

# ةكبش ىلإ AnyConnect Client لوصو نيوكت ةيلحمل LAN

## تايوتحمل

---

[ةمدقمل](#)

[ةيساسألا تابلطتمل](#)

[تابلطتمل](#)

[ةمدختسمل تانوكمل](#)

[ةكبش لىطىطختل مسرل](#)

[ةيساسأ تامولعم](#)

[Cisco AnyConnect Secure Mobility Client لةيلحمل LAN ةكبش ىلإ لوصول نيوكت](#)

[ASDM ربع ASA نيوكت](#)

[رماوأل رطس ةهجو ربع ASA نيوكت](#)

[Cisco AnyConnect Secure Mobility Client نيوكت](#)

[مدختسمل تالىضفت](#)

[XML فيرعت فلم ىلع لىلم](#)

[ةحصلل نم ققحتل](#)

[Cisco AnyConnect Secure Mobility Client](#)

[لإصتال رابتخا مادختساب ةيلحمل LAN ةكبش ىلإ لوصول رابتخا](#)

[هجالصاو عاطخألا فاشكتسا](#)

[مسالاب سح ضارعتسالا وأ ةعابطل رذعتى](#)

[قلصت اذ تامولعم](#)

---

## ةمدقمل

LAN ل ذفني نأ نوبز ةيكرح نم أي Cisco AnyConnect ل حمسي نأ فيك ةقيثو اذه فصبي Cisco ASA ىلإ طبري ءانثأ يلحمل.

## ةيساسألا تابلطتمل

### تابلطتمل

زاهج ىلع لعفلاب دوجوم ي فيظول دعب نع لوصول VPN نيوكت نأ دنتسمل اذه ضررت في Cisco نم (ASA) فيكتلل لباقل نامأل.

9.17 رادصلال، [Cisco ASA Series VPN نم رماوأل رطس ةهجو نيوكت لىلد: CLI Book 3](#) ىلإ عجرا رمال مزل اذا نيوكتلا ةدعاسم ىلع لوصولل.

### ةمدختسمل تانوكمل

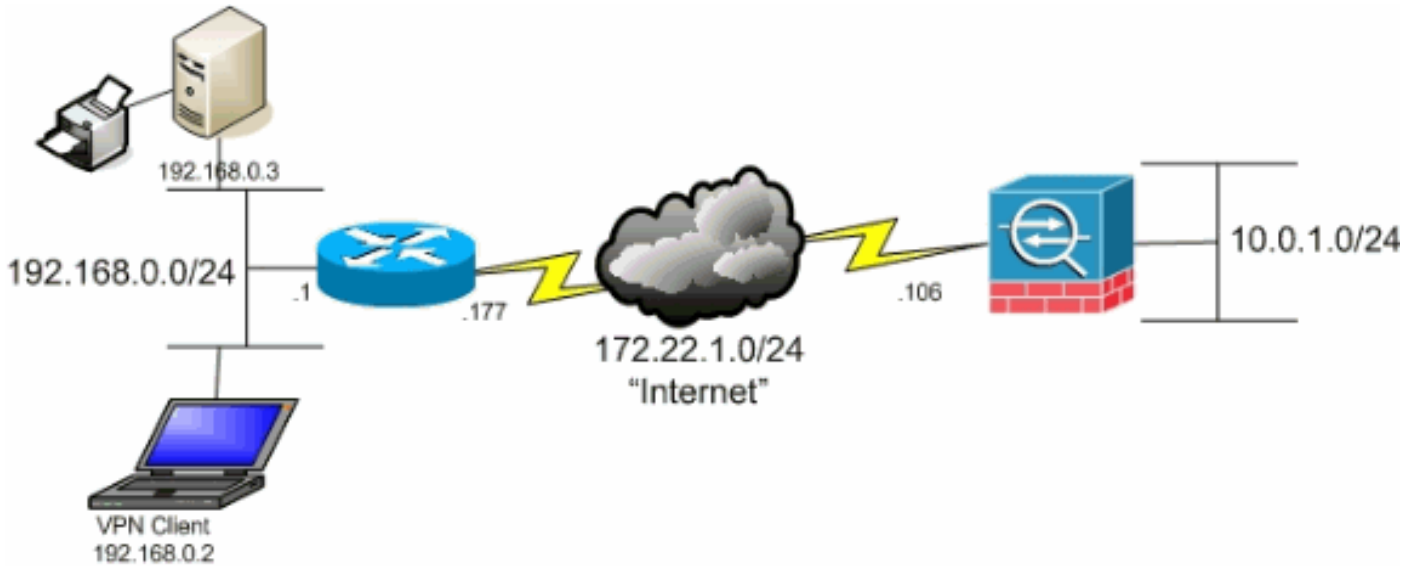
ةيلال ةيدامل تانوكمل او جماربل تارادصل ىلإ دنتسمل اذه في ةدراول تامولعمل دنتست

- Cisco ASA 5500 Series، رادصإلا 9(2)1
- Cisco Adaptive Security Device Manager (ASDM)، رادصإلا 7.1(6)
- Cisco AnyConnect Secure Mobility Client، رادصإلا 3.1.05152

ةصاخ ةي لمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسمل اذه يف ةدراولا تامولعمل ءاشنإ مت تناك اذا (يضارتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجالا عيمج تادب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف ،لغشتلا ديقتك تكبش

## ةكبش لل يطختلا مسرلا

لصتو (SOHO) ةيلزنملا بتاكلما / ةريغصلا بتاكلل ةيجزومن ةكبش يلعل ليمعلا دجوي يسيرلا بتكلما بتنرتنإل ربع



## ةيساسا تامولعم

ةكرشلا دراوم يلإ نمألا لوصول Cisco AnyConnect Secure Mobility Client ل نيوكتلا اذه حيتي تنرتنإل احاتفم لدابت نم 2 رادصإلا و (SSL) ةنمألا ليصوتلا ذخأم ةقبط و IPsec ربع ليمعلا عقوم يف ةعابطلال لثم ةطشنأ ذيفنت يلعل ةردقلا ليمعلا حنمي كلذ عم و (IKEv2) ASA. للاقطنلا ربع ةلصوم لازت ال تنرتنإل ةهجوملا رورملا ةكرح نإف ،هب احوسمم ناك

،ةرفشم ريغ تنرتنإل رورم ةكرح لاسرا هيف متي يديلق تي قفن ماسقنا ويراني س فالخب ءالؤهل حمست اهنإف ،VPN ءالمعل ةيلحمل LAN ةكبش يلإ لوصول نيكم تب موقت ام دنع نودجاوتي يتلا ةكبشلا يلعل طقف ةزهجالا مادختساب رفشمل ريغ لاصتالاب ءالمعل LAN ةكبش يلإ لوصولاب هل حامسلا متي يذلا ليمعلا نكمي ،لاثمل لابس يلعل .اهيلع هنكمي ال نكلو ةصاخلا هتعباط يلإ ةعابطلال لزنملا نم ASA ب هلاصتإ ءانثأ ةيلحملال قفنل ربع تانايابل رورم ةكرح الو لسري مل ام تنرتنإل يلإ لوصول

ةقيرطال س فنب ةيلحمل LAN ةكبش يلإ لوصولاب حامسلل لوصول ةمئاق مادختسا متي ويراني س س كع يلعلو ،كلذ عم و ASA. يلعل مسقنملا يقفنل لاصتال نيوكت اهب مت يتلا اهري فشت بجي يتلا تاكبشلا هذه لوصول ةمئاق ددحت ال ،يقفنل لاصتال ميسقت فالخب ،اضيأ .اهري فشت متي ال ببجي يتلا تاكبشلا رايلخا اذه ددحي ،كلذ نم ال دبو نأ يلإ ةمئاقلا يف ةيلعمل تاكبشلا جاتحت ال ،يقفنل لاصتال ميسقت ويراني س



# Secure Mobility Client

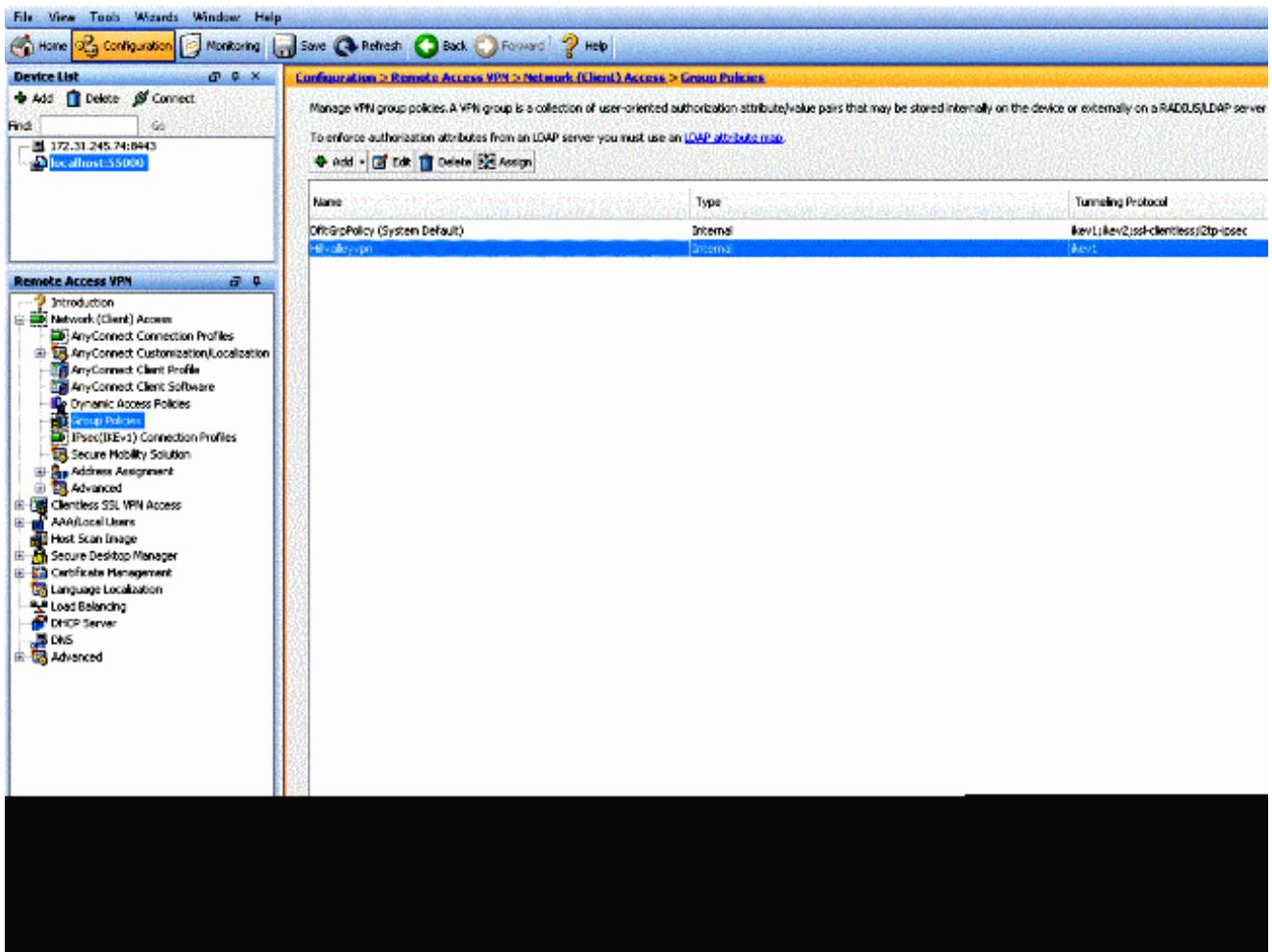
LAN ةكبش ىلإ لوصولاب Cisco AnyConnect Secure Mobility Client ل حامس لل ماهملا هذه لمكأ  
ASA: ب لاصلتالاءانثأ مهب ةصاخلا ل ةيلحملا

- [ASA رعب نيوكت](#) أو [ASA رعب ASDM](#) [ASA رعب نيوكت](#)
- [Cisco AnyConnect Secure Mobility Client رعب نيوكت](#)

## ASA رعب نيوكت ASDM

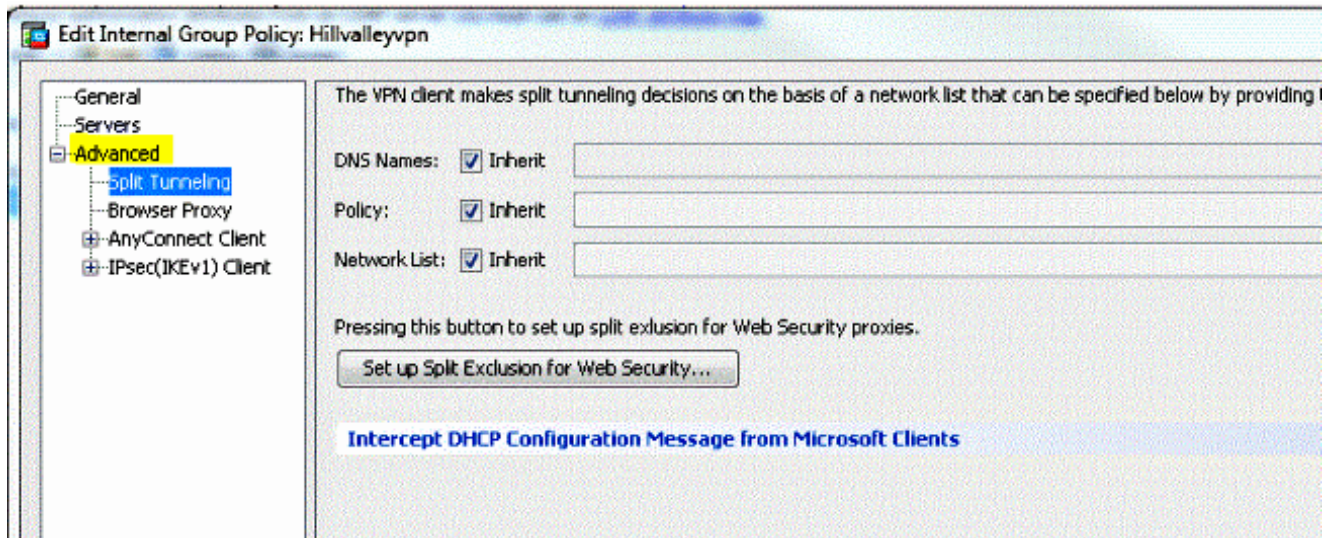
امن ب ذفنم lan يلحم ىقل تي نأ نوبز VPN تحمس ل ASDM ل في steps اذه تمأ  
ASA ل ل طبري:

1. في بغيرت يذلا "ةوعومل جهن" ددحو **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** رتخأ.  
**Edit** رقنا م. هـ في ةيلحملا LAN ةكبش ىلإ لوصول نيوكت م.

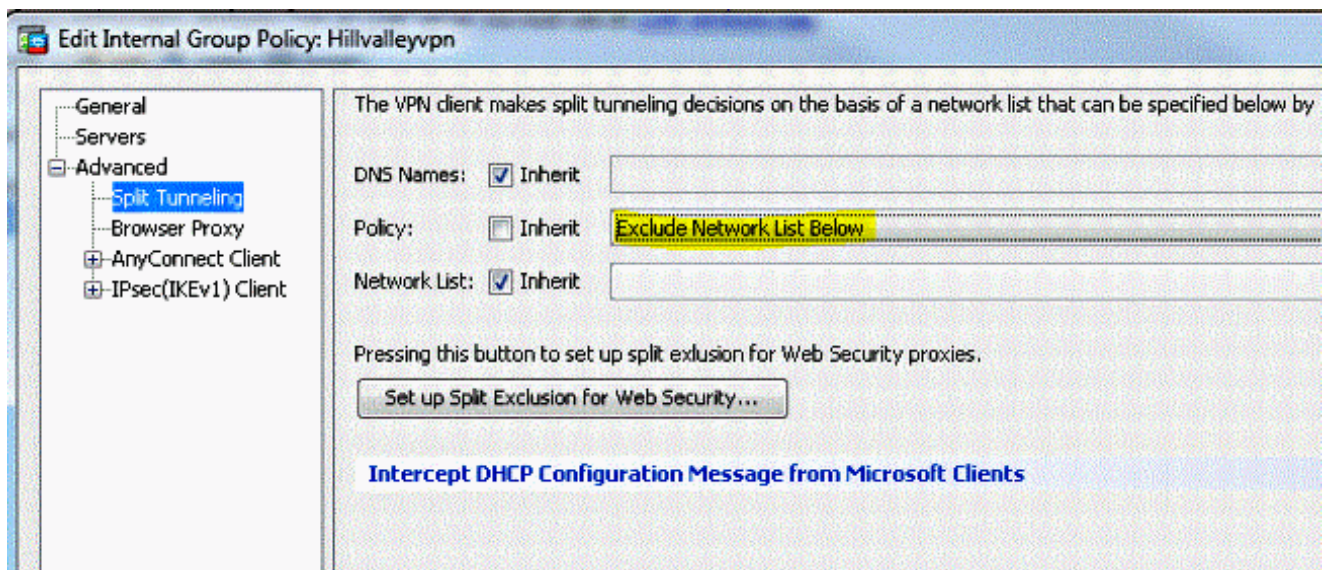


- **Advanced > Split Tunneling** ل لقتنا.

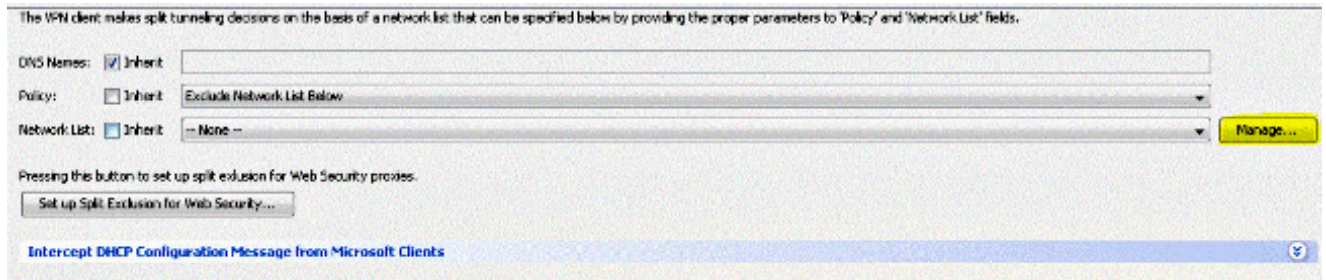




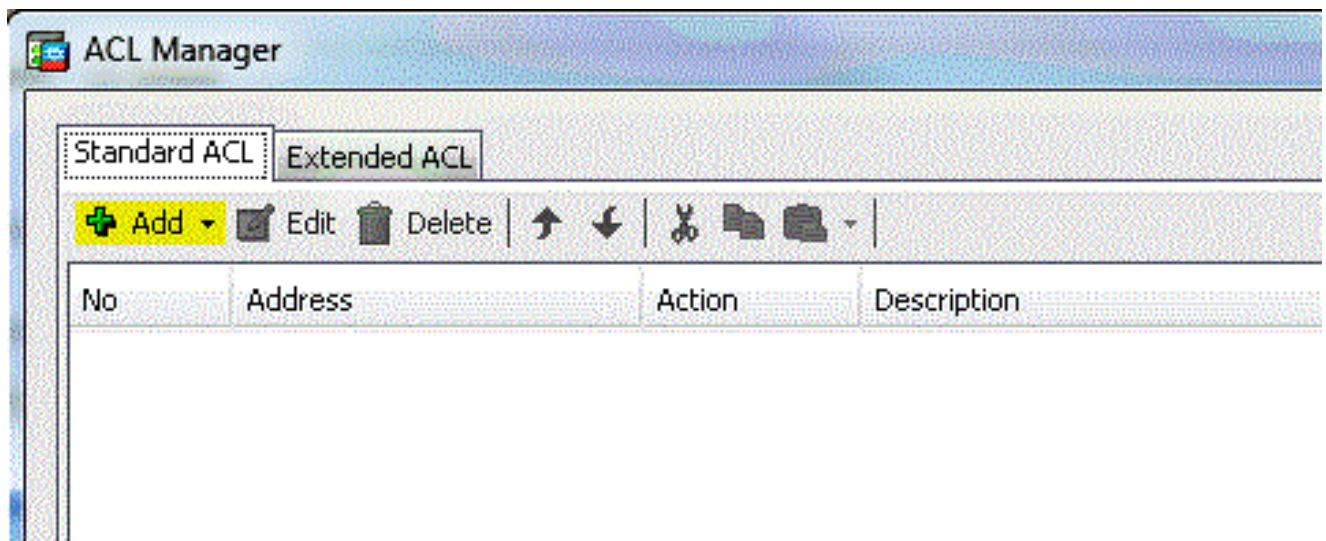
- **Exclude Network List Below.** رتخاوجهنال ع برم **Inherit** دي دحت اءاغل اب مق



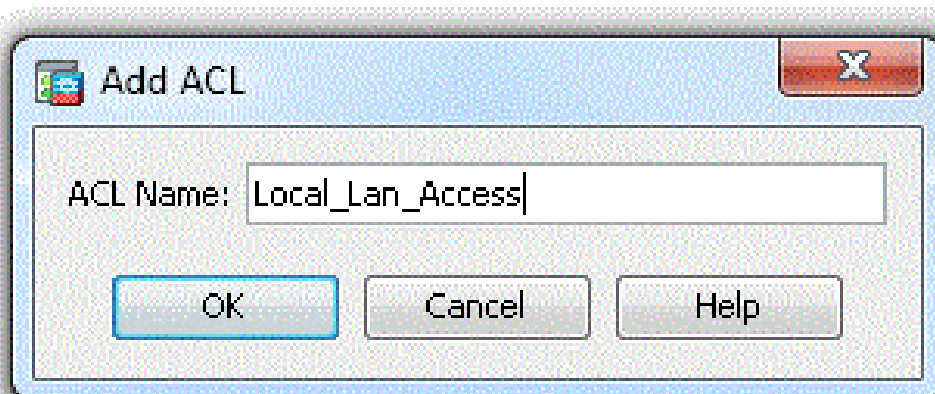
- **Manage** رقنا مثة كبشلال ةمئاقول ع برم ال **Inherit** دي دحت اءاغل اب مق (ACL) لوصول.



- ةديج لوصول ةمئاق ءاشنا لجأ نم **Add > Add ACL...** رتخأ، لوصولا يف مكحتلا ةمئاق ةرادا نمض .

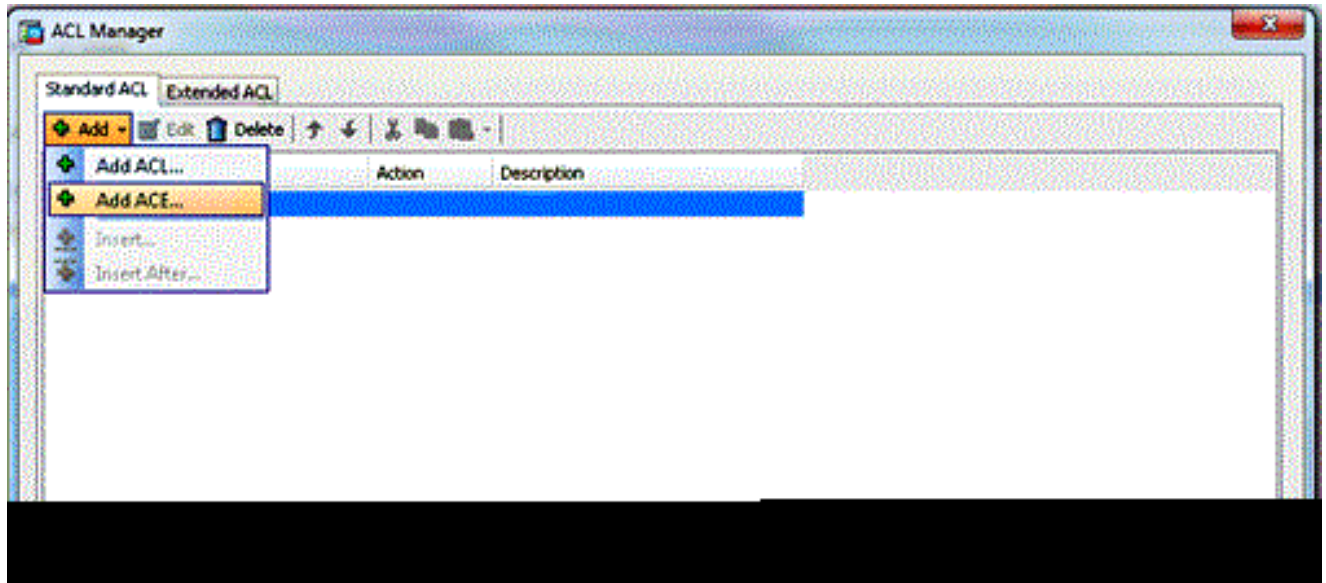


- **OK** قوف رقناو (ACL) لوصولاب مكحتلا ةمئاقول مسا ريفوتب مق .





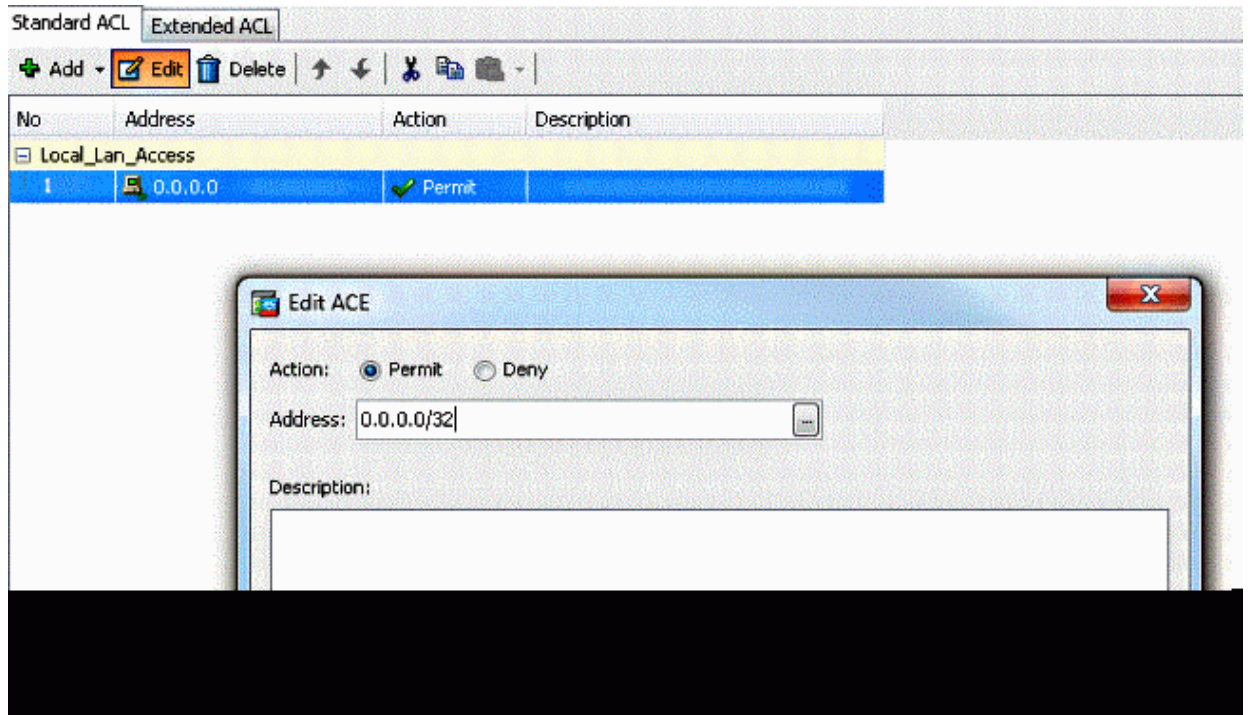
- (ACE) لوصولي ف مكحتلا لاخدا ة فاضال **Add > Add ACE...** رتخأ، (ACL) لوصولي ف مكحتلا ةمئاق عاشن| درجمب



- ليمعملل (LAN) ة ل حمل ة ك ب ش ل عم ق فاوتي يذلا ACE في رعتب مق

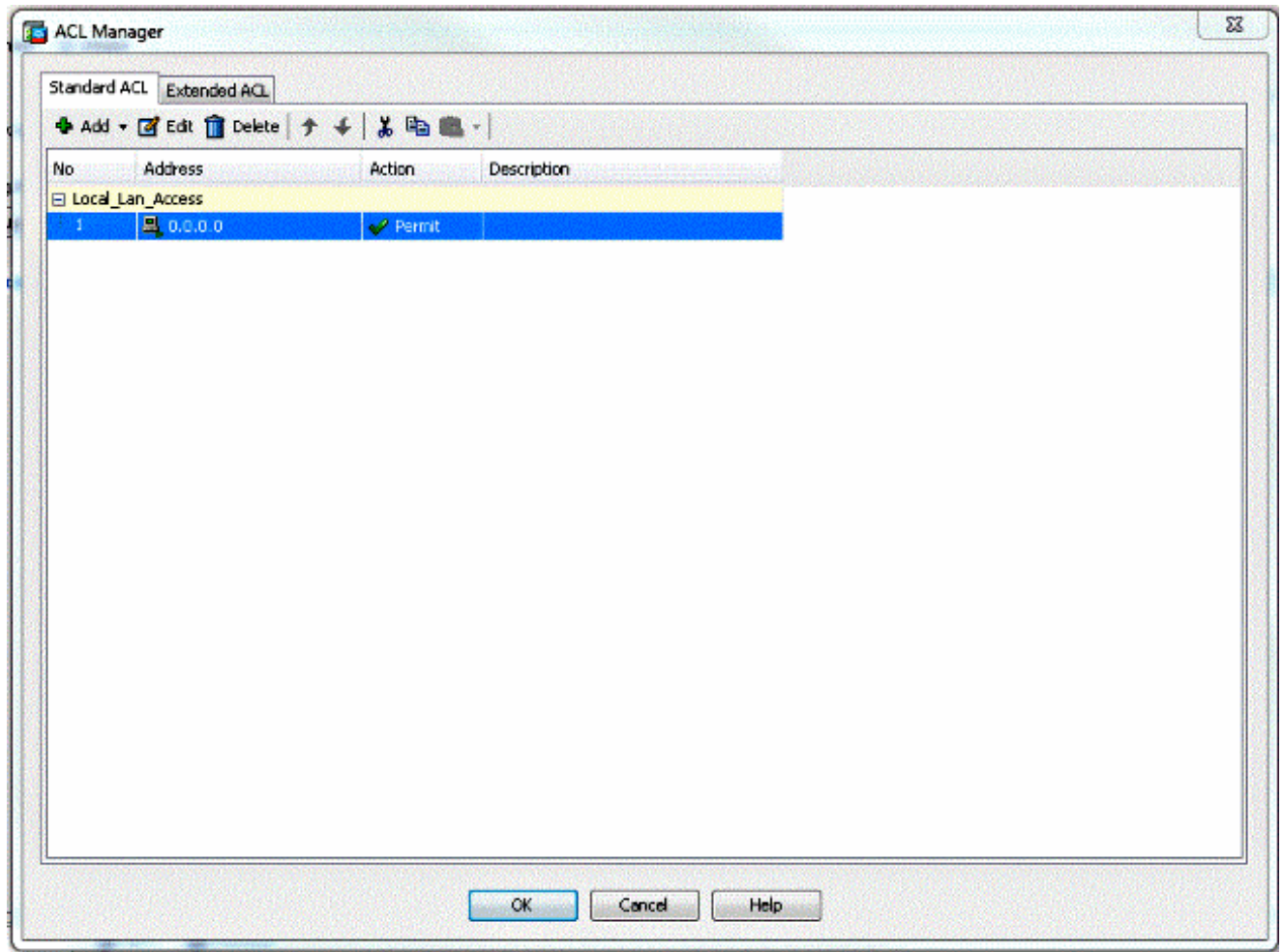
a. رتخأ. **Permit**

- ناوئع ترتخأ **0.0.0.0**
- ل NetMask ترتخأ **/32**.
- فصوري فوتب مق (يرايتخأ).
- رونا **OK**

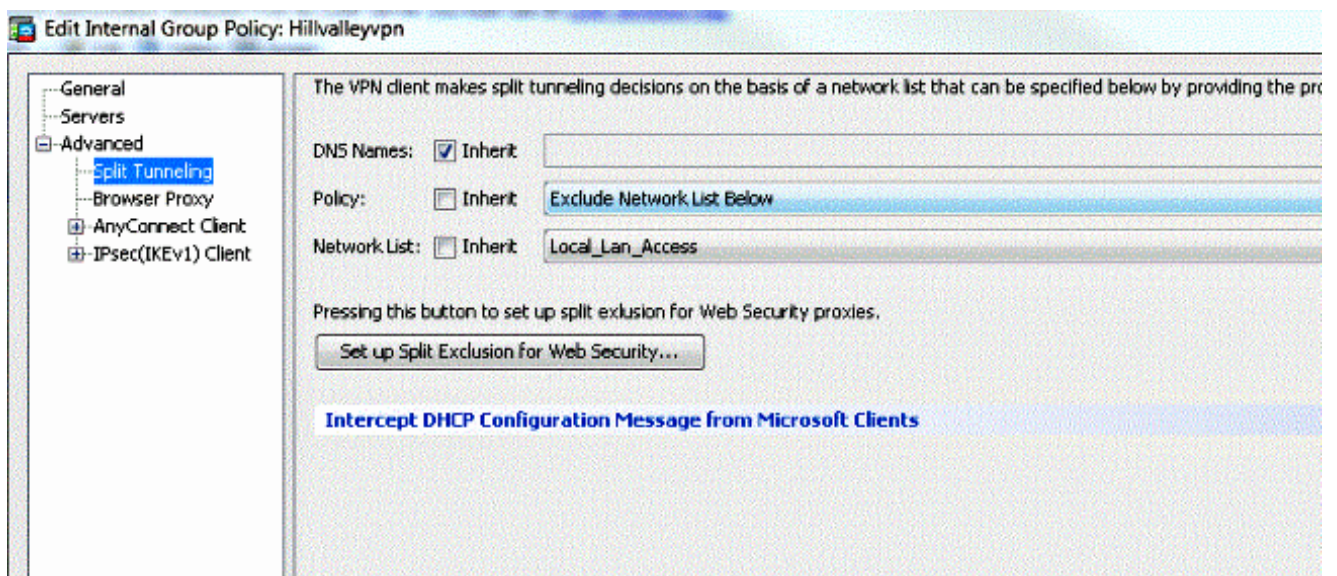


- (ACL) لوصولها في مكدحتلا عمئاق ةرادا نم جورخلل OK رقنا





- مسق قف نل اك بش ةمئاق ل وتل ل اهئاشن اب تمق يتل (ACL) لوصول ا ف مكحتل ةمئاق دتحت نم دكأت





- "ةومحمل جهن" نيوكت ىل ةدوجلل OK رقنا

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameter

DNS Names:  Inherit

Policy:  Inherit Exclude Network List Below

Network List:  Inherit Local\_Lan\_Access

Pressing this button to set up split exclusion for Web Security proxies.

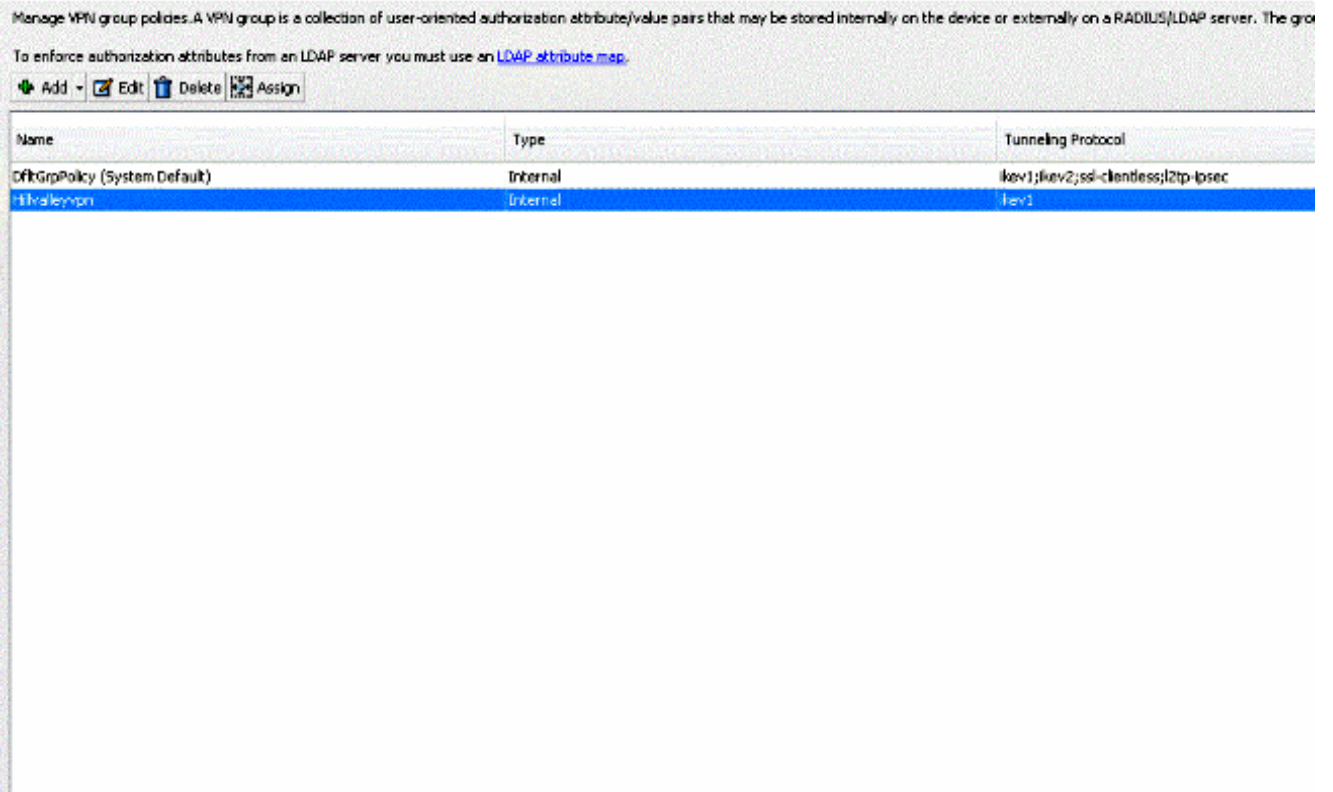
Set up Split Exclusion for Web Security...

**Intercept DHCP Configuration Message from Microsoft Clients**

Next Previous

OK Cancel Help

- ASA لى رمألا تل سرأ (ب ل ط تي نا) Send كلذ دعبو Apply تق طقط



رم اوألا رطاس ةهجاو ربع ASA نيوكت

ذفنم lan يلحم يقلتني نأ نوبز VPN تحمس لآ في steps اذه تمت أعيطتسي تنأ ASDM مادختسا نم الدب لآ لآ لآ طبري امنيب

- نيوكتلا عضو لآ لآ دا

<#root>

ciscoasa>

`enable`

Password:  
ciscoasa#

`configure terminal`

ciscoasa(config)#

- في حمل الـ LAN ةكبش ىلا لوصول اب حامس لل لوصول ةمئاق ءاشن اب مق .

<#root>

ciscoasa(config)#

`access-list Local_LAN_Access remark Client Local LAN Access`

ciscoasa(config)#

`access-list Local_LAN_Access standard permit host 0.0.0.0`

- هـل يدعت في بـغرت يذلا جهن لل "ةومحمل جهن" نيوكت عضول خـدا .

<#root>

ciscoasa(config)#



**group-policy hillvalleyvpn attributes**

ciscoasa(config-group-policy)#

- `excludespecified` هي عبارة عن إشارة ، لإحالة هذه في .ميسقتل قف ن جهن ددح

<#root>

ciscoasa(config-group-policy)#

**split-tunnel-policy excludespecified**

- `Local_LAN_Access` هي عبارة عن إشارة ، لإحالة هذه في .مسق م ل قف ن ل ل لوصول ةمئاق ددح

<#root>

ciscoasa(config-group-policy)#

**split-tunnel-network-list value Local\_LAN\_Access**

- رمأل اذه رادصاب مق :

<#root>

```
ciscoasa(config)#
```

```
tunnel-group hillvalleyvpn general-attributes
```

- قف نللة ةوم جم بة ةوم جم للة هة ن نارقا.

```
<#root>
```

```
ciscoasa(config-tunnel-ipsec)#
```

```
default-group-policy hillvalleyvpn
```

- بولسأ لة كشة ن انة الة ءرء.

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
exit
```

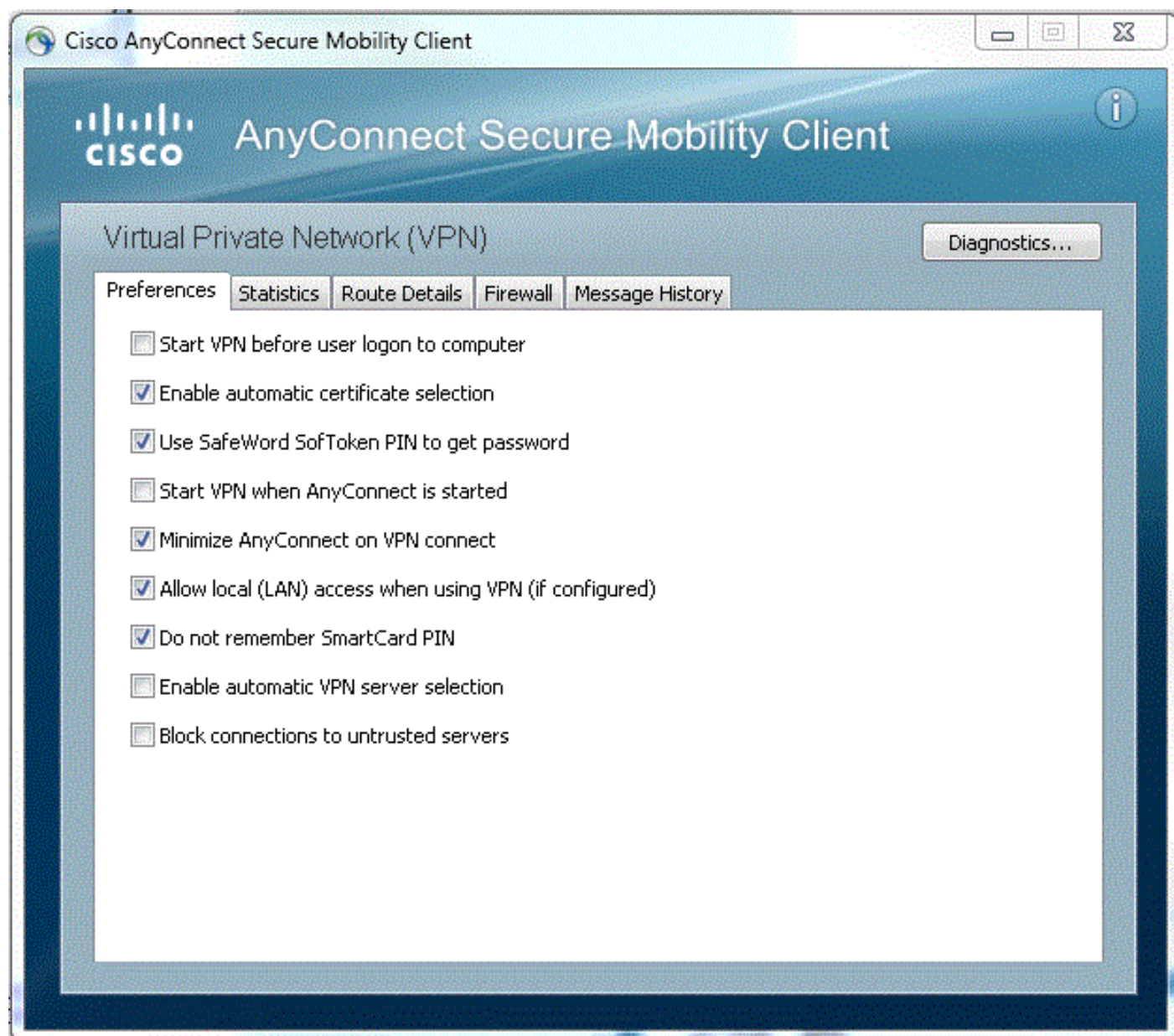
```
ciscoasa(config)#
```

```
exit
```

```
ciscoasa#
```

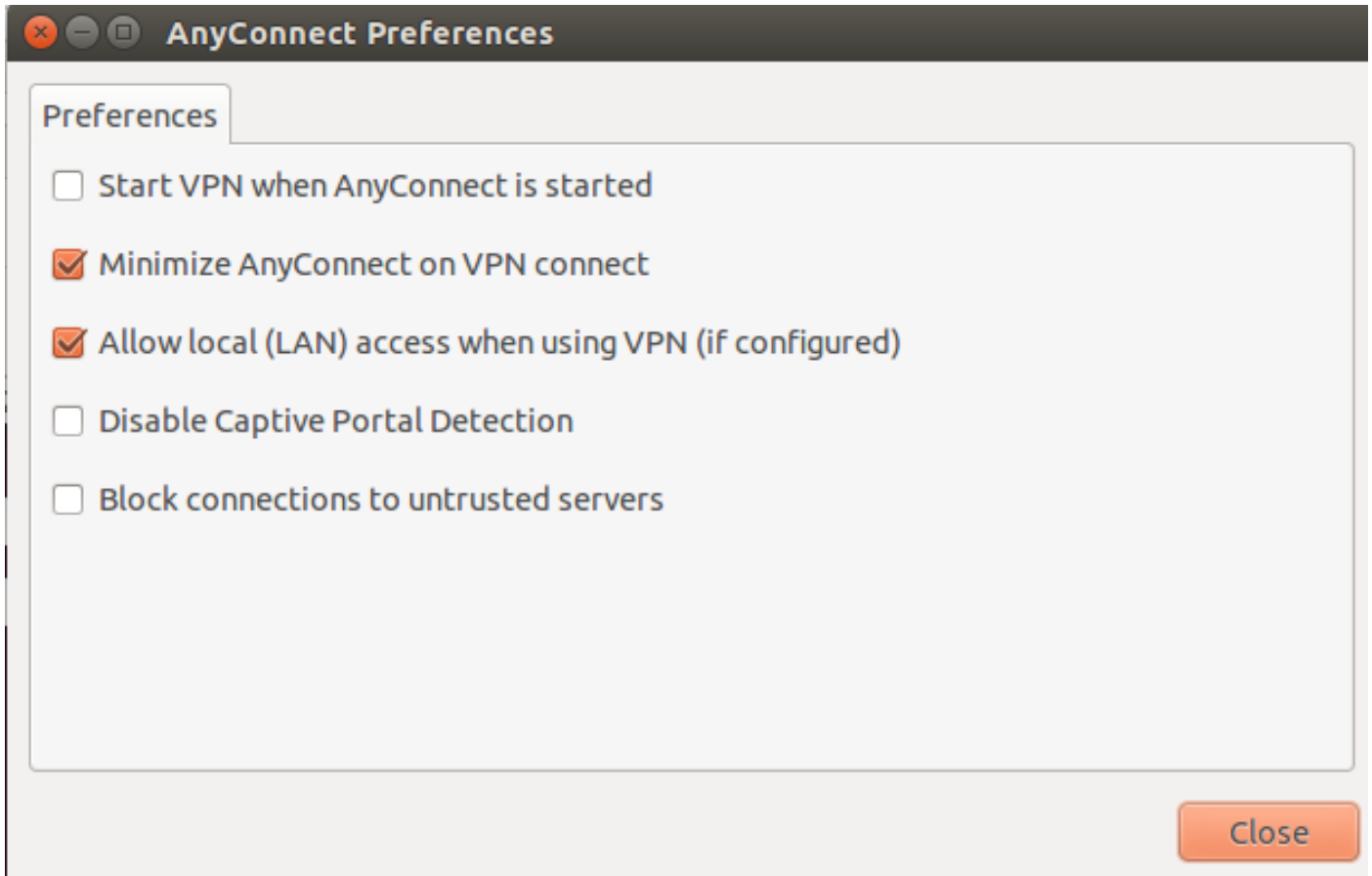


ةيلحم ال LAN ةكبش ىل لوصول اب حامس لل



سك نيل ىلع





XML فيرعت فلم ىلع لاثم

XML مادختساب VPN ةكبش ليمع فيرعت فلم نيوكت ةيفيكي ىلع لاثم يلى اميفو

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSA SecurIDIntegration UserControllable="false">Automatic
```

```
</RSA SecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPEXclusion UserControllable="false">Disable
<PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
</PPPEXclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">>false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
</ClientInitialization>
</AnyConnectProfile>
```

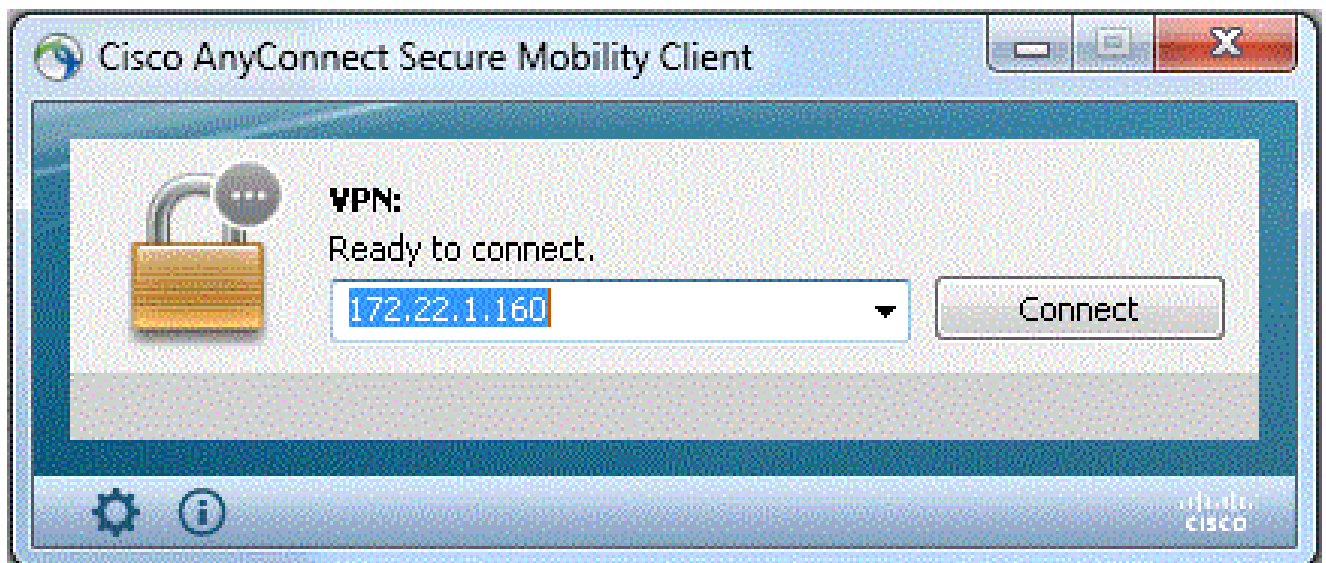
ةحصلا نم ققحتلا

كليكشت تققد in order to مسق اذه في steps ال تمأ

- [ضرع dart](#)
- [لاصتال رابطت ساب ةيلحمل ل LAN ةكبش ل لوصول رابطت](#)

كب صاخلا نيوكتلا نم ققحتل ل ASA ب Cisco AnyConnect Secure Mobility Client ل لصوتب مق

- **Connect** قوف رقناو مداوخال ةمئاق نم كب صاخلا ل لوصول رابطت ل اذارتخأ



- بولسا قفنىلا تضرع **Advanced Window for All Components > Statistics...** in order to تترتخأ

**Statistics**

VPN

## Virtual Private Network (VPN)

Statistics | Route Details | Firewall | Message History


Connection Information		Address Information	
State:	Connected	Client (IPv4):	192.168.11.1
Tunnel Mode (IPv4):	Split Exclude	Client (IPv6):	Not Available
Tunnel Mode (IPv6):	Drop All Traffic	Server:	64.102.156.87
Duration:	00:01:11	Transport Information	
<b>Bytes</b>		Protocol:	DTLS
Sent:	49749	Cipher:	RSA_3DES_168_SHA1
Received:	9298	Compression:	LZS
<b>Frames</b>		Proxy Address:	No Proxy
Sent:	710	Feature Configuration	
Received:	3	FIPS Mode:	Disabled
<b>Control Frames</b>		Trusted Network Detection:	Disabled
Sent:	7	Always On:	Disabled
Received:	5	Secure Mobility Solution	
<b>Client Management</b>		Status:	Unconfirmed
Profile Name:	pro_locallan.xml	Appliance:	Not Available
Administrative Domain:	Undefined		

Reset Export Stats...

سك نيل ىلع

Cisco AnyConnect Secure Mobility Client Statistics

Statistics Route Details



<b>Connection Information</b>		<b>Address Information</b>	
State:	Connected	Client (IPv4):	20.20.20.1
Connection Mode (IPv4):	Split Exclude	Server:	10.48.67.223
Connection Mode (IPv6):	Drop All Traffic	Client (IPv6):	Not Available
Duration:	00:16:22		
Session Disconnect:	None		
<b>Bytes</b>		<b>Transport Information</b>	
Sent:	0	Protocol:	DTLS
Received:	20550	Cipher:	RSA_AES_256_SHA1
		Compression:	None
		Proxy Address:	No Proxy
<b>Frames</b>		<b>Feature Configuration</b>	
Sent:	0	FIPS Mode:	Disabled
Received:	5	Trusted Network Detection:	Disabled
<b>Control Frames</b>			
Sent:	132		
Received:	65		

• Cisco AnyConnect Secure Mobility Client ىدل لازي ال يتال تاهج ومال ضرعل بيوبتال **Route Details** ةمالع قوف رقنا اهلا يلحم لوصو

امن بي 169.254.0.0/16 و 10.150.52.0/22 ىل ةيلحمال LAN ةكبش ىل لوصولاب ليملعلل حامسلا متي، لاثملا اذه في قفنل ربع اهلا سراو ىرخأل رورمال ةكرح عيمج ريفشت متي.



Statistics

VPN

## Virtual Private Network (VPN)

Statistics | **Route Details** | Firewall | Message History


### Route Details

- ▼ Non-Secured Routes (IPv4)
  - 10.150.52.0/22
  - 169.254.0.0/16
- ▼ Secured Routes (IPv4)
  - 0.0.0.0/0
- Non-Secured Routes (IPv6)
- Secured Routes (IPv6)

سكڻپل ىلع

Cisco AnyConnect Secure Mobility Client Statistics

Statistics Route Details



**Non-Secured Routes**

Destination	Subnet Mask
192.168.171.0	24

**Secured Routes**

Destination	Subnet Mask
0.0.0.0	0

Cisco AnyConnect Secure Mobility Client

ال وأ إذا ام تددح عي طتسي تنأ ،ةم زح (DART) رير اقاتلا ةادأو صيخش تالنا نم ةعرس سايقم لجس AnyConnect تنأ صرحفي ام دنع تتبث ذفنم lan يلحم حمسي نأ ةم لعملا.

\*\*\*\*\*

Date : 11/25/2011  
 Time : 13:01:48  
 Type : Information  
 Source : acvpndownloader

Description : Current Preference Settings:  
 ServiceDisable: false  
 CertificateStoreOverride: false  
 CertificateStore: All  
 ShowPreConnectMessage: false  
 AutoConnectOnStart: false  
 MinimizeOnConnect: true  
 LocalLanAccess: true  
 AutoReconnect: true  
 AutoReconnectBehavior: DisconnectOnSuspend  
 UseStartBeforeLogon: false  
 AutoUpdate: true  
 RSA SecurID Integration: Automatic  
 Windows Logon Enforcement: SingleLocalLogon  
 Windows VPN Establishment: LocalUsersOnly  
 Proxy Settings: Native  
 AllowLocalProxyConnections: true

PPPExclusion: Disable  
PPPExclusionServerIP:  
AutomaticVPNPolicy: false  
TrustedNetworkPolicy: Disconnect  
UntrustedNetworkPolicy: Connect  
TrustedDNSDomains:  
TrustedDNSServers:  
AlwaysOn: false  
ConnectFailurePolicy: Closed  
AllowCaptivePortalRemediation: false  
CaptivePortalRemediationTimeout: 5  
ApplyLastVPNLocalResourceRules: false  
AllowVPNDisconnect: true  
EnableScripting: false  
TerminateScriptOnNextEvent: false  
EnablePostSBLOnConnectScript: true  
AutomaticCertSelection: true  
RetainVpnOnLogoff: false  
UserEnforcement: SameUserOnly  
EnableAutomaticServerSelection: false  
AutoServerSelectionImprovement: 20  
AutoServerSelectionSuspendTime: 4  
AuthenticationTimeout: 12  
SafeWordSoftTokenIntegration: false  
AllowIPsecOverSSL: false  
ClearSmartcardPin: true

\*\*\*\*\*

لاصتال رابتخ| مادختساب ة لحي ل LAN ةكبش | ل لوصول رابتخ|

ثبلاو لابقتسال ةدحو | ل تاونق عاشن| اناثأ لحي ل LAN لوصول هيدل لازي ام VPN ليمع نأ رابتخال ةيفاض| ةقيرط كانه نوكت ثيح لاثم انه . Microsoft Windows في رماوالا رطس في رمال ping مادختسا | هي (VPN) ةيره اظلا ةصاخال ةكبش لابة صاخال ناونعب ةكبشال لىل ةدجوم رخآ فيضمو 192.168.0.0/24 ليمعلل ةلحي ل ةكبشال

<#root>

C:\>

ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=255  
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255  
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255  
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms

سكنيل ىلع

```
malhyari@ubuntu:~$ ping 192.168.171.131
PING 192.168.171.131 (192.168.171.131) 56(84) bytes of data.
64 bytes from 192.168.171.131: icmp_seq=1 ttl=128 time=0.474 ms
64 bytes from 192.168.171.131: icmp_seq=2 ttl=128 time=0.315 ms
64 bytes from 192.168.171.131: icmp_seq=3 ttl=128 time=0.336 ms
64 bytes from 192.168.171.131: icmp_seq=4 ttl=128 time=0.475 ms
64 bytes from 192.168.171.131: icmp_seq=5 ttl=128 time=0.337 ms
64 bytes from 192.168.171.131: icmp_seq=6 ttl=128 time=0.286 ms
64 bytes from 192.168.171.131: icmp_seq=7 ttl=128 time=0.252 ms
```

اهالصالوا عاطخأال فاشكتسا

اهالصالوا نيوكتللا عاطخأ فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي

مسالا بسح ضارعتسال او عابطلال رذعتي

مسالا بسح ضارعتسال او عابطلال كنكمي ال، ةلحملال LAN ةكبش ىل لوصولل هنيوكتل و VPN ةكبش لي مع لاصتا دنع  
عضولا اذه ىلع بلغلل ناحتام نارايخ كانه. ةلحملال LAN ةكبش ىلع

- IP ناووع بسح عابطلال او ضارعتسال

• رتوي بمك لل IP ناووع  $x.x.x.x$  نوكي شيح  $x.x.x.x$  ةغاىصال مدختسا  $\\sharename$ ، ةغاىصال نم ال دب، ضارعتسال  
فيضمال

- لاثمال لىبس ىلع. مسالا نم ال دب IP ناووع مادختسال ةكبشال عباط صئاصخ ريغت ب مق، عابطلال  
IP ناووع  $x.x.x.x$  نوكي شيح،  $\\x.x.x.x\printername$ ، مدختسا  $\\sharename\printername$ ، ةغاىصال نم ال دب

- Microsoft Windows رتوي بمك ىلع LMHOSTS فلم كل حمسي. هليدعت او VPN لي مع ل LMHOSTS فلم عاشناب مق  
امك LMHOSTS فلم ودي نأ نكمي، لاثمال لىبس ىلع. IP نيوانعو فيضمال امسا نيبتات تانيي عت عاشناب  
يلى:

```
192.168.0.3 SERVER1
192.168.0.4 SERVER2
192.168.0.5 SERVER3
```

قئاث و عجار. %SystemRoot%\System32\Drivers\Etc. ف LMHOSTS فلم دجوي، Microsoft Windows XP Professional Edition ف  
تامول عمل نم ديزم ىلع لوصحلل Microsoft.

ةلص تاذا تامول عم

- [9.17 رادصلال، Cisco ASA Series VPN نم رماوالا رطس ةهجاو ني وكت لىلد: CLI Book 3](#)
- [Cisco ASA 5500-X Series ىلاتال لىجلا نم ةىامحلل ناردج](#)
- [Cisco Systems - تادنستس مل او ىنقتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل