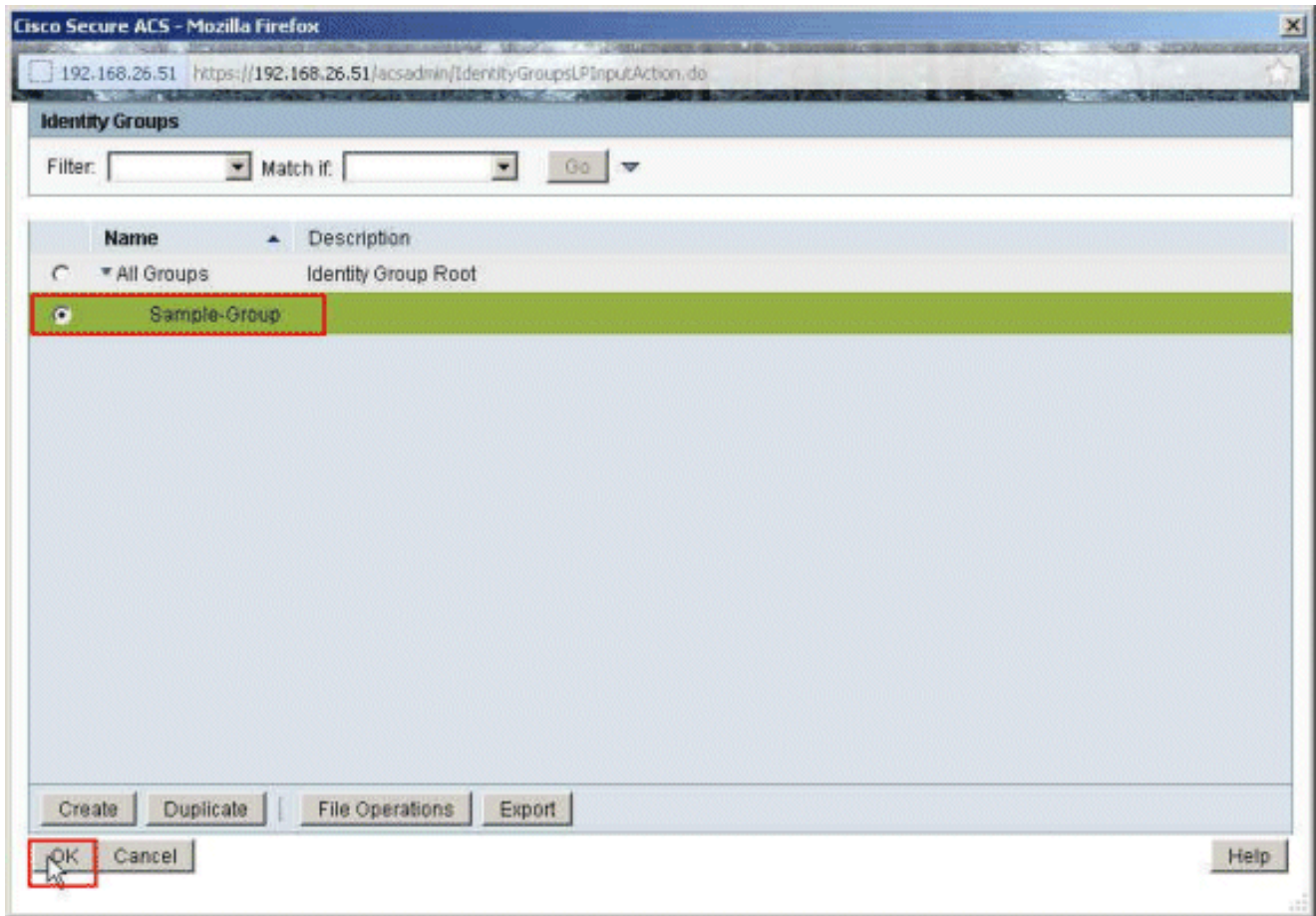
3. م دختسم لادحو ، ني م دختسم لادلا ةي وهلا نزاخم > م دختسم لادلا ةي وهلا نزاخم رتخأ
م دختسم لادلا اذهل ةومجمل اةي وضع ريغتل ريرحت قوف رقنا Cisco.



4. ەي وەلا ەوموم راجب دي دحت قوف رونا



5. ق ف اوم رونا و، (ەني ع ل ا ەوموم يە ي ت ل ا و) ا ث ي د ح ا ه و ا ش ن ا م ت ي ت ل ا ەوموم ل ا د ح



6. لاس را یل ع رقنا

Users and Identity Stores > Internal Identity Stores > Users > Edit: "cisco"

General

Name: **Status:**

Description:

Identity Group:

User Information

There are no additional identity attributes defined for user records

Creation/Modification Information

Date Created: Wed Feb 15 16:32:25 IST 2012

Date Modified: Wed Feb 15 16:32:25 IST 2012

Date Enabled: Wed Feb 15 16:32:25 IST 2012

= Required fields

7. > ةكبشلا لىل ي ضارتفال لوصول > لوصول تامدخ > لوصول اساس رتخ
ةديج ةدعاق عاشنال عاشنل قوف رقناو، ضيوفتلا

Access Policies > Access Services > Default Network Access > Authorization

Standard Policy | Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

Status	Name	Conditions	Results	Hit Count
		NDG Location System.UserName Identity Group	Authorization Profiles	
No data to display				
<input type="checkbox"/>	Default	If no rules defined or no enabled rule matches.	Permit Access	0


Create... | Duplicates... | Edit | Delete | Move to... | Customize | Hit Count


Save Changes | Discard Changes

8. > دىجت رقناو، ةدجم ةيوهالا ةعمومجل ةرواجملا راي تخالا ةناخ نأ نم دكأت

Cisco Secure ACS - Mozilla Firefox

192.168.26.51 https://192.168.26.51/acsadmin/PolicyInputAction.do



General
Name: Rule-1 Status: Enabled 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

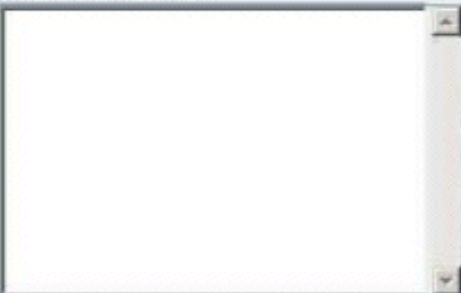




Conditions

NDG:Location: -ANY

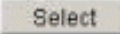
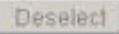
System:UserName: -ANY

Identity Group: in  

Results
Authorization Profiles:

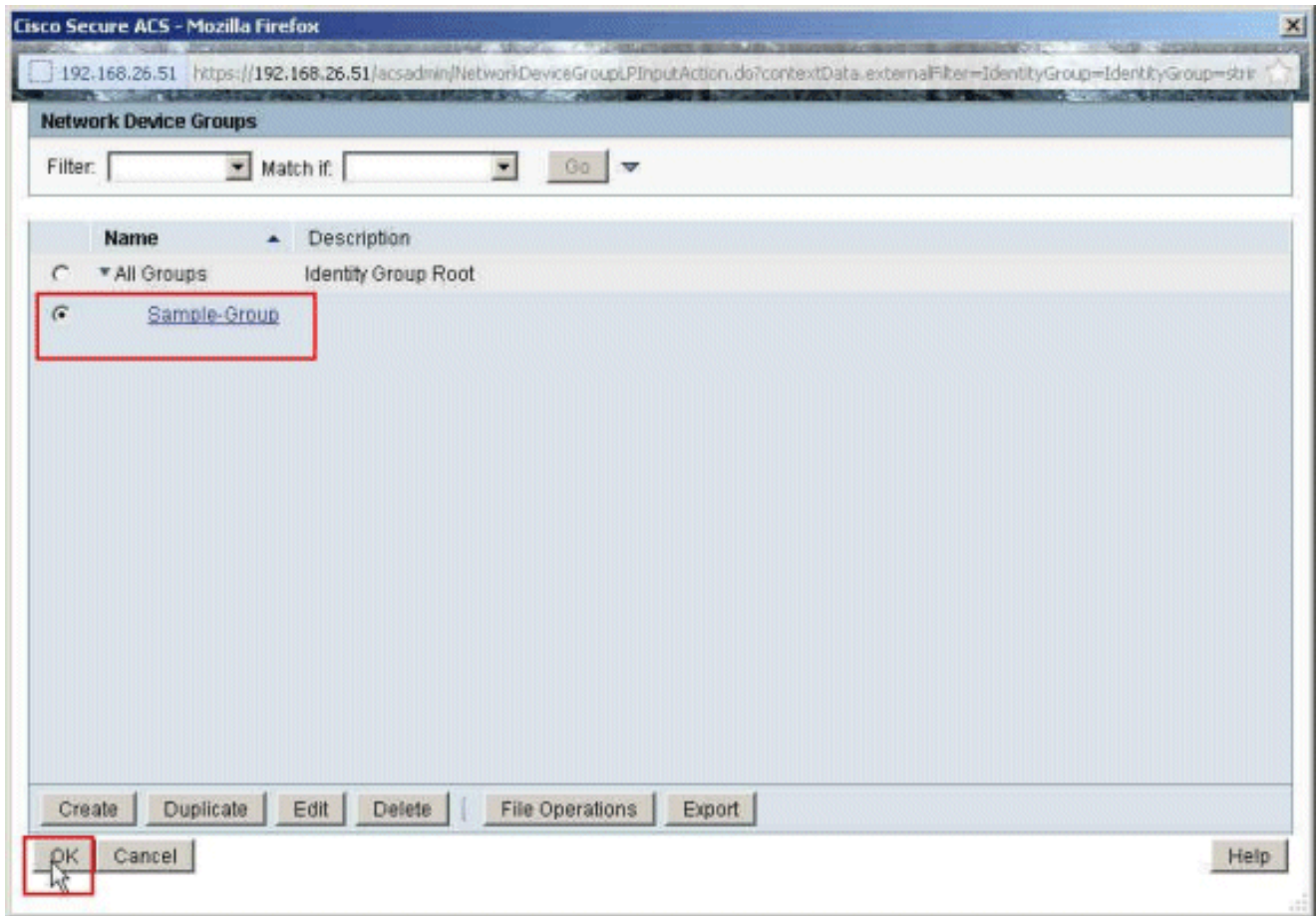
    

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

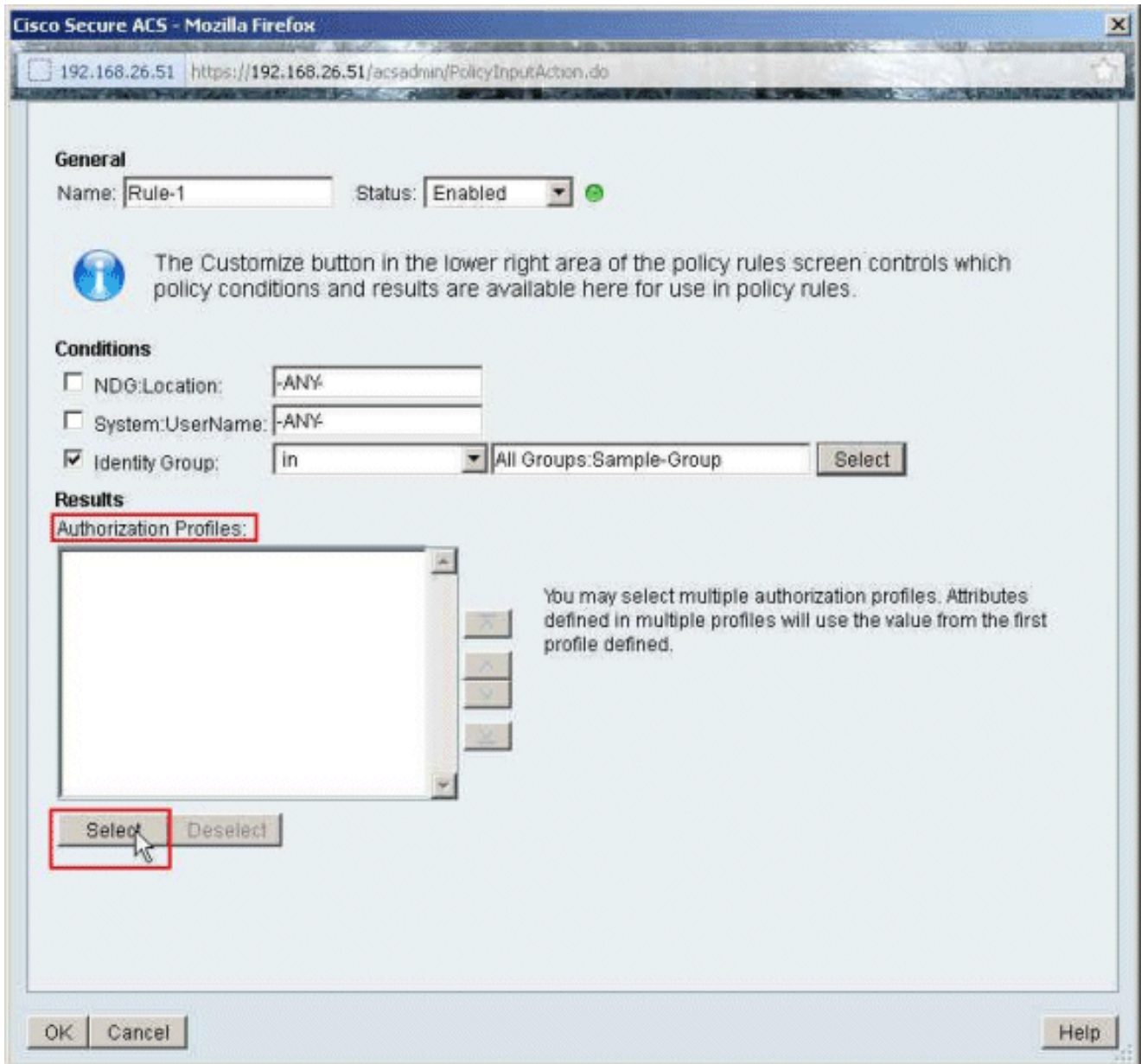
 

OK Cancel Help

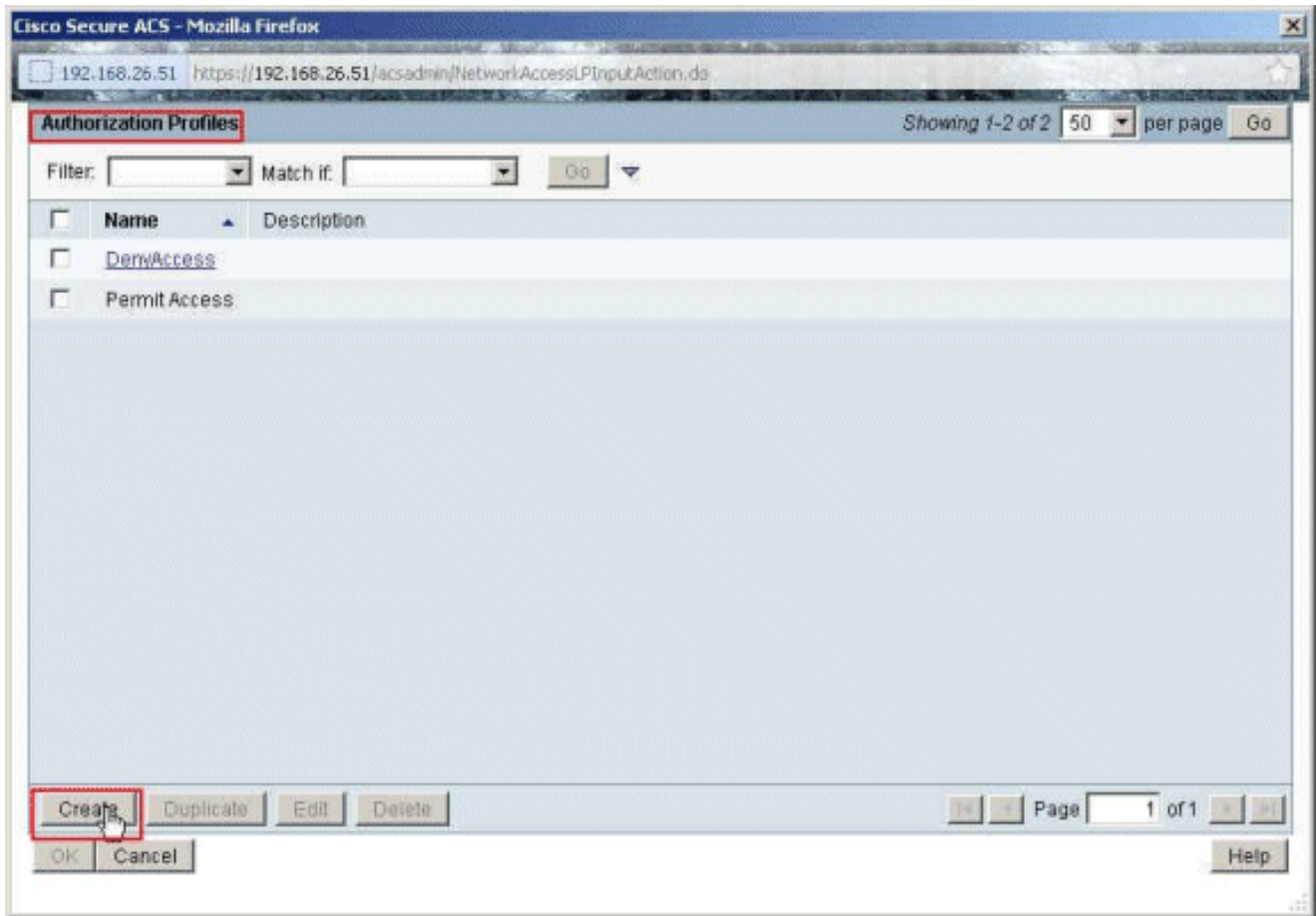
9.ok ةق قوطو، ةومجم ةني ع ترتخأ



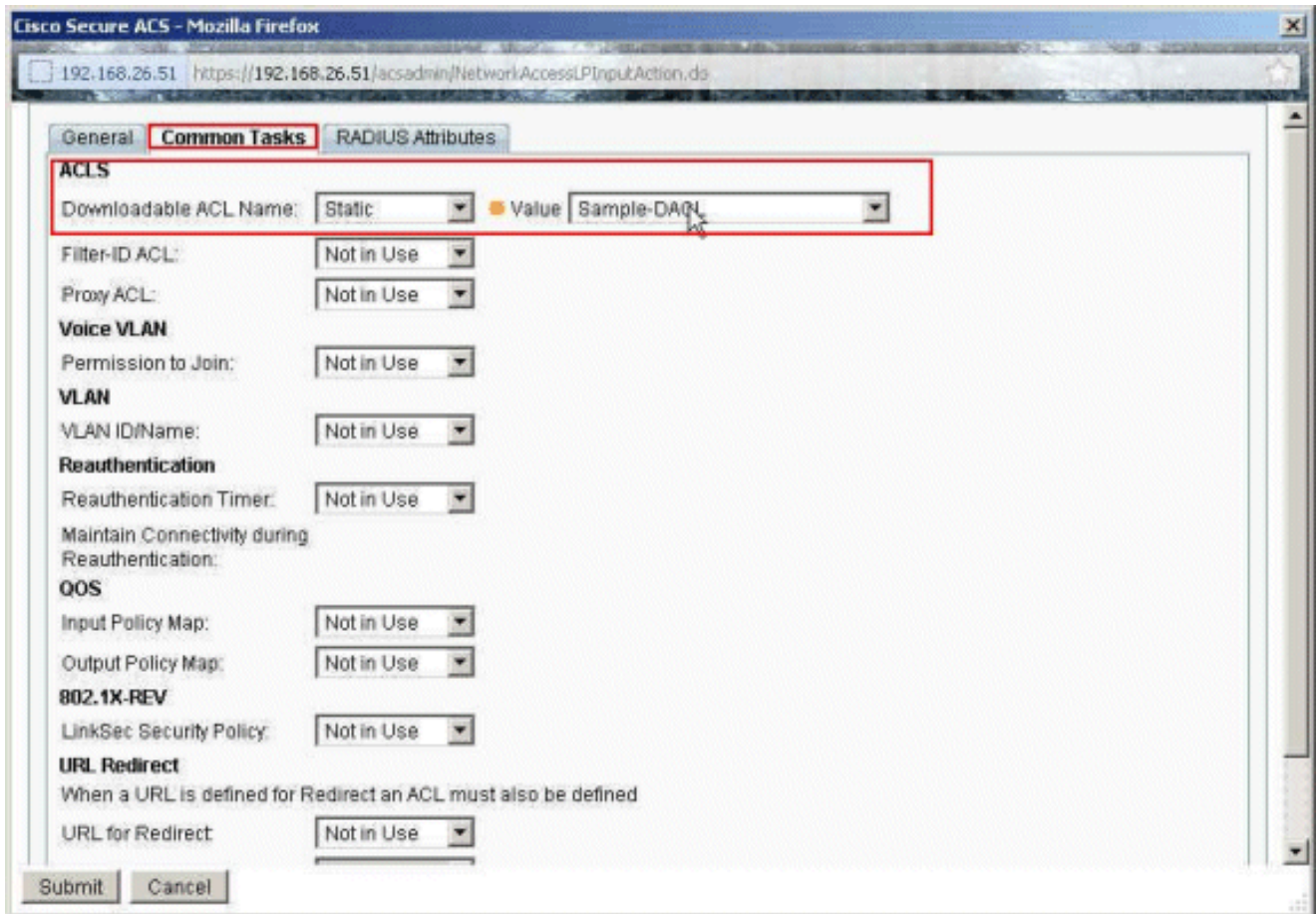
10. ليوختلا تافيصوت مسق يف ، ديحت ىلع رقنا



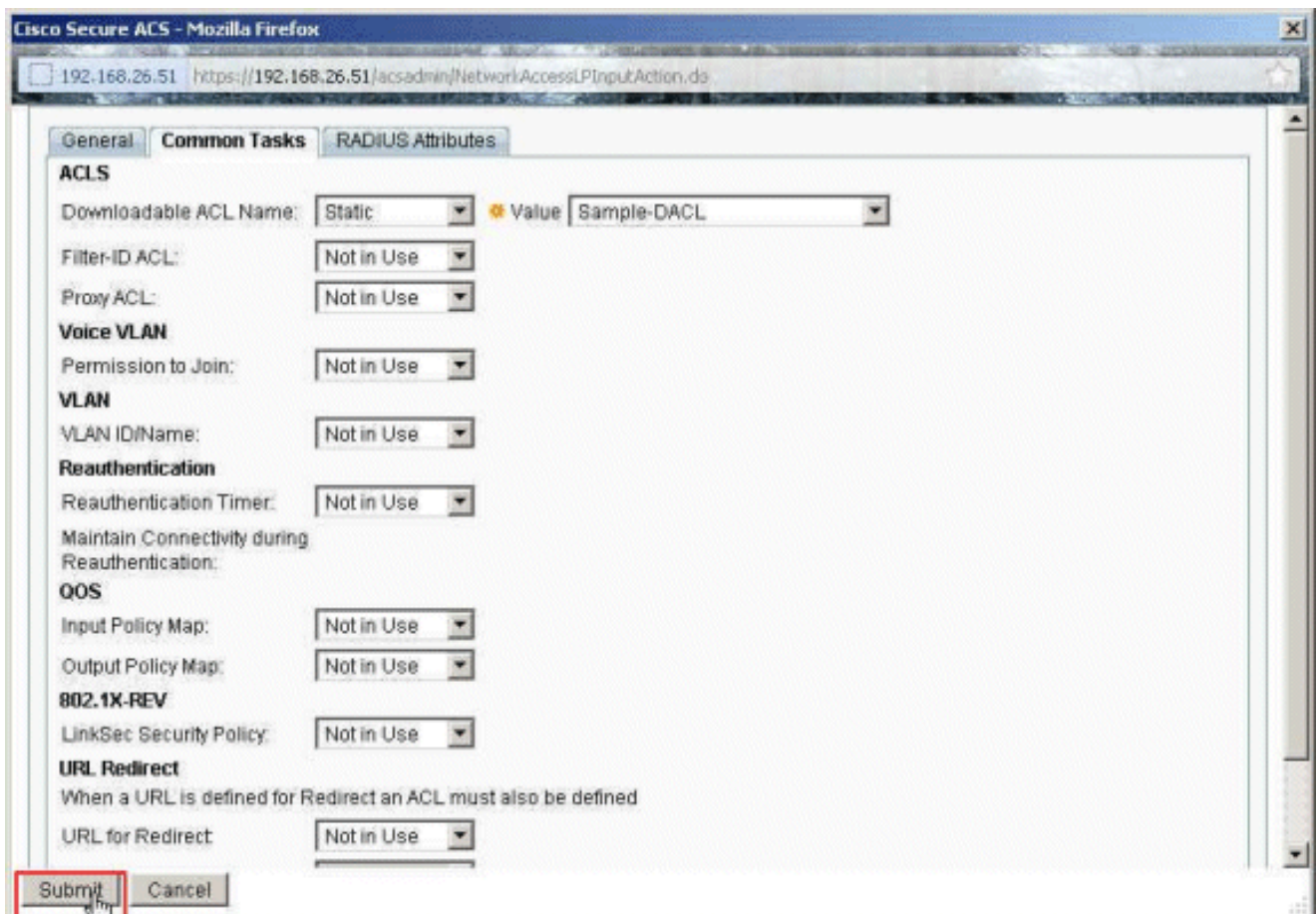
11. دېدج لېوخت فيرعت فلم عاشن ال عاشن ال ىل ع رقنا



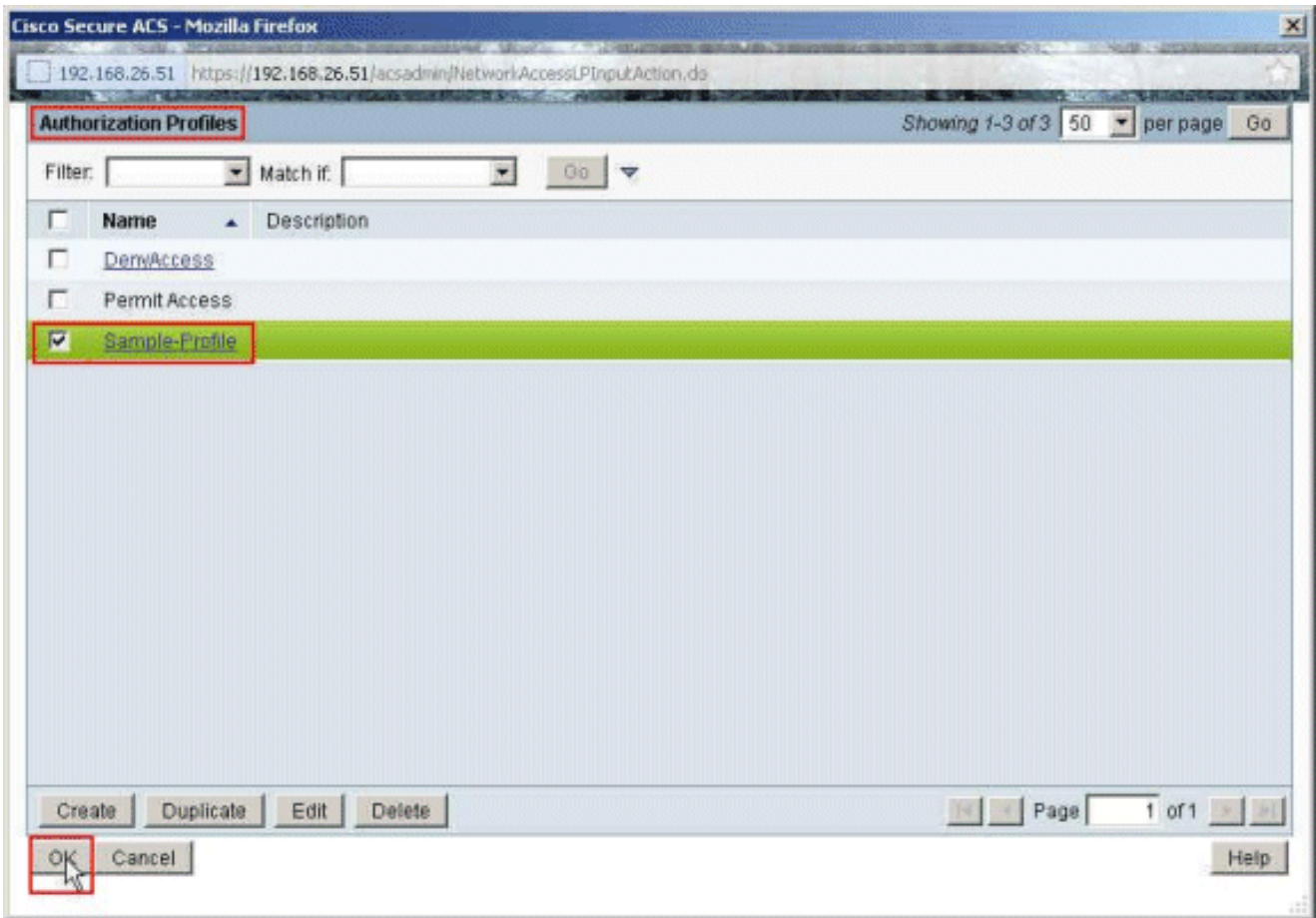
12. اذہ ۾ ڊخست سالا مسالا وه ڦيرتالا فل م . ليوختالا ڦيرتالا فل م سالا ري فوٽ ۾ ٿالا .



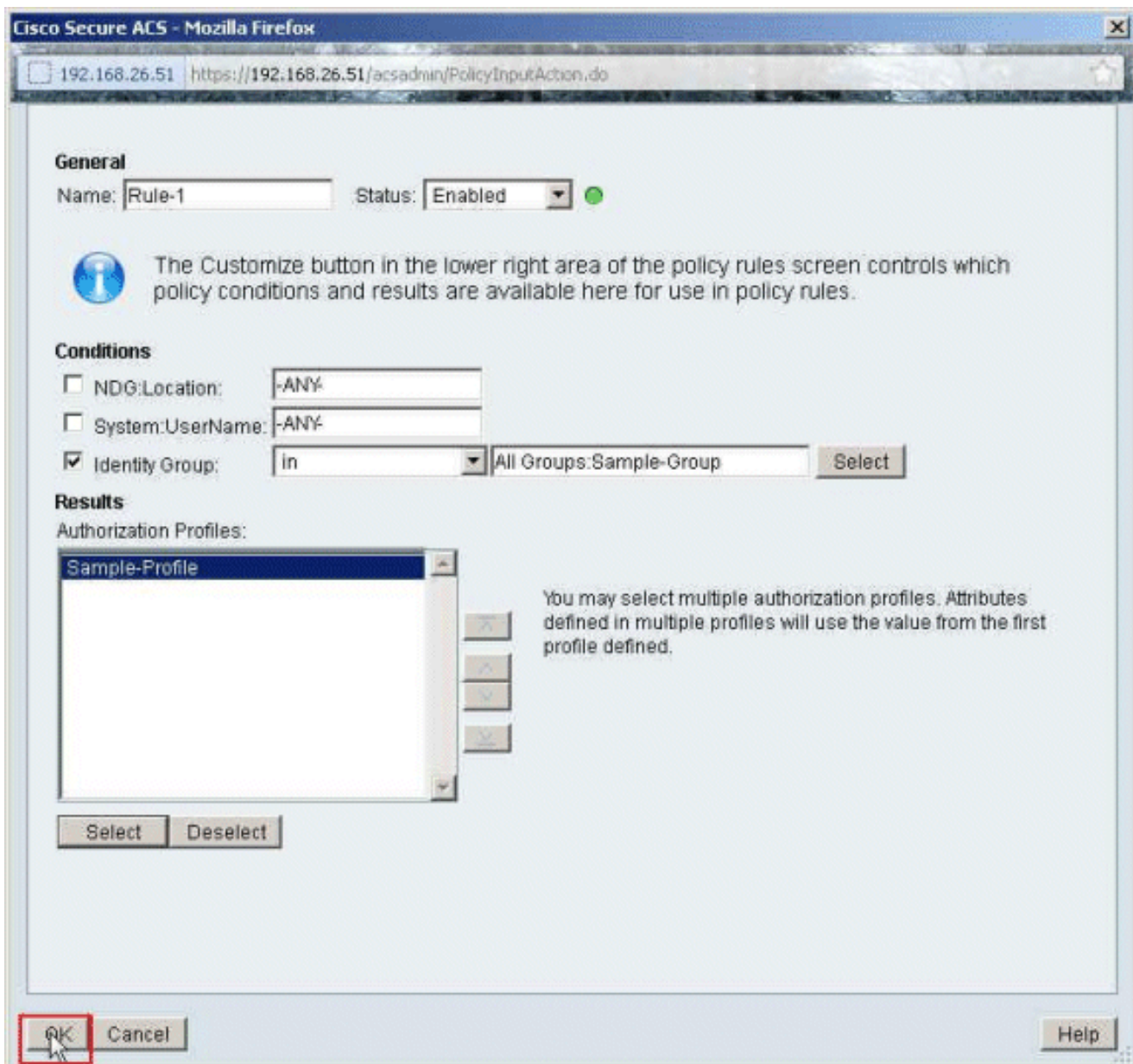
14. لاسرا دلع رقنا



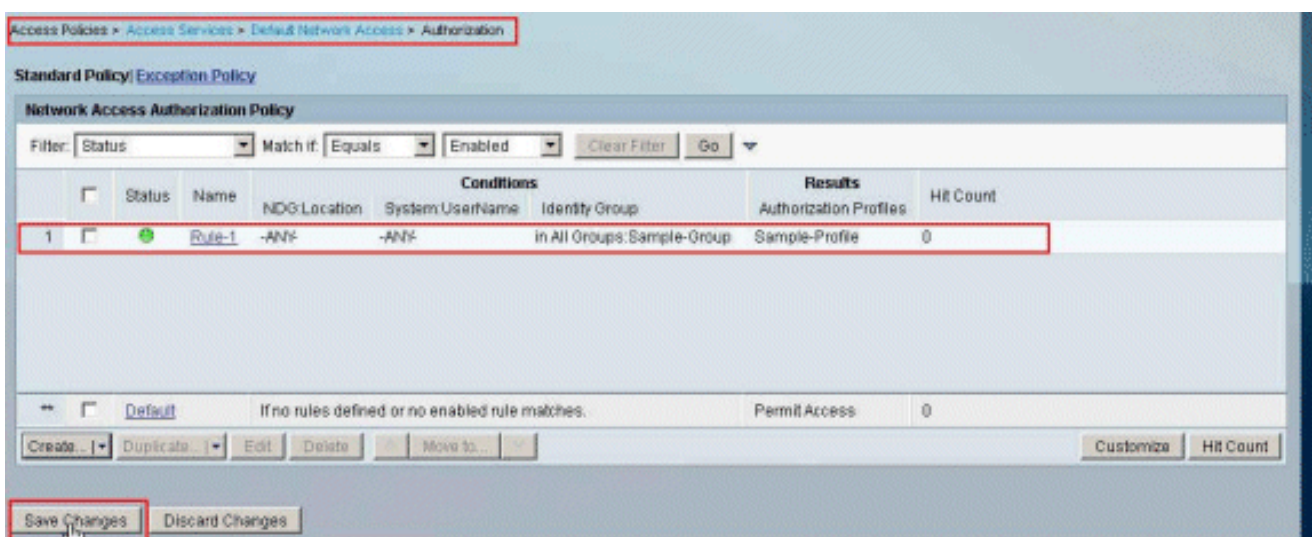
15. قفاوم قوف رقناو، اقبس م هؤاشنإ مت يذلا ليوختلا فيرعت فلم جذومن رتخأ



16. OK قوف رقناو



17. جدول وطرشك ةومومجم ل ةو ة صاخ ل ةني ة ل ةومومجم ل ةم 1 ةءاق ل ءاش ن ةم ققحت ءاربي ءل طفح قوف رقنا .ك لذل ةءي ءنك في رءء ل ءلم

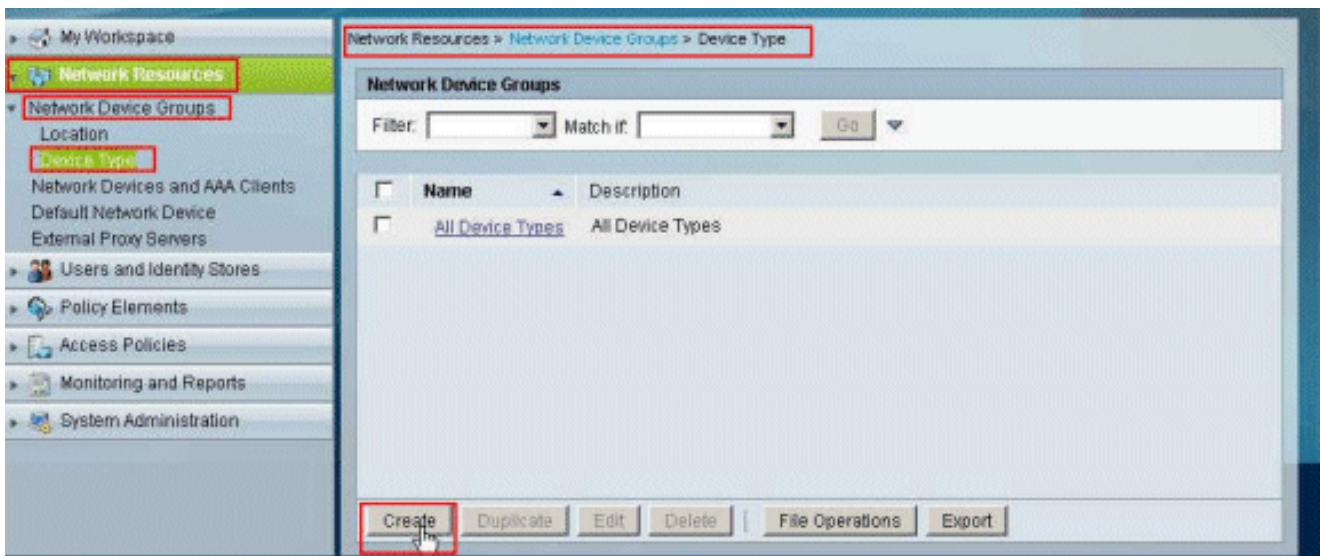


ةومجم ل ليزنتل ةلباقلا (ACL) لوصول ي ف مكحتلا ةمئاق ACS نيوكت ةكبشلا ةزهجأ

[ةلباقلا \(ACL\) لوصول ي ف مكحتلا ةمئاق ACS نيوكت](#) نم 12 لىا 1 نم تاوطخلا لمكأ (ACL) لوصول ي ف مكحتلا ةمئاق نيوكتل تاوطخلا هذه ىرجأو [يدر فلأ مدختسم ل ل ليزنتل ل](#) Cisco Secure ACS. ف ةكبشلا ةزهجأ ةومجم ل ليزنتل ةلباقلا

ةزهجأ ةومجم ب ةصاخلا VPN تاباوب لىا (ASA) RADIUS ليمع يمتني ،لاثلما اذه ي ف لسريو ،"Cisco" مدختسم ل ل ASA نم دراو ل VPN ةقداصم بلط لاسرا حاجنب متي .ةكبشلا لوصول "cisco" مدختسم ل ل نكمي .نامألا زاهج لىا ليزنتل ةلباق لوصول ةمئاق RADIUS مداخ لوصول ي ف مكحتلا ةمئاق نم ققحتل .رخآلا لوصول عيمج ضفريو طقف 10.1.1.2 مداخ لىا [ليزنتل ةلباقلا \(ACL\) لوصول ي ف مكحتلا ةمئاق](#) مسق لىا عرجا ،(ACL) [ةومجم ل /مدختسم ل ل](#).

1. ةكبش نقلخ in order to نقلخي ةقطقو ،عون ةادأ ةومجم ةادأ ةكبش >دروم ةكبش نترخأ ديدج ةومجم ةادأ



2. لاسرا قوف رقناو ،(لاثلما اذه ي ف VPN تاباوب) ةكبشلا ةزهجأ ةومجم مساري فوتب مق

Network Resources > Network Device Groups > Device Type > Create

Device Group - General

Name:

Description:

Parent:

= Required fields

3. تمت يذال RADIUS Sample-asa ليمع ددو، AAA عالمعو ةكبشلا ةزهجأةكبشلا دراوم رتخأ اذه نم ةيوضع ةعومجم ةادأةكبشلا تريغ in order to ررحي ةققوط . اقباس هؤاشنإ RADIUS نوبز (ASA).

Network Resources > Network Devices and AAA Clients

Network Devices Showing 1-1 of 1 50 per page Go

Filter: Match if:

<input checked="" type="checkbox"/>	Name	IP Address	Description	NDG:Location	NDG:Device Type
<input checked="" type="checkbox"/>	sample-asa	192.168.26.13		All Locations	All Device Types

| Page 1 of 1

4. زاهجلا عون راجب ديدحت قوف رقنا

Network Resources > Network Devices and AAA Clients > Edit: "sample-asa"

Name:

Description:

Network Device Groups

Location

Device Type

IP Address

Single IP Address IP Range(s) By Mask IP Range(s)

IP:

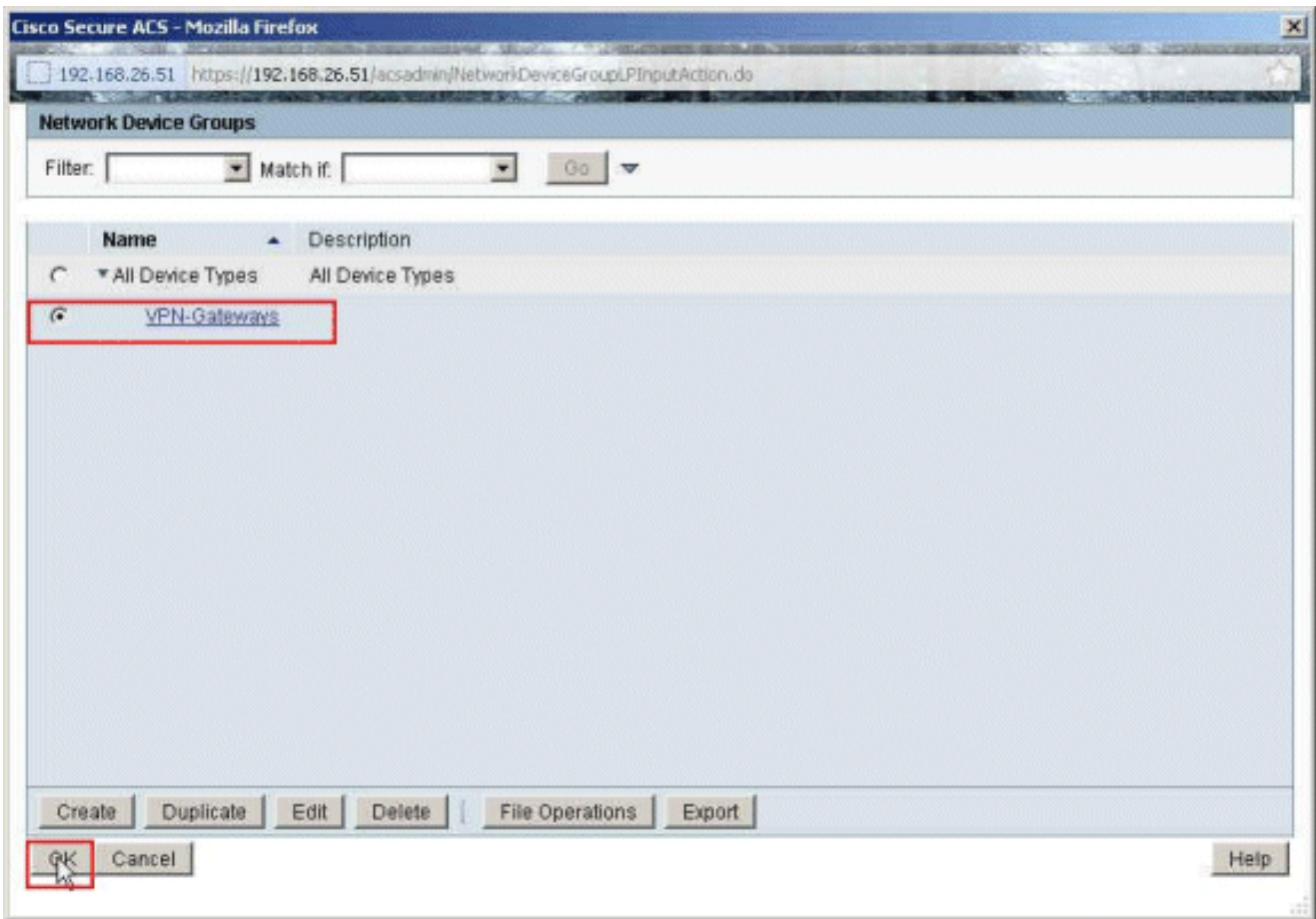
= Required fields

Authentication Options

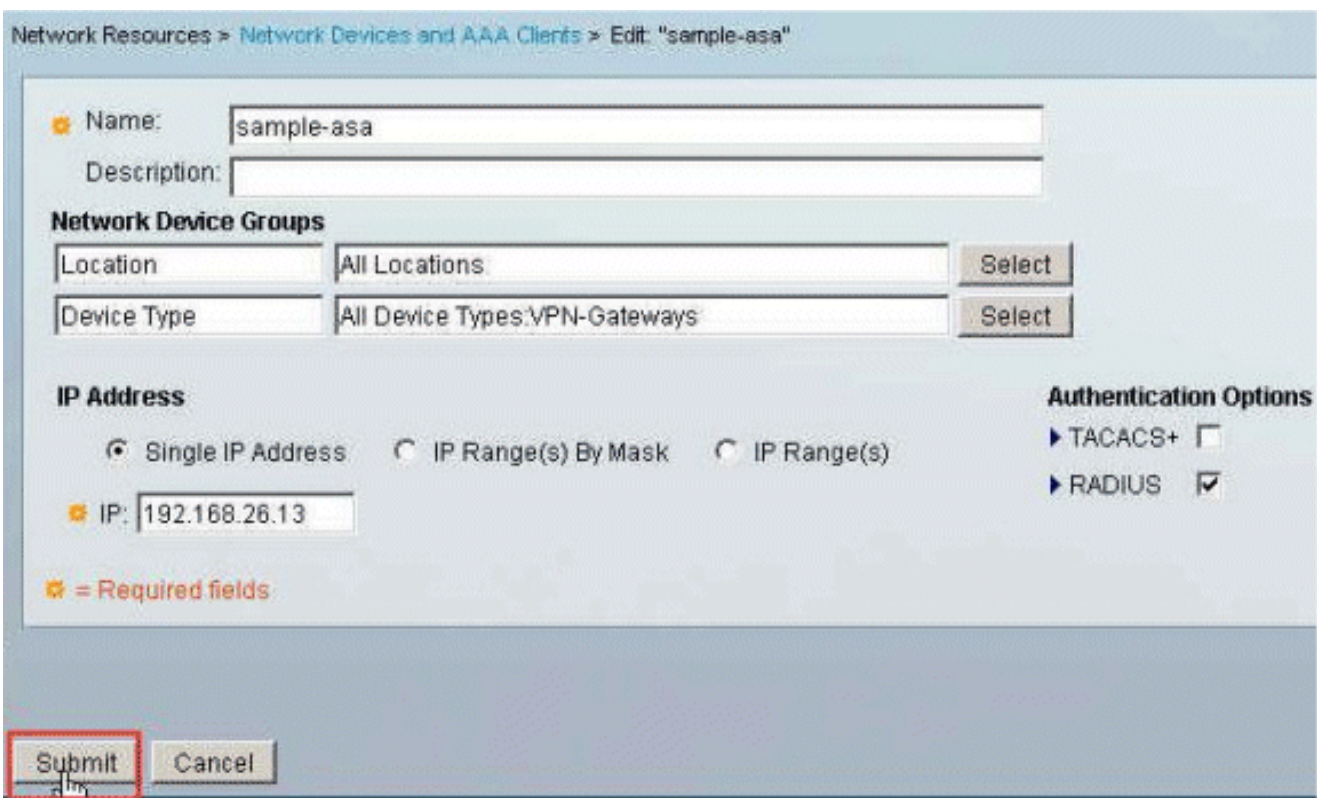
TACACS+

RADIUS

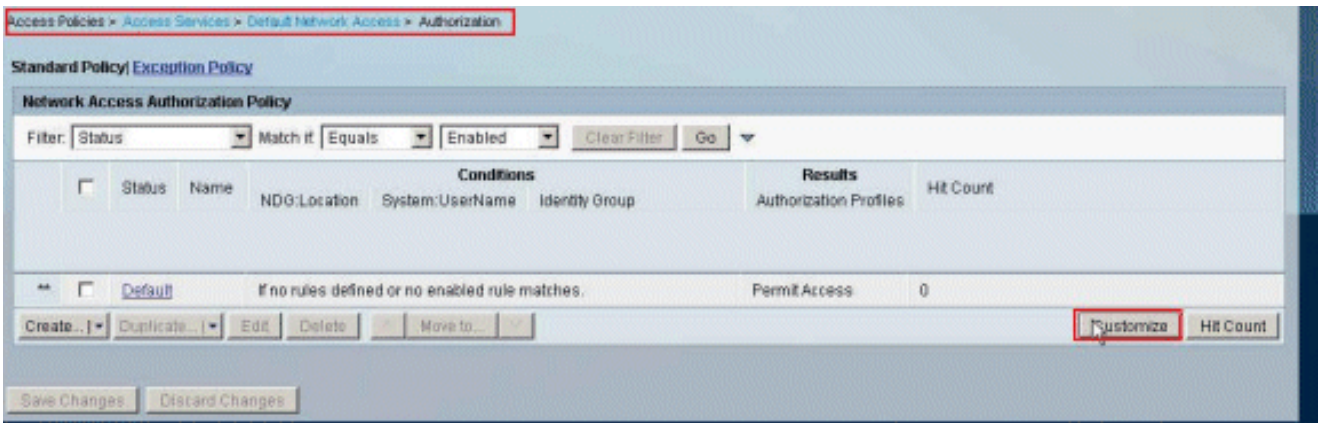
5. قوف رقناو، (VPN تبابوب يه يتلاو) اتيح اهواشن امت يتلا ةكبشلا ةزهجة ومجم ددح قفاوم.



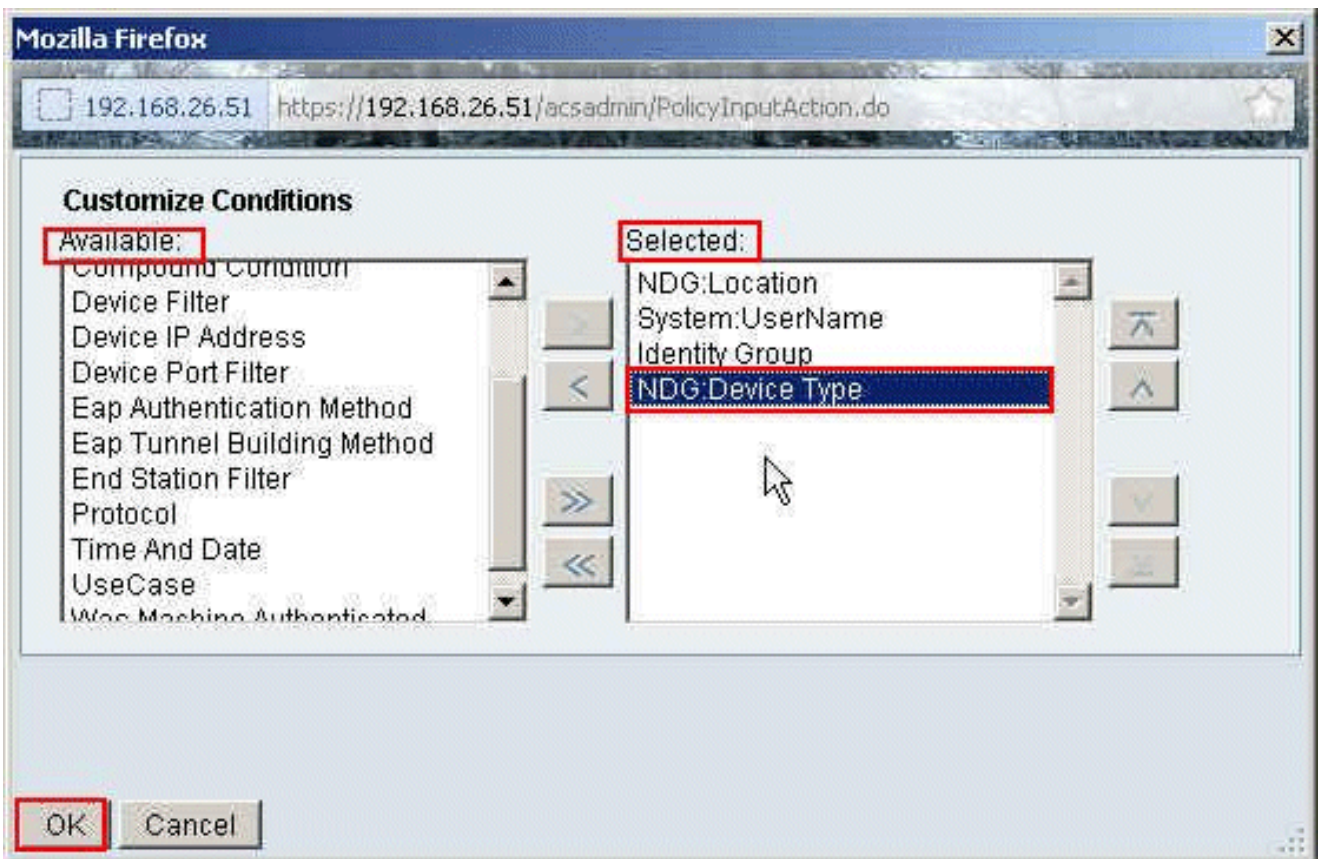
6. لاسرا يلع رقنا



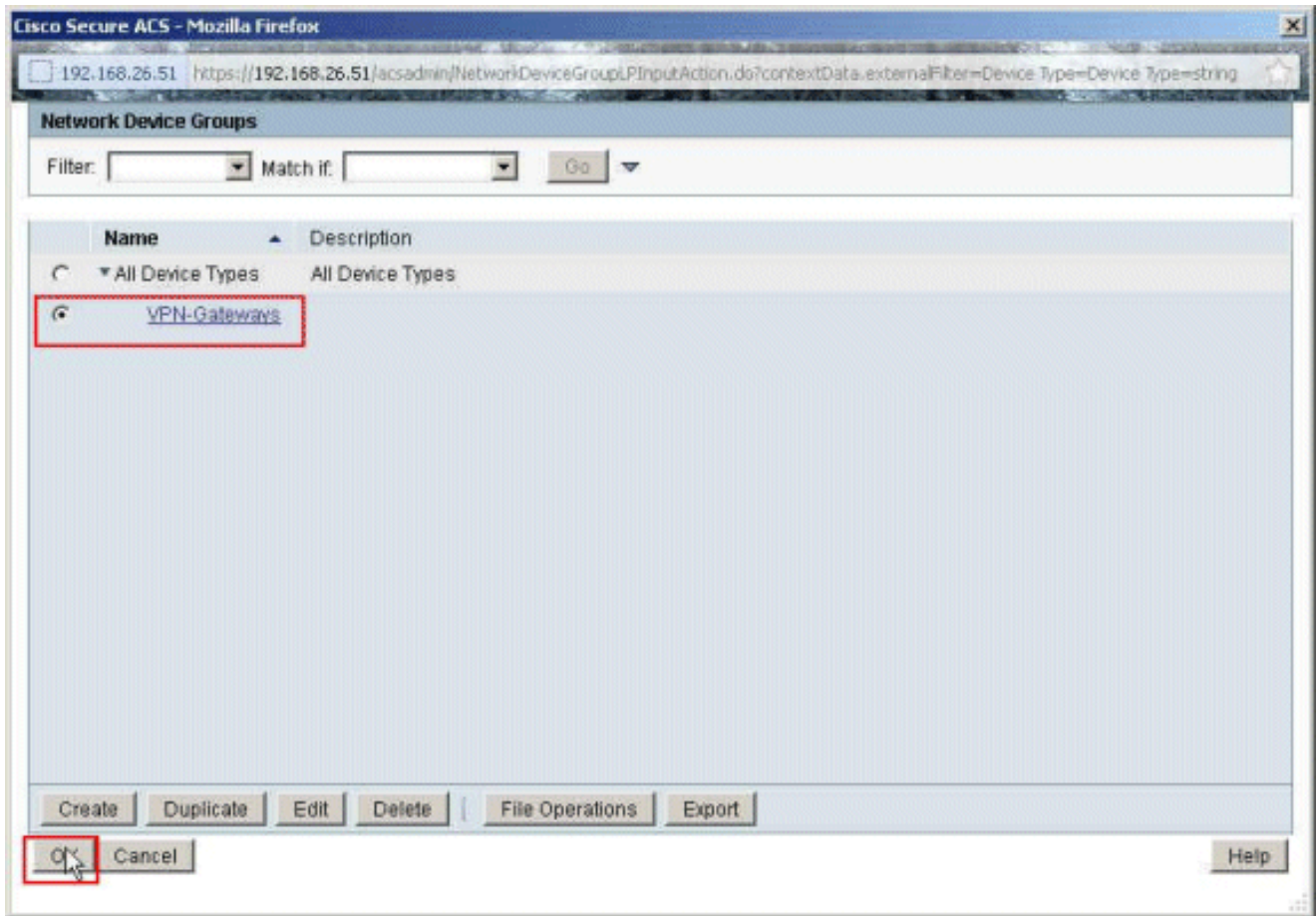
7. اضيف وقت الا > كة بش لل يضارت فال لوصول > لوصول تام دخ > لوصول تاسايس رتخأ
صيصخت قوف رقناو



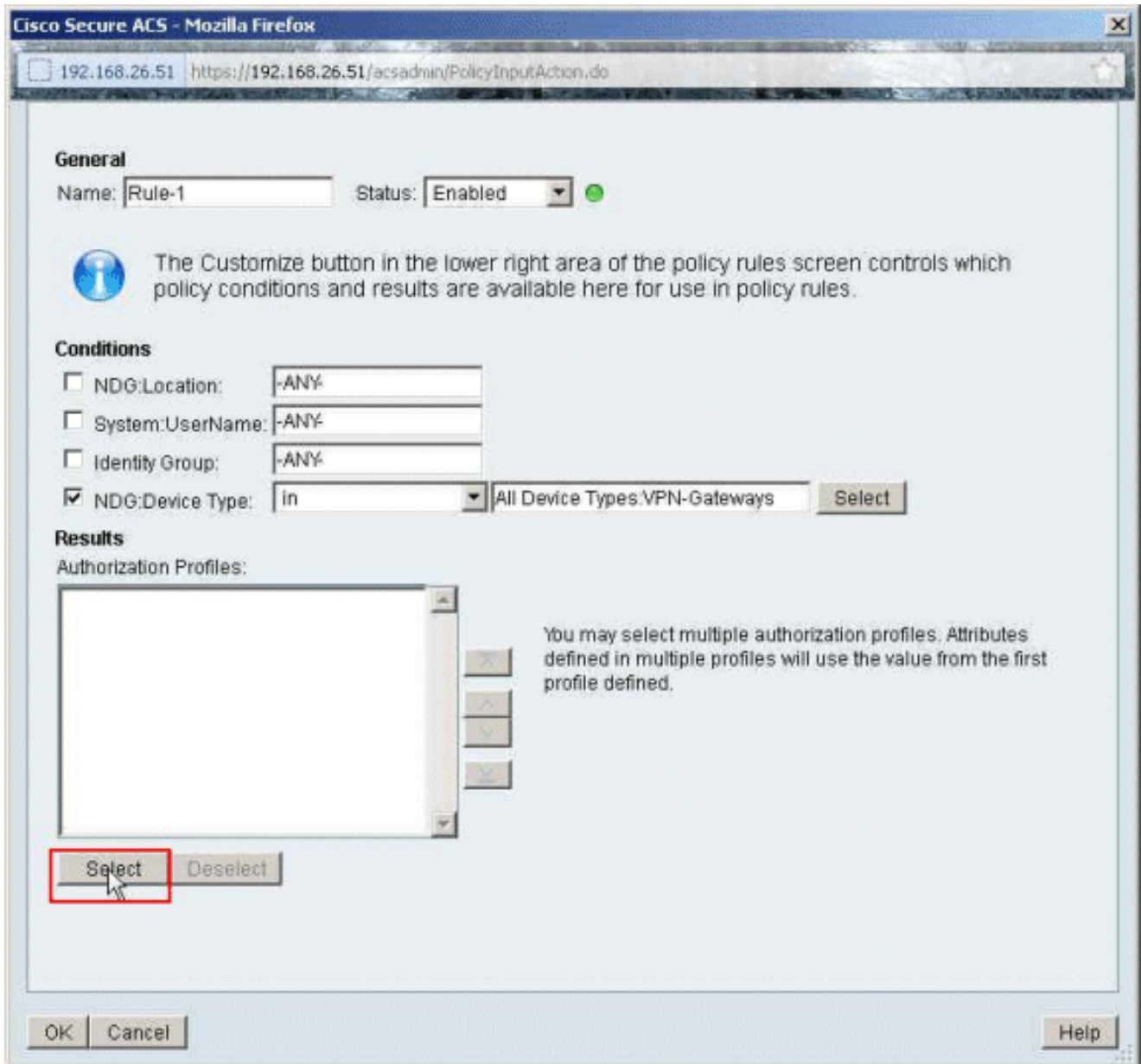
8. قفاوم قوف رقناو، ددحمال مسقلا لى رفوتم مسقلا نم زاهجال عون: NDG لقنا



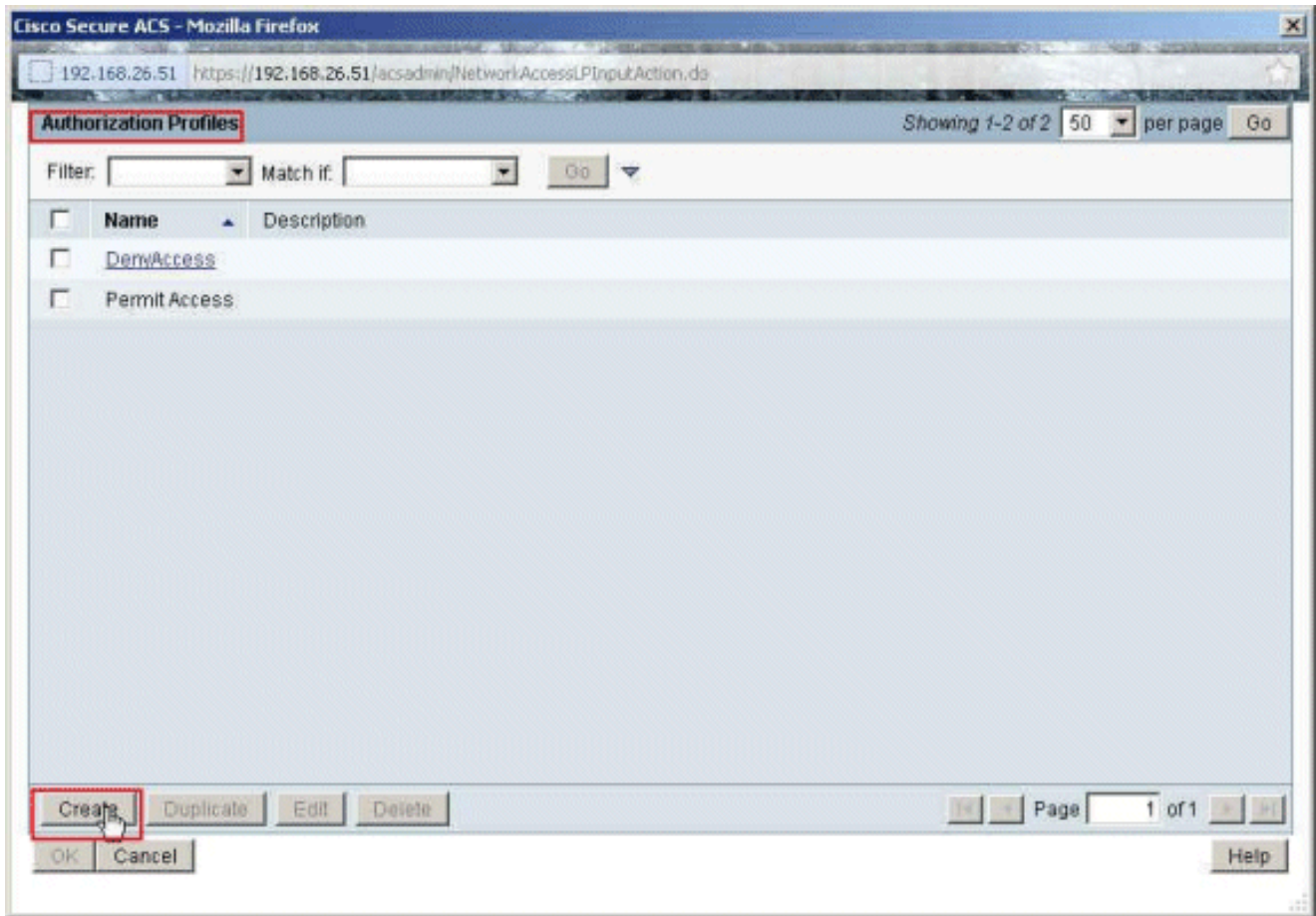
9. ةديج ةدعاق عاشنال عاشنال قوف رقنا



12. ڊيڊت قوف رونا



13. دېدج لېوخت فيرعت فلم عاشن ال عاشن ال ىل ع رقنا



14. اذہ ڀي مڊختس مل مسالا وه ڦيرتال فل م . ليوختال ڦيرت فل مل مسال ري فوتب مق لامل.

Cisco Secure ACS - Mozilla Firefox

192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do

General Common Tasks RADIUS Attributes

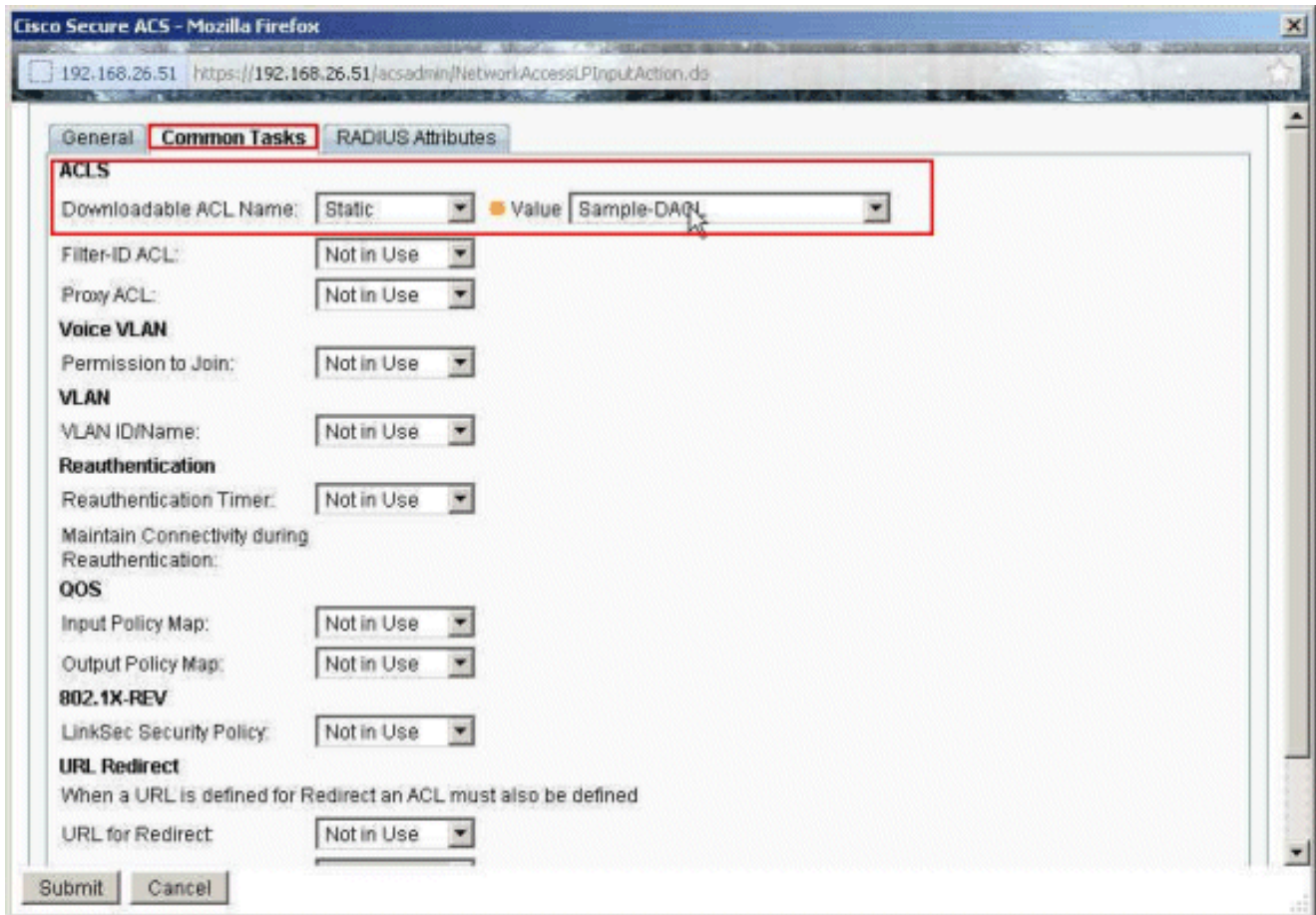
Name: Sample-Profile

Description:

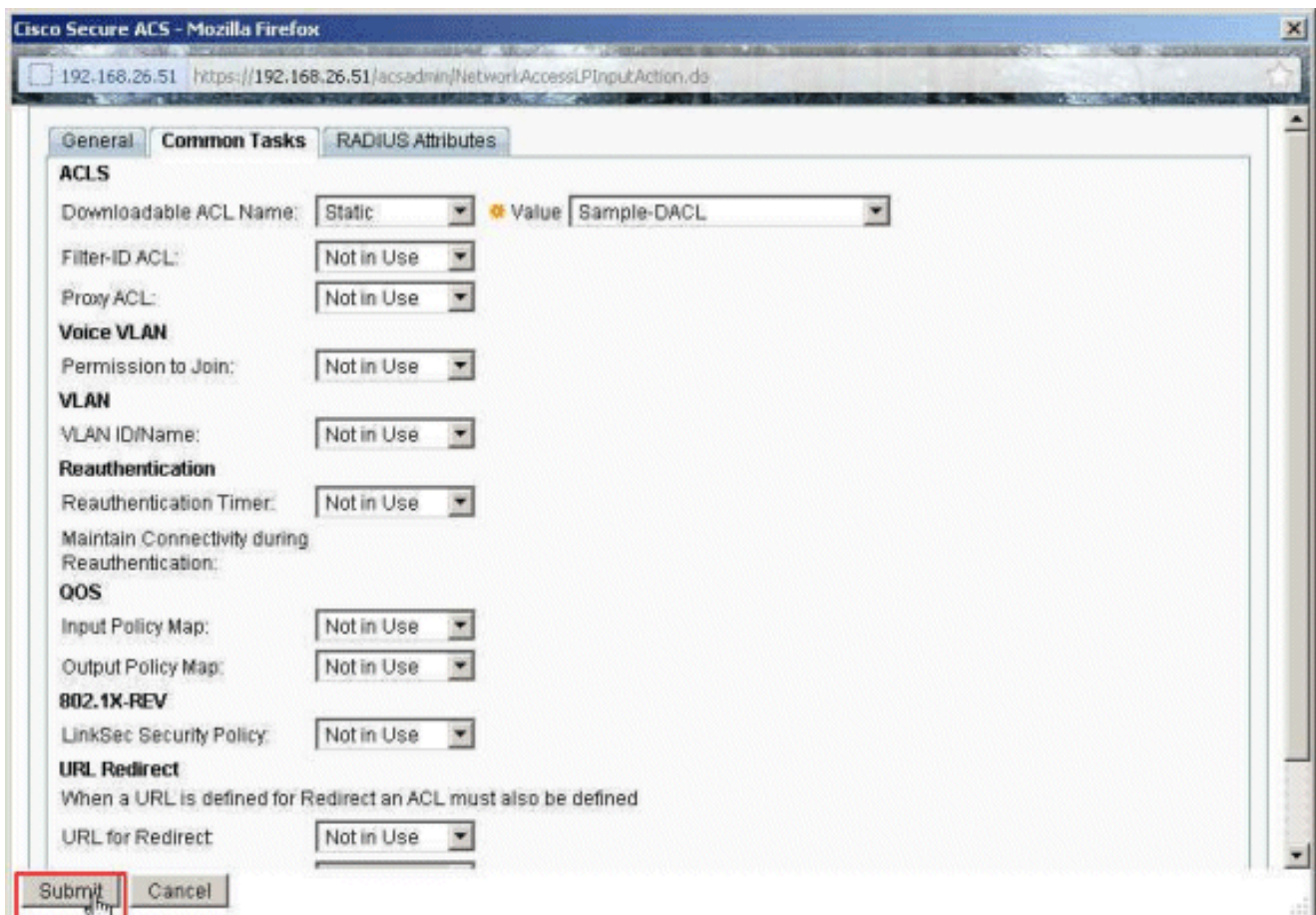
= Required fields

Submit Cancel

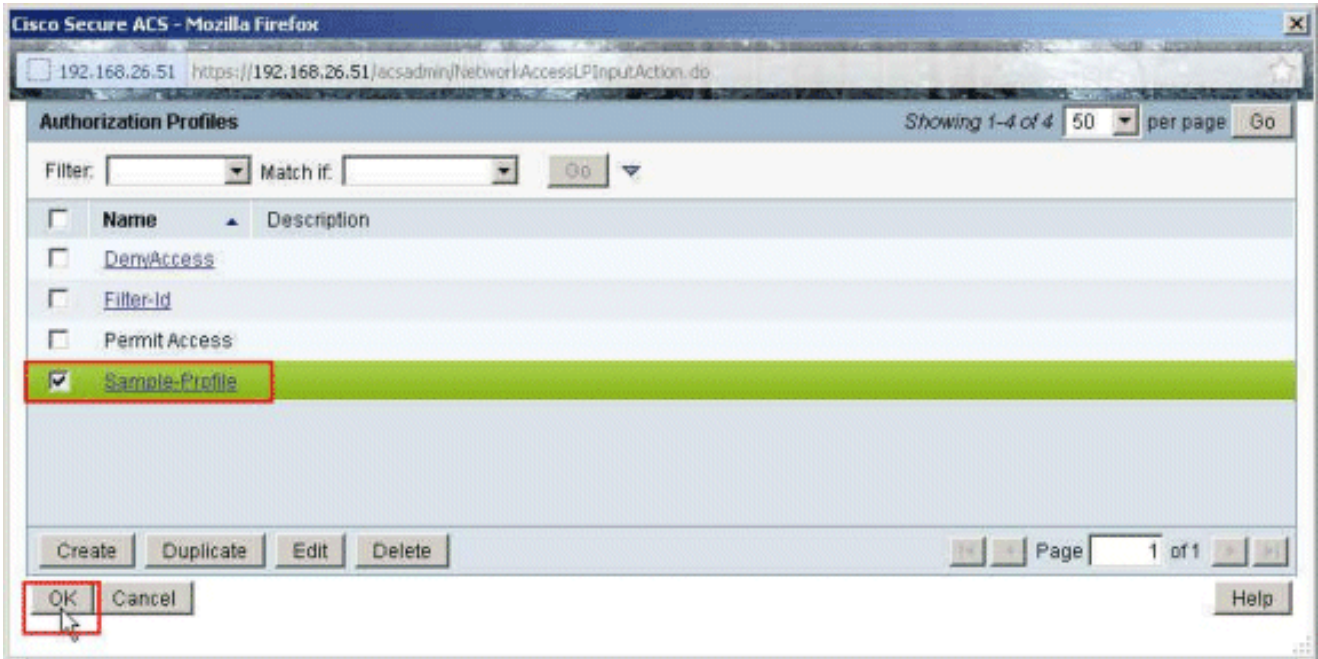
15. عمىاق مسال ةلدسنملا عمىاقلا نم تابا ددحو، ةكرشم ماهم بيوبتلا عمال ع رتخأ
جذومن) اتي دح هؤاشنإ مت يذلا DACL رتخأ. لي زنتلل لباقلا (ACL) لوصول ي ف مكحتلا
عميقلل ةلدسنملا عمىاقلا نم (DACL)



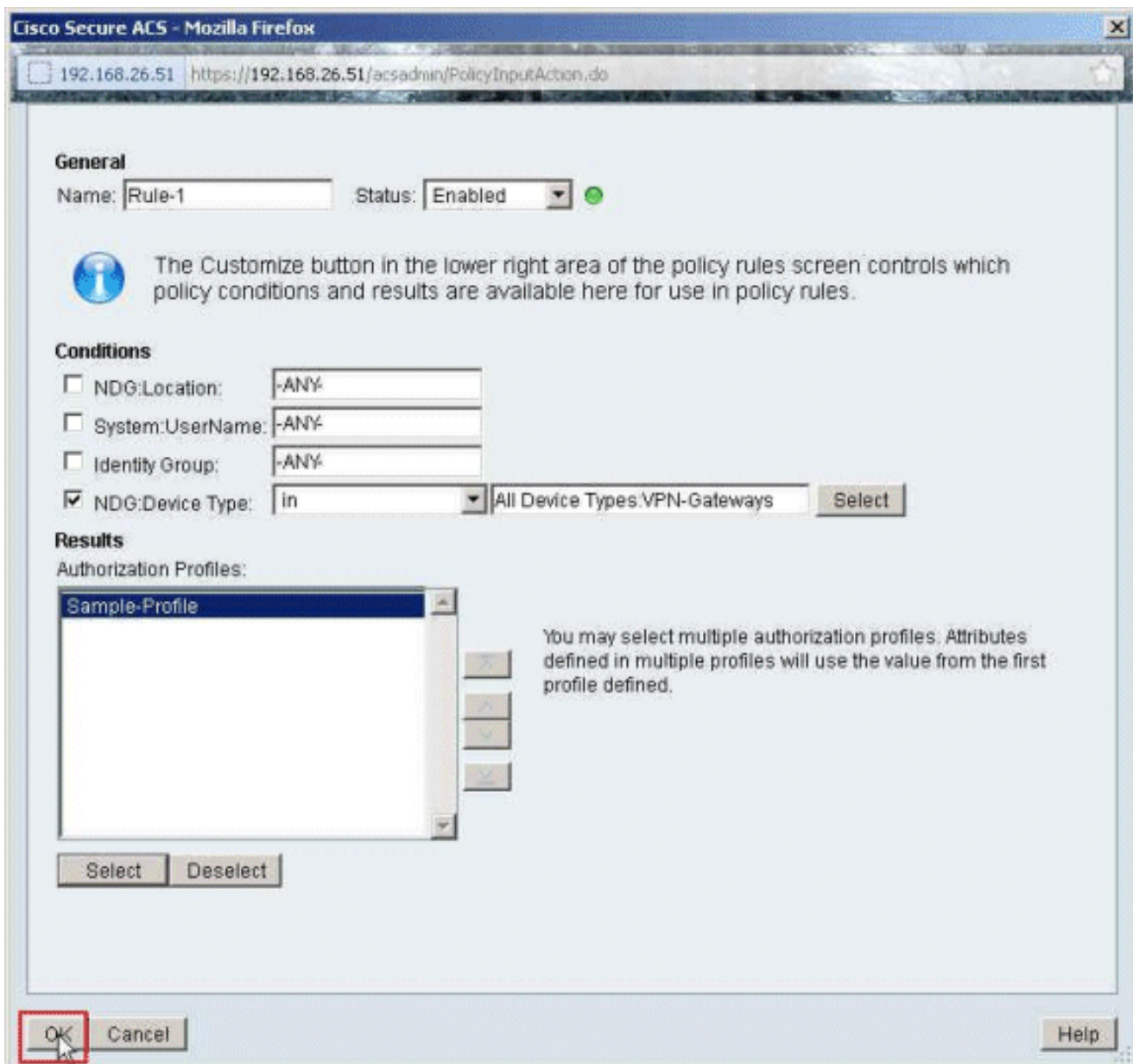
16. لاسر را دلج رقنا



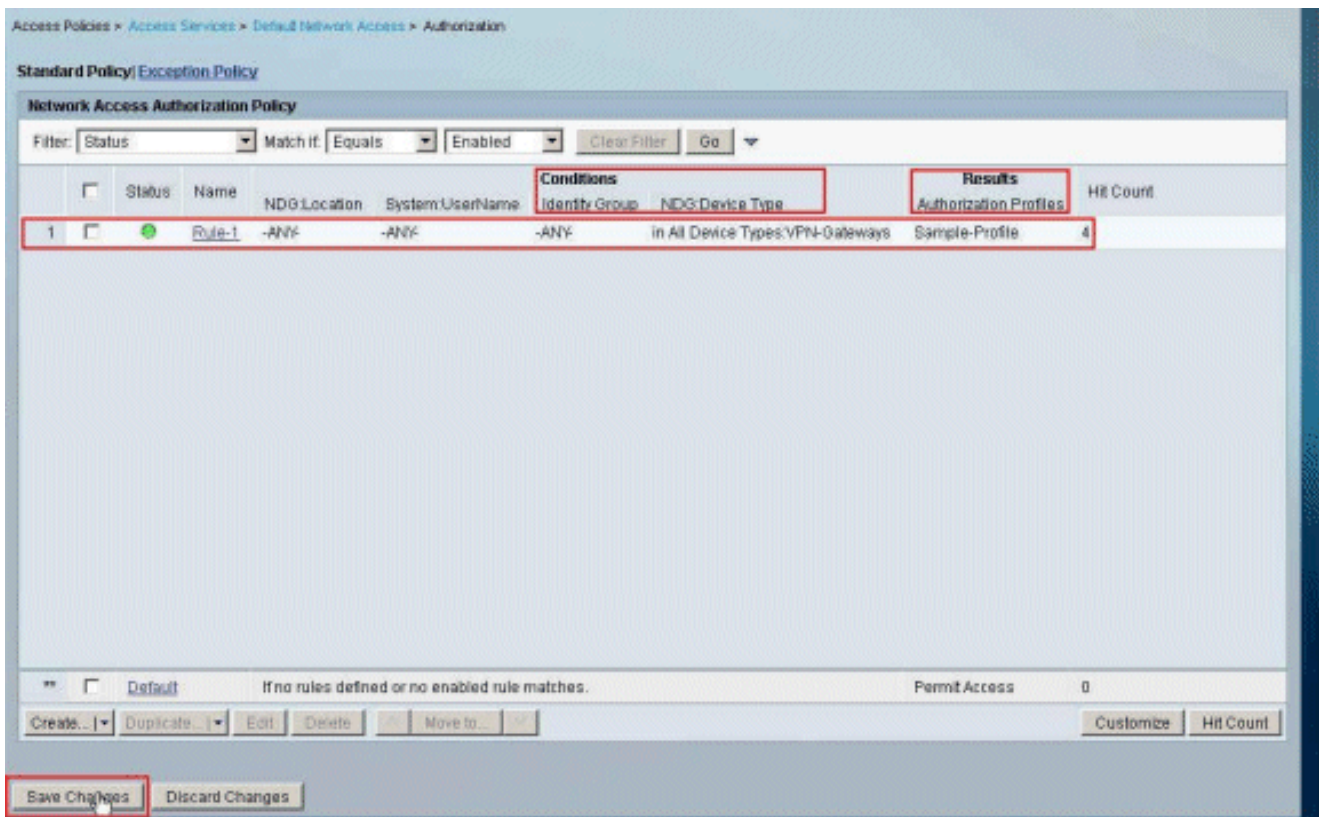
17. قفاوم رقناو، اقباس هؤاشنإ مت يذلا فيرعتلا فلم جذومن ددح



18. OK قوف رقناو



19. عېتن نم و، زاهال عون:NDG ؤلا ك VPN تارابع مادختساب 1-ءءءال ءاشن نم ققءت تاريغءال ظفء قوف رقنا . فءرءال فلم ءءومن ك لء



نېم دځتسم ؤعومچمل IETF RADIUS تادادع| نېوكت

دنع RADIUS م داځ نم نامألا زاځ ىلع لعفلاب اهئاشناب تمق لوصو ؤمئاق ل مسا لېزننل (11 مقر ؤمسلا) IETF RADIUS filter-id ؤمسلا نېوكتب مق ،م دځتسم ل ؤقداصم

```
<#root>
```

```
filter-id=acl_name
```

مسا لېزننن راديوس م داځ موقو و ،حاجنن Cisco ؤقداصمب ؤنېعلا ؤعومچم م دځتسم موقو نامألا زاځ ىلع لعفلاب اهئاشناب تمق لوصو ؤمئاق ل (دېج) لوصولو ي ف مكحتلا ؤمئاق م داځ اناثتساب ASA ؤكبش لخاد ؤدوچوملا ؤزهألا عيمج ىل لوصولو "cisco" م دځتسم ل نكمي [ي ف مكحتلا ؤمئاق](#) مسق عجار ،(ACL) لوصولو ي ف مكحتلا ؤمئاق نم ققحتلل 10.1.1.2. [ي ف صتلا فرع م ىلا لوصولو](#).

ي ف ؤي فصتلا ؤديج ؤامسلا (ACL) لوصولو ي ف مكحتلا ؤمئاق نېوكت مت ،لاثلل اق فو ASA:

```
<#root>
```

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

نېوكتب تمق دقل . ؤحېحص نوكت ام دنع طقف تامل عمل هذه رهظت

• ةكبش لال نيوكت في RADIUS تالوكوتورب دحأ مادختسال AAA ليمع

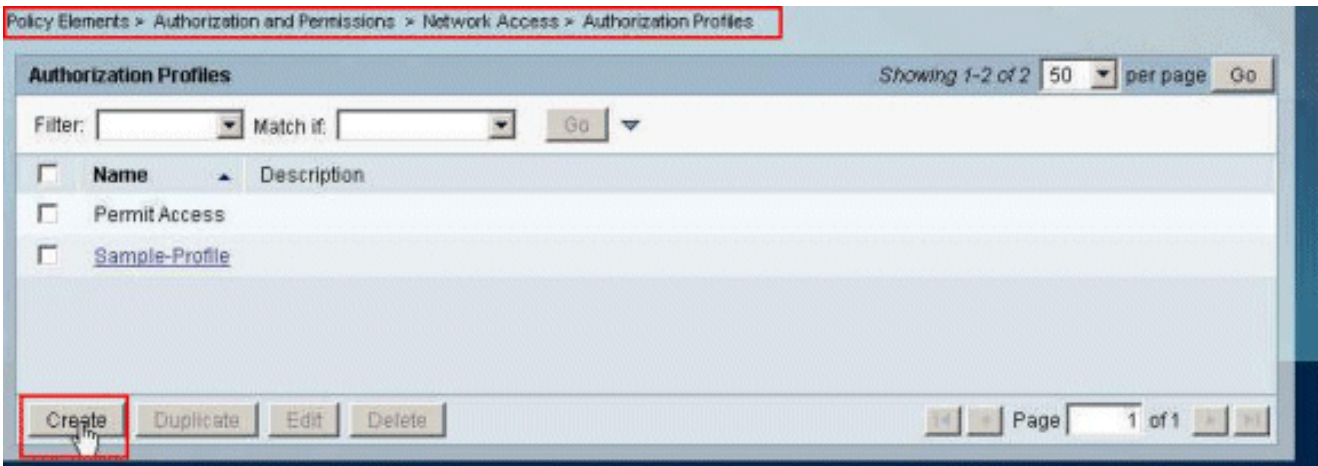
• مسق نمض (IETF) RADIUS فرعم ةيفصت لاماعب ضيوفت فيرعت فلم ديدحت متي لوصول ةمدخ في ةدعاقلا نم جئاتنلا

بلاطال AAA ليمع لى ACS نم مدختسم لك فيرعت فلمك RADIUS تامس لاسرا متي

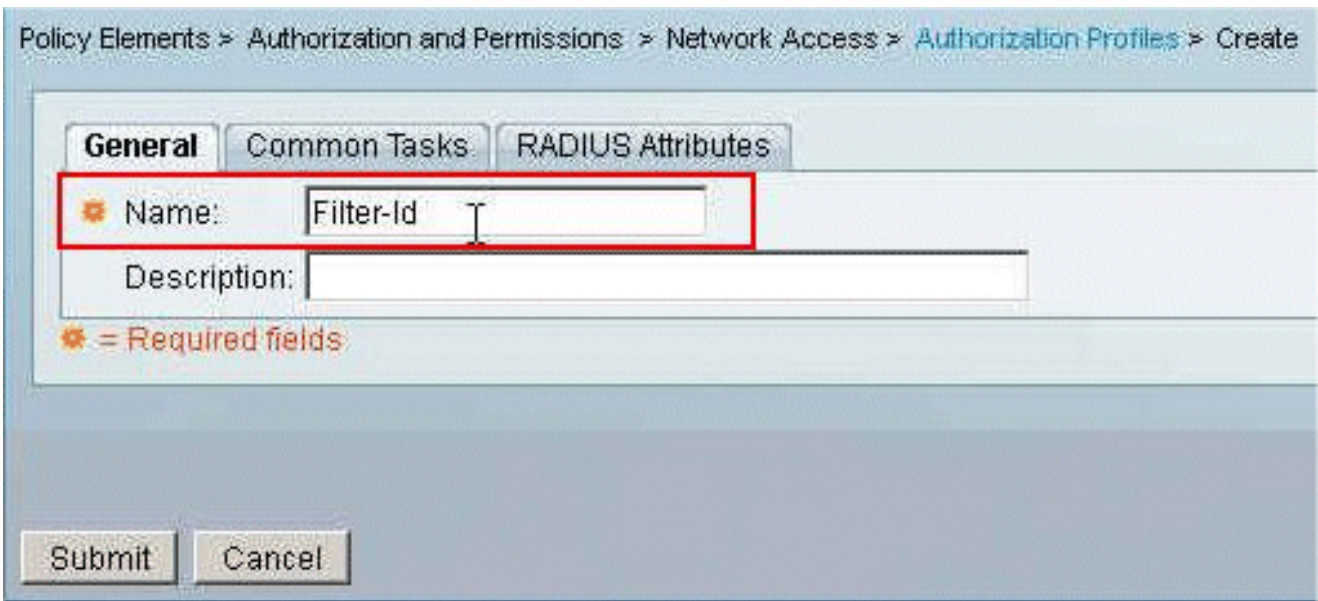
(ACL) لوصولاب مكحتلا ةمئاقلا ACS نيوكت نم 12 لى 10 و 6 لى 1 نم تاوطخلا لمكأ ACS نيوكت نم 6 لى 1 نم تاوطخلا ب ةعوبتم ، فيدر فلما مدختسم لى لى زنتلل ةلباقلا مسقلا اذه في تاوطخلا هذه مقأو ، ةعومجمل لى زنتلل ةلباقلا لوصولاب في مكحتلا ةمئاقلا . نم آل ACS Cisco في ةيفصتلا فرعم نيوكتل

ذفن ، ليوختلا فيصوت في لجال وه امك اهقبيبطتل IETF RADIUS ةمس تاداعل نيوكتل ةلياتلا تاوطخلا

1. فيرعت تافلما > ةكبش لال لى لوصولاب > اتانوذال او ضيوفتلا > جهنلا رصانع رتخأ ديدج ضيوفت فيرعت فلم عاشنال عاشنل قوف رقناو ، ضيوفتلا



2. فيرعت فلم مسا وه ةيفصتلا لاماع فرعم . ليوختلا فيرعت فلم مسا ريفوتب مق ة. طاسبلل لاثملا اذه في هرايتخا مت يذلا ليوختلا



3. عمىاق ل ءلءسنم ل عمىاق ل نم ءءبء رءءاو؁ ءك رءشم مام بىوبء ل عمال ء قوف رءن اءءء ل وءول عمىاق مسا لءءا. ءى فءء ل فرعم ب ءصاء ل (ACL) ل وءول ءى مءء ل ل. اسرل قوف رءن او؁ عمىق ل لءء ءى

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

General **Common Tasks** RADIUS Attributes

ACLs

Downloadable ACL Name: Not in Use

Filter-ID ACL: Static Value new

Proxy ACL: Not in Use

Voice VLAN

Permission to Join: Not in Use

VLAN

VLAN ID/Name: Not in Use

Reauthentication

Reauthentication Timer: Not in Use

Maintain Connectivity during Reauthentication:

QoS

Input Policy Map: Not in Use

Output Policy Map: Not in Use

802.1X-REV

LinkSec Security Policy: Not in Use

URL Redirect

When a URL is defined for Redirect an ACL must also be defined

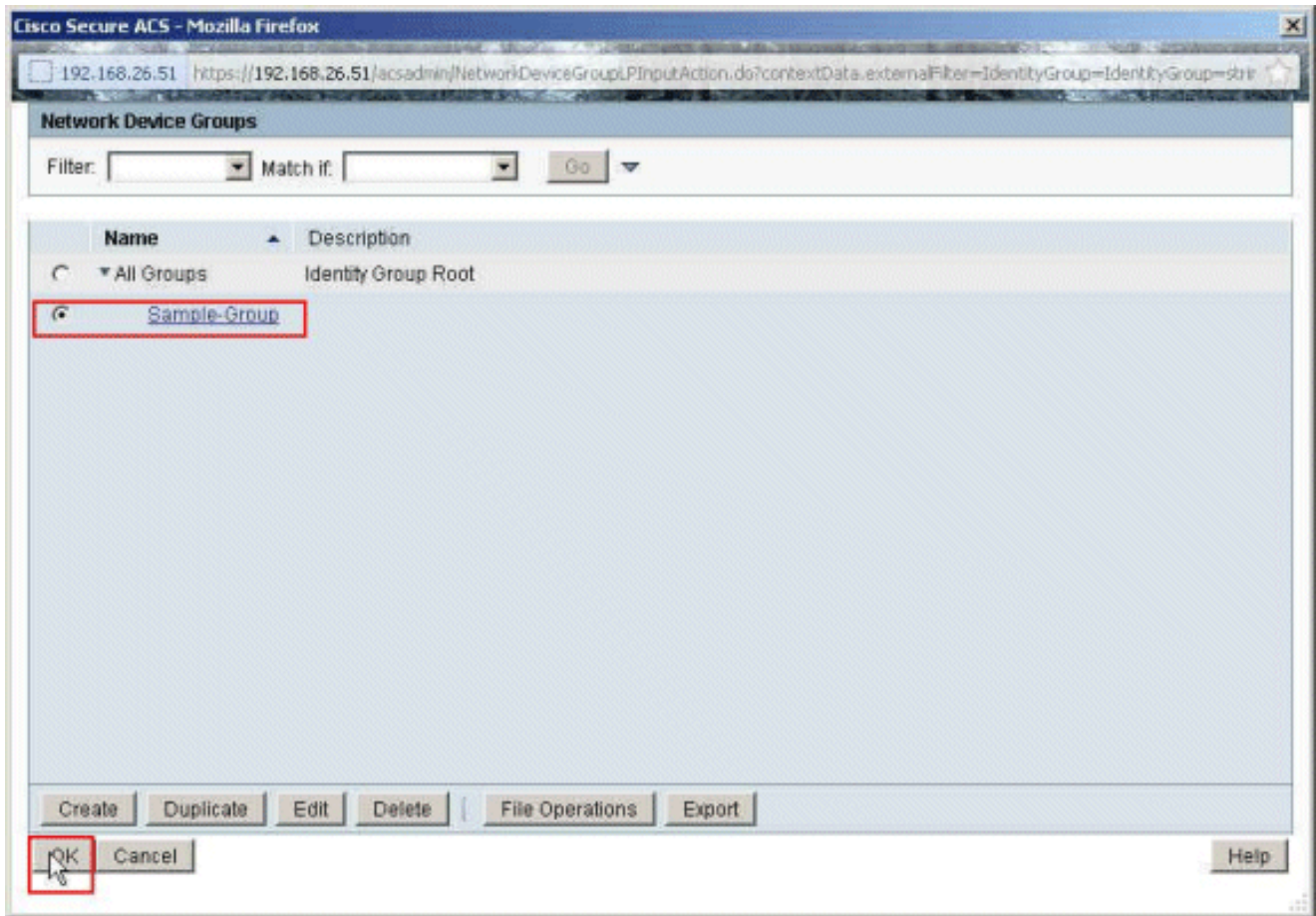
URL for Redirect: Not in Use

URL Redirect ACL: Not in Use

☛ = Required fields

Submit Cancel

4. > ءك بء ل ل ءى ءارء ف ال ل وءول > ل وءول ءامءء > ل وءول ءاسل رءءا ءءءء ءءءاق ءاشن ال ءاشن ل قوف رءن او؁ ءى وء ل




7. ليوختلا تافى صوت مسق ي ف ديدحت لىل ع رقنا

Cisco Secure ACS - Mozilla Firefox

192.168.26.51 https://192.168.26.51/acsadmin/PolicyInputAction.do

General
Name: Rule-1 Status: Enabled

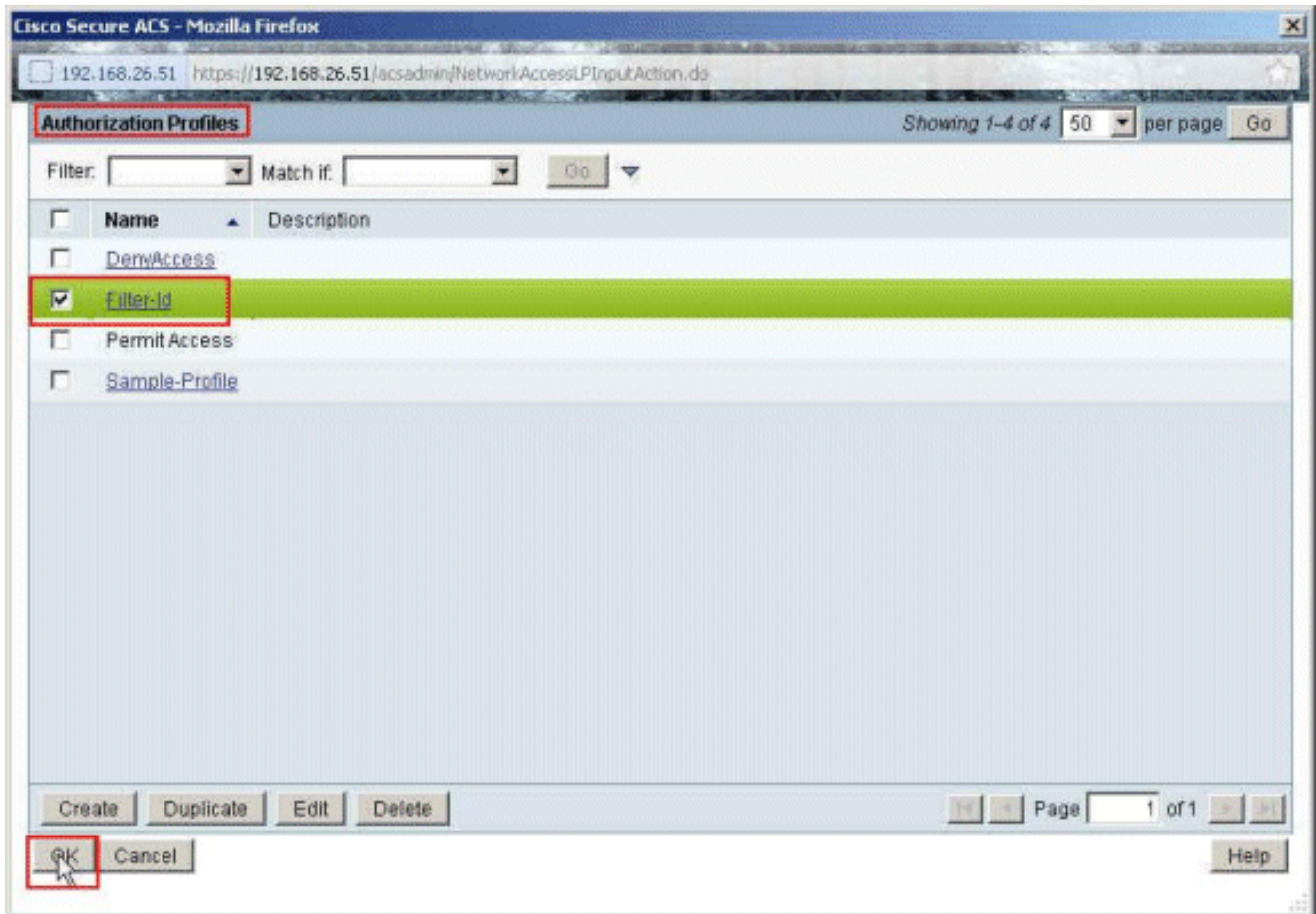
 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 NDG:Location: -ANY
 System:UserName: -ANY
 Identity Group: In All Groups:Sample-Group

Results
Authorization Profiles:

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.


8. قوف روناو، اقبس م هاشنا م يذلا ليوختلا فيرت فلم ةيفرت لماع فرعم رتخأ قفاوم.




9. OK قوف روناو

Cisco Secure ACS - Mozilla Firefox

192.168.26.51 https://192.168.26.51/acsadmin/PolicyInputAction.do



General
 Name: Rule-1 Status: Enabled 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions



NDG:Location: -ANY

System:UserName: -ANY




Identity Group: In  All Groups:Sample-Group 

Results
 Authorization Profiles:

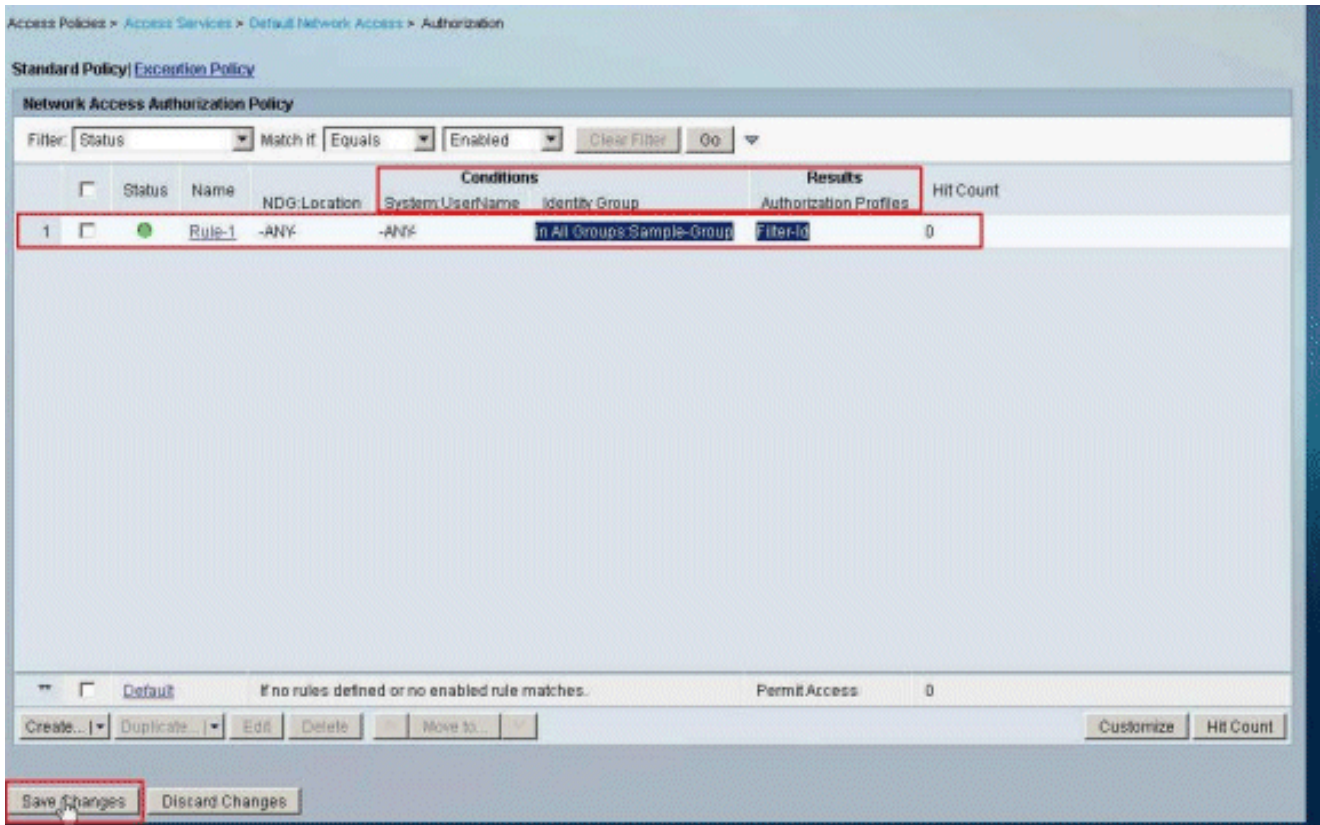
Filter-Id

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

10. filter-id وطرشك ةومجم لة ةوه تان ةومجم مادختساب 1- ةءاق لءاشنا نم ققحت تاريغ لءاطفح قوف رقنا .كلذل ةءيتن



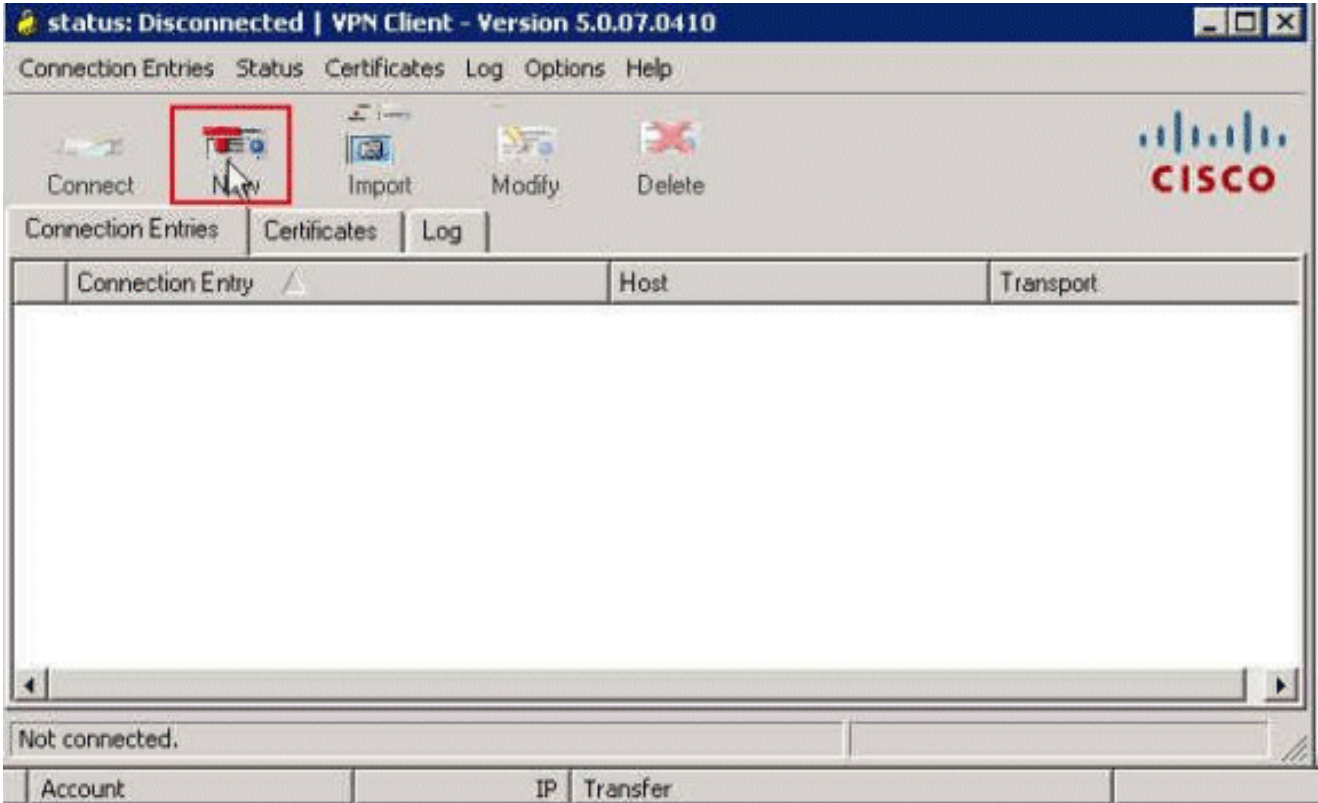
Cisco VPN ةكبش ليمع نيوكت

حاجب ASA نيوكت نم ققحتلل Cisco VPN ليمع مادختساب Cisco ASA ب لاصتالاب مق

ةيلاتلا تاوطخلا لمكأ

1. نوبز VPN > نوبز VPN ماظن cisco > م انرب > ةيادب ترتخأ

2. ةذفان لخدم ليصوت VPN ديح create ل تقلطأ in order to ديح تقطوط



3. ديدجلا كلاصتلا ليصافت ألاما

a. فصو عم "لاصتالا لاخدا" مسالاخدا

b. قودنص فيضمالا في ASA لانا ميجراخ ناووعلا تلخد

c. اقابسما كرتشم حاتفم) رورملا ةملكو (VPN (Cisco-Tunnel) قفنة وعومجم مسالاخدا
ASA في اهن يوكت متامك (Cisco123)

d. ظفح قوف رقنا

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

CISCO

Authentication: Transport: Backup Servers: Dial-Up:

Group Authentication Mutual Group Authentication

Name:

Password:

Confirm Password:

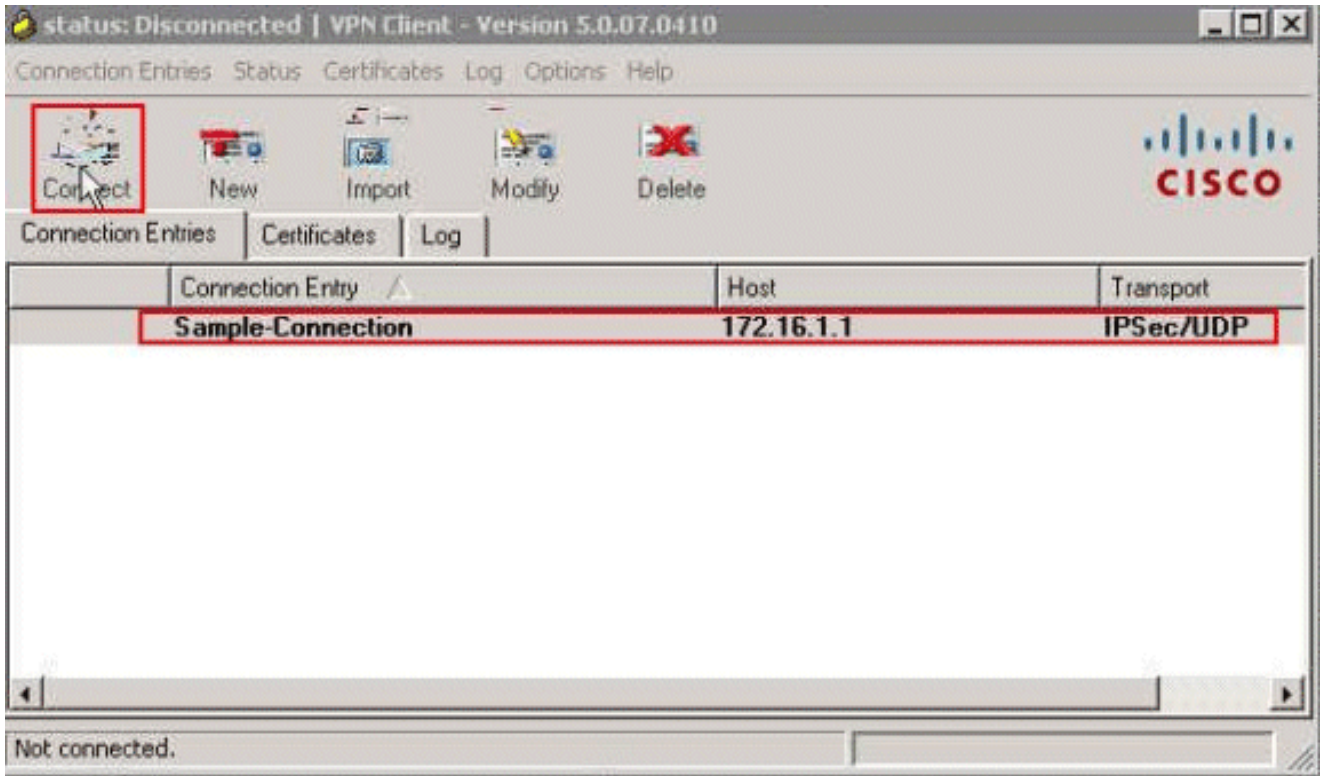
Certificate Authentication

Name:

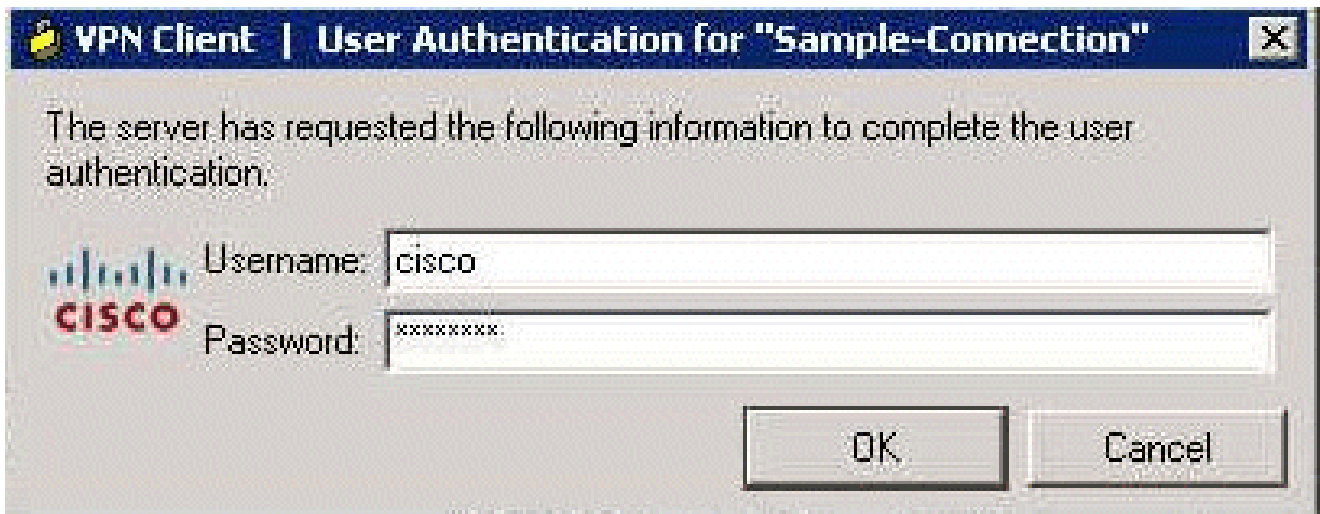
Send CA Certificate Chain

Erase User Password

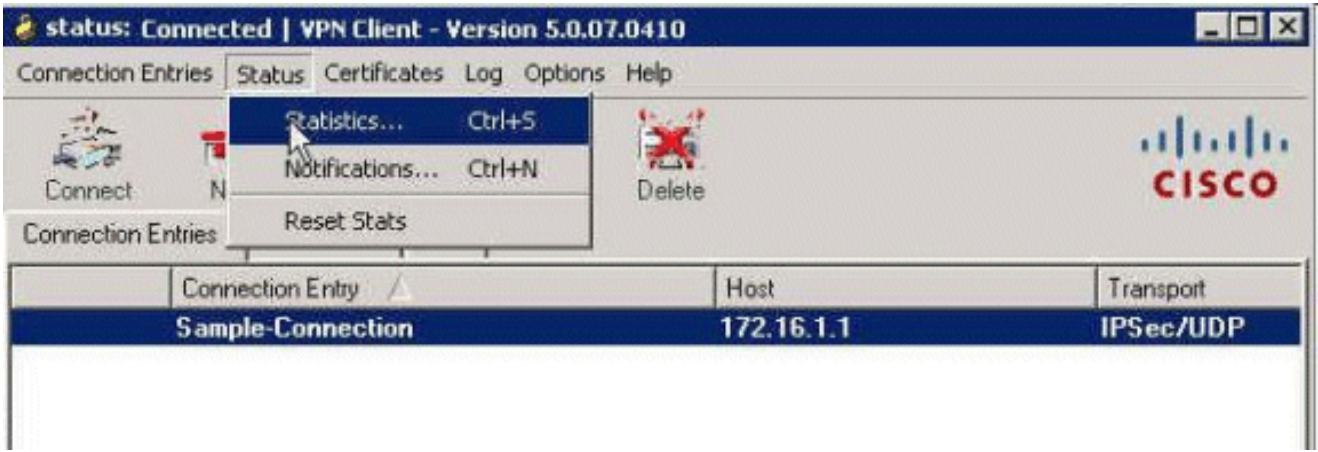
4. يسيئرلا راطالال نم لاصتالال قوف رونا م، همادختسا ڊرت يذلا لاصتالال قوف رونا
VPN ةكبش ليمعل



5. ةقداصم لل ASA لا يف تلكش امك cisco123 ةم لك و username cisco لا ، ثح ام دنع تلخد ديعب ةكبش لا ال تطبر ok in order to ةق طقو



6. لى صافات نم ققحت لل ةلاح ال ةمئاق نم تاىئاصح ارتخأ ، حاجنب لاصتال سىسأت درجمب ققنلا



ةحصل لا نم ققحت لا

ححص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

مجرتم ةادأ مدختسا. show رماوا ضعب (طقف ني لجس ملءالمعلل) جارخالا مجرتم ةادأ معدت
show رمالا جرّم ليلحت ضرعل (OIT) جارخالا .

ري فشتلا رماوا راهظا

- ريظن يي ف (SAs) ةيلال IKE نامأ تانارتقا عيمج ضرعي - show crypto isakmp sa

```
<#root>
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#
```

- ةيلال SAs لبق نم ةمدختس مل تادادعإل ضرعي - show crypto ipSec

```
<#root>
ciscoasa#
sh crypto ipsec sa

interface: outside
Crypto map tag: SYSTEM_DEFAULT_CRYPTOMAP, 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_CRYPTOMAP
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_CRYPTOMAP
sa timing: remaining key lifetime (sec): 28678
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ةومجمل/مدختسملل ليزنللةلباقلا (ACL) لوصولا يف مكحتلاةمئاق

متي Cisco. مدختسملل ليزنللةلباقلا (ACL) لوصولا يف مكحتلاةمئاق نم ققحت
CSACS. نم (ACL) لوصولا يف مكحتلاةمئاق ليزنللةلباقلا

<#root>

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

```

ةيفصتلا لماع فرعمل (ACL) لوصولا يف مكحتلا ةمئاق

ةومجملا يف مدختسم ةيفصت متي و، Sample-Group - ةومجملا ىلع Filter-ID [011] قيبطت مت
 ASA. يف ةدحمل (ةديجل) (ACL) لوصولا يف مكحتلا ةمئاق لاقو

```
<#root>
```

```
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

```

اهالصالو ءاطخال فاشكتسا

متي. اهالصالو نيوكتلا ءاطخال فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي
 ةنيعلل ءاطخال حيحصت جارخا ضرع اضيأ

IPsec ب ءصال VPN ءكبش ءاطخال فاشكتسال لوح تامولعمل نم ديزم ىلع لوصولل: ءظالم
 (VPN) ءرهاظلا ءصال ءكبشلا ءاطخال فاشكتسال [لوح](#) ىلإ عجرا، اهالصالو دعب نع لوصولل
 .دعب نع لوصولو L2L ل

ةينمألا تانارتقالا حسم

يف. ريغت ءارخا دعب ءدومل SA تالاح حسم نم دكأت، اهالصالو ءاطخال فاشكتسال دنع
 ءيلاتل رموأل مدختسا، PIX ل تازايتمالا يذ عضولا

- ءيساسألا ءملكلا ريفشت. ءطشنل IPsec تاكبش فذحي - ipSec sa [crypto] حسم
 يرايخا

- ءيساسألا ءملكلا ريفشت. ءطشنل IKE تاكبش فذحي - isakmp sa [crypto] حسم
 يرايخا

اهحالصإو عاطخألا فاشكتسا رماوأ

مجرتم ةادأ مدختسا . show رماوأ ضعب (طوقف نيلجس ملءالمعلل) جارخالا مجرتم ةادأ معدت . show رمالا جرخم ليلحت ضرعل (OIT) جارخالا

debug رماوأ مادختسا لباق حيصتلا رماوأ لوح ةمهم تامولعم ىلا عجرا :ةظحالم

- 2. ةلحرم لل IPsec تاضوافم ضرعي - debug crypto ipSec 7
- 1. ةلحرم لل ISAKMP تاضوافم ضرعي - debug crypto isakmp 7

ةلص تاذا تامولعم

- [Cisco ASA 5500 Series](#) نم فيكتلل ةلباقلا نامألا ةزهجأ معد ةحفص
- [Cisco ASA 5500 Series Adaptive Security Appliances Command References](#)
- [Cisco](#) نم ةلدعمل نامألا لولح ةزهجأ ريديم
- [IKE](#) تالوكوتورب/IPsec ةضوافم معد ةحفص
- [Cisco](#) نم VPN ةكبش لييمع معد ةحفص
- [Cisco](#) نم نامألا لوصولا يف مكحتلا ماظن
- [\(RFCs\)](#) تاقيلعتلا تابلط
- [Cisco Systems](#) - تادنتس ملأو ينقتلا معدلا

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت
ملاعلاء انء مچ م ف ن م دخت تسمل معد و ت م م دقت ل م شرب ل و
امك ة قق د نوك ت نل ةللأل مچرت ل ضف أن ة ظحال م مچر م . ة صا ل م م ت غ ل ب
Cisco مچرت م م دقت م م ت ل ة م ف ارت حال ة مچرت ل م لاعل و م
للإمءاد وچرلاب م صؤت و ت مچرتل هذه ة قق د ن م م ة ل وئ م م
Systems م (رف و تم ط بارل) م ل صأل م م مچر ل ن ل دن تسمل