

هجوم ب لاصتال Microsoft VPN ليمع نيوكت RV34X ةلسلسلا نم

فدهلا

هجوم ب لاصتال Show Soft VPN ليمع مادختسا ةيفيك حيصوت وه دنتسمل اذه نم فدهلا RV340 ةلسلسلا نم.

انه نم Shrew Soft VPN Client جم انرب نم رادصا شدا ليزنت كنكمي

<https://www.shrew.net/download/vpn>

جماربال رادصا | قيبتلل ةلباقلا ةزهجالا

RV340 | 1.0.3.17 (شدا ليزنت)

RV340W | 1.0.3.17 ([شدا ليزنت](#))

RV345 | 1.0.3.17 ([شدا ليزنت](#))

RV345P | 1.0.3.17 ([شدا ليزنت](#)) زارطلا

مادختسا ةلاح / ةمدقم

ةصاخلا ةكبشلا (IPSec ل VPN) ةيرهاظلا ةصاخلا ةكبشلا كل حمست قفناش نالال نم نم لكشب ةديعبلا دراوملا لعل لوصحلاب (ةيرهاظلا معدتو VPN IPSec مداوخك RV34X series تاهجوم لمعت. تنرتنإل ربع رفشم ليمعلاو هجوملا نيوكت ةيفيك كل ليلدلا اذه حصوي Core VPN Soft ليمع VPN ةكبش لاصتا نيما تل طيسبلا

نيزنجل لعل دنتسمل اذه يوتحي:

RV340 ةلسلسلا هجوم نيوكت

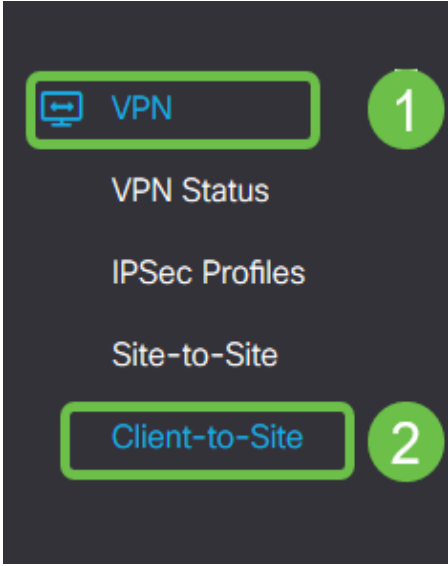
Core Soft VPN ليمع نيوكت

RV34X: ةلسلسلا نم هجوم نيوكت

RV34x ىل ع قو م ىل ل ل ي م ع ن م VPN ة ك ب ش ن ي و ك ت ب أ د ب ن س

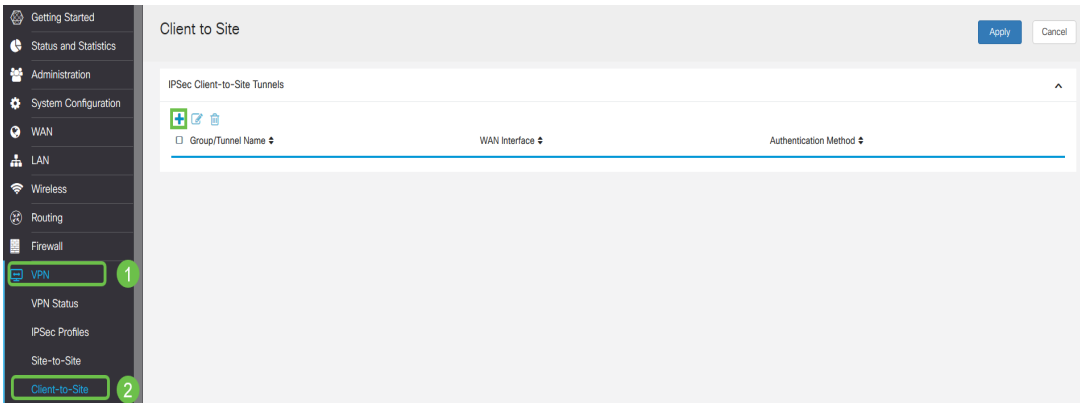
1 ة و ط خ ل ا

ع قو م ىل ل ل ي م ع ن م (VPN) ة ي ر ه ا ظ ل ا ة ص ا خ ل ا ة ك ب ش ل ا ي ف ،



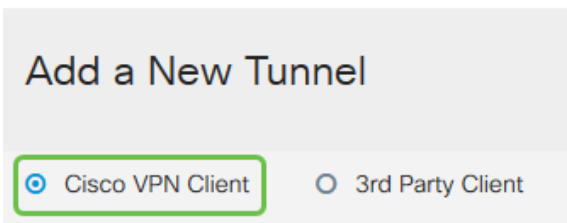
2 ة و ط خ ل ا

ع قو م ىل ل ل ي م ع ن م VPN ف ي ر ع ت ف ل م ة ف ا ض ا



3 ة و ط خ ل ا

Cisco VPN ل ي م ع ر ا ي خ د د ح



4 ة و ط خ ل ا

ة و م ج م ل ا م س ا ن ي و ك ت ب م و ق ن س ا م ك . ا ط ا ش ن VPN ل ي م ع ف ي ر ع ت ف ل م ل ع ج ل ن ي ك م ت ل ا ع ب ر م د د ح ، ا ق ب س م ك ر ت ش م ح ا ت ف م ل ا خ د ا و ، WAN ة ه ج ا و د ي د ح ت و ،

امهم ادخستس ا متيس شيح اق بس م كرتش م ل ا ح ا ت ف م ل ا و ع و م ج م ل ا م س ا ع ط ح ا ل م ا ج ر ل ا : ع ط ح ا ل م ل ا . ل ا م ع ل ا ن ي و ك ت د ن ع ا ق ح ا ل .

Enable:

Group Name:

Interface:

IKE Authentication Method

Pre-shared Key:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

5 ة و ط خ ل ا

ه و م ل ا ي ل ع ن ي م د خ ت س م ل ا ع و م ج م ب ص ا خ ا ذ ه . ن ا ل ا ا غ ر ا ف ن ي م د خ ت س م ل ا ع و م ج م ل و د ج ك ر ت ا ، ل a n ة ك ب ش ل ع م ج ت ل ا ق ا ط ن ل خ د ا . ل ا م ع ل ا ي ل ع ع ض و ل ا ن ي ي ع ت ن م د ك ا ت . د ع ب ه ن و ك ن م ل ا ن ن ك ل و 172.16.10.10 ي ل ا 172.16.10.1 ن م م د خ ت س ن س . ل ا م ع ل ا ب ة ص ا خ ل ا

ي ل ع ن ا ك م ي ا ي ف ة م د خ ت س م ر ي غ ة د ي ر ف ة ي ع ر ف ة ك ب ش ع م ج ت ل ا ق ا ط ن م د خ ت س ي ن ا ب ج ي : ع ط ح ا ل م ل ا ة ك ب ش ل ا .

User Group:

User Group Table

+ Group Name

Mode: Client NEM

Pool Range for Client LAN

Start IP:

End IP:

6 ة و ط خ ل ا

اه م د خ ت س ن س ي ت ل ا ت ا د ا د ا ل ا ي ه ه ذ ه . د ا د ا ع ا ي ل م ع ل ي ك ش ت ب و ل س ا ل ا ل ك ش ن شيح ا ن ه :

DNS م د ا خ م ا د خ ت س ا ي ف ب غ ر ت ت ن ك و ا ي ل خ ا د DNS م د ا خ ك ي د ل ن ا ك ا ذ ا : ي س ا س ا ل ا DNS م د ا خ ن ا و ن ع RV340 ل ا ي ل ا ر ي ص ق ت ل ا ت ت ب ث ، ك ل ذ ف ا ل خ . ا ن ه ه ل ا خ د ا ك ن ك م ي ، ي ج ر ا خ ا ن ل ا ث م ي ف ي ض ا ر ت ف ا ل ا م د خ ت س ن س .

ر ا ي خ ل ا ا ذ ه م ا د خ ت س ا م ت ي . ي ق ف ن ل ا ل ا ص ت ا ل ا م ي س ق ت ن ي ك م ت ل ق ق ح ت : ق ف ن ل ا م ي س ق ت ي ف " ق ف ن ل ا م ي س ق ت " م د خ ت س ن س . VPN ق ف ن ر ب ع ر م ت ف و س ي ت ل ا ر و ر م ل ا ة ك ر ح د ي د ح ت ل ا ن ل ا ث م .

اهيلا لوصول قح VPN ليمعل نوكي نأ بجي يتلا تاكبش لال خذا: قفنلا لودج ميسقت
LAN RV340 ةكبش ةكبش لاثملا اذه مدختسي. VPN ةكبش ربع

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain:

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Split Tunnel:

Split Tunnel Table

+ [edit] [delete]

IP Address Netmask

| IP Address | Netmask |
|---|---|
| <input checked="" type="checkbox"/> 192.168.1.0 | <input checked="" type="checkbox"/> 255.255.255.0 |

7 ةوطخلا

للا ليمع تاعومجم ةمئاق ي ف فيرعتلا فلم لعل عالطالا اننكمي، ظفح قوف رقنلا دعب
IPSec عقوم

Client to Site

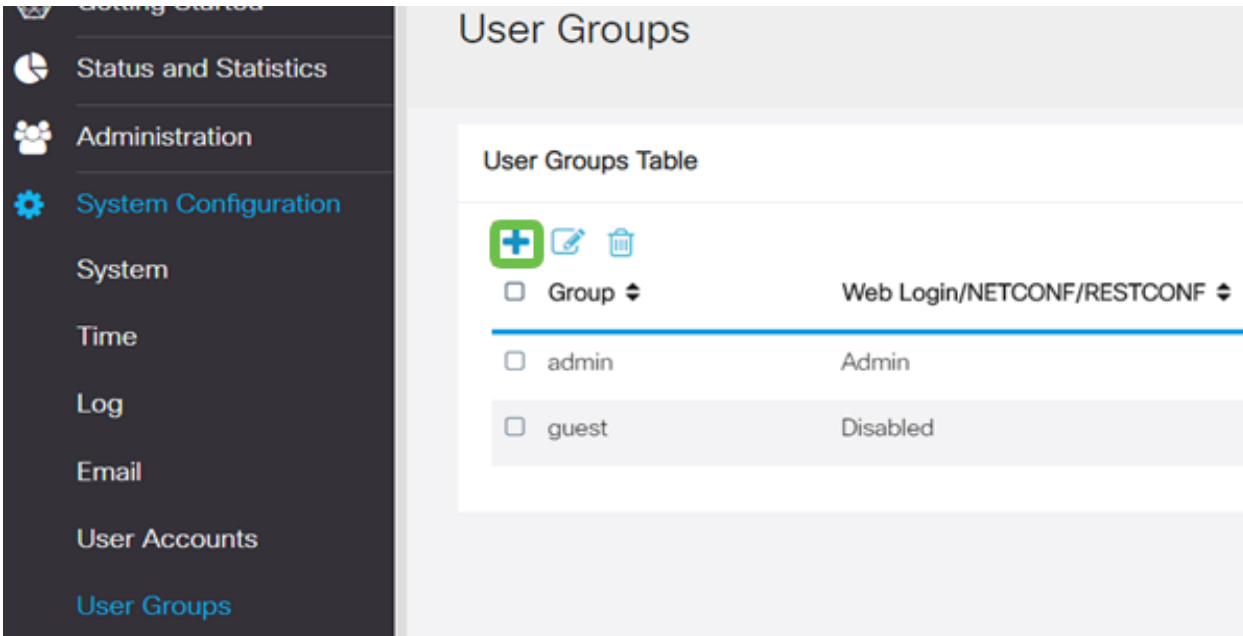
IPSec Client-to-Site Tunnels

+ [edit] [delete]

| Group/Tunnel Name | WAN Interface | Authentication Method |
|----------------------------------|---------------|-----------------------|
| <input type="checkbox"/> Clients | WAN1 | Pre-shared Key |

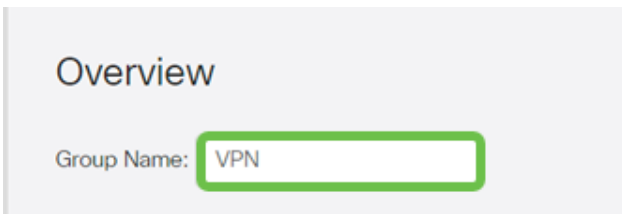
8 ةوطخلا

في VPN ليمع يمدختسم ةقداصل اهم ادختسال ني مدختسم ةعومجم نيوكتب نالا موقنس
ني مدختسم ةعومجم ةفاضل '+' قوف رقنا، ني مدختسم لال تاعومجم > ماظنلا نيوكت



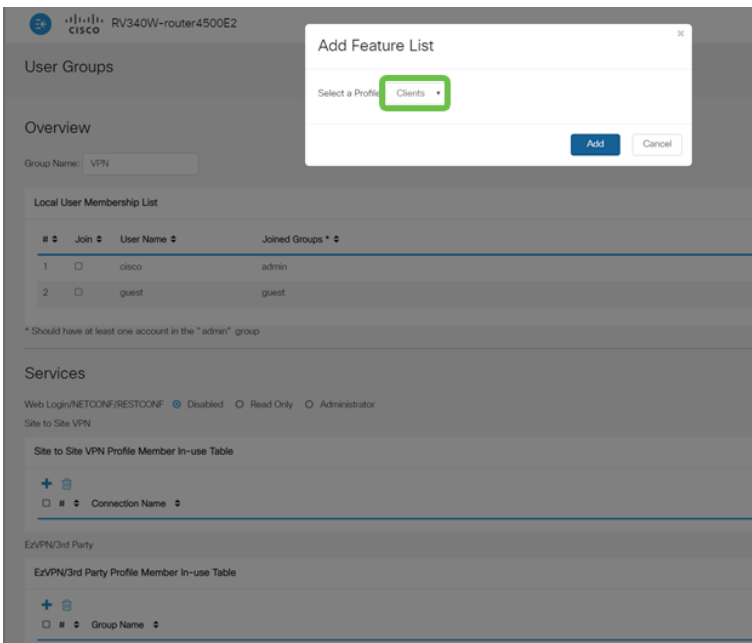
9 ةوطخل

ةومجم مسا لخدأ.



10 ةوطخل

هذه نيمدختسمل ةومجم طبرلة فاضل قوف رقنا ، ثلاثل فرطل/EzVPN > تامدخل مسق يف اقباس هنيوكتب انمق يذل عقوملا لىل ليمعلا فيرعت فلمب.



11 ةوطخل

ثلاثا ل فرطال/EzVPN ل ةمئاقلا يف عقوملا ل ل لمعلا نم ةومجم مسا نآلا ىرت نأ بجي

EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

+

Group Name

1 Clients

12 ةوطخال

نيمدختسملا تاعومجم ةمئاق يف هارتس، نيمدختسملا ةومجم نيوكت قيبطت دعب
يذال عقوملا ل ل لمعلا ل فيرعت فلم عم ةديجال نيمدختسملا ةومجم مادختسا رهظيسو
اقباس هاناش نأ.

Getting Started

Status and Statistics

Administration

System Configuration

System

Time

Log

Email

User Accounts

User Groups

User Groups

User Groups Table

+

| <input type="checkbox"/> Group <input type="checkbox"/> | Web Login/NETCONF/RESTCONF <input type="checkbox"/> | S2S-VPN <input type="checkbox"/> | EzVPN/3rd Party <input type="checkbox"/> |
|---|---|----------------------------------|--|
| <input type="checkbox"/> VPN | Disabled | Disabled | Clients |
| <input type="checkbox"/> admin | Admin | Disabled | Disabled |
| <input type="checkbox"/> guest | Disabled | Disabled | Disabled |

13 ةوطخال

+ قوف رقنا. مدمدختسملا تاباسح >ماظنلا نيوكت يف ديجمدختسم نيوكت نآلا موقنس
ديجمدختسم ءاش نأ.

Local Users

Local User Membership List

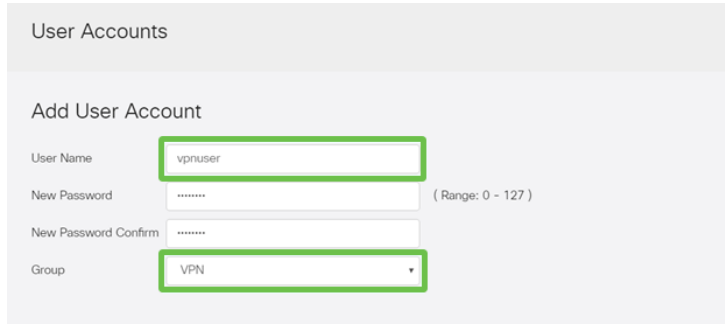
+

| <input type="checkbox"/> # <input type="checkbox"/> | User Name <input type="checkbox"/> | Group * <input type="checkbox"/> |
|---|------------------------------------|----------------------------------|
| <input type="checkbox"/> 1 | cisco | admin |
| <input type="checkbox"/> 2 | guest | guest |

* Should have at least one account in the " admin " group

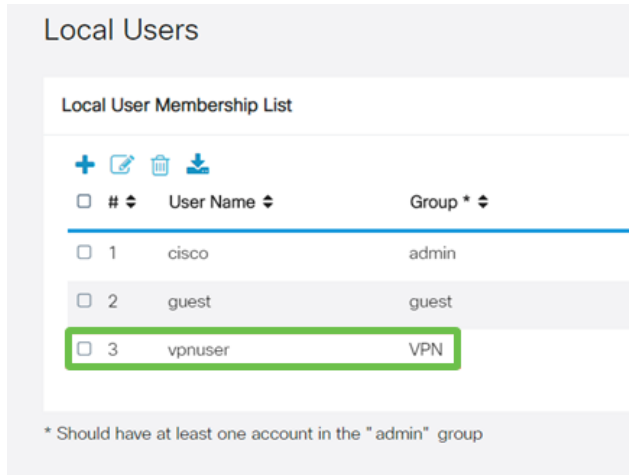
14 ةوطخل

ةومجم لىل ةومجم لىل نىيىت نم ققحت .ةديجل رورملا ةملك عم ديجل مدختسمل مس لخدأ ءاهتال دنل قىببط قوف رونا .وتلل اهنيوكتب انمق يتل ةديجل ني مدختسمل



15 ةوطخل

نىيىلحمل ني مدختسمل ةمئاق يى ديجل مدختسمل رهظيى



| # | User Name | Group * |
|---|-----------|---------|
| 1 | cisco | admin |
| 2 | guest | guest |
| 3 | vpnuser | VPN |

* Should have at least one account in the "admin" group

Shrew Soft لىم عم نيوكتب نأل موقنس .ديدخت جاحسم RV340 sery لىل لىل لكشتال متي اذه VPN.

ShrewSoft VPN لىم عم نيوكت

Shrew Soft VPN لىم عم نيوكتب نأل موقنس.

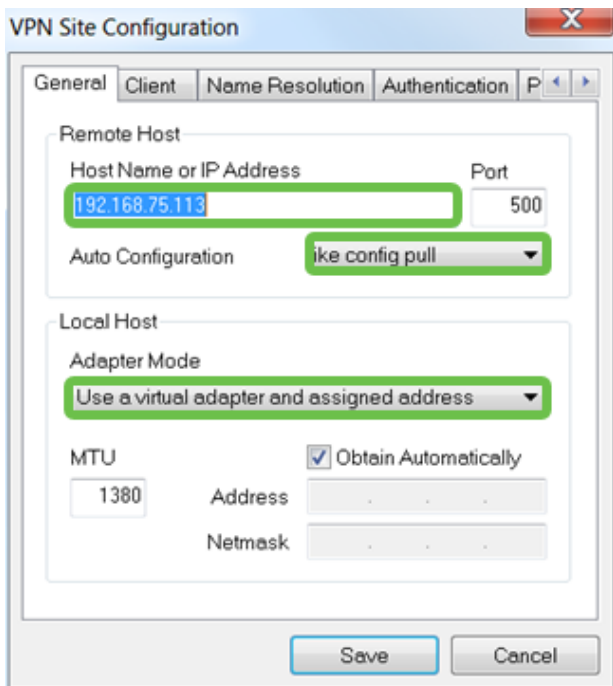
1 ةوطخل

ةذفان يى .فىرعت فلم ةفاضل ةفاضل قوف رونا و ShowSoft VPN Access Manager حتفا :ماع بيوبتل ةمال عم نيوكتب مق ،رهظت يتل VPN عم قوم نيوكت

RV340 ب صاخل فىضمال مس (أ WAN IP ناوعم مدختسأ :IP ناوعم وأ فىضمال مس)

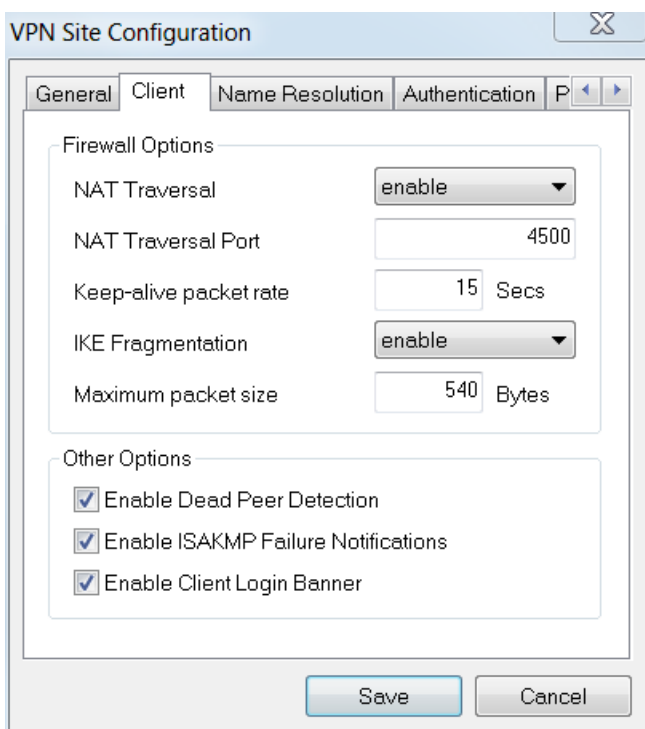
نيوكتل بحس ديحت :ئىاقلتل نيوكتل

نىعم ناوعم ويرهظ ئىاهم مادختس | ددح :لوحمل عضو



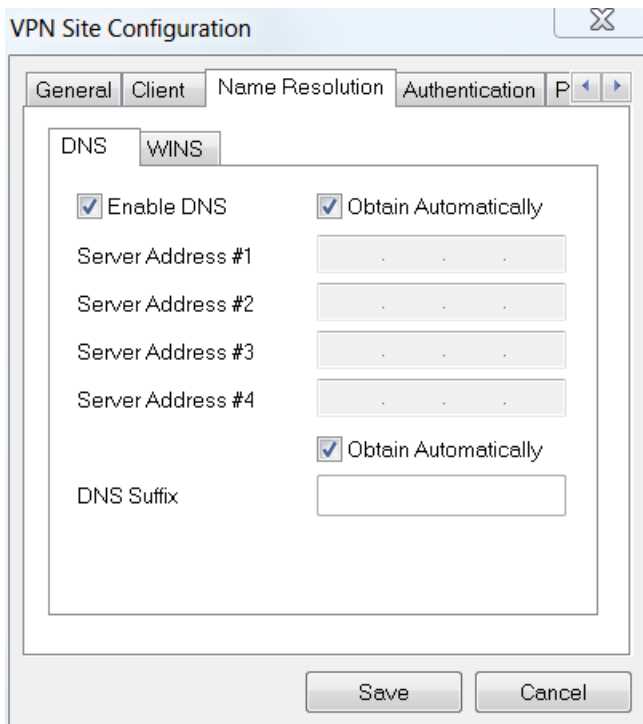
2 ةوطخلال

ةيضا رتفالا تادادعالا طقف مدختسنس .للمعمال بيوبتلا ةمالع نيوكتب مق



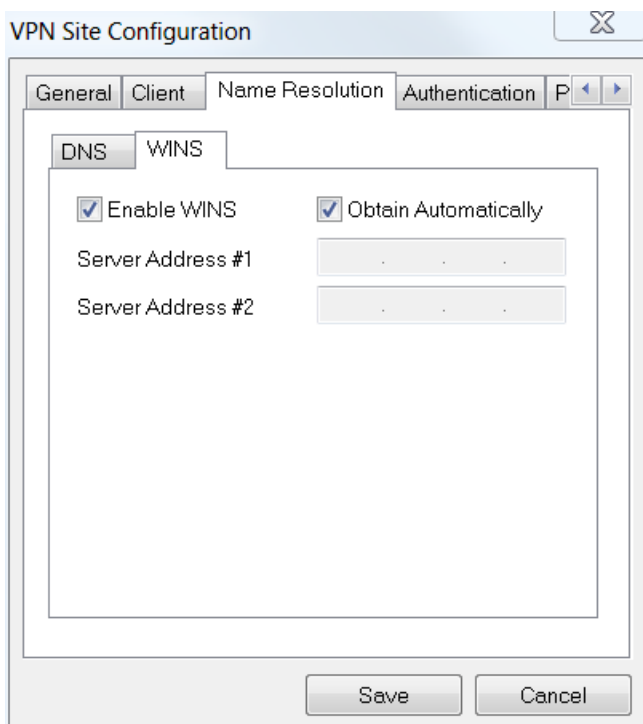
3 ةوطخلال

Obtain تاعبرم كرتاو Enable DNS عبرملا دح ، Name Resolution > DNS بيوبتلا ةمالع يف ةدح م.



4 ةوطخال

رايتخال ةناخ كرت او WINS ني كمت ع برم ددح، Name Resolution > WINS بي وبت ال ةمال ع ي ف اي ئاقت Obtain.

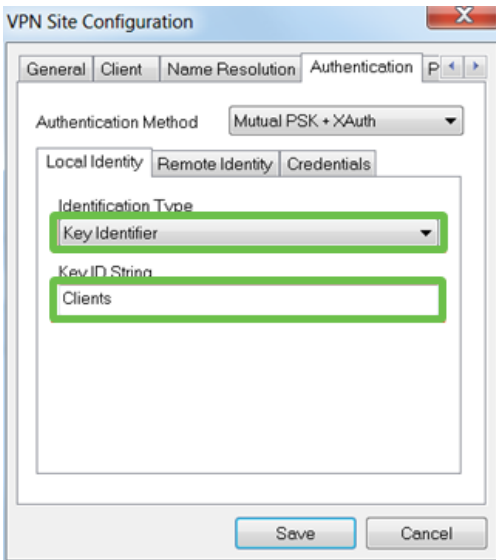


5 ةوطخال

ةي ةمال ةي وبت ال ةمال ع > ةقداصل ال بي وبت ال ةمال ع ني وكت ب مق

حاتفم ال فرم دي دحت: في رعت ال عون

RV34x لى ع هني وكت مت يذلا ةومجم ال مسا لخدأ: حاتفم ال فرم ةلسلس



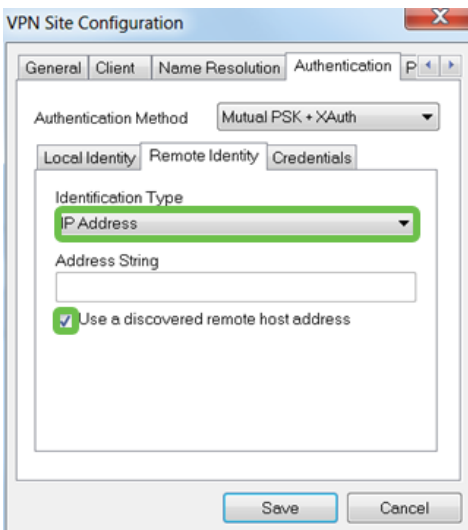
6 ةوطخلال

ةيضا رتفالال تادادإلال كرتنس، ةديعب ةيوه > ةقداصم بيوبتلال ةمالع يف

IP ناوع: فيرتلال عون

<blank> ناوعلال ةلسلس

دحم: فشتم ديعب فيضم ناوع ع برم مادختسلا

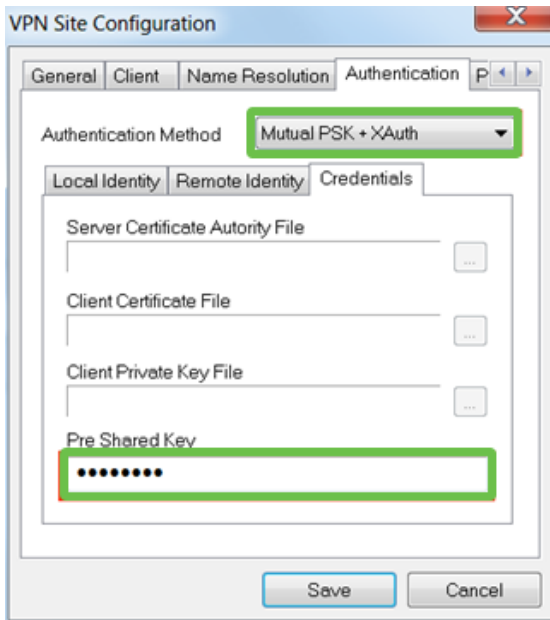


7 ةوطخلال

ي: لي ام نيوكتب مق، دامتعلا تانايب > ةقداصم بيوبتلال ةمالع يف

PSK + XAuth لدابت م ديحت: ةقداصملا بولسأ

ليمع فيرتت فلم يف نوكملا اق بس م كرتشملا حاتملا لخدأ: اق بس م كرتشم حاتم
RV340



8 ةوطخل

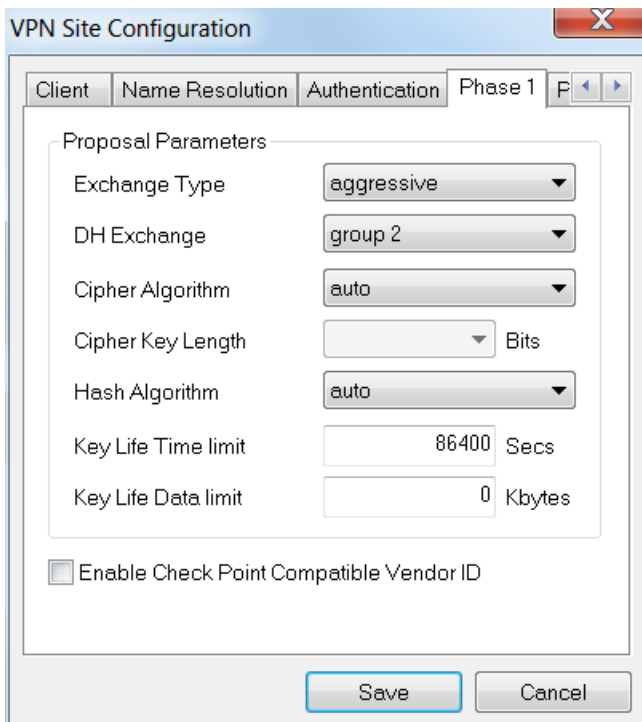
اهانكم في ةيضارتفالا تاداعإلا كرتنس ، 1 ةلحرملال بيوبتلال ةمالعل

فيعن ع Exchange:

2 ةومحملال DH: لدا بت

يئاقلت :ريفشتلال ةيمزراوخ

يئاقلت :ةئزجتلال ةيمزراوخ



9 ةوطخل

2: ةلحرمل ا بيوبتل ةمالعل ةيضارتفالا تاداعإل اضيأ مدختسنس

يئاقلت :ليوحتل ةيمزراوخ

يئاقلت : HMAC ةيمزراوخ

لطم : PFS لدابت

لطم : ةيمزراوخل طغض

VPN Site Configuration

Name Resolution Authentication Phase 1 Phase 2

Proposal Parameters

Transform Algorithm auto

Transform Key Length Bits

HMAC Algorithm auto

PFS Exchange disabled

Compress Algorithm disabled

Key Life Time limit 3600 Secs

Key Life Data limit 0 Kbytes

Save Cancel

10 ةوطخل

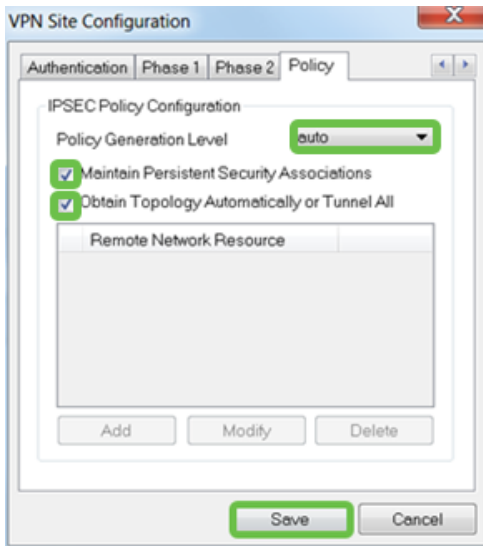
ةيلال تاداعإل مدختسنس، جهن بيوبتل ةمالعل ةبسنلاب

يئاقلت : ةسايسلا عاشن | يوتسم

ققحتلا مت : ةتباثل نامأل تانارتق اب ظافتحال

ققحتلا مت : لكلا قفن وأ ايئاقلت ططخمل يلعل لوصحلا

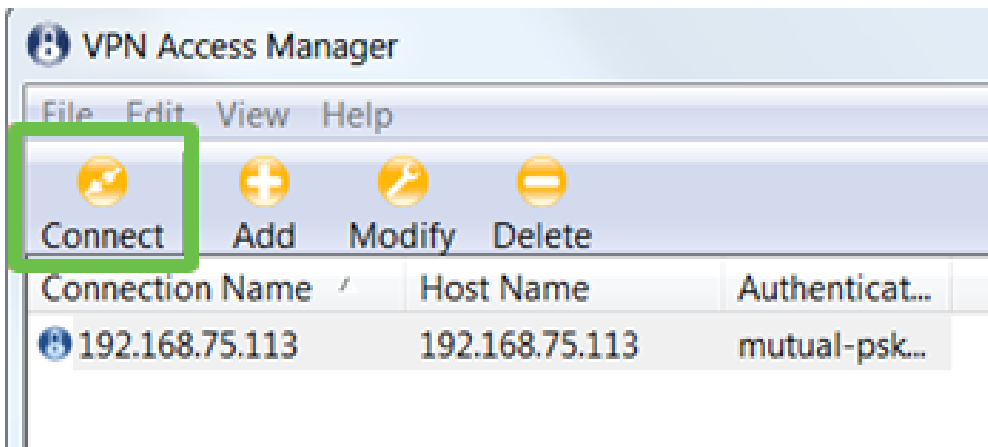
نظرا لأننا قمنا بتكوين اتصال نفقي منفصل على RV340، فلا حاجة إلى تكوينه هنا.



ظفح قوف رقنا ،ءاهتال دنع .

11 ةوطخلال

لېصوتال فيرعت فلم ىلع تزكر ،VPN لوصوري دم في . لاصتال رابخال نوزهاج نآال نحن
لېصوت رزىل ع رقناو .



12 ةوطخلال

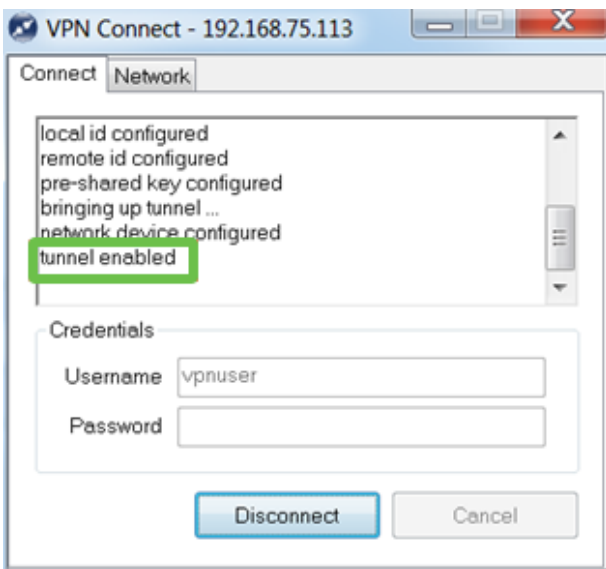
تانايب مادختساب رورملا ةملكو مدختسملا مسا لخدأ ،رهظي يذال VPN Connect راطالال في
13 و 14 ةوطخلال) RV340 ىلع هاناشنا يذال مدختسملا باسحل دامتعالال .



لې صوت ىل ع رقنا ،ءاهت نال دنع

13 ةوطخلال

نكمم قفنللا ىرت نأ بجي . قفنللا لاصتا نم ققحت



رارقلال

VPN ربق كتك بشب لاصتالل دادعإلا دي نآلا تنأ ،كانه

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا