

# VPN RV315W هجوم ىلع SNMP نيوكت

## فدهلا

ةكبشلا ةرادال TCP/IP لوكوتورب وه (SNMP) طيسبلا تاكبشلا ةرادال لوكوتورب نكمي امك. عاخالال تالدعمو ةكبشلا عاذا ةبقارم ني لوؤسملل SNMP حيتي و ةثال نـ SNMP لوكوتورب لمع راطا نوكتي. ةكبشلا رفوت ني عت SNMP لوكوتورب لثمتت. ةرادال تامولعم ةدعاقو SNMP لوكوتورب ليك وو SNMP لوكوتورب ري دم؛ رصانع SNMP م دختست يتلا ةكبشلا يف فيضم ةطشنأ يف مكحتلا يف SNMP ري دم ةفيظو ةرادال تانايبلا ةنايص يف دعاسي وهو زاوجلل جم انرب يف SNMP ليكو دجوي. اهتبقارمو تامولعمل ةيضارتفا ني زخت ةقطنم (MIB) ةرادال تامولعم ةدعاق دعت، اريخأو. ماطنلا اهتراداو ام ةكبش يف ةزهجالا ةبقارم ل ةثال ل ةزهجالا هذه عمجتو. ةكبشلا ةرادا

VPN RV315W هجوم ىلع SNMP نيوكت ةيفيكي حرش يف ةلاقملا هذه دعاست

## قيبطتلا لباقلا زاوجل

RV315W زارطلا.

## جماربال رادصا

1.01.03

## SNMP نيوكت

طقف لمعي و ةني عم فئاظو ىل رقت في يذلا، SNMP، نم ي لصلأا رادصا ل وه SNMP v1 طقف لمعي و ةني عم فئاظو ىل رقت في يذلا، SNMP، نم ي لصلأا رادصا ل وه SNMP v1&v2 راي تخا بجي. v1 ل انسجم اراركت SNMP v2 ربتعي و، TCP/IP تاكبش ىلع ريياعم ثدحأ SNMP v3 دعوي. SNMPv1 و SNMPv2 م دختست يتلا تاكبش ل طقف اذو جلاعي، صوصخلا هجو ىلعو. v1 و v2 ل كاشم نم دي دعال جلاعي و SNMP لوكوتورب حمسي امك. ينال ل لوال ني رادصا ل نم ةني نمأا فعضلا طاقن نم دي دعال جم انرب ل عئاش دحاو SNMP راي عم ىل لاقن نالاب ني لوؤسم لل SNMP v3.

> ماطنلا ةرادا رتخاو بيولا نيوكتل ةدعاسملا ةادالا ىل لوخدلا لي جستب مق. 1 ةوطخلا > SNMP: ةحفص حتف متي.

SNMP	
SNMP:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SNMP Version:	<input checked="" type="radio"/> SNMP v1&v2 <input type="radio"/> SNMP v3
System Contact:	<input type="text"/> (1-200 characters)
System Name:	<input type="text" value="RV315W"/> *(1-30 characters)
System Location:	<input type="text" value="Office"/> *(1-200 characters)
Security Username:	<input type="text"/> (1-32 characters)
Authentication Password:	<input type="text"/> (8-64 characters)
Authentication Method:	<input checked="" type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA
Encrypted Password:	<input type="text"/> (8-64 characters)
Encryption Method:	<input checked="" type="radio"/> None <input type="radio"/> CBC-DES
SNMP Read-Only Community:	<input type="text" value="public"/> *(1-32 characters)
SNMP Read-Write Community:	<input type="text" value="private"/> *(1-32 characters)
Trap Community:	<input type="text" value="public"/> *(1-32 characters)
SNMP Trusted Host:	<input type="text" value="0.0.0.0"/>
Trap Receiver Host:	<input type="text" value="192.168.1.100"/> *
* indicates a mandatory option.	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

SNMP نېكمتل رايخال نېكمت رزىل ع رونا 2. ةوطخلال

ببولطامل SNMP رادصل ويدر رز قوف رونا 3. ةوطخلال

SNMP لوكوتوربب لصلال راركتال SNMP نم لوأال رادصلال دعى — SNMP v1&v2 .  
يذال ثدخال رادصلال SNMP نم ينالال رادصلال ربتعو، ةنعم فئاظو لىل رقتفو  
رادصلال لغشت يتال تاكبش لل طقف رايخال اذ رايخال بچي نكلو، فئاظوال نسحى  
SNMP لوكوتوربب نم ينالال رادصلال و SNMP لوكوتوربب نم لوأال

بجى .دحاو رايعم مادختساب نيلوؤس ملل حمسى ،رادصلال ثدخال 3 SNMP دعى — SNMP v3 .  
V1 و V2 لخاد نامال بويع نم ديدعلال ححصتب موقى هنال رايخال اذ رايخال

## SNMP ل SNMP v1&v2 نيوكت

The screenshot shows the SNMP configuration page with the following fields and values:

- SNMP:  Enable  Disable
- SNMP Version:  SNMP v1&v2  SNMP v3
- System Contact: (1-200 characters)
- System Name: RV315W \*(1-30 characters)
- System Location: Office \*(1-200 characters)
- Security Username: (1-32 characters)
- Authentication Password: (8-64 characters)
- Authentication Method:  HMAC-MD5  HMAC-SHA
- Encrypted Password: (8-64 characters)
- Encryption Method:  None  CBC-DES
- SNMP Read-Only Community: public \*(1-32 characters)
- SNMP Read-Write Community: private \*(1-32 characters)
- Trap Community: public \*(1-32 characters)
- SNMP Trusted Host: 0.0.0.0
- Trap Receiver Host: 192.168.1.100 \*

\* indicates a mandatory option.

وه اذ .ماظنل لاصتا ةه ل قح يف لاصتال ةه تامولعم لخدأ (يرايخال). 4. ةوطخلال  
ةكبشلا يف ةدعاسم لىل لوصحلل هب لاصتال بجى يذال صخشلا

SNMP دادعال صصخملا مسالا وه اذ .ماظنل مسا لقحلا يف امسا لخدأ 5. ةوطخلال

ماظنل اعقوم وه اذ .ماظنل اعقوم لقح يف اعقوم لخدأ 6. ةوطخلال

للمل عملم يه هذ .طقف SNMP ةعارق عمتم لقح يف اعتم لخدأ 7. ةوطخلال  
SNMP دادعال لىل طقف ةعارقلل لوصولل

للمل عملم يه هذ . SNMP ةباتك-ةعارق عمتم لقح يف اعتم لخدأ 8. ةوطخلال  
SNMP دادعال ةباتكلاو ةعارقلل لوصولل

لىل ةردقلل هيدل يذال عمتم لخدأ وه اذ .ةمئالملا عمتم لقح يف اعتم لخدأ 9. ةوطخلال  
حمست .لوؤسمل لىل اهلاسرلا متي ةهجوم تامالعال يه تامئالملا . SNMP تارابخال مادختساب  
مهالعال مهيمدختسمل حامسلا قيرط نع زاهج لك ةرادب لوؤسمل ل تامئالملا  
ةمئالم مادختساب

فيملم IP ناوع وه اذ .هب قوثومال SNMP فيملم لقح يف افيملم لخدأ 10. ةوطخلال  
SNMP دادعال ةقتال

صخال IP ناوع وه اذ .ةمئالملا لبقتسم فيملم لقح يف فيملم لخدأ 11. ةوطخلال  
تامئالملا يقئلل لوؤسمل لاب

تادادعال قيبطتل طفح لىل رونا 12. ةوطخلال

## SNMP v3 ل SNMP ني وكت

وه اذه .ماظنلا لاصتا هج لقح ي ف لاصتالا هج تامولعم لخدأ (يراي تخإ). 4. ةوطخللا ةكبشللا ي ف ةدعاسم ىلع لوصحلل هب لاصتالا بجي يذلا صخشلا

SNMP. دادعإل صصخملا مسالا وه اذه .ماظنلا مسا لقحلا ي ف امسا لخدأ. 5. ةوطخللا

.ماظنلا عقوم وه اذه .ماظنلا عقوم لقح ي ف اعقوم لخدأ. 6. ةوطخللا

SNMP

SNMP:  Enable  Disable

SNMP Version:  SNMP v1&v2  SNMP v3

System Contact: (1-200 characters)

System Name: RV315W \*(1-30 characters)

System Location: Office \*(1-200 characters)

Security Username: Profile1 (1-32 characters)

Authentication Password: (8-64 characters)

Authentication Method:  HMAC-MD5  HMAC-SHA

Encrypted Password: (8-64 characters)

Encryption Method:  None  CBC-DES

SNMP Read-Only Community: public \*(1-32 characters)

SNMP Read-Write Community: private \*(1-32 characters)

Trap Community: public \*(1-32 characters)

SNMP Trusted Host: 0.0.0.0

Trap Receiver Host: 192.168.1.100 \*

\* indicates a mandatory option.

Save Cancel

يذلا مدختسملا مسا وه اذه .لاجم username نامأل ي ف username (يراي تخإ). 7. ةوطخللا مدي SNMP. دادعإل لوصوللا ىلع لوصحلل همادختسا متي

متي يتلا رورملا ةملك يه هذه .لاجم ةملك ةقداصملا ي ف ةملك (يراي تخإ). 8. ةوطخللا مدي SNMP. دادعإل لوصوللا ىلع لوصحلل اهمادختسا

زمر .ةقداصملا ةقيرط لقح ي ف HMAC-SHA و HMAC-MD5 وي دار رز رقنا. 9. ةوطخللا ةقداصم زمر ني ب عمج ي رفشم زمر وه (HMAC) ةئزجتلا ىل ةدنتسملا لئاسرلا ةقداصم HMAC موقيس .ةلاسرلا ني مات وه HMAC نم ي اساسا لاضرغلا .يرس ريفشت حاتفم و اهجاتنإ مت يتلا ةيرسلا حيتافملا ىل ةدنتسملا تانايابل ةقداصم ب

قارتخأ نكمي و نامأل بوي ع نم ديدعلا ىلع هذه ةئزجتلا ةيمزراوخ يوتحت — HMAC MD5 .ريفشت ةئزجت فئاطو مادختساب ةلاسرلا ةقداصملا ةيلأ وه HMAC MD5 .تانايابل ،ام ماظنلا ايويح ارمأ ةقئافل اءادال ةعرس اه ي ف نوكت يتلا تالاحلا ي ف MD5 مدختسي ،انامأ لقا ناك نإو

هذه .لضفأل يه ريفشتلا ةقيرط نأل انامأ رثكأ هذه ةئزجتلا ةيمزراوخ — HMAC SHA .ريفشتلا ةئزجت فئاطو مادختساب لئاسرلا ةقداصملا انامأ رثكأ ةيلأ مادختسا بجي .ريفشتلا ةئزجت فئاطو مادختساب لئاسرلا ةقداصملا انامأ رثكأ ةيلأ ةيويح ةيمهأ اذ نامأل نوكتي ام دنع HMAC SHA ماظنلا

SNMP

SNMP:  Enable  Disable

SNMP Version:  SNMP v1&v2  SNMP v3

System Contact:  (1-200 characters)

System Name:  \*(1-30 characters)

System Location:  \*(1-200 characters)

Security Username:  (1-32 characters)

Authentication Password:  (8-64 characters)

Authentication Method:  HMAC-MD5  HMAC-SHA

Encrypted Password:  (8-64 characters)

Encryption Method:  None  CBC-DES

SNMP Read-Only Community:  \*(1-32 characters)

SNMP Read-Write Community:  \*(1-32 characters)

Trap Community:  \*(1-32 characters)

SNMP Trusted Host:

Trap Receiver Host:  \*

\* indicates a mandatory option.

Save Cancel

10. لاجم ةملك ريشي لاي ةملك تلخد ةوطخل.

ريياعم يه DES و CBC. ريشتلا ةقيرط لقح يه CBC-DES وي دار رز رقنا. 11. ةوطخل اهلقن متي يتلا تانايب لاني مأتلا هجم متي ريشت

لبيمعل ةملم يه هذ. طقف SNMP ةءارق ةمتم لقح يه اعتمتم لخدا. 12. ةوطخل SNMP دادعلا لىل طقف ةءارقلل لوصولل

لبيمعل ةملم يه هذ. SNMP ةباتك-ءءارق ةمتم لقح يه اعتمتم لخدا. 13. ةوطخل SNMP دادعلا ةباتكلاو ةءارقلل لوصولل

لىل ةردقل هيدل يذل اعتمتملا وه اذ. ةمئالملا اعتمتم لقح يه اعتمتم لخدا. 14. ةوطخل حمست. تامئالملا نع لوؤسمل لىل هجوم مالعل لاسرا متي. SNMP تاراب تلخا مادختسا مه مالعل مهي مدختسم لىل حامس لىل قيرط نع زاهج لك ةرادب لوؤسمل لىل تامئالملا ةمئالم مادختساب

فيملم IP ناو نع وه اذ. هب قوئومل SNMP فيملم لقح يه افيملم لخدا. 15. ةوطخل SNMP دادعلا ةقئلا

صاخلا IP ناو نع وه اذ. ةمئالملا لبقتم فيملم لقح يه افيملم لخدا. 16. ةوطخل تامئالملا يقئلل لوؤسمل لىل

تاداعلا قيبطتل طفح لىل رقنا. 17. ةوطخل

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة 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 دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوءو تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل