

تاهجوم ىل ع Greenbow جم انرب عم C2G نيوكت VPN RV016 و RV042 و RV042G و RV082

فادهال

نم نيوكت ةحفص مادختساب GreenBow ليمع ىل ع (قراب ع ىل ليمع نم) C2G دادعإ متي جمارب ريفوت ىل ع زكري جم انرب وه GreenBow. NAT-T رايخ دجوي شيح ةباوبلا ىل ع قراب علا ريوطت ب GreenBow ماق دقو. امامت ةنم آجمارب ةعومجم ىل ع اذانتسا تاسس وم لل نامأ دع ب نع نيومدختس ملل حمسي واطيس ب دع ب نع لوصولل عجي تاسس وم لل نامأ جم انرب. نامأ مهتاك رش ةكبش ىل ع لوصولاب

ىل ع Greenbow جم انرب مادختساب IPsec VPN C2G نيوكت ةيفيك دننتس ملل اذه حرشي VPN RV082 و RV042G و RV042 و RV016 تاهجوم

قيبطت لل ةلباقلا ةزهجالا

- زارطلا RV016
- زارطلا RV042
- زارطلا RV042G
- زارطلا RV082

جماربل رادصا

- رادصا 4.2.1.02

GreenBow و C2G جمارب نيوكت

> VPN راتخي نأ ةدعاسم ةادأ ليكشت ديدخت جاحس ملل لخاد ةعرس سايقم لجمس 1. ةوطخلا
:ةباوبلا ىل ع قراب علا ةحفص حتف متي. ةباوب ىل ع ةباوب

Gateway To Gateway

Add a New Tunnel

Tunnel No. : 2

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

ةلحلملةومجملا دادعلةقطنمىللىلفسألريرمتلاب مق

Local Group Setup

Local Security Gateway Type :

IP Address : 59.105.113.180

Local Security Group Type :

IP Address :

Subnet Mask :

ةلحلملنامألةرابععونةلدسنملاةمئاقلالنمطقفIPرتخأ. 2ةوطخللا

ةلحلملنامألةومجمعونةلدسنملاةمئاقلالنمفةعرفلالكبشلالرتخأ. 3ةوطخللا

ةوملابصاخاللIPناونعلاخدأ، IPناونعلاقف. 4ةوطخللا

ةوملللةعرفلالكبشلالعانقلاخدأفةعرفلالكبشلالعانقلاقف. 5ةوطخللا

"ةديعب لة عومجم لاداع" ةقطنم ىلإ لاقئنا لل لفسأل ريرمتلاب مق 6. ةوطخال
ةحفصلاب

Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 59.105.113.148

Remote Security Group Type : IP

IP Address : 192.168.2.101

ةديعب لة نامأل ةرابع عون ةلدسنم لة مئاقلا نم طقف IP رتخأ 7. ةوطخال

بناج ىلإ ناليم ةمئاق ناووع لخدم نم أديعب لة نم عون ناووعلا ترتخأ 8. ةوطخال

ةديعب لة هجوملاب صاخلا IP WAN ناووع لخدأ، IP ناووع لقح يف 9. ةوطخال

"ةديعب لة نامأل ةعومجم عون" ةلدسنم لة مئاقلا نم IP دح 10. ةوطخال

هجوملاب صاخلا IPv4 ناووع لخدأ، IP ناووع لقح يف 11. ةوطخال

IPSec Setup

Keying Mode : IKE with Preshared key ▼

Phase 1 DH Group : Group 1 - 768 bit ▼

Phase 1 Encryption : DES ▼

Phase 1 Authentication : MD5 ▼

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit ▼


Phase 2 Encryption : DES ▼

Phase 2 Authentication : MD5 ▼

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

[Advanced +](#)

عضو ةلدسننملا ةمئاقلا نم اقبس م كرتشملا حاتفملا مادختساب IKE رتخأ. 12 ةوطخل ظفحل.

ةلحرملل DH ةومجم ةلدسننملا ةمئاقلا نم تب 1-768 ةومجملا رتخأ. 13 ةوطخل لولأا.

لولأا ةلحرمل ريفشتل ةلدسننملا ةمئاقلا نم DES رتخأ. 14 ةوطخل.

لولأا ةلحرمل ةقداصم ةلدسننملا ةمئاقلا نم MD5 رتخأ. 15 ةوطخل.

ةينات 28800 SA ةايح ةم لقح ةميق لخدت 1 ةلحرمل يف. 16 ةوطخل.

2. ةلحرمل DH ةومحمل ةلدسنملا ةمئاقلا نم تب 768-1 ةومحمل رتخأ. 17 ةوطخل

2. ةلحرمل ريفشتل ةلدسنملا ةمئاقلا نم DES رتخأ. 18 ةوطخل

2. ةلحرمل ةقداصل ةلدسنملا ةمئاقلا نم MD5 رتخأ. 19 ةوطخل

ةيناث SA 3600 ةيصالص ةم لقح ةميق لخدت 2 ةلحرمل ي ف. 20 ةوطخل

وأومأقراأل نم ةبولطملا ةومحمل لخدأ اقبسم كرتشملا حاتفملا لقح ي ف. 21 ةوطخل
"1234678" ةلحال هذه ي ف هو. فورحلا

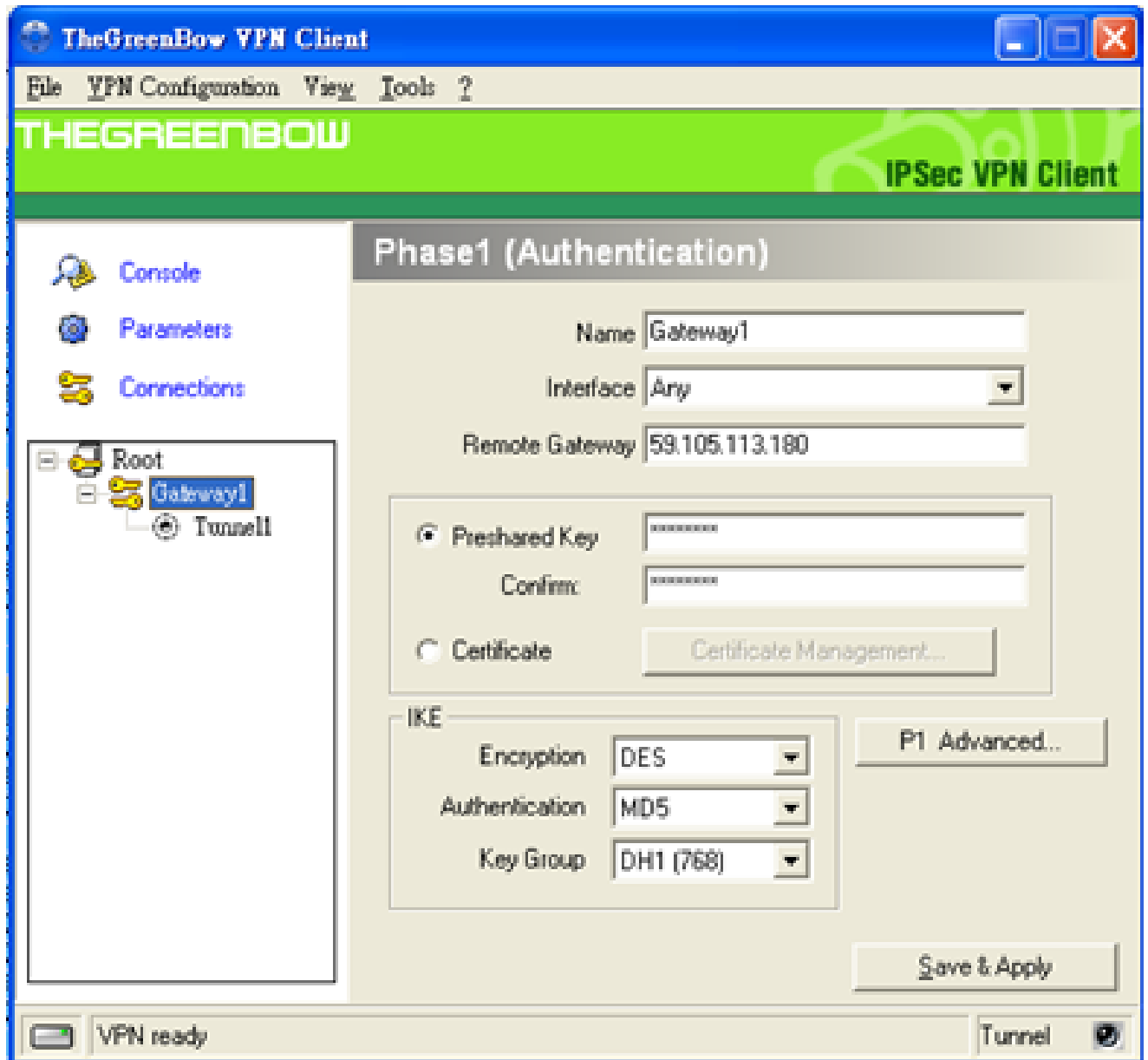
Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5 ▼
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval 10 seconds

مدمقتملا ةحفص حتفت + مدمقتم قوف رونا. 22 ةوطخل

NAT Traversal رايخال ةناخ دح. 23 ةوطخل

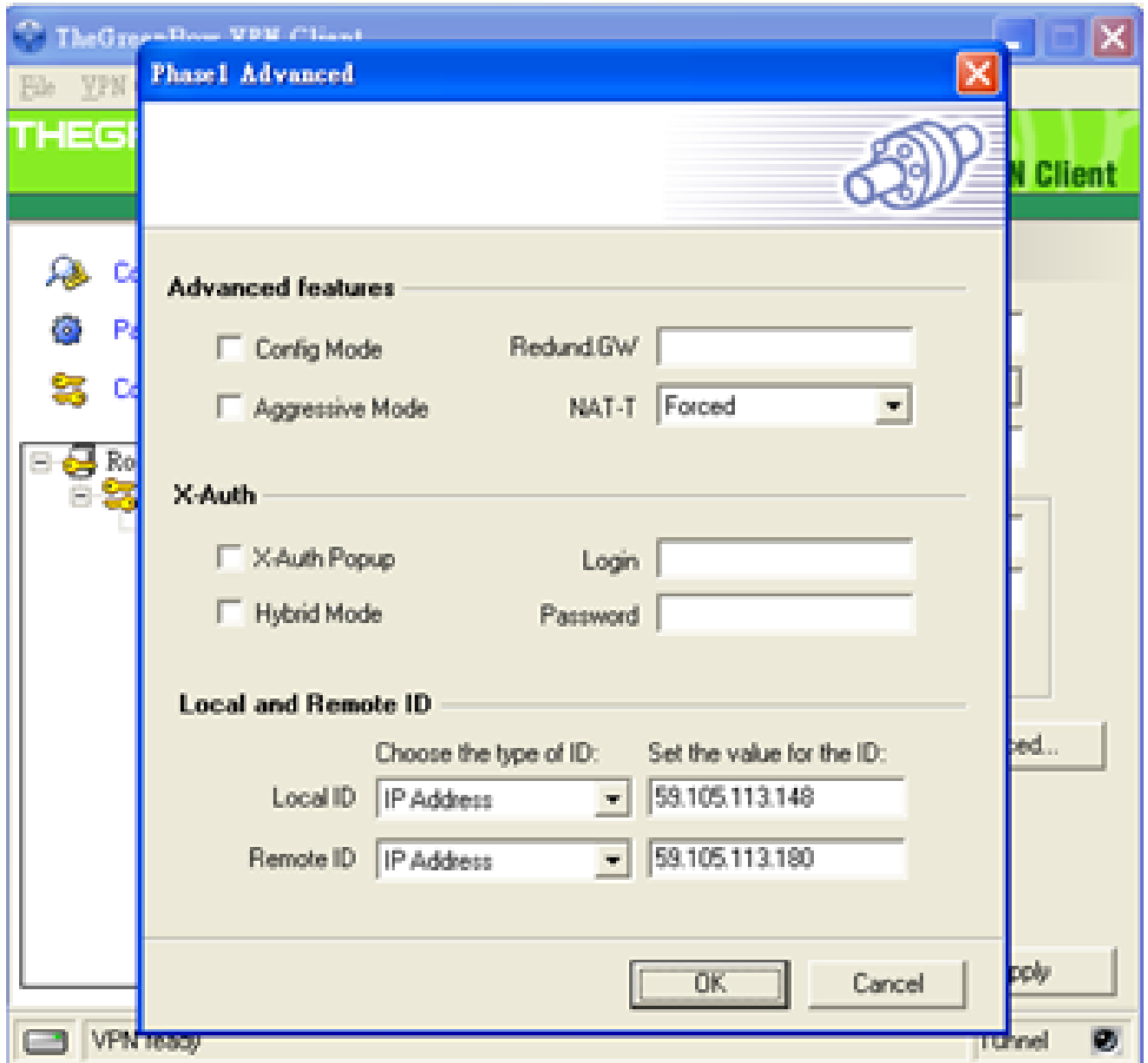
رتويبمكلا زاخ يلع IPSec VPN ليمعل Greenbow جم انرب ليغشتب مق. 24 ةوطخل
كب صخال



ديعبال هجوملاب صاخال IP WAN ناوع لخدأ، ةديعبال ةباوبال ل قح ي ف. 25 ةوطخال



ةمدقتمال لولوال ةلجرمال ةحفص رهظت. P1 مدقتم رز لعل رقنا. 26 ةوطخال



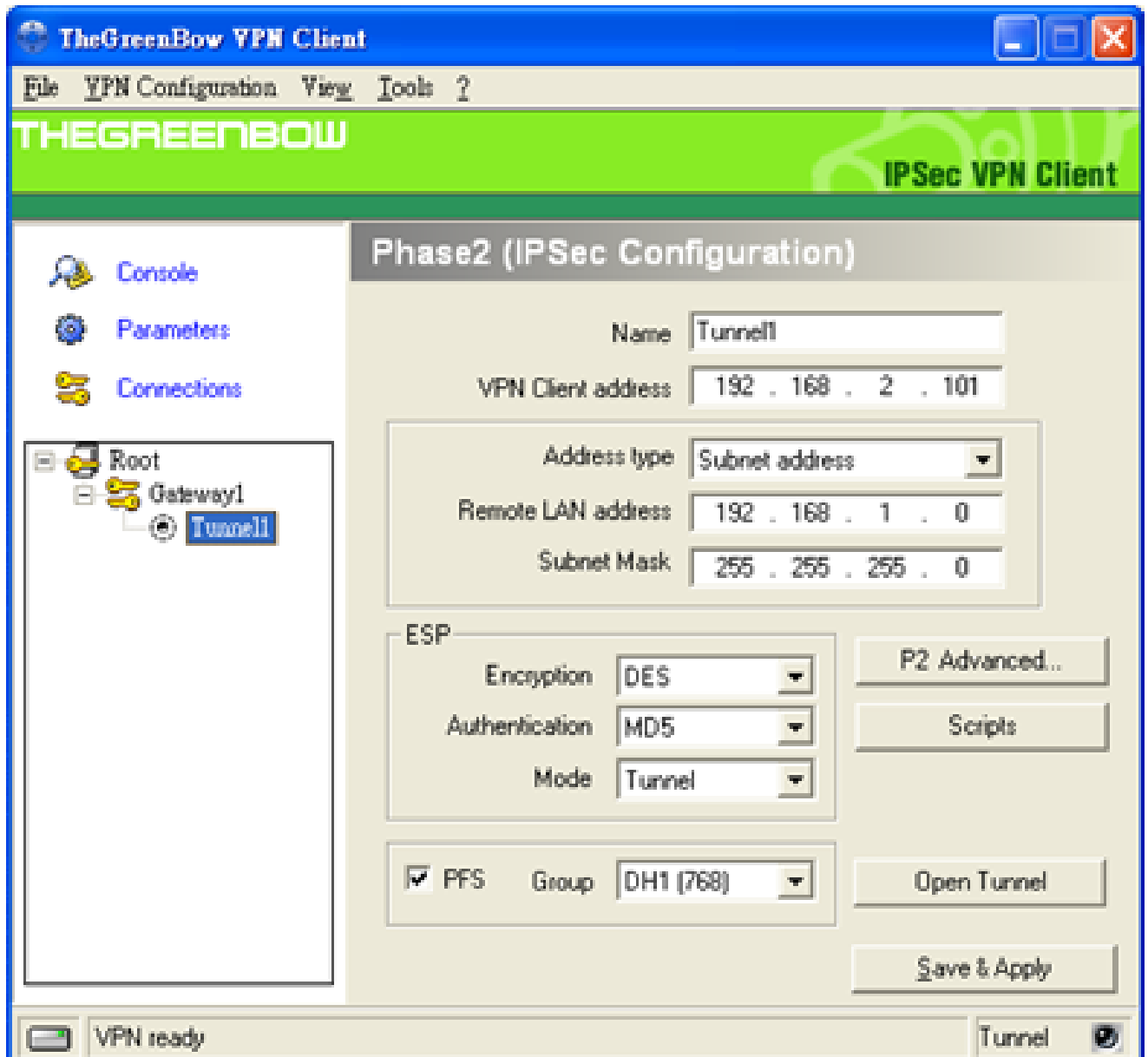
NAT-T. ةلدسنملا ةمئاقلا نم ضرف رتخأ. 27 ةوطخلا

ديعب فرعمو يلحم فرعم ةلدسنملا ةمئاقلا يف IP ناو نع رتخأ. 28 ةوطخلا

هجوملاب صاخلا IP WAN ناو نع لخدأ، يلحملا فرعملا لقح يف. 29 ةوطخلا

ديعبلا هجوملاب صاخلا IP WAN ناو نع لخدأ، "ديعبلا فرعملا" لقح يف. 30 ةوطخلا

OK قوف رقناو. 31 ةوطخلا



32. ةوطخلال Tunnel1 قوف رقنا .

33. ةوطخلال VPN ةكبش ليمع ناوع لقح ي .

34. ةوطخلال نم ةيعرفلا ةكبشلا ناوع رتخأ .

35. ةوطخلال LAN ناوع لخدأ ، ةيديعلا (LAN) ةكبشلا ناوع لقح ي .

36. ةوطخلال ةكبشلا عانق لخدأ ةيعرفلا ةكبشلا عانق لقح ي .

37. ةوطخلال قيبطتو ظفح قوف رقنا .

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل