

ىل ع (IKE) تنرتنإل اجات فم لدابت جهن تاداعإ RV130W و VPN RV130 تاهجوم

فدهل ا

نيتك بيش نيب نم آلاصتا سسؤي لوكوتورب وه (IKE) تنرتنإل اجات فم لدابت
حيتافملا مادختساب اهني مات اغلاو اهني مات مزحل ريفشت متي، IKE مادختساب
نيرط لبق نم دمختسمل ا

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

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

قيبطتل ل ةلباقلا ةزهجال ا

- RV130
- RV130W

ةيئارج ا تاوطخ

عقوم نم VPN > IPsec VPN رايتخال هجوملا نيوكتل ةدعاسملا ةادل ا مدختسأ. 1. ةوطخال
دادع ا ةحفص رهظت. راسيلا لىل ةدوجوملا ةمئاقلا نم مدقتملا VPN دادع ا > 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 رهطت . 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 متهف يذلا عضولا رتخأ ، Exchange عضو ءلدسنملا ءمئاقلا نم 4. ءوطخلا
نمأ لاصتا عاشنال حيتافملا لدابت

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Main
Aggressive

ييلات وحنلا ىلع ءحاتملا تارايلخلا ديحت متي

· نامألا ءدايزل نارقالا ءيوه يمتحت - ءيسيلزلا

· عرسأ الاصلتا رفوت نكلو ريلظنلا ءيوه ءيامح رفوت ال — ءقئاف

يوتحي يتلا ءيوهلا عون رتخأ يلمحلا فرعملا عون ءلدسنملا ءمئاقلا نم 5. ءوطخل

Local

Local Identifier Type:

Local Identifier:

ييلات وحنلا ىلع ءحاتملا تارايلخلا ديحت متي

· تنرتنإلا ربع لصتي — ءيلمحلا WAN ءكبشل (IP) تنرتنإلا لوكوتورب

· مءختسي زاك لك فرعت تارتفب ءلصفنم ماقرال نم ءيرف ءلسلس — IP ناوع ءكبشلا ربع لاصلتلا تنرتنإلا لوكوتورب

لخدأف 5، ءوطخل ي ءلدسنملا ءمئاقلا نم IP ناوع ديحت مت اذا (يرايخا). 6. ءوطخل

Local

Local Identifier Type:

Local Identifier:

اهنمضتي يتلا ءيوهلا عون رتخأ ديعلبلا فرعملا عون ءلدسنملا ءمئاقلا نم 7. ءوطخل

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
ديعبال فرعمال ل قح ي ف ديعبال IP ناوع

Remote

Remote Identifier Type: Remote WAN IP ▼

Remote Identifier: 192.168.2.100

ري فشتل ةيمزراوخ رتخأ، ريفشتل 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 ةسی ای قلا 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 یضارتفاك 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 وحنللا ىلع ةحاتملا تارايلخلا 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 : ةطخالم 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 زارطالا دعوي . مداصتلا ةمواقم ىلا ةجاج كانه نوكت ال ثيح ةريغصلال لجأ نم . ةريبك ةجردب لقا تاعرسب لصفأ انامأ رفوي هنأل MD5 زارطالا 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 ةوطخالافرح

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 ريشي. DH ةومجم رتخأ، DH ةومجم ةلدسنملا ةمئاقلا نم 12. ةوطخلا
ةومجملا سفن في لاصتالا يفرطالك 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 نارتقا اهي ف نوكيس يتلا ةدملا لخدأ، SA-Lifetime لحو في 13. ةوطخلا
يناث 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 لاهذه ددحتس. DPD ريخأت
 لي مل.

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

في فة ميق لخدأف، حيصال ريغ ريظنلال فشك نيكم تب 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:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

تاريغتلل ظفلح قوف رقنا. 17 ة وطلال

IKE SA Parameters	
Encryption Algorithm:	<input type="text" value="AES-128"/>
Authentication Algorithm:	<input type="text" value="SHA-1"/>
Pre-Shared Key:	<input type="text"/>
DH Group:	<input type="text" value="Group1 (768 bit)"/>
SA-Lifetime:	<input type="text" value="28800"/> Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>	

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد ةوچرلاب يصوت وتامچرتل هذه ةقदन ةتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزىلچنلإل دن تسمل