

AnyConnect Secure Mobility Client نيوكت ىلع مّسقملا يقفنلا لاصتالا مادختساب ASA

تايوتحملا

[عمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[AnyConnect صيخرت تامولعم](#)

[نيوكتلا](#)

[ةكبش لىل يطيختلا مسرلا](#)

[ASDM AnyConnect نيوكت جلاعم](#)

[ميسقتلا قفن نيوكت](#)

[هتبيثتو AnyConnect Client ليزنت](#)

[بيولا رشن](#)

[لقستسملا رشنلا](#)

[\(CLI\) رماوالا رطس ةهجاو نيوكت](#)

[ةحصلا نم ققحتلا](#)

[اهخالص او اطاخال افاشكتسا](#)

[DART تيبتت](#)

[DART ليغشت](#)

[ةلص تاذا تامولعم](#)

عمدقملا

ةزهجأ ريديم ربع Cisco AnyConnect Secure Mobility Client نيوكت ةيفيك دننتملا اذه فصبي رادصلا لغشي يذلا (ASA) فيكتلل لباقل نامالا زاغ ىلع Cisco نم (ASDM) ةلدعمل نامالا جمانربلا نم 9.3(2).

ةيساسألا تابلطتملا

تابلطتملا

حطس ىلى Cisco AnyConnect Secure Mobility Client ب ةصاخلا بيولا رشن ةمزح ليزنت بجي ةحفص ىلى عجرا، ليمعلا ةمزح ليزنتل ASA ىلى ASDM لوصو هنم دجوي ذللا يلحملا بتكملا ليغشت ةمظنال بيولا رشن مزح ليحت نكمي. [Cisco AnyConnect Secure Mobility Client](#) بيو تقولا سفن في ASA ىلى (OS) ةفلتخم.

ةفلتخملا ليغشتلا ةمظنال بيولا رشن تافلما ءامسأ يه هذه:

- Microsoft Windows - AnyConnect-win-<version>-k9.pkg لي غشتلا ةمظنا
- Macintosh (MAC) - AnyConnect-Macosx-i386-<version>-k9.pkg لي غشت ةمظنا
- Linux - AnyConnect-Linux-<version>-k9.pkg لي غشت ةمظنا

ةمدختس مالتا نوكملا

ةيالاتلا ةيداملا تانوكملا وجماربال تارادصلإ لىل دننتس مالا اذو يف ةدراولا تامولعمل دننتست

- ASA رادصلإ 9.3(2)
- ASDM رادصلإ 7.3(1)101
- AnyConnect، رادصلإ 3.1

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دننتس مالا اذو يف ةدراولا تامولعمل عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دننتس مالا اذو يف ةمدختس مالا ةزهجال عيمج تادب رما يال لمحتحمل ريثاتلل كمهف نم دكأتف، ةرشابم كتكبش

ةيساسأ تامولعم

Cisco نيوكت جلالعم مادختسا ةيفيك لوح ةوطخب ةوطخ ليصافت دننتس مالا اذو مدقي ماسقنملا يقفنلا لاصتالا نيوكمتو AnyConnect ليمع نيوكتل ASDM ربع AnyConnect

تاونق عاشنإ اهي بجي يتلا تاهوي رانيسلا يف ماسقنملا يقفنلا لاصتالا مادختسا متي رورم تاكرح عيمج اهي قفدتت يتلا تاهوي رانيسلاب ةنراقم، طوقف ةنيعم رورم ةكرحل دنن (VPN) ةيره اظلا ةصاخلا ةكبشلا ربع ليمعلا زاهج ةطساوب اهواشنإ متي يتلا تانايبلا tunnel-all نيوكت لىل يضا رتفا لكشب AnyConnect نيوكت جلالعم مادختسا يدويس. لاصتالا حورش متي ام وهو، لصفنم لكشب ماسقنملا يقفنلا لاصتالا نيوكت بجي. ASA لىل دننتس مالا اذو ماسقنملا يقفنلا لاصتالا نيوكت بجي. ASA لىل دننتس مالا اذو ماسقنملا يقفنلا لاصتالا نيوكت بجي.

10.10.10.0/24 ةي عرفلا ةكبشلا تانايبلا رورم ةكرح لاسرا وه فدهلا، اذو نيوكتلا لاثم يف عيمج هي جوت ةداعإ متت VPN قفن ربع، ASA فلخ LAN ةكبشلا ةي عرفلا ةكبشلا يه يتلا وه ةصاخلا تنرتنإل ةرئاد ربع ليمعلا زاهج نم ىرخالا تانايبلا رورم تاكرح

AnyConnect صيخرت تامولعم

Cisco AnyConnect Secure صيخرت لوح ةديفم تامولعم لىل تااطابترا لىل ضعبي اميف Mobility Client:

- دننتسم [لي غشتلا ةمظنا او، صيخرتلا او، AnyConnect Secure Mobility Client تازيم](#) لىل عجرا تازيملاو AnyConnect Secure Mobility Client ل ةبولطملا صيخرتلا دي دختل [3.1 رادصلإ](#) ةلصل تاذا
- AnyConnect صيخرت لوح تامولعم لىل لوصحلل [Cisco AnyConnect بولط لىل](#) لىل عجرا Top و Plus.
- دننتس مالا [؟ لومحمل افتاهلل VPN و IP Phone تالاصتال مزلي يذلا ASA صيخرت](#) لىل عجرا IP و IP Phone تالاصتال ةيفاضالا صيخرتلا تابلطتم لوح تامولعم لىل لوصحلل

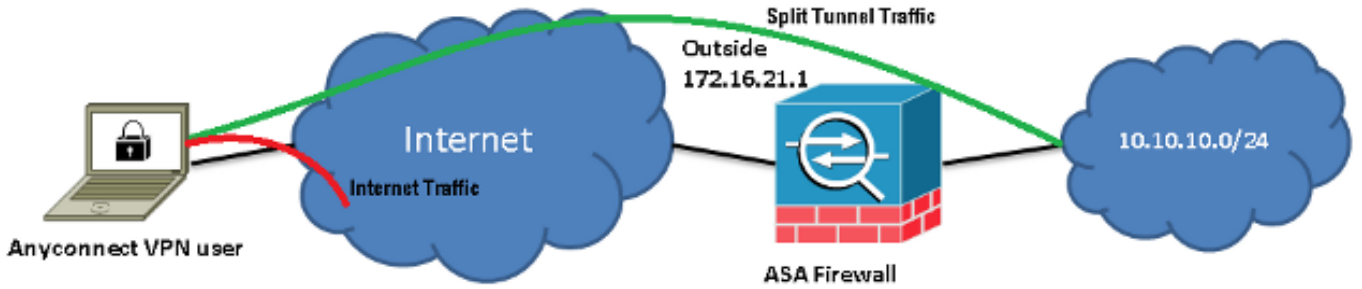
لومحمل فتاهلل.

نيوكتلا

ASA على Cisco AnyConnect Secure Mobility Client نيوكتة في فيك مسقلا اذه فصري

ةكبش لل يطي طختلا مسرلا

دنتس مالا اذه في ةدراولا ةلثمألل همادختسا متي يذلا ططخملا وه اذه

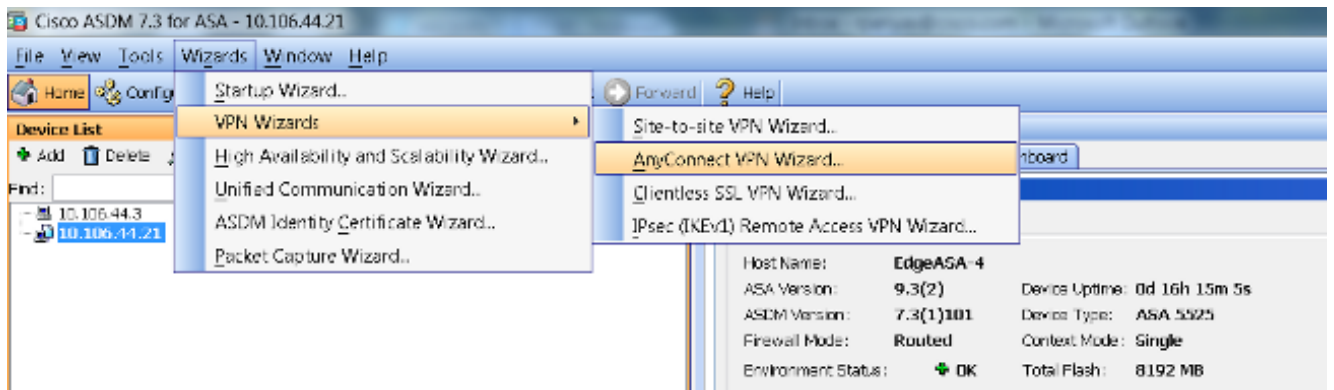


ASDM AnyConnect نيوكت جلاعم

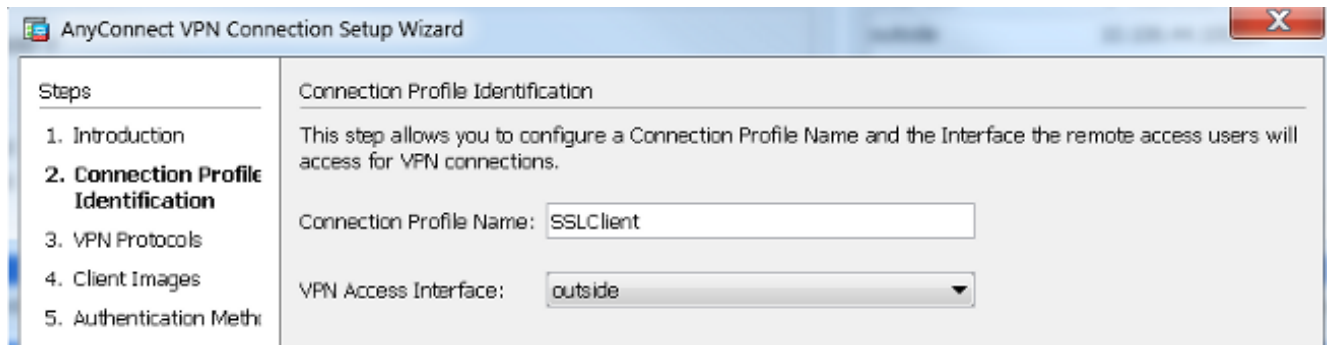
دكأت AnyConnect Secure Mobility Client نيوكتلا AnyConnect نيوكت جلاعم مادختسا نكمي ةعباتملا لبق ASA ةيامح رادجل Flash/disk ةركاذى لى AnyConnect ليمع ةمزل ليحت نم

نيوكتلا جلاعم لالخنم AnyConnect Secure Mobility Client نيوكتلا تاوطخلل هذه لمكأ

1. يلاتلا قوف رقناو، نيوكتلا جلاعم ليغش تب مقو، ASDM لى لوخللا لجس:



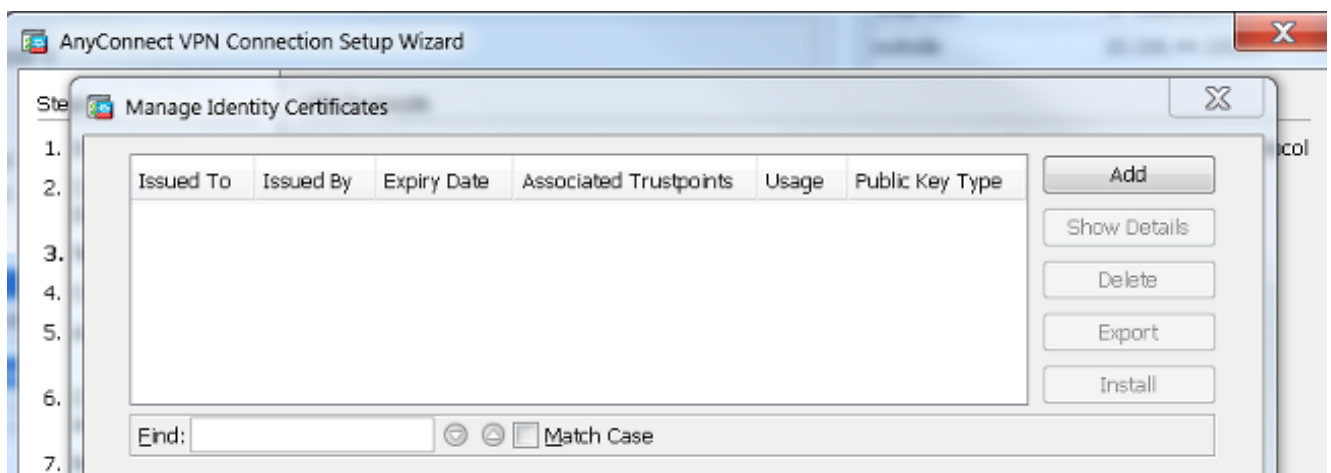
2. ةمئاقلا نم اهليع VPN ءاهن متيس يتلا ةهجاولا رتخاو، لاصتالا فيرعت فلم مسالا لخدأ. يلاتلا قوف رقناو، VPN ةكبش لى لوصول ةهجاو ةلدسنملا



3. نوكت نأ نكمي (SSL) ةنمآلا لئصوتلا ذخآم ةقبط نئيكم تل SSL رايئتخالا ةناخ دح (Verising لثم) ةيجراخلا ةهجلل ةعبات قيصدت ةئيه نع ةرداص ةداهش زاوجل ةداهش نكمي ف ASA، لعل لعفلاب ةتبتثم ةداهشلا تناك اذا. ايتاذ ةعقوم ةداهش وأ (Entrust) مداخل بناج نم ةداهشلا يه ةداهشلا هذه: **ةطحالم**. ةلدسنملا ةمئاقلا لالخنم اهرايتخا ةداهش عاشنا بجيو، ASA لعل ايلاح ةتبتثم تاداهش دجوت مل اذا. اهريفوت متيس يتلا ةحوضوملا تاوطخلا لامكإب مق، ةيجراخ ةهج ةداهش تيبتتل. **ةراد** قوف رقناف، ايتاذ ةعقوم نيوكت لاثم عم اهم ادختس ال ايودي ةيجراخ ةهج دروم تاداهش تيبتتب مق، ASA 8.x يف [WebVPN](#) Cisco دننتم.



4. فيضي ةق طوط:



5. ةديج ةيوه ةداهش ةفاضل رزلا قوف رقنوا، TrustPoint مسلا ل قح يف ابسانم امسا بتكا.

رقنا، زاهجلا ىلع ةدوجوم Rivest-Shamir-Addleman (RSA) حيتافم جاوزاً كانه نكي مل اذا دحاو عاشنإل ديديج قوف:

Trustpoint Name: SelfsignedCert

Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From: Browse...

Add a new identity certificate:

Key Pair: <Default-RSA-Key> Show... New...

Certificate Subject DN: CN=anyconnect.cisco.com Select...

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Advanced...

Add Certificate Cancel Help

6. مسا لخدأو ديديج حيتافم جوز مسا لخدأو رز رقنا وأ يضارتفالال حيتافملا جوز مسا رز رقنا 6. نألأ عاشنإل رقنا م، حيتافملا مچج دح. ديديج:

Key Type: RSA ECDSA

Name: Use default key pair name Enter new key pair name: sslcert

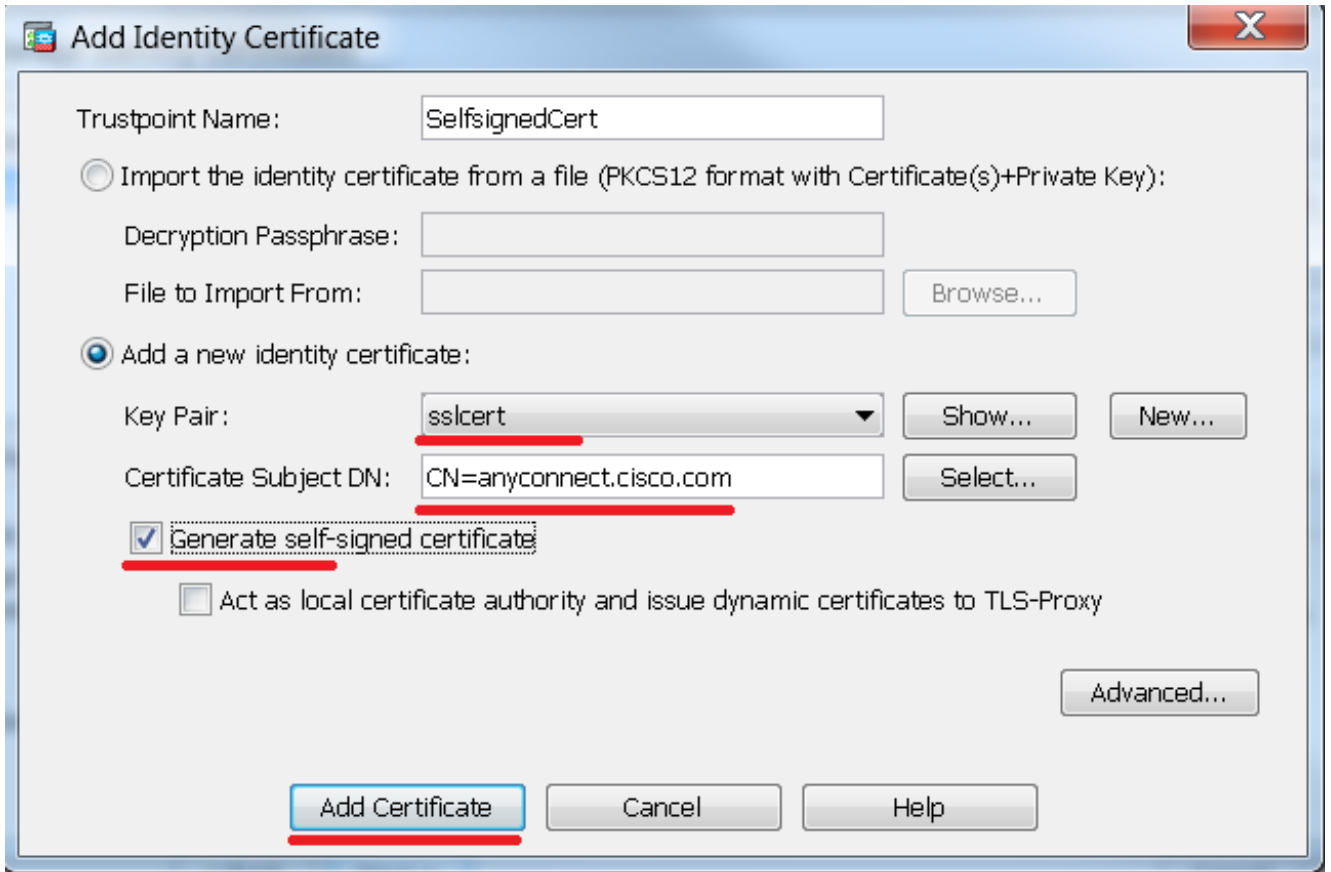
Size: 2048

Usage: General purpose Special

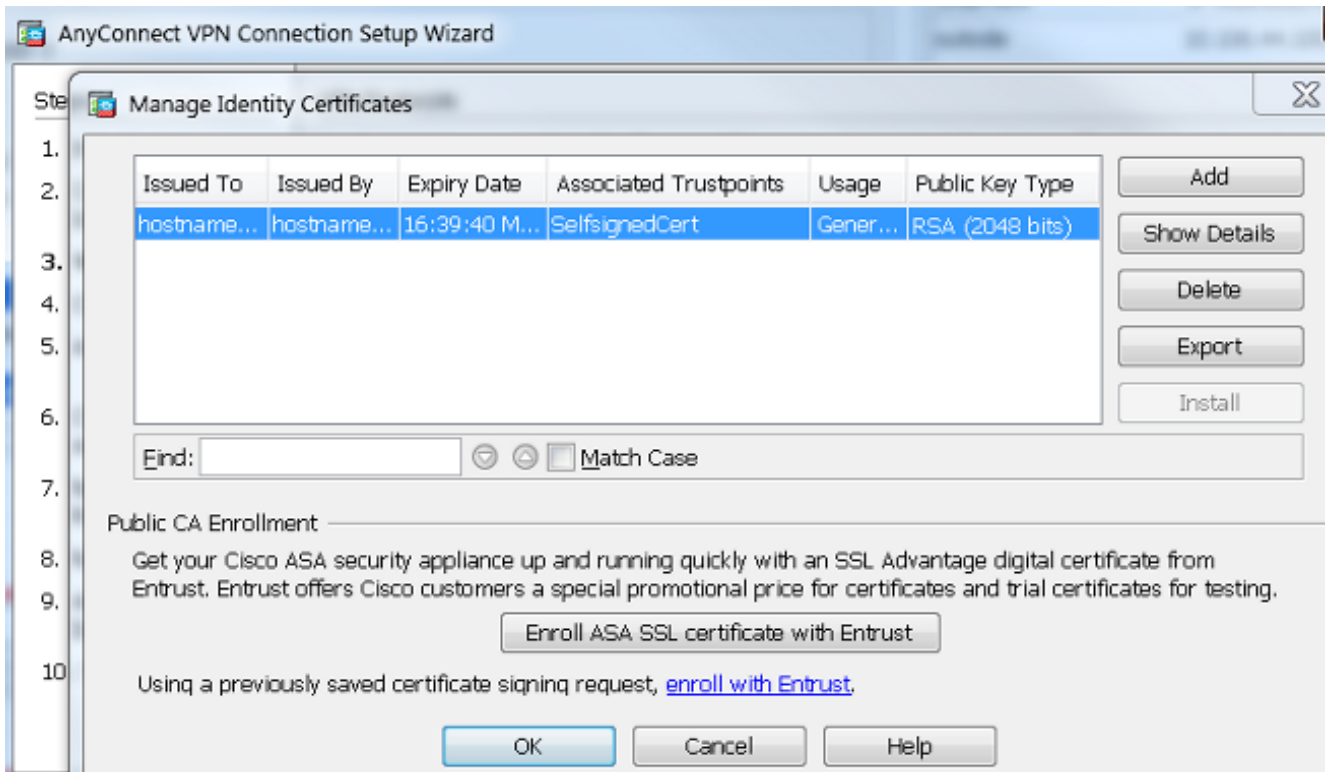
Generate Now Cancel Help

7. ايتاذ ةعقوم ةداهش عاشنإل رايخالا ةناخ ددحوحاتفملا رتخأ، RSA حيتافم جوز عاشنإل دعب. ىلع رقنا م، DN ةداهشلا عوضوم لقح ي ف بولطملا (DN) عوضوملا لاجم مسا لخدأ

عداش ةفاضل:

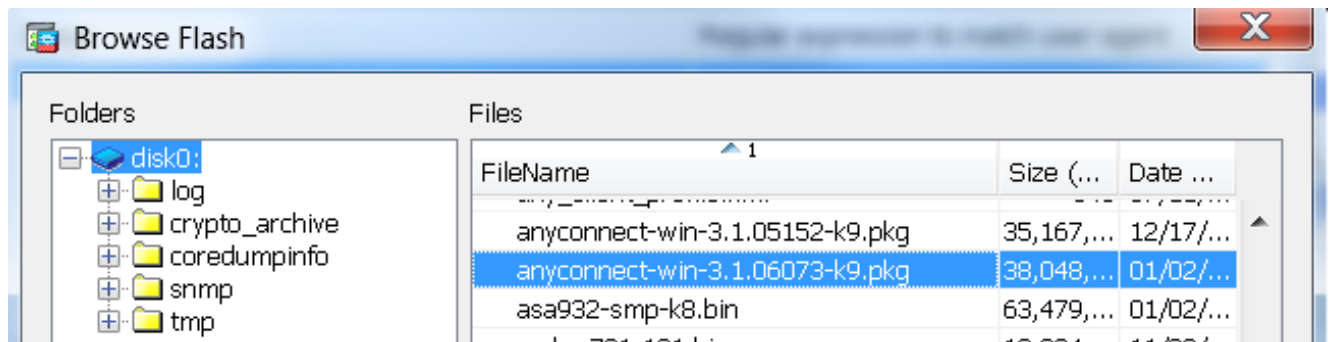
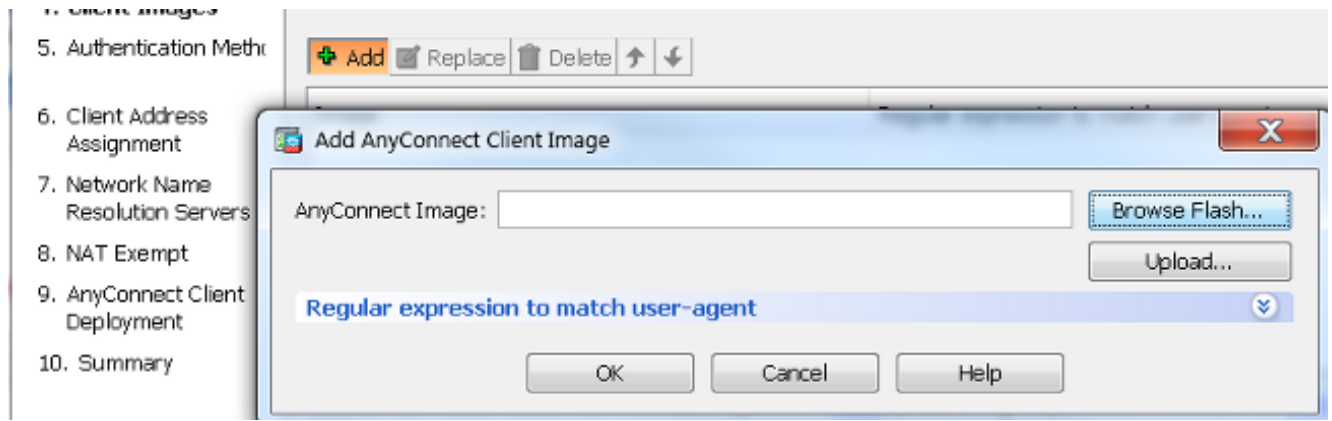


8. ڤلالتل قوف مٲ ، قفاوم ، قفاوم قوف رقنا ، لڤجستلا لامتكلا درجم ب:

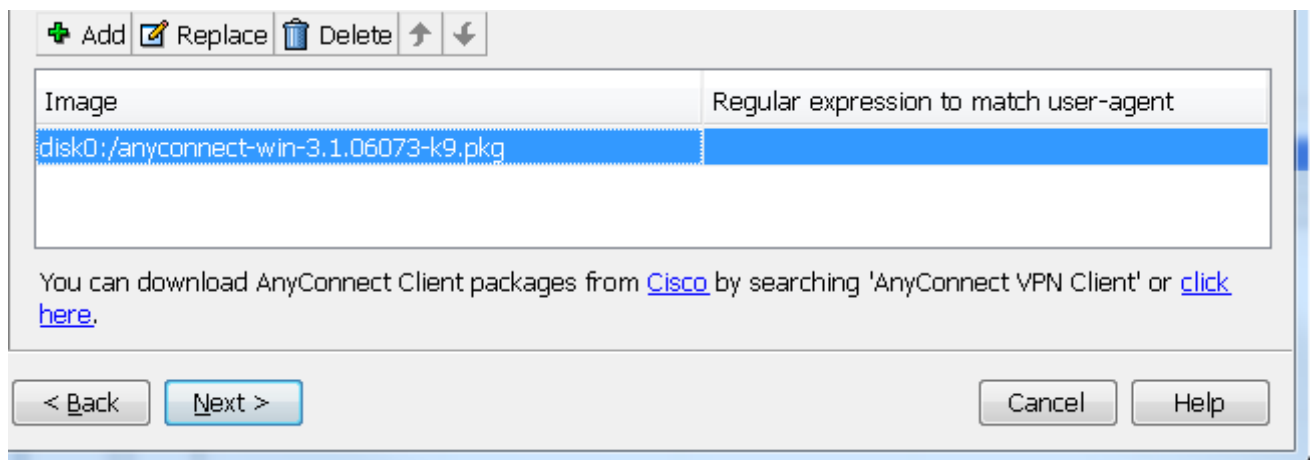


9. رت وڤبمكللا نم (.pkg فللم) AnyConnect لڤمع ةروص ةفاضل ةفاضل قوف رقنا. ةركاذلا Flash ةركاذ ضارعتسل قوف رقنا. (ةتقؤملا ةركاذلا) Flash ةركاذ نم وأ ڤصخشلا لڤمحت قوف رقنا وأ، (ةتقؤملا ةركاذلا) Flash صارقأ كرحم نم ةروصللا ةفاضل (ةتقؤملا)

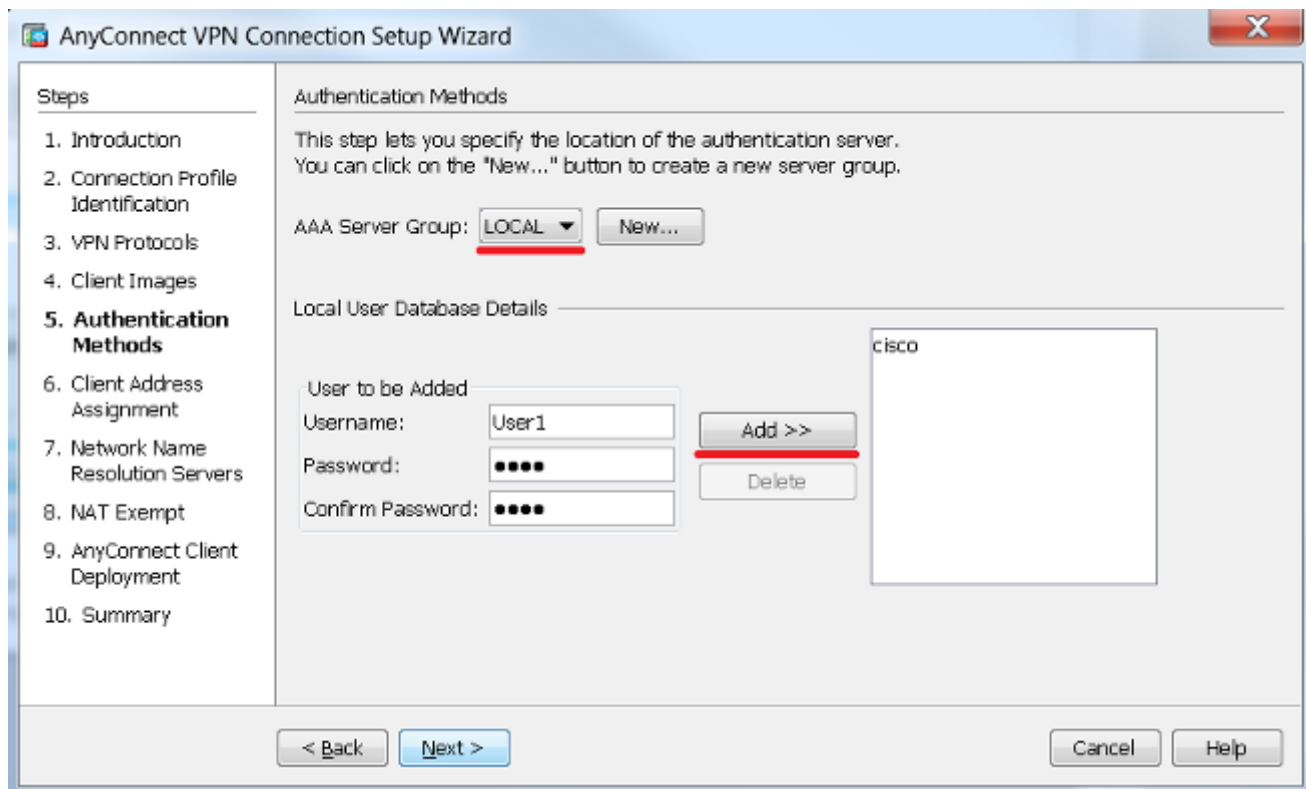
ةرشابم فيضمل زاهجل نم ةروصل ةفاضل:



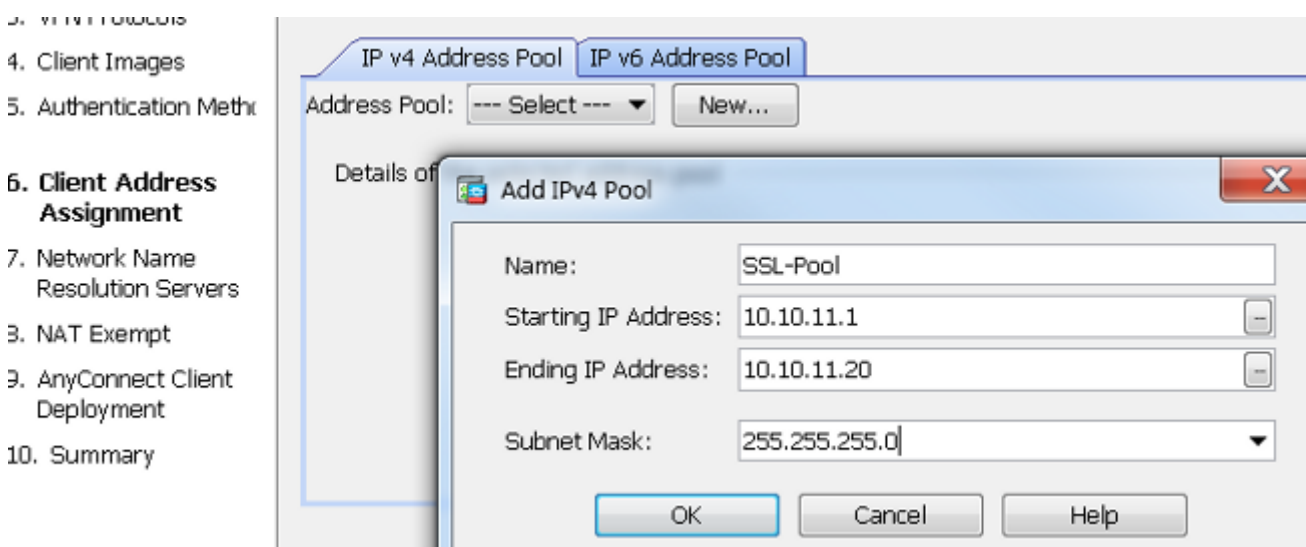
10. يلاتل رقنا، ةروصل ةفاضل درجم:



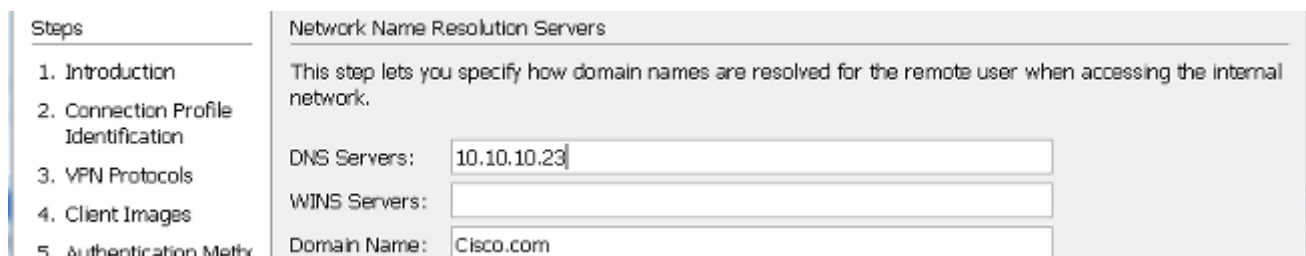
11. ةبسا حمل او ضي وفتل او ةقداصل مل مداوخ تا عومجم ربع مدختس مل ةقداصل مل امك نكمي. ةطحالم. يلاتل قوف رقناو LOCA رتخأف، لعفلاب ني مدختس مل نيوكت مت اذا (AAA). تانايب ةدعاق مادختسا ينعي امم، ةي لحمل ةقداصل مل نيوكت متي، لاثمل اذ في ASA يلع ةي لحمل مدختس مل ةقداصل مل.



12. هدي دجت ب مقف ، لعل فلاب اهدح ا ني وك ت مت اذا . VPN لي عمل ني وان عل ع مجت ني وك ت ب جي .
 دجو و ني وك ت ل دي دج قوف ر قن اف ، ة حاس م كانه ن كت مل اذا و . ة لدس نمل ة م ئا ق ل ن م
 : كل ذ دعب ، متي ن ا م ت ق ط ق ط . ة دي دج



13. لك شب لاجملا مساو DNS ي ل قح ي ف DN تاكبشو (DNS) لاجملا مسا ماظن مداوخ لخدأ .
 ي ل ات ل ل عل ر قن ا م ت ، ب س ان م



14. ةكبشلا لىل VPN ةكبش ربع لوصولا دىقت وه فدهلا ،ويرانيسلا اذه يف ةكبش فلخ (LAN ةكبش وأ) ةيلخاد ةعرف ةكبشك اهنوكت مت يتلا 10.10.10.0/24 نم ةيلخادلا ةعرفلا ةكبشلا اوليمعلا نيب تانايبلا رورم ةكرح ءانثتسا بجي ASA. ةكيمانيد (NAT) ةكبش ناوع ةمجرت ي

و LAN ل تلكشو وقيقت ةمجرت ناوع ةكبش نم رورم ةكرح VPN يفعي ل تصحف و اءافلل تلمعتسا نوكي نا نراق WAN :

2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Method
6. Client Address Assignment
7. Network Name Resolution Servers
- 8. NAT Exempt**
9. AnyConnect Client

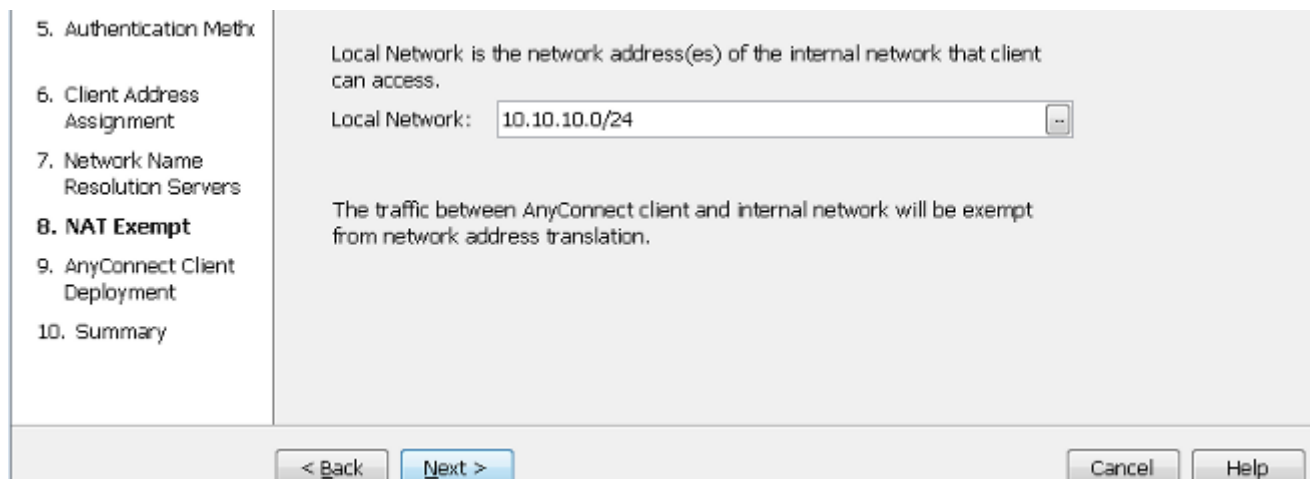
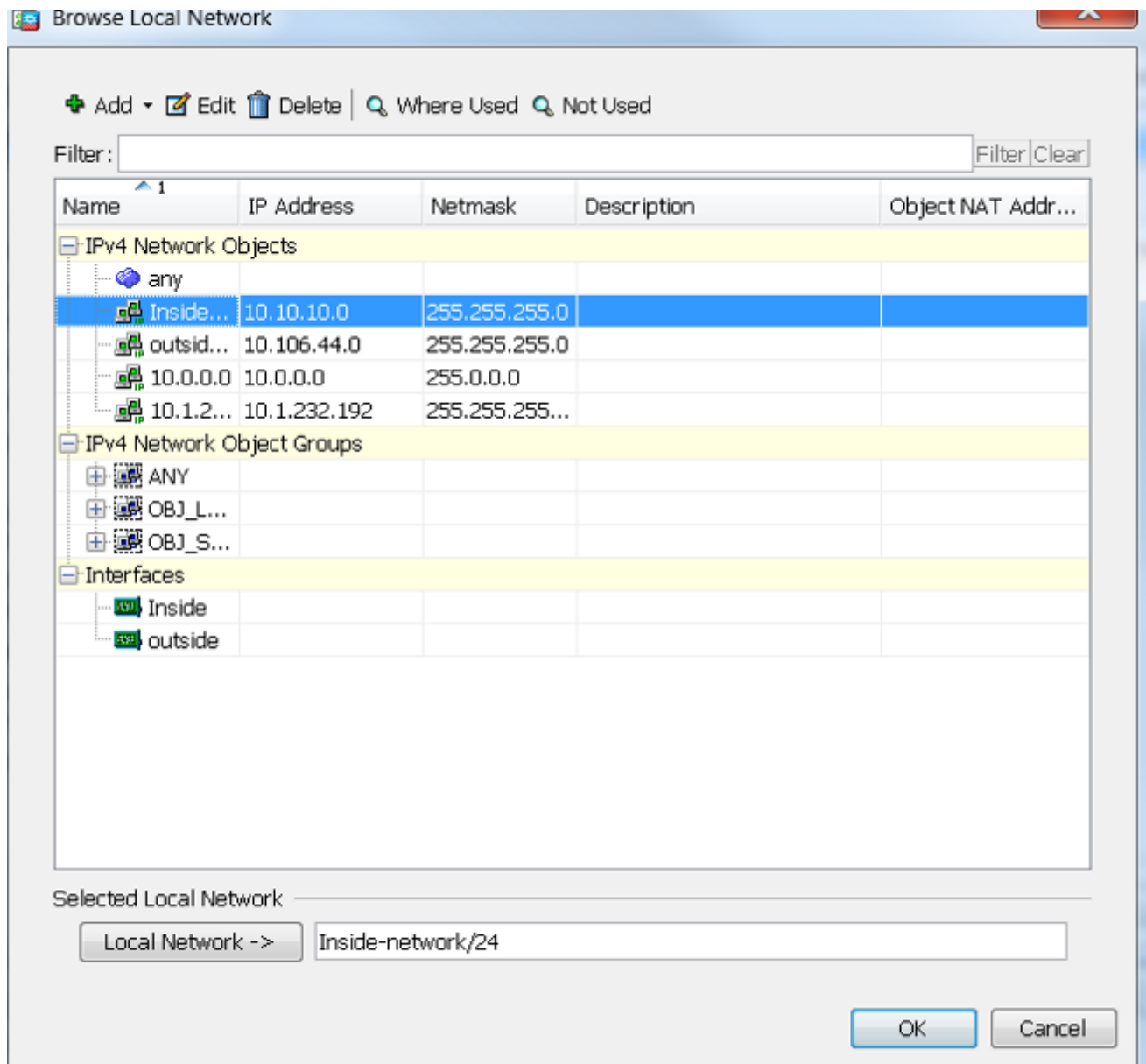
Exempt VPN traffic from network address translation

Inside Interface is the interface directly connected to your internal network.
Inside Interface:

Local Network is the network address(es) of the internal network that client can access.
Local Network:

The traffic between AnyConnect client and internal network will be exempt from network address translation.

15. اهؤافع بجي يتلا ةيلحمل تاكلشلا رتخأ:



زاجن | كلذ دعبو، كلذ دعب، كلذ دعب تقطوط 16.
 نيوكتال جلالع ربع AnyConnect نيوكت دنع، كلذ عمو. نآال AnyConnect لي مع نيوكت لم تكا،
 ةكرح قفن in order to. يضا رتفا لكشب Tunnelall جهنك Split Tunnel جهن نيوكت ب موقوي هنإف
 تقبب يغبني tunneling قشنني، طقف صاخ رورم.

ميسقت جهن شي روت ميس، يقفن لال ميسقت لاصتا نيوكت مدع ةلاح يف: ةطالحم

لكشبه هنييعة متي يذلاو (DfltGrpPolicy) يضارتفالا ةومجملا جهن نم قفنا (أ) رورم ةكرحلا لك VPN ربح نوبزلا تطبرنا ام هنا ينعي اذه Tunnelall. لىل يضارتفا قفنا ربح تلسرا (بيولى رورم ةكرحلا نمضتي

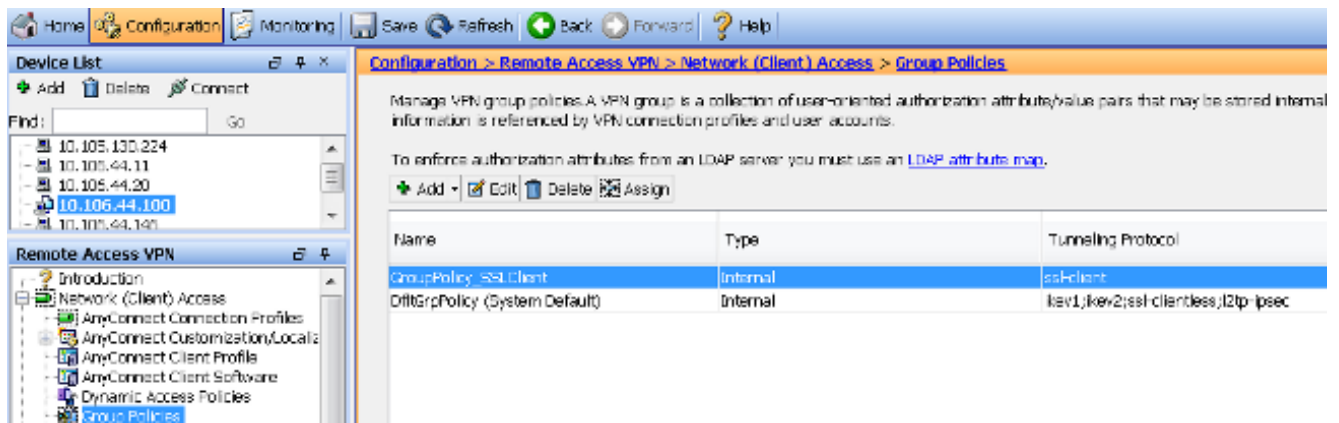
لىل tunneling لىل زواجتي ناونع (يجرأ) لىل ديم نوكي نأ رورم ةكرحلا طوق Microsoft Windows. ةزهجأ لىل راسملا ةعابط رما جأرخا يلى ك لذة ظحالم نكميو. ةادأ نوبزلا

ميسقتلا قفنا نيوكت

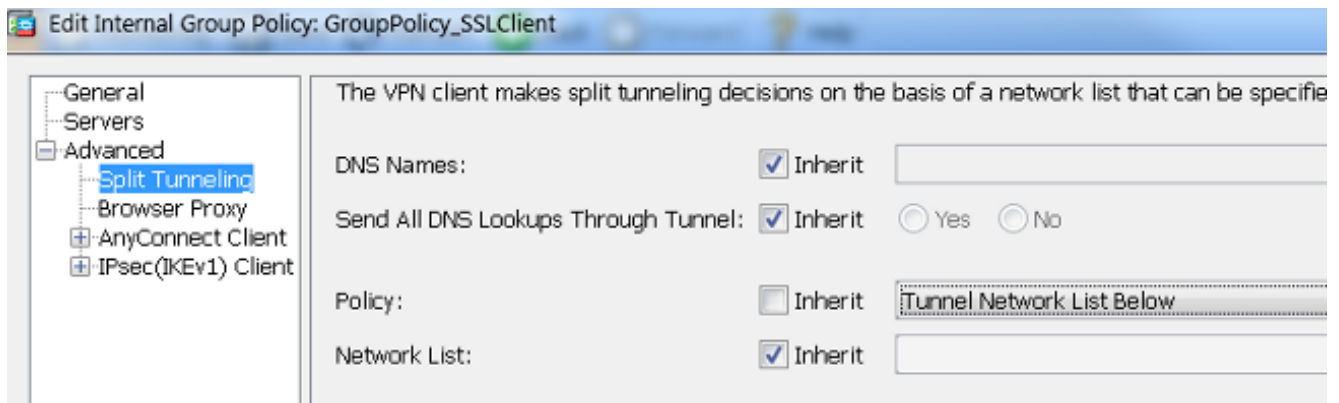
تانايبلا رورم ةكرح ديحتل اهمادختسا كنكمي ةزيم يه يلى قفنا لىل اصتالا ماسقنا ةمئاق نيوكت نمضتي اذهو. اهريفتت بجي يتلا ةفيضملا ةزهجالا وأ ةيىرفلا تاكبشلا رورم ةكرح ريفشت متيس. ةزيملا هذبه اهنارتقا متيس يتلا (ACL) لوصول يلى مكرحلا لوصول يلى مكرحلا ةمئاق لىل اهفيرعت مت يتلا ةفيضملا ةزهجالا وأ ةيىرفلا تاكبشلا ةيىرفلا تاكبشلا هذبه تاراسملا تيبثت متيو، لىلمعلا ةياهن نم قفنا ربح هذبه (ACL) يلى صخشلا رتويبمكلا هيحوت لودج لىل

ميسقتلا قفنا نيوكت لىل all-قفنا نيوكت نم لىل قنالا تاوطخلا هذبه لمكأ

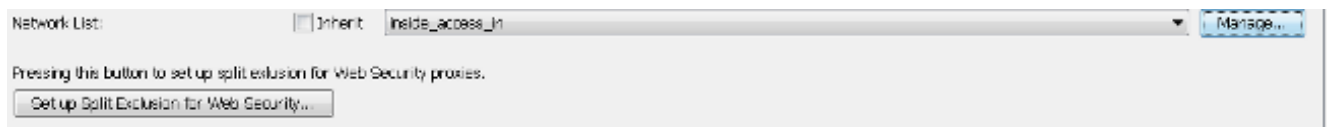
1. ةومجملا تاسايس > (دعب نى لوصول) Remote Access VPN > نيوكتلا لىل لىل قنالا



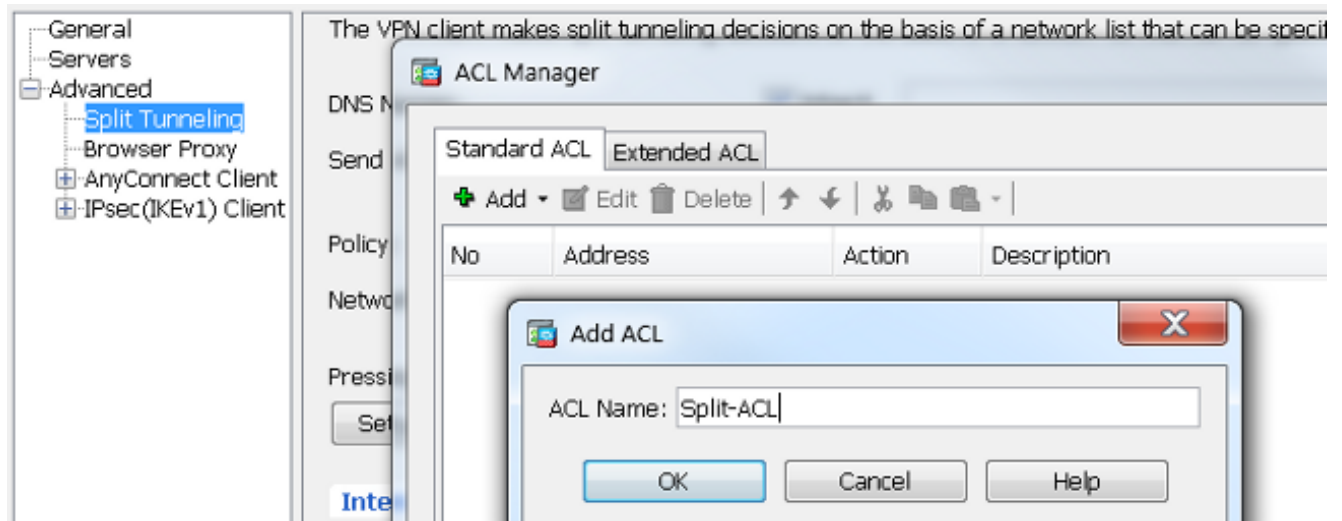
2. ميسقت > ةمدقتم تاراخي لىل لىل قنالا لىل قنالا ةرچش مدختساو، ريرحت قوف رقنا ةمئاق ددجو، جهنلا مسق يلى Inherit رايختالا ةناخ ديحت ءاغلاب مق. يلى قفنا لىل اصتالا ةلدىس نملا ةمئاقلا نم هنادأ قفنا تاكبش



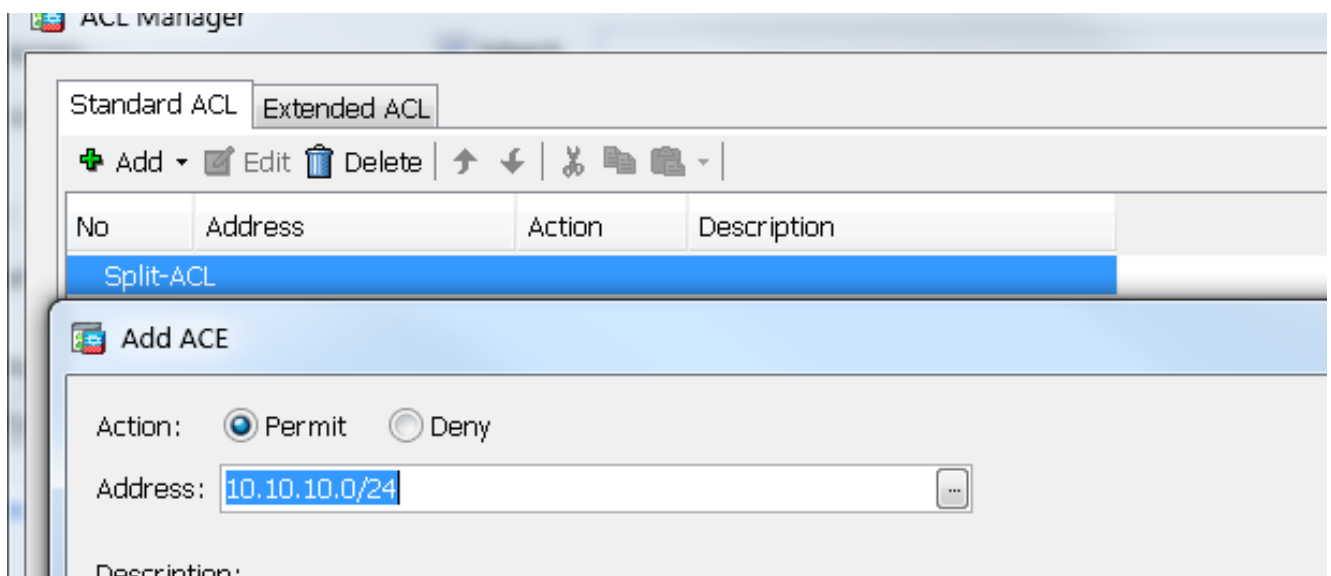
3. قراذ قوف رقناو، تاكبشلا ةمئاق مسق يلى Inherit رايختالا ةناخ ديحت ءاغلاب مق. جاتحي يتلا LAN (تاكبش) ةكبش ددحت يتلا (ACL) لوصول يلى مكرحلا ةمئاق ديحتل اهلى لوصول لىل لىلمعلا



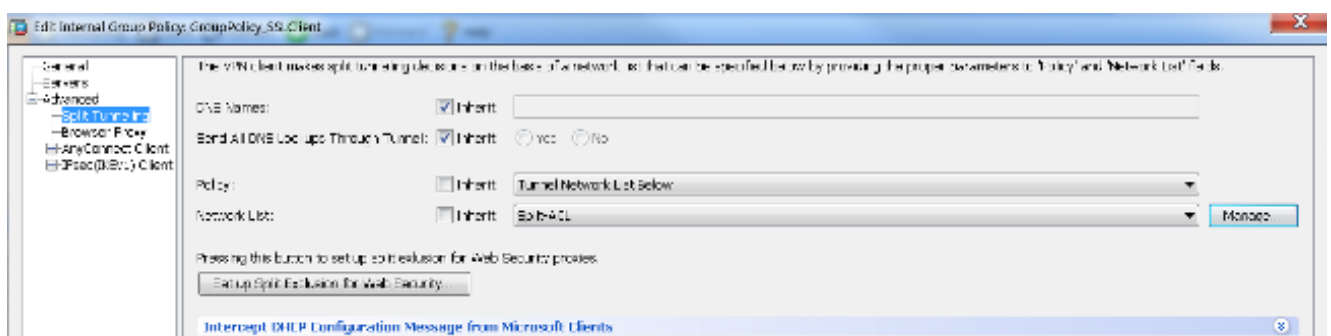
4. **ةفاضل مئ ،ةفاضل قوف مئ ،ةسايقل ال (ACL) لوصول ال ف مكحتل ال ةمئاق قوف رقنا ال (ACL) لوصول ال ف مكحتل ال ةمئاق مسا مئ ، لوصول ال ف مكحتل ال ةمئاق:**



5. **ةدءاق ال ةفاضل ال ACE ةفاضل قوف رقنا ال:**



6. **OK قوف رقنا ال.**



7. قبطي ة ققط ط.

ة دوجوم ل ة فيض م ل ة زه ج أ ل وأ ة ي عرف ل ل ت اك ب ش ل ل ت اه ج و م ل ة فاض إ م ت ت ، ل اص ت ال ا در ج م ب و ة زه ج أ ل ع و . ل ي م ع ل ل زاه ج ه ي ج و ت ل و د ج ل ل ة م س ق م ل ا (ACL) ل و ص و ل ا ي ف م ك ح ت ل ل ة م ئ ا ق ل ع ه ذ ه ل ة ي ل ل ا ل ة و ط خ ل ل ن و ك ت س . ر ا س م ل ا ة ع ا ب ط ر م ا ج ا ر خ إ ي ف ك ل ذ ض ر ع ن ك م ي ، Microsoft Windows ، ة ك ب ش ل ل IP ن ا و ن ع ل و ا ة د ا ع) ل ي م ع ل ل IP ع م ج ت ل ة ي عرف ل ل ة ك ب ش ل ل م IP ن ا و ن ع ت ا ر ا س م ل ا (ة ي عرف ل ل):

```
C:\Users\admin>route print
IPv4 Route Table
=====
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261
10.10.10.0 255.255.255.0 10.10.11.2 10.10.11.1 2

!! This is the split tunnel route.

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261
172.16.21.1 255.255.255.255 On-link 10.106.44.243 6

!! This is the route for the ASA Public IP Address.
```

ي ص خ ش ل ل ر ت و ي ب م ك ل ل ه ي ج و ت ل و د ج ض ر ع ل `netstat -r` ر م أ ل ل خ د أ ، Mac OS ة زه ج أ ل ع :

```
$ netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Netif Expire
default hsrp-64-103-236-1. UGSc 34 0 en1
10.10.10/24 10.10.11.2 UGSc 0 44 utun1

!! This is the split tunnel route.

10.10.11.2/32 localhost UGSc 1 0 lo0
172.16.21.1/32 hsrp-64-103-236-1. UGSc 1 0 en1

!! This is the route for the ASA Public IP Address.
```

ه ت ي ب ث ت و AnyConnect Client ل ي ز ن ت

زاه ج ل ع Cisco AnyConnect Secure Mobility Client ر ش ن ل ا م ه م ا د خ ت س إ ك ن ك م ي ن ا ت ق ي ر ط ك ا ن ه م د خ ت س م ل :

- ب ي و ل ا ر ش ن

- ل ق ت س م ل ا ر ش ن ل ا

ة ي ل ل ا ل م ا س ق ا ل ا ي ف ر ب ك أ ل ي ص ف ت ب ا ه ج ر ش ي ر ج ي ن ي ت ق ي ر ط ل ل ن ي ت ا ه ن م ل ك و .

ب ي و ل ا ر ش ن

`https://<ASA'FQDN>URL` و `<ASA' IP>URL` ص ا خ ل ل URL ن ا و ن ع ل خ د أ ، ب ي و ل ا ر ش ن ة ق ي ر ط م ا د خ ت س ا ل `https://` ل خ د م ة ح ف ص ل ل ك ل ق ن ي ي ذ ل ا و ، ل ي م ع ل ل زاه ج ل ع ض ر ع ت س م ي ف `WebVPN`.

ل ا ل خ ن م ا ب ل ا غ ت ي ب ث ت ل ل ا م ك إ م ت ي ، Internet Explorer (IE) م ا د خ ت س ا ة ل ا ح ي ف : ة ط ح ا ل م

يُرخألأ تاضرعتسملأ ةفاك مدختست Java. مادختسإ لىل ع كرابجإ متي مل ام ActiveX، Java.

لىل ع بجي امك، لىل عمال زاهج لىل ع تيبتتال أدبي نأ بجي، ةحفصلا لىل لوخدلا لىل عست درجم بو تيبتتال لامتكأ دعب ASA ب لاصتال لىل عمال.

ةعباتم لك لذب حامسلا بجي Java وأ ActiveX لىل عشتب نذال ك نم بلطي دق: **ةظالم** تيبتتال.

Logon	
Group	SSLClient ▼
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Logon"/>	



CISCO AnyConnect Secure Mobility Client

WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Java
- Download
- Connected

Attempting to use Java for Installation

Sun Java applet has started. This could take up to 60 seconds. **Please wait...**

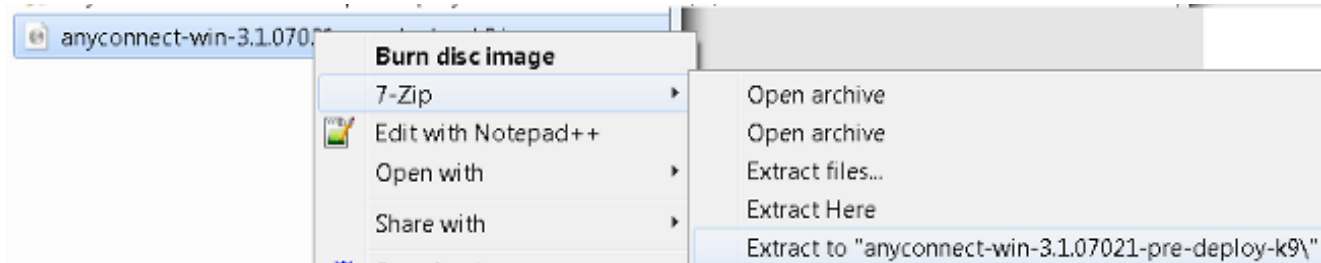
لقستسملأ رشنلا

ةلقستسملأ رشنلا ةقيرط مادختسال ةيلال ت اوطلال لمكأ:

1. ةحفصلا ةروصلا رايخال .بىولا لىل ع Cisco ع قوم نم AnyConnect لىل عم ةروص لىل عزنت .

ري فوت م تي [Cisco AnyConnect Secure Mobility Client](#) بي و ءحفص ىل ا عجا ، لىزنننل رادص ا ددو لىزنننل ءحفص ىل ا لقتنا . ءحفص ا هذ ىل ع لىزنننن طابننرا نبننم ا / ناراط ا ا نبننن ءاا - ل م ا ل ا نبنننن ءمزن ن ع نحب ا رجا . بس انم ا لىزنننن لثم) *AnyConnect-win-3.1.06073-pre-deploy-k9.iso* : ءظ ا م تي .

2. ءمزن ن ا نوتنم ص ا ل ن س ا ل 7-ZIP و WinRAR م ن ن س ا .



3. نىننل ءىنم نل ا ن ا نول رنن او **Setup.exe** فلم لى ن ن س ن م ق ، ن ا نوتنم ص ا ل ن س ا ل ن ن م ب .

[AnyConnect VPN ل ن ش نى](#) ل ا ن ل ن ل ن فاض ا ن ا ن ءىل م ع ن ل ن ش : فرط و 8.4 ، *CLI* ل ا ل م ع ن س نى ن ش ر م لى ن ش ن *cisco ASA 5500 sery* ل ا ن م س ق لى صو ن نوبز 8.6.

رم او ا ل رطس ءه جا و نى و نك (CLI)

ع ن م ص ا ق م ل نوبز ءىل ن م ا نى *cisco AnyConnect* ل ل لى ن ش ن *CLI* ل ا م س ق ا ن ءو نى .

```
ASA Version 9.3(2)
!
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224

access-list all extended permit ip any any

!*****Split ACL configuration*****

access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
no pager
```

```
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-721.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

!***** NAT exemption Configuration *****
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.
```

```
nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp
route-lookup
access-group all in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
```

```
!***** Trustpoint for Selfsigned certificate*****
!Generate the key pair and then configure the trustpoint
!Enroll the trustpoint generate the self-signed certificate
```

```
crypto ca trustpoint SelfsignedCert
enrollment self
subject-name CN=anyconnect.cisco.com
keypair sslcert
crl configure
crypto ca trustpool policy
crypto ca certificate chain SelfsignedCert
certificate 4748e654
308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105
0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e
636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e
170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a
311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31
19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d
06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0
55a975ec a1f2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4
ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0
7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7
53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34
03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
```



```
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 bala5541 ed719680 ee49abe8
```

quit

telnet timeout 5

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

management-access inside

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

ssl server-version tlsv1-only

ssl encryption des-sha1 3des-sha1 aes128-sha1 aes256-sha1

*!***** Bind the certificate to the outside interface******

ssl trust-point SelfsignedCert outside

*!*****Configure the Anyconnect Image and enable Anyconnect****

webvpn

enable outside

anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1

anyconnect enable

tunnel-group-list enable

*!*****Group Policy configuration******

!Tunnel protocol, Split tunnel policy, Split

!ACL, etc. can be configured.

group-policy GroupPolicy_SSLClient internal

group-policy GroupPolicy_SSLClient attributes

wins-server none

dns-server value 10.10.10.23

vpn-tunnel-protocol ikev2 ssl-client

split-tunnel-policy tunnelspecified

split-tunnel-network-list value Split-ACL

default-domain value Cisco.com

username User1 password Pfenk7qp9b4LbLV5 encrypted

username cisco password 3USUCOPFUIMCO4JK encrypted privilege 15

*!*****Tunnel-Group (Connection Profile) Configuraiton******

tunnel-group SSLClient type remote-access

tunnel-group SSLClient general-attributes

address-pool SSL-Pool

default-group-policy GroupPolicy_SSLClient

tunnel-group SSLClient webvpn-attributes

group-alias SSLClient enable

!

class-map inspection_default

match default-inspection-traffic

!

!

policy-map type inspect dns preset_dns_map

parameters

message-length maximum client auto

message-length maximum 512

policy-map global_policy

```

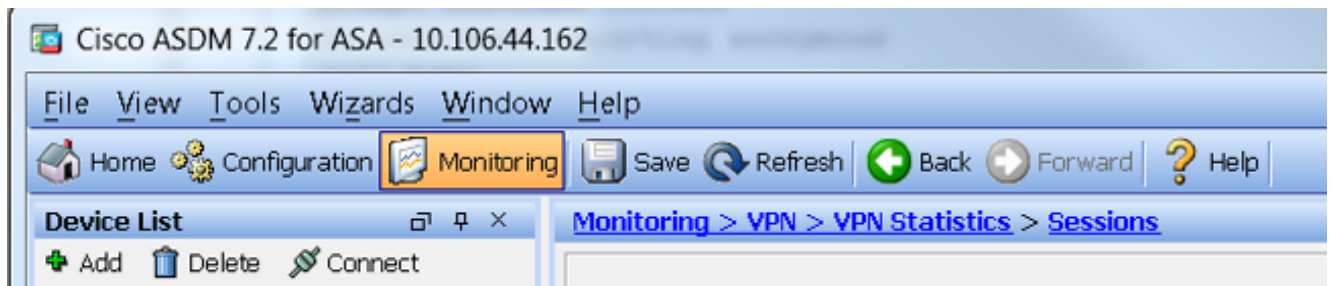
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum: 8d492b10911d1a8fbcc93aa4405930a0
: end

```

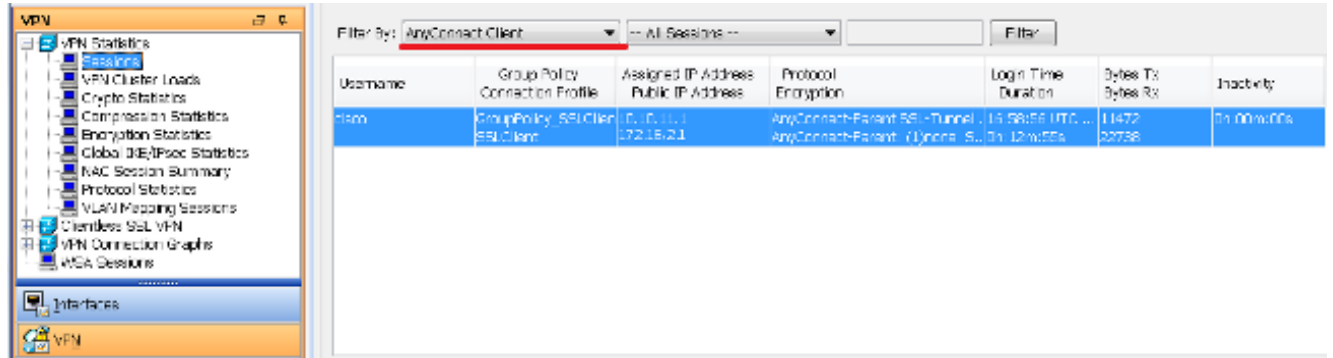
تحصيل نام ققحتلا

اذه بة نرتقملة قفلتخملة تاملعملواو ليمعلا لاصتلا نم ققحتلل ةيلا ت او طخل لمكأ لاصتلا:

1. ASDM على VPN > ةبقارملا لىل لقتنا:



2. VPN ةكبش عون ةيفصتل بسح ةيفصتلا راىخ مادختسا كنكمي. ليمع دح AnyConnect ليمع لمع تاسلج عيمجو ةلدسنملا ةمئاقلا نم AnyConnect كيمى: حيملت. رىخال رىياعملا مادختساب ربكأ لكشب لمعلا تاسلج ةيفصت مادختسملا مسلا لثم، ناوعو IP.



3. ةسلجلا كلت لوح لىصافتلا نم ديزم لىل لوصحلل ةسلج قوف اجدزم ارقن رقنا. ةدحمل:

Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Inactivity
cisco	GroupPolicy_SSLClien SSLClient	10.10.11.1 172.16.21.1	AnyConnect-Parent AnyConnect-Parent: (1)none	SSL-Tunnel . 16:58:56 UTC ... S..Ch:21m:09s	11472 26653	0h:00m:00s

ID	Type	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Encryption	Other	Bytes Tx Bytes Rx
	AnyConn...		none	Tunnel ID: 14.1 Public IP: 172.16.21.1 Hashing: none TCP Src Port: 57828 TCP Dst Port: 443 Authentication Mode: userPassword Idle Time Out: 30 Minutes Idle TO Left: 9 Minutes Client OS Type: Windows Client Type: AnyConnect Client Ver: Cisco AnyConnect VPN Agent.	5954 1046

4. ليصافات ةسلجلا تلن لآ لخد رمأ يأ `vpn-sessionDB` ضرعلا تلخد .

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1   Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient   Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. جئاتنلا نيسحت لجأ نم ىرخألا حشرملا تاراىخ مادختسا كنكمي .

```
# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19
Assigned IP : 10.10.11.1   Public IP : 10.106.44.243
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11036 Bytes Rx : 4977
Pkts Tx : 8 Pkts Rx : 60
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSLClient   Tunnel Group : SSLClient
Login Time : 20:33:34 UTC Mon Apr 6 2015
Duration : 0h:01m:19s

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

AnyConnect-Parent:
Tunnel ID : 19.1
Public IP : 10.106.44.243
Encryption : none Hashing : none
TCP Src Port : 58311 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 772
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 19.2
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : 3DES Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 58315
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 190
Pkts Tx : 4 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 19.3
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : DES Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 58269
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows **3.1.06073**
Bytes Tx : 0 Bytes Rx : 4150
Pkts Tx : 0 Pkts Rx : 59
Pkts **Tx Drop** : 0 Pkts **Rx Drop** : 0

اهحالصإو ءاطخأل فاشكسا

تانايايبل اعمجتل AnyConnect (DART) تاصيخش توري راق تال دادعإ ءادأ مادختسا كنكمي جلاع م ادختسا متي. اهحالصإو AnyConnect ليصوتو تيبتت ءاطخأ فاشكسا ءديفملا تالجسلا اعمجتب DART موق ي. AnyConnect ليغش ت ب موق ي ذل رتوي بمكلا لىل DART الو Cisco نم (TAC) ءة نفل ءءعاسملا زكرم لي لحتل ءة صيخش تال تامول عملاو ءالحو او لي م عملا زاهج لىل ليغش ت لل لوؤسملا تازايتما بلط تي.

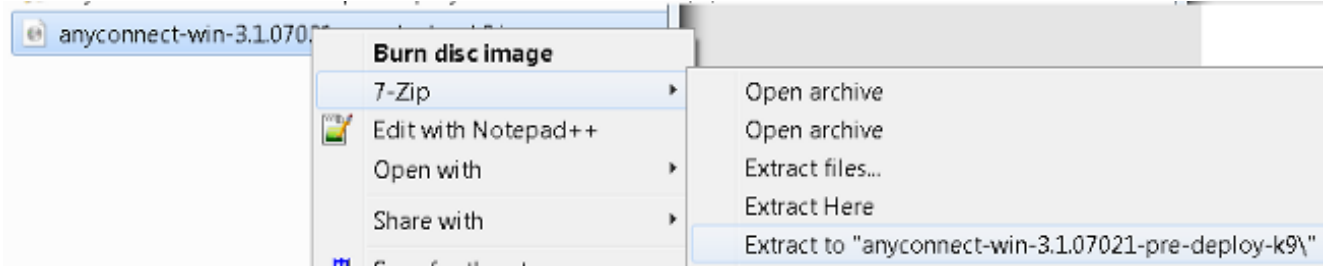
DART تيبتت

ل DART ت ب كر لىل اءه ت متأ:

1. ءءحصل ءروصل رايتخال. بيولا لىل Cisco ءقوم نم AnyConnect لي م ءروصل لي زن ت. ريفوت متي [Cisco AnyConnect Secure Mobility Client](#) بيو ءحفص لىل ءجرا، لي زن ت لل رادصل اءءو لي زن تال ءحفص لىل لقتنا. ءحفصل اءه لىل لي زن ت طاب ترا

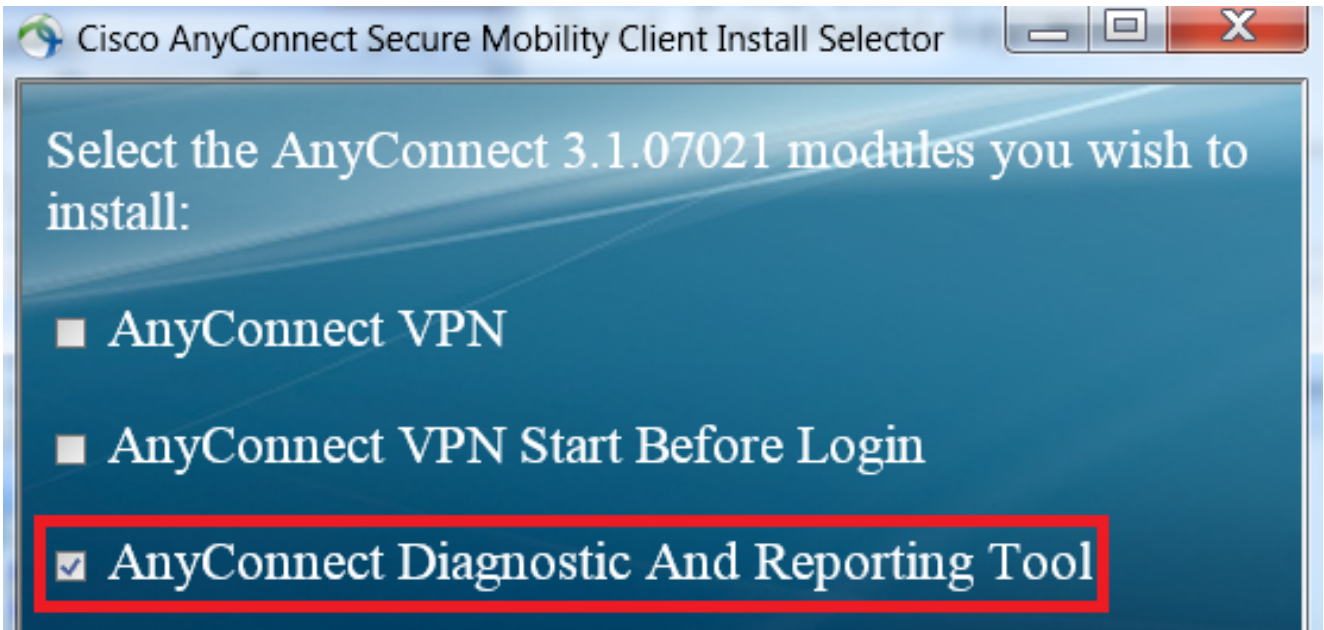
تېبثم لاء / تاراطال تېبثت ءادا - لمالكلا تېبثتلا ءمزح نع شحب ءارج. بسانم لاء
AnyConnect-win-3.1.06073-pre-deploy-k9 (ISO) ءروس لېزنت كلذ ءعب مئې: ءطءالم (ISO) لقتسم لاء

2. ISO ءمزح تايوتحم صالءتسال 7-ZIP او WinRAR مءءتسا:



3. هئلا تايوتحم لاء ءارءتسا مئ يءلا ءلءم لاء لاء لوصولل ضرءتسا.

4. AnyConnect ل ريراقءتلا ءاءءاو صئءشءتلا ءادا طقف ءءو Setup.exe فلم لئغشءب مق.

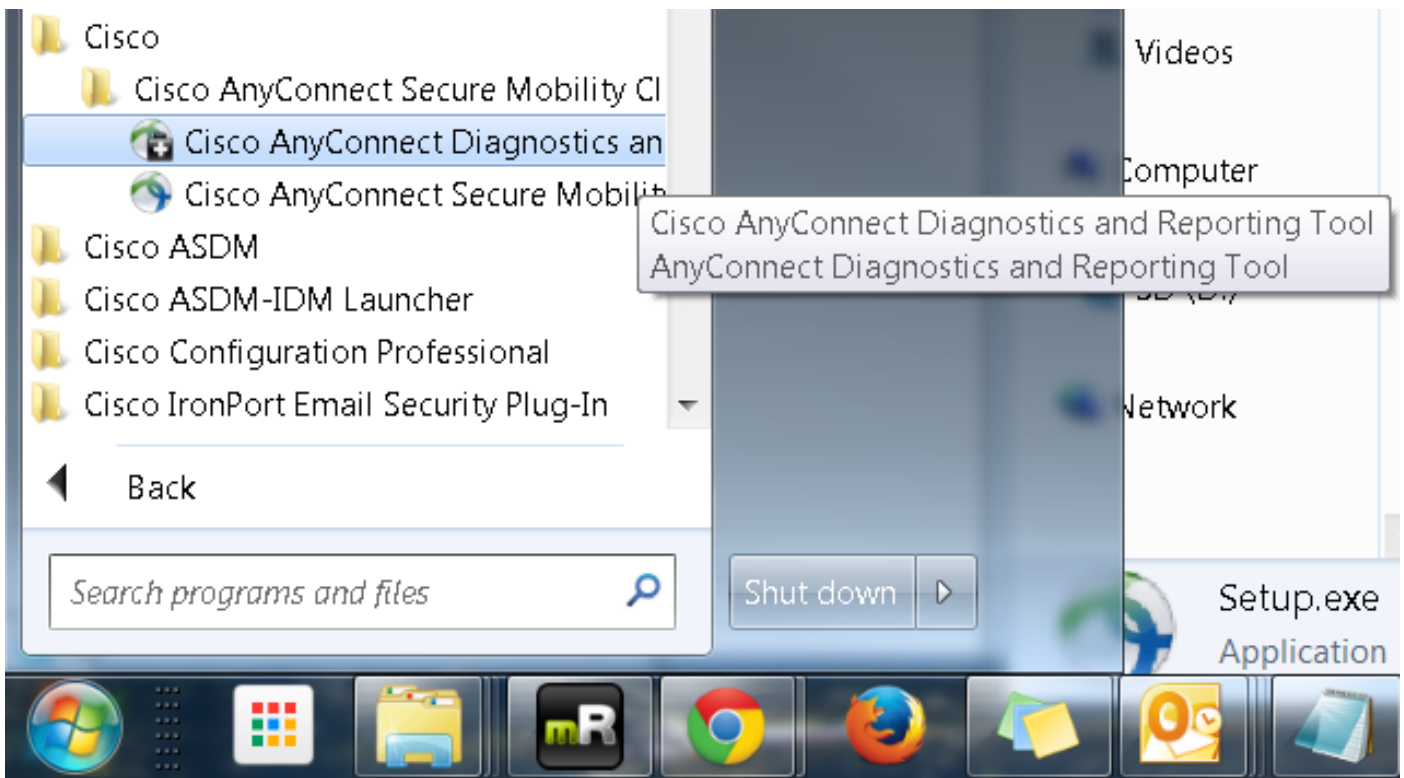


DART لئغشء

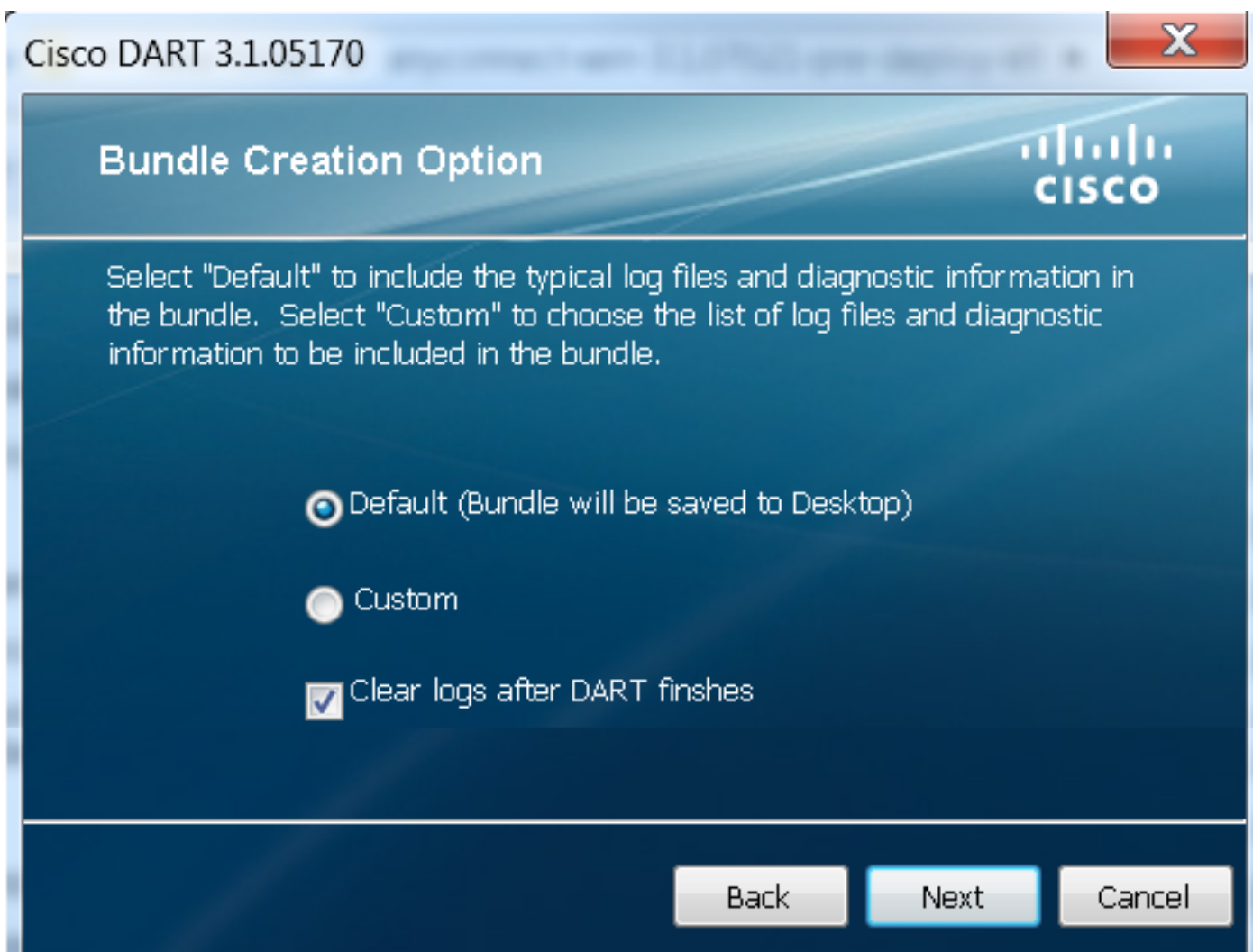
DART: لئغشء لبق اهءاءارم بءئ يءتلا ءمءم لاء ءامولءم لاء ضعب لئ امئف

• DART لئغشء لبق لءالاء لء ءءاو ءرم ءلكشم لاء ءاشن ءءاء بءئ.

• ءلكشم لاء ءاشن ءءاء ءنء مءءتسم لاء زاءء لءء ءقول او ءئراءءتلا ءطءالم بءئ.
لئمءل زاءء لءء "ءءب" ءمءءل لاء نم DART لئغشء



في DART لتأضكري نأ ي صوي cisco. ص صخمل وأ ي ضارت فال ا عضولا اما ديحت نكمي
 ة دحاو ة عفدي ف تطقت لت نك عي طتسي ة مولعم all of the نأ بولسأ ري صقت لت



دعب .لي عمل بتكم لت حطس ي لت zip .DART ة مزح فلم ظفحت اه نأ ف ، ة أدال هذه لامتكا درجمب

ةدعاسملا زكرم ةلاح حتف دعب) TAC ىلإ ينورتكلإلا ديربلا ربع ةمزلال لاسرا نكمي كلذل
لحلحتلا نم ديزمل (ةينفلا

ةلص تاذا تاملولعم

- [ةعئاش لكاشم - اهالصلإو AnyConnect VPN ليمع ءاطخأ فاشكتسأ ليلد](#)
- [ءاطخألا فاشكتسأ ليلد - WebVPN و CSD/Hostscan و AnyConnect عم Java 7 تالكشم
اهالصلإو](#)
- [تادنتسمل او ينقتلا معدلا - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد ىوت مء مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرت مء مء مء دقتل ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءء ءوچرلاب ىصوء و تاملرتل هذه ةقء نء اهتلى وئس م Cisco
Systems (رفوتم طبارل) ىلصلأل ىزىلچنلأل دن تسمل