

تنرتنإل لوكوتورب نامأ فيرعت فلم نيوكت RV34x ةلسلسلا نم هجوم ىلع (IPSec)

فدهلأ

بجي .نیهجوم لثم ،نیراظن نیب ةنمأ اقافنأ (IPSec) تنرتنإل لوكوتورب نامأ رفوي ةفاضإلاب ،ةنمألأ قافنألأ هذه لالخنم اهلأسرا بجيو ةساسح دعت يتلا مزحلأ ديحت صئاصخ ديحت لالخنم ةساسحلأ مزحلأ هذه ةياملأ اهمادختسإ بجي يتلا تاملعملأ ىلإ دادعإب موقی هنإف ،هذهك ةساسح ةمزح IPsec ریزن یری امदनع ،كلذ دعب .قافنألأ هذه ديعلأ ریزنلأ ىلإ قفنلأ اذہ ربع ةمزحلأ لاسراو بسانملا نمألأ قفنلأ

ىلع هقپطت نكمي ايوق انامأ رفوي هنإف ،هجوم وأ ةياملأ رادج في IPsec ذي فنت دنع ةعومجم وأ ةكرشلأ لخد رورملأ ةكرح لمحتت ال .قاطنلأ ربعت يتلا رورملأ ةكرح عيمج ةدئزلأ نامألأب ةقلعتملا ةجلعملأ تاقفن لمعلأ

نم هجوم ىلع IPSec فيرعت فلم نيوكت ةيفيكي حيصوت وه دننسملا اذہ نم فدهلأ RV34x ةلسلسلا

قپطتلل ةلباقلا ةزهجالأ

- RV34x Series

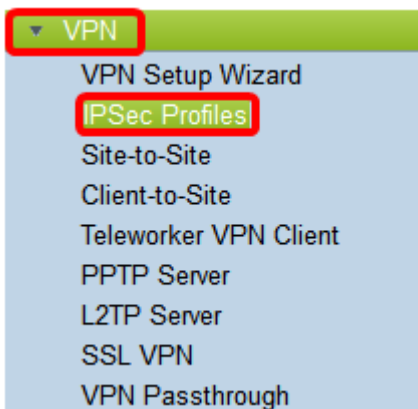
جماربلأ رادصلأ

- 1.0.1.16

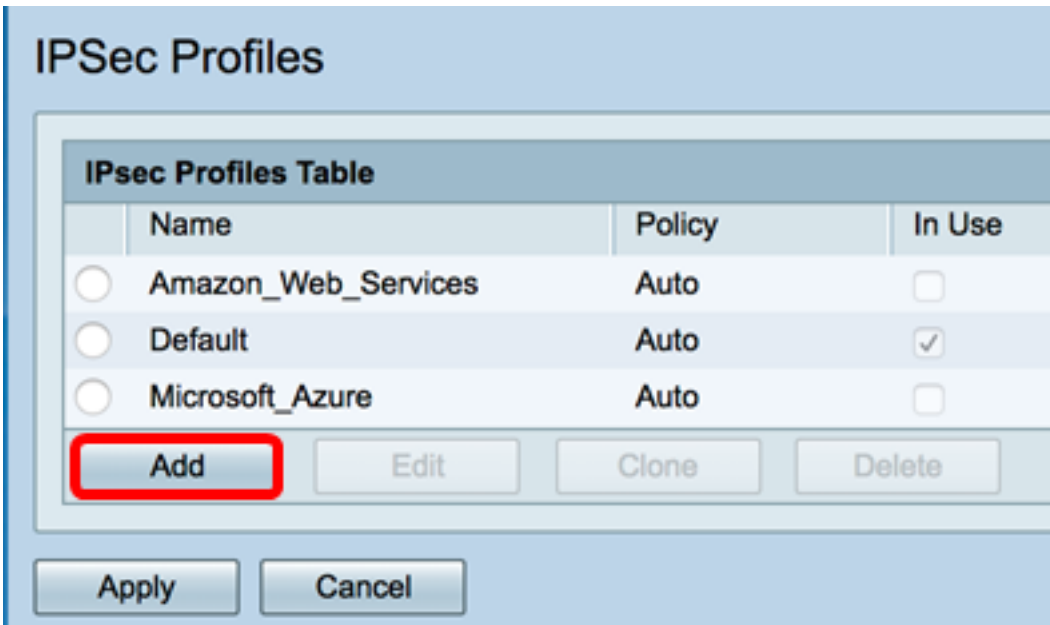
IPSec فيرعت فلم نيوكت

IPSec فيرعت فلم عاشنإ

VPN رتخاو هجوملأ في بيولأ ىلإ ةدننسملا ةدعاسملا ةادألأ ىلإ لوخدلا لفس 1. ةوطخلأ > IPSec تافيصوت

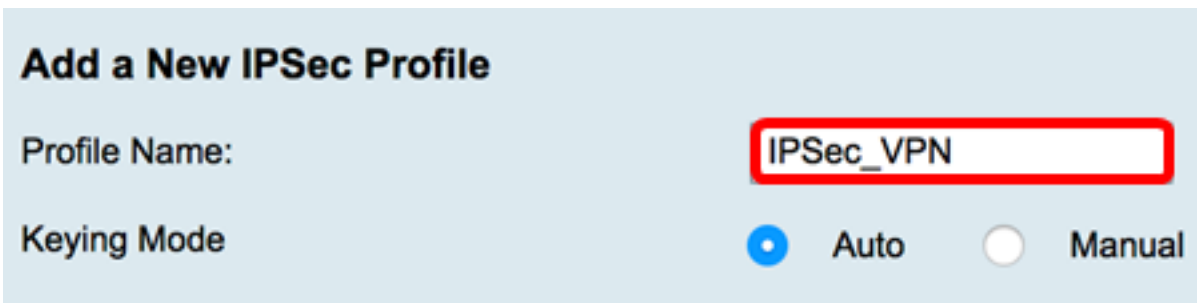


ءاشنإل ةفاضلأ ىلع رقنا .ةدوجوملأ تافيصوتلأ IPsec تافيصوت لودج رهظي 2. ةوطخلأ ديذج فيصوت



مسا يوتحي نأ بجي. فيصوت ل مسا ل قح ي فيصوت ل مسا عاشن اب مق 3. ةوطخل
 ةصاخلا فورخلل () ةيلفس ةمالع و طقف ةيمقر ةيدجبا فرحأ يلع فيرعتلا فلم

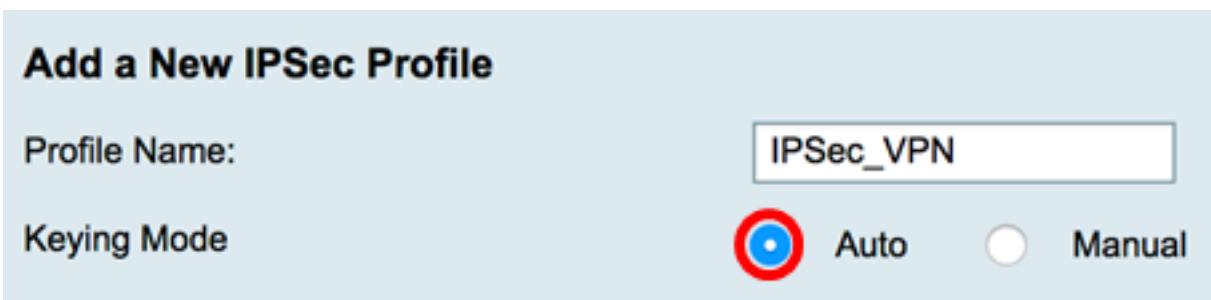
IPsec فيرعت فلم مساك IPsec_VPN مادختسا متي، لاثملا اذه ي ف: ةظحالم



اهمدختسسي يتلا حيتافملا لدابت ةقيرط ديدحتل رايخا رز يلع رقنا 4. ةوطخل
 يه تاراخلا. ةقداصملا ل فيصوتلا

- Internet Key Exchange (IKE) ةسايس رايخلا اذه مدختسي. ايئاقلت جهنلا تاملعم نييعت متي — ايئاقلت
 ةلاحي ف. حيتافملا لدابت تايلمعل اهريفتوت و تانايبلا ةمالسل (IKE) ايئاقلتلا جهنلا تاملعم ةقطنم نمض نيوكتلا تاداعل نيكمت متي، رايخلا اذه رايخا
 ةيئاقلتلا تاداعل نيوكتلا [ينه](#) رقنا.
- اهتامالس و تانايبلا ريفشتل ايودي حيتافملا نيوكتب كل رايخلا اذه حمسي — ايودي
 تاداعل نيكمت متي، رايخلا اذه رايخا ةلاحي ف. (VPN) ةيرهاظلا ةصاخلا ةكبشلا قف
 ةيوديلا تاداعل نيوكتلا [ينه](#) رقنا. ايوديلا جهنلا تاملعم ةقطنم نمض نيوكتلا

"ايئاقلت" رايخا مت، لاثملا ليلبس يلع: ةظحالم



[ةيئاقلتلا تاداعل نيوكت](#)

ةبسانم ال DH (Diffie-Hellman) ةومجم رتخأ، لوالا ةلحرم ال تاراخي ةقطنم ي ف 1. ةوطخل DH. ةومجم ةلدسنم ال ةمئاق ال نم 1 ةلحرم ال ي ف حاتم ال عم اهم ادختس ا متيس ي ال لدابتل لاصل ال ي ف هم ادختس ا متي ر فشم حيتافم لدابت لوكوتورب وه Diffie-Hellman. تب تادحو ةطساوب ةيمزراوخل ةوق ديدحت متي. اق بس م ةكرتشم ال حيتافم ال تاعومجم يه تاراخي ال:

- 1. ةومجم ال نم انام رثك اهنكل، اطبا حاتم ال بسحي — تب 1024 - 2 ةومجم ال.
- انام رثك ال اهنكل، ئطبا حاتم ال بسحت — تب 1536 - 5 ةومجم ال.

2-1024 ةومجم ال تب راي تخ ا متي، لاثم ال اذه ي ف: **عظالم**



ةبسانم ال ريفش ال ةقيرط رتخأ، ريفش لل ةلدسنم ال ةمئاق ال نم 2. ةوطخل ةرادا لوكوتوربو تنرتن ال انام نارثقاوا ه ريفش ت ك فو (ESP) نام ال ةلومح ريفش لل حيتافم ال (ISAKMP). يه تاراخي ال:

- تانا ي بل ريفش لل يثالثل راي عم ال — 3DES راي عم.
- تب 128 رادصا حاتم ال ريفش ال راي عم مدختسي — AES-128 زارطال.
- تب-192 حاتم ال ريفش ال راي عم مدختسي — AES-192.
- تب 256 رادصا حاتم ال ريفش ال راي عم مدختسي — AES-256 زارطال.

هنم أو هئادا ةدايزل 3DES و DES ربع ريفش لل ةيساي ق ال ةقيرط ال يه AES: **عظالم**، لاثم ال ل ي بس يلع. ضفخنم ةادا مادختساب نام ال ةدايز ال AES حاتم ال ةلاط ا ي دؤيس AES-256 راي تخ ا متي.



ةيفي ك ددحي ةقداصم بولسا رتخأ، ةقداصم لل ةلدسنم ال ةمئاق ال نم 3. ةوطخل يه تاراخي ال: ESP و ISAKMP ةقداصم

- تب 128 ةئزت ةميق يلع يوتحت ةلاسرل صخلم ةيمزراوخ — MD5.
- تب-160 ةئزت ةميق يلع ةنم ال ةئزت ال ةيمزراوخ يوتحت — SHA-1.
- تب-256 ةئزت ةميق عم ةنم ال ةئزت ال ةيمزراوخ — SHA2-256.

اهطغضت، تانا ي بل نم ةعطق ذخأت. ناترفشم ةئزت اتلاد امه SHA و MD5: **عظالم**، لاثم ال اذه ي ف. اهجاتن ا ةداع ا نكمي ال ةديرف ةيرشع ةيسادس تاجرخم ئشننو و SHA2-256 راي تخ ا متي.

DH Group: Group2 - 1024 bit

Encryption: MD5

Authentication: SHA2-256

ة ن م ز ل ا ة د م ل ا ي ه ه ذ ه . 86400 و 120 ن ب ح و ا ر ت ت ة م ي ق ل خ د ا ، SA ر م ع ل ق ح ي ف . 4 ة و ط خ ل ا ة ل ح ر م ل ا ه ذ ه ي ف ا ط ش ن (IKE) ت ن ر ت ن ا ل ا ح ي ت ا ف م ل د ا ب ت ن ا م ا ن ا ر ت ق ا ا ه ي ف ل ط ي س ي ت ل ا 28800 ي ه ة ي ض ا ر ت ف ا ل ا ة م ي ق ل ا .

28801 م ا د خ ت س ا م ت ي ، ل ا ث م ل ا ا ذ ه ي ف : ة ظ ح ا ل م

Authentication: SHA2-256

SA Lifetime: 28801

Perfect Forward Secrecy: Enable

د ي د ج ح ا ت ف م ء ا ش ن ا ل enable perfect forward secret ر ا ي ت خ ا ل ا ة ن ا خ د د ح (ي ر ا ي ت خ ا ل ا) . 5 ة و ط خ ل ا ة ق د ا ص م ل ا و IPsec ر و ر م ة ك ر ح ر ي ف ش ت ل ا .

Authentication: SHA2-256

SA Lifetime: 28801

Perfect Forward Secrecy: Enable

ة ل ح ر م ل ا ت ا ر ا ي خ ة ق ط ن م ي ف ل و ك و ت و ر ب ل ا د ي د ح ت ة ل د س ن م ل ا ة م ئ ا ق ل ا ن م . 6 ة و ط خ ل ا ت ا ر ا ي خ ل ا . ض و ا ف ت ل ا ن م ة ي ن ا ث ل ا ة ل ح ر م ل ا ي ل ع ه ق ي ب ط ت ل ل و ك و ت و ر ب ع و ن ر ت خ ا ، ة ي ن ا ث ل ا ه ي :

- ESP — ل و ح ر ي ف ش ت ة ق ي ر ط ر ا ي ت خ ا ل [7 ة و ط خ ل ا](#) ي ل ا ل ق ت ن ا ف ، ر ا ي خ ل ا ا ذ ه ر ا ي ت خ ا ل م ت ا ذ ا — ESP ة ي ص و ص خ ت ا م د خ ر ف و ي ن ا م ا ل و ك و ت و ر ب . ا ه ر ي ف ش ت ك ف و ESP م ز ح ر ي ف ش ت ة ي ف ي ك ESP م و ق ي . ل ي غ ش ت ل ا ة د ا ع ا ل ة د ا ص م ل ا ت ا م د خ ل ا و ة ي ر ا ي ت خ ا ل ا ت ا ن ا ي ب ل ا ة ق د ا ص م و ت ا ن ا ي ب ل ا ا ه ت ي ا م ح د ا ر م ل ا ت ا ن ا ي ب ل ا ن ي م ض ت ب .
- AH — ت ا م د خ ل ا و ت ا ن ا ي ب ل ا ة ق د ا ص م ر ف و ي ن ا م ا ل و ك و ت و ر ب و ه (AH) ة ق د ا ص م ل ا س ا ر — م ت ي س ي ت ل ا ت ا ن ا ي ب ل ا ي ف AH ن ي م ض ت م ت . ل ي غ ش ت ل ا ة د ا ع ا ل ة د ا ص م ل ا ة ي ر ا ي ت خ ا ل ا ر ا ي خ ل ا ا ذ ه ر ا ي ت خ ا ل م ت ا ذ ا [8 ة و ط خ ل ا](#) ي ط خ ت . (ل م ا ك IP ت ا ن ا ي ب ط ط خ م) ا ه ت ي ا م ح

Phase II Options

Protocol Selection:

✓ ESP

AH

Encryption:

بِسَانَمَلَا رِيْفَشْتَلَا قِيْرَط رْتَخْأَفْ، 6 ةِوِطْخَلَا يِ فِ ESP رَايْتِخْإِ مِتْ اِذَا [7. ةِوِطْخَلَا](#) تَارَايْخَلَا. رِيْفَشْتَلَلْ ةَلْدَسْنَمَلَا ةَمِئَاقَلَا نَمْ اَمْرِيْفَشْتِ كَفْ وِ ISAKMP وِ ESP رِيْفَشْتَلْ هِي:

- تَانَايِبَلَا رِيْفَشْتَلْ يِ ثَالِثَلَا رَايْعَمَلَا — 3DES رَايْعَمْ
- تَبْ 128 رَاِصْلَا حَاتِفَمْ مَدَقْتَمَلَا رِيْفَشْتَلَا رَايْعَمْ مَدِخْتَسِيْ — AES-128 زَارَطَلَا
- تَبْ-192 حَاتِفَمْ مَدَقْتَمَلَا رِيْفَشْتَلَا رَايْعَمْ مَدِخْتَسِيْ — AES-192
- تَبْ 256 رَاِصْلَا حَاتِفَمْ مَدَقْتَمَلَا رِيْفَشْتَلَا رَايْعَمْ مَدِخْتَسِيْ — AES-256 زَارَطَلَا

مِظْحَالَمْ AES-256 رَايْتِخْإِ مِتْ يِ، لَاتْمَلَا اِذَا يِ فِ: ةِظْحَالَمْ

Phase II Options

Protocol Selection:

3DES

AES-128

AES-192

Encryption:

✓ AES-256

ةِيْفِيْكَ دِدْجِيْ ةِوِطْخَلَا بَوْلَسْأ رْتَخْأَفْ، ةِوِطْخَلَا ةَلْدَسْنَمَلَا ةَمِئَاقَلَا نَمْ [8. ةِوِطْخَلَا](#) هِي تَارَايْخَلَا. ISAKMP وِ ESP ةِوِطْخَلَا:

- تَبْ 128 ةِئِزْجَتْ ةَمِيْقِيْ لَعِ يِوْتِخْتِ ةَلَسْرَلَا صِخْلَمْ ةِيْمَزْرَاوْخْ — MD5
- تَبْ-160 ةِئِزْجَتْ ةَمِيْقِيْ لَعِ ةَنْمَالَا ةِئِزْجَتَلَا ةِيْمَزْرَاوْخْ يِوْتِخْتِ — SHA-1
- تَبْ-256 ةِئِزْجَتْ ةَمِيْقِيْ عَمْ ةَنْمَالَا ةِئِزْجَتَلَا ةِيْمَزْرَاوْخْ — SHA2-256

مِظْحَالَمْ SHA2-256 مَادِخْتَسِإِ مِتْ يِ، لَاتْمَلَا اِذَا يِ فِ: ةِظْحَالَمْ

Protocol Selection:

ESP

Encryption:

MD5

SHA1

Authentication:

✓ SHA2-256

يِتَلَا ةَدْمَلَا لُوْطْ وَهْ اِذَا. 28800 وِ 120 نِيْبْ حَوَارْتَتْ ةَمِيْقِيْ لَخْدَا، SA رَمْعْ لَقْحِ يِ فِ [9. ةِوِطْخَلَا](#) 3600. هِي ةِيْمِضَارْتَفَالَا ةَمِيْقِيْ لَقْحِ رَمْلَا هِذَا يِ فِ اِطْشَنْ SA IKE اِهِيْ لَطِيْسْ

مِظْحَالَمْ 28799 مَادِخْتَسِإِ مِتْ يِ، لَاتْمَلَا اِذَا يِ فِ: ةِظْحَالَمْ

SA Lifetime:

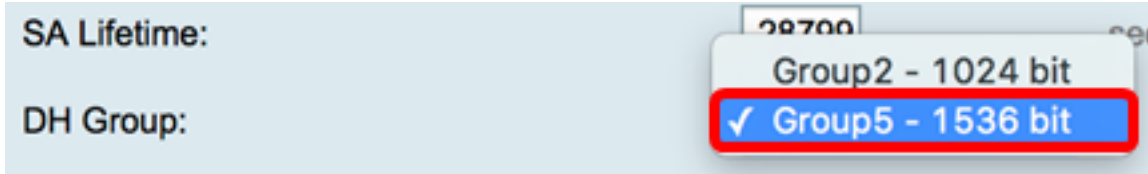
28799


Diffie-Hellman (DH) ةِوِطْخَلَا، DH ةِوِطْخَلَا ةَلْدَسْنَمَلَا ةَمِئَاقَلَا نَمْ [10. ةِوِطْخَلَا](#)

يہ تارايلخ ل 2. ةلحرمل ا يف حاتفرملا عم اهمادختسا متيس يتلا ةبسانملا

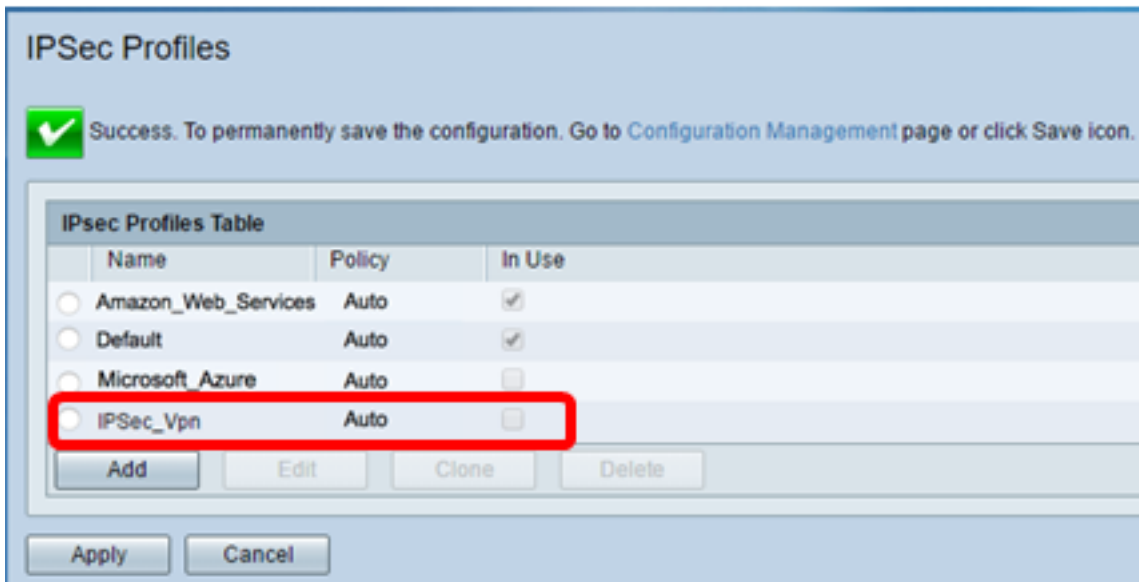
- ةعومجرملا نم انام ا رثك ا هنكل ، ا طب ا حاتفرملا بسحي — تب 1024 - 2 ةعومجرملا
- انام ا رثك ا ل هنكل ، ا طب ا حاتفرملا بسحي — تب 1536 - 5 ةعومجرملا

تب 1536 - Group5 رايتخ متي ، لاثملا اذہ يف : ةظحالم



ةقطقط 11. ةوطخل 

IPSec فيرعت فلم رهظي ن ا بچي و IPSec فيرعت تافل م لودج ي ل ا كتداع ا متتس : ةظحالم
ن ا ل ا ا ي د ح ه و ا ش ن ا مت ي ذ ل ا



ظفح/خسن ةحفص ي ل ا لقتنا ، مئاد لكشب نيوكتلا ظفحل (يرايتخ ا) . 12. ةوطخل

ةحفصل نم يولعل اعزل ا يف زمرلا  قوف رقنا و ا نيوكتلا

هجوم يلع حاجنب ي ئاقل ل IPSec فيرعت فلم نيوكت نم ن ا ل ا تي هتنا دق نوكت ن ا بچي
RV34x ةلسلسلا نم

ةيوديلا تاداعلا نيوكت

ال 100 نم حوارتي رشع يسادس مقرر ل خ د ا ، SPI-Incoming ل قح يف 1. ةوطخل
VPN ل اصتا يلع ة دراوال رورملا ة ك رحل (SPI) نام ا ل تام ل عم سرهف ةم ال عل
ةسلج ر خ ا نم رورم ة ك رحل نم ةسلج دحاو نم رورم ة ك رحل زي مي ن ا ة قاطب تلمعتسا

ةظحالم : 0xABCD م ادختسا متي ، لاثملا اذہل

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

FFFFF إلى 100 نم حوارتي رشع ايسادس امقرر لخدأ، *SPI-Outgoing* ل قح ي ف 2. ةوطخلال VPN لاصتا إلى عةرداصلال رورملا ةكرحل SPI ةمالع

مادختسا متي، لاثملا اذهل: **مظحالم** 0x1234.

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

و AES-128 و 3DES ه تاراخلا. ريفشتلل ةلدسنملا ةمئاقلا نم اراخي رتخأ. [3. ةوطخلال](#) AES-192 و AES-256.

AES-256 رايتخا متي، لاثملا اذه ي ف: **مظحالم**

SPI Incoming:

SPI Outgoing:

Encryption:

3DES

AES-128

AES-192

✓ AES-256

يلع حاتفملا لوط دمتعي. درااولا جهنلل حاتفم "حاتفملا" ل قح ي ف لخدأ. 4. ةوطخلال [3. ةوطخلال](#) ي ف ةراتخملا ةيمزراوخلال

- فرح 48 نم نوكم حاتفم 3DES رايعم مدختسي
- افرح 32 حاتفم AES-128 مدختسي
- فرح 48 نم نوكم حاتفم AES-192 مدختسي
- فرح 64 حاتفم AES-256 مدختسي

مادختسا متي، لاثملا اذه ي ف: **مظحالم** 123456789123456789123.

Key-In: 123456789123456789123

Key-Out: 1a1a1a1a1a1a1a1a1212121

يلع حاتفملا لوط دمتعي. رداصلال جهنلل حاتفم، لاجم چراخ حاتفملا ي ف تلخد. 5. ةوطخلال 3. ةوطخلال ي ف ةراتخملا ةيمزراوخلال

مادختسا متي، لاثملا اذه ي ف: **مظحالم** 1a1a1a1a1a1a1a1a121212...

| | |
|----------|-------------------------|
| Key-In: | 123456789123456789123 |
| Key-Out: | 1a1a1a1a1a1a1a1a1212121 |

ةيودي ل لم اكلت لةي م زراوخل ةلدس نمل ةم ئاقل ل نم ارايخ رتخأ [6. ةوطخل](#).

- MD5 لقا رذقب MD5 زارطل زيم تي . تانايب ل ةمالسل تب 128 ةئزت ةمي ق مدختسي — SHA-1 و SHA2-256 نيزارطل نم عرسأ هنكلو نامأل نم
- SHA-1 أطبأ زارطل دعي و . تانايب ل ةمالسل تب 160 ةئزت ةمي ق مدختسي — SHA-1 نم انامأ لقا هنكلو ةعرس رثكأ SHA-1 زارطل نأ امك ، MD5 زارطل نم انامأ رثكأ هنكلو SHA2-256 زارطل
- SHA2-256 هنكلو أطبأ SHA2-256 . تانايب ل ةمالسل تب 256 ةئزت ةمي ق مدختسي — SHA-1 و MD5 نم نم أ

MD5 رايتخا متي ، لاثم ل اذه في : **ةظحال**

| | |
|-----------------|--------------------------------------|
| Authentication: | <input checked="" type="radio"/> MD5 |
| Key-In | <input type="radio"/> SHA1 |
| Key-Out | <input type="radio"/> SHA2-256 |

ل ع حاتفم ل لوط دمتعي . دراو ل جهنل ل حاتفم ، ل اجم ل خاد حاتفم ل في تلخد [7. ةوطخل](#) [6. ةوطخل](#) في ةراتخم ل ةي م زراوخل

- افرح 32 نم نوكم حاتفم MD5 مدختسي
- افرح 40 نم نوكم حاتفم SHA-1 مدختسي
- افرح 64 حاتفم SHA2-256 مدختسي

123456789123456789123. مادختسا متي ، لاثم ل اذه في : **ةظحال**

| | |
|----------|-------------------------|
| Key-In: | 123456789123456789123 |
| Key-Out: | 1a1a1a1a1a1a1a1a1212121 |

ل ع حاتفم ل لوط دمتعي . رداصل ل جهنل ل حاتفم ، ل اجم ج راخ حاتفم ل في تلخد [8. ةوطخل](#) [6. ةوطخل](#) في ةراتخم ل ةي م زراوخل

1a1a1a1a1a1a1a1a121212..... لاثم ل اذه في : **ةظحال**


| | |
|----------|-------------------------|
| Key-In: | 123456789123456789123 |
| Key-Out: | 1a1a1a1a1a1a1a1a1212121 |

Apply

ةق ط ق 9. ةوطخل

IPSec فيرعت فلم رهظي نأ بجي و IPSec فيرعت تافل م لودج يلى كتداعإ متتس :ةظحالم نألا اتيح هؤاشنإ مت يذلا

IPSec Profiles

 Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

| IPsec Profiles Table | | |
|---|--------|-------------------------------------|
| Name | Policy | In Use |
| <input type="radio"/> Amazon_Web_Services | Auto | <input checked="" type="checkbox"/> |
| <input type="radio"/> Default | Auto | <input checked="" type="checkbox"/> |
| <input type="radio"/> Microsoft_Azure | Auto | <input type="checkbox"/> |
| <input type="radio"/> IPSec_Vpn | Manual | <input type="checkbox"/> |

ظفح/خسن ةحفص يلى لقتنا ،مئاد لكشب نيوكتلا ظفحل (يرايتخإ). 10 ةوطخلا

ةحفصلا نم يولعلا ءزجالا يف زمرلا  قوف رقنا وأ نيوكتلا

نم هجوم يلى ع حاجنب ايودي IPSec فيرعت فلم نيوكت نم نألا تيهتنا دق نوكت نأ بجي
RV34x ةلسلسلا

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. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل