

# ىلج (IKE) تنرتنإل حاتفم لدابت جهن تادادعإ RV130W و VPN RV130 تاهجوم

## فدهل

نيتكبش نيب نم آلاصتا سسؤي لوكوتورب وه (IKE) تنرتنإل حاتفم لدابت  
حيتافملا مادختساب اهنيمأت اغلإو اهنيمأت مزحل ريفشت متي، IKE مادختساب  
نيرط لبق نم ةمدختسمل

نيوكت عجار VPN جهن نيوكت لبق Internet Key Exchange جهن عاشنإ لىل حاتحت  
تامولعمل نم ديزم لىل لوصحلل [RV130 و RV130W لىلج VPN ةسايس](#)

VPN تاهجوم لىل IKE فيرعت فلم ةفاضل ةيفيك حيصوت وه دنتسمل اذه نم فدهل  
RV130 و RV130W.

## قيبطتل ةلباقلا ةزهجالا

- RV130
- RV130W

## ةيئارجا تاوطخ

عقوم نم VPN > IPsec VPN رايخال هجوملا نيوكتل ةدعاسملا ةادلأ مدختسأ. 1. ةوطخل  
دادعإ ةحفص رهظت. راسيلا لىل ةدوجوملا ةمئاقلا نم مدقتملا VPN دادعإ > عقوم لىل  
مدقتملا VPN

### Advanced VPN Setup

NAT Traversal:  Enable

IKE Policy Table							
<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group
<input type="checkbox"/> No data to display							
Add Row		Edit		Delete			

VPN Policy Table									
<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Algorithm	Local	Remote		
<input type="checkbox"/> No data to display									
Add Row		Edit		Enable		Disable		Delete	

Save Cancel

IPSec Connection Status

مديج ءذفان رهظت. فص ءفاضاً قوف رقنا، IKE، جهن لودج تحت 2. ءوطخلا

IKE Policy Table							
<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group
<input type="checkbox"/> No data to display							
Add Row		Edit		Delete			

IKE مسا لوق يه IKE جهنل مسا لخدأ 3. ءوطخلا

### Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

مادختسا ههف مه تي يذلا عضولا رتخأ، Exchange، عضو ءلدسنملا ءمئاقلا نم 4. ءوطخلا  
نمأ لاصتا ءاشنال حيتافملا لدابت

### Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Main  
Aggressive

ييلات وحنلا ىلع ةحاتملا تارايلخا ديحت متي

· نامألا ةدايزل نارقألا ةيوه يمتحت - ةيسيئرلا

· عرسأ الاصتا رفوت نكلو ريظنلا ةيوه ةيامح رفوت ال — ةقئاف

يوتحي يتلا ةيوهلا عون رتخأ يلمحلا فرعملا عون ةلدسنملا ةمئاقلا نم 5. ةوطخل

**Local**

Local Identifier Type:

Local Identifier:

ييلات وحنلا ىلع ةحاتملا تارايلخا ديحت متي

· تنرتنإلا ربع لصتي — ةيلمحلا WAN ةكبشل (IP) تنرتنإلا لوكوتورب

· مدختسي زاهج لك فرعت تارتفب ةلصفنم ماقرألا نم ةديرف ةلسلس — IP ناوع ةكبشلا ربع لاصتالا تنرتنإلا لوكوتورب

لخدأف 5، ةوطخل ي ةلدسنملا ةمئاقلا نم IP ناوع ديحت مت اذا (ياريخا). 6. ةوطخل

**Local**

Local Identifier Type:

Local Identifier:

اهنمضتي يتلا ةيوهلا عون رتخأ ديعلبلا فرعملا عون ةلدسنملا ةمئاقلا نم 7. ةوطخل

**Remote**

Remote Identifier Type: Remote WAN IP ▼

Remote Identifier: IP Address

يلااتال وحنلا لىل عحاتمال تارايلال ديحت متي

- تنرتنال ربع لصتي — ةيحلحال WAN ةكبشل (IP) تنرتنال لوكوتورب
- مدختسي زاهج لك فرعت تارتفب ةلصفنم ماقرال نم ةديرف ةلسلس — IP ناوع ةكبشل ربع لاصتال تنرتنال لوكوتورب

لخداف 7، ةوطخال ي ةلدسنمال ةمئاقال نم IP ناوع ديحت مت اذا (ي رايتخا). 8 ةوطخال ديعلال فرعمال لقح ي ديعلال IP ناوع

**Remote**

Remote Identifier Type: Remote WAN IP ▼

Remote Identifier: 192.168.2.100

ريفتل ةيمزراوختخا، ريفشتال ةيمزراوخل ةلدسنمال ةمئاقال نم 9. ةوطخال يضا رتفاك AES-128 رايتخا متي. تالاصتال

**IKE SA Parameters**

Encryption Algorithm: DES ▼

Authentication Algorithm: DES

Pre-Shared Key: 3DES

DH Group: AES-128

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

نېماتللا نم یوتسم یلعأ یل ی نندا نم یلی امك ةحاتملا تارایخلا درس متی

DES — تانا یبل ری فشت رای عم

تانا یبل ری فشت ل یثالثلا رای عم — 3DES رای عم

ت ب 128 رادصا حاتم مدقتملا ری فشتلا رای عم مدختسی — AES-128 زارطلا

ت ب 192 رادصا حاتم مدقتملا ری فشتلا رای عم مدختسی — AES-192 زارطلا

ت ب 256 رادصا حاتم مدقتملا ری فشتلا رای عم مدختسی — AES-256 زارطلا

هنمأو هئادا ةدا یزل 3DES و DES ربع ری فشتلل ةسیسایقلا ةقیرطلا یه AES: ةظحالم زارطلا مادختساب یصوی. ءادال ضافخنا عم نامأل ةدا یز یل AES حاتم ةلاط ی دؤیس نامأل او ةرسلا نیب طسولح ل ضفأ رفوی هنأل AES-128

ةقداصملا ةیمزراوخ رتخأ، ةقداصملا ةیمزراوخ ةلدسنملا ةمئاقلا نم 10 ةوطخلا یضارثفاك SHA-1 رای تخا متی. كتالاصتا

**IKE SA Parameters**

Encryption Algorithm: AES-128

Authentication Algorithm: MD5

Pre-Shared Key: [Empty Field]

DH Group: Group1 (768 bit)

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

يالاتل وحننلا ىلع ةحاتملا تاراىخلا ديحت متي

- تب 128 ةئجت ةميق ىلع ةلاسرلا صخلم ةيمزراوخ يوتحت — MD5
- تب 160 ةئجت ةميق ىلع ةنمآلا ةئجتلا ةيمزراوخ يوتحت — SHA-1
- تب 256 ةئجت ةميق عم ةنمآلا ةئجتلا ةيمزراوخ — SHA2-256

اهطغضت ، تانايبلا نم ةعطق ذخأت . ناترفشم ةئجت اتلاد امه SHA و MD5 : ةطحالم لكشب MD5 رفوي ال . اهجاتنإ ةداع نكمي ال ةديرف ةيرشع ةيسادس تاجرخم ئشننتو لامعآلا ةئيب دادع ي ف طقف همادختسا بجيو ةئجتلا تامداصتلا دض نامأ ي ياساسأ ارايخ SHA1 زارطلا دعوي . مداصتلا ةمواقم ىلإ ةجاج كانه نوكت ال ثيح ةريغصلال لجأ نم . ةريبك ةجردب لقا تاعرسب لصفأ انامأ رفوي هنأل MD5 زارطلا نم لصفأ ، ةيلمع ةيمهأ تاذو ةفورعم تامجه ىلع SHA2-256 رفوتي ال ، جئاتنلا لصفأ قيقتحت نمآلا يوتسم عافترا نإف ، اقباس ركذامكو . نامآلا نم يوتسم لصفأ رفوي فوسو . أطبأ تاعرس ينعوي

49 و 8 نيب اهلوط حوارتي رورم ةملك لخدا ، اقباسم كرتشم حاتفم لقح ي ف . 11 ةوطخلا افح

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

إلى تب تادحو ددع ري شي. DH ةومجم رتخأ، DH ةومجم ةلدس نم ةمئاقلا نم 12. ةوطخلا  
 ةومجم لا سفن في لاصتالا في فرط الك نوكي نا بجي. نامألا يوتسم

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾  
 Group1 (768 bit)  
 Group2 (1024 bit)  
 Group5 (1536 bit)

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

في اخلص نامألا نارثقا اهي في نوكي س يتلا ةدملا لخدأ، SA-Lifetime لحو في 13. ةوطخلا  
 يثا 28800 ريصقتلا. ناوث

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

إننا لاجم فشك ريظن Dead في قودنص قيقدت نكمي لاصحف (يراي تخ). 14 ةوطخ  
 نكمم تب موقت مل اذا 17 ةوطخل اي طخت. طشن ريغ ريظن عم ليصوت زجعي نأ تنأ دي ري  
 "تي مل ريظن لافاشتك".

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

لقح في ةمي ق لخدأف، تي مل ريظن لافشك نكمم تب تمق اذا (يراي تخ). 15 ةوطخل  
 لاصتا نم ققحتلل هجوم لاهي ف رظتن نيس يتي الة ةدم لة مي ق لاهه ددحتس. DPD ريخأت  
 لي مل.

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

في فة ميق لخدأف، حيصال ريغ ريظنلال فشك نيكمتب تمق اذا (يراي تخا). 16 ة وطلال  
يتح الصتم اهلالخ ليمعلال لظيس يتلال ةدملال ةميقلل هذه ددحتس. DPD ةلهم لوق  
ةلهملا يهتنت

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

تاريغتلل ظفلح ظفلح قوف رقنا. 17 ة وطلال

**IKE SA Parameters**

Encryption Algorithm:  ▾

Authentication Algorithm:  ▾

Pre-Shared Key:

DH Group:  ▾

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نء مء 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 ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءء ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل