

# تاهجوم ةلسلس ىلع ماظنلا لچس نيوكت RV320 و RV325 VPN

## فدهلا

مهفل اهمادختسا متي ةمهم ةادأ يه تالچسلا . ةكبشلا شادحأل تالچس يه ماظنلا تالچس ةكبشلا ءاطخأ فاشكتساو ةكبشلا ةرادإل ةديفم اهنأ شيح . ةكبشلا لمع ةيفيك اهحالصإو .

ضرع ةيفيكو ، اهليچست دارملا تالچسلا عاونأ نيوكت ةيفيك ةلاقملا هذه حرشت ربع ملتسملا ىل تالچسلا لاسرا ةيفيكو ، VPN RV32x هجوم ةلسلس ىلع تالچسلا ينورتكللال ديربلا ربع ملتسم ىلأ ، ماظنلا لچس مداخ ىلأ ، SMS ،

## قيبطتلل ةلباقلا ةزهجالا

- ةجودزم WAN ةكبش ب VPN RV320 هجوم
- RV325 Gigabit WAN VPN Router هجوملا

## جماربلا رادصا

·v1.1.0.09

## ماظنلا لچس نيوكت

ليچست رتخاو بيولا نيوكتل ةدعاسملا ةادألا ىلأ لوخدلا ليچست ب مق 1. ةوطخلا  
:ماظنلا لچس ةحفص رهظت . ماظنلا لچس > لوخدلا

### System Log

**Send SMS**

SMS:  Enable  
 USB1  USB2

Dial Number1 :

Dial Number2 :

Link Up  Link Down  Authentication Failed  
 System Startup

---

**Syslog Configuration**

Syslog1:  Enable

Syslog Server 1:  Name or IPv4 / IPv6 Address

Syslog2:  Enable

Syslog Server 2:  Name or IPv4 / IPv6 Address

---

**Email**

Email:  Enable

Mail Server:  Name or IPv4 / IPv6 Address

Authentication:

SMTP Port:  Range: 1-65535 Default 25

Username:

ماظنلا لاجس ةحفص لوح تامولعم ىلع لوصحلل ةيلاتلا ماسقألا عجار

SMS ربع فتاه ىلإ ماظنلا تالاجس لاسرا ةيفيك — [SMS ةطساوب ماظنلا تالاجس](#).

لاجس مداخ ىلإ ماظنلا تالاجس لاسرا ةيفيك — [ماظنلا لاجس مداوخ ىلع ماظنلا تالاجس](#).  
ماظنلا

ىلإ ماظنلا تالاجس لاسرا ةيفيك — [ينورتكلالا ديربلاب ماظنلا تالاجس لاسرا](#).  
ينورتكلال ديرب ناووع

لاجسلا يف اهظفح متي يتلا لئاسرلا عون نيوكت ةيفيك — [لاجسلا تاداعا](#).

زاهجال ىلع ماظنلا تالاجس ضرع ةيفيك — [ماظنلا لاجس ضرع](#).

مزحلاب طقف طبترت يتلا ماظنلا تالاجس ضرع ةيفيك — [رداصل لاجسلا لودج ضرع](#).  
ةرداصل

طقف قلعتت يتلا ماظنلا تالاجس ضرع ةيفيك — [ةدراولا تالاجسلا لودج ضرع](#).  
ةدراولا مزحلاب

## SMS ةطساوب ماظنلا تالاجس

**Send SMS**

SMS:  Enable

USB1  USB2

Dial Number1 :  1234567890

Dial Number2 :

Link Up  Link Down  Authentication Failed

System Startup

لإرسال SMS لفتح في فني كمت نم ققحت 1. ةوطخال (SMS) ةريصقلا لئاسرلا ةمدخ لئاسر

لإرسال نم USB مدموب لصتتي يتل USB ذفانمب ةصاخلا رايخالا تاناخ ددح 2. ةوطخال ثلاثلا.

لإرسال متي يذلا فتاهال مقرر لخدأو "1 بلطال مقرر" لفتح في رايخالا ةناخ ددح 3. ةوطخال لئاسرلا.

يذلا مقررلا ملتسي مل اذا 1. مقرر بلطالاب لاصتالا رايخالا رايخالا لعل رقنا :**ةطخال مقرر** لفتح في حيحص لكشب فتاهال مقرر لخدأ نم دكأتف ، رايخالا ةلاسره نيوكت مت "1 بلطال".

يذلا فتاهال مقرر لخدأو "2 بلطال مقرر" لفتح في رايخالا ةناخ ددح (يرايخالا) 4. ةوطخال لئاسرلا لئاسرلا متي.

يذلا مقررلا ملتسي مل اذا 2. مقرر بلطالاب لاصتالا رايخالا رايخالا لعل رقنا :**ةطخال مقرر** لفتح في حيحص لكشب فتاهال مقرر لخدأ نم دكأتف ، رايخالا ةلاسره نيوكت مت "2 بلطال".

متيل لجلس ليغشت لئاسرلا يذوتس يتل اذالاب ةصاخلا رايخالا تاناخ ددح 5. ةوطخال لئاسرلا.

· RV320 ب لاصتالا ءاشنإ مت — طابترالال.

· RV320 ب لاصتالا عطق مت — لطمع طابترالال.

· ةقداصملا تلشف — ةقداصملا تلشف.

· هجوملا ديهمت مت — ماظنلا ليغشت ءدب.

SMS ربع ماظنلا تالجلس نيوكت مت .ظفح ةقطق 6. ةوطخال

## ماظنلا لجلس مداوخ لعل ماظنلا تالجلس

**Syslog Configuration**

Syslog1:  Enable

Syslog Server 1:  Name or IPv4 / IPv6 Address

Syslog2:  Enable

Syslog Server 2:  Name or IPv4 / IPv6 Address

لجس مداخل إلى مازنل التاليس لاسرال syslog1 لقي في نيكيتم نم قحت 1. ةوطخل مازنل.

لجس مداخل إلى مازنل لجس مداخل صاخل IP ناونع وأ فيضمال مسا لخدأ 2. ةوطخل Syslog Server 1.

لجس مداخل إلى مازنل لجس مداخل لاسرال (يرايخ) 3. ةوطخل syslog2.

لجس مداخل إلى مازنل لجس مداخل صاخل IP ناونع وأ فيضمال مسا لخدأ، syslog2 لقي في رايخال ةناخ ديحت مت اذا 4. ةوطخل Syslog Server 2.

مازنل لجس مداوخل لالخن م مازنل التاليس نيوكت مت. ظفح ةقطقط 5. ةوطخل.

## ينورتكلال ديبرل مازنل التاليس

**Email**

Email:  Enable

Mail Server:  Name or IPv4 / IPv6 Address

Authentication:  ▾

SMTP Port:  Range: 1-65535 Default 25

Username:

Password:

Send Email to 1:  Email Address

Send Email to 2:  Email Address(Optional)

Log Queue Length:  entries

Log Time Threshold:  min

Real Time Alert:  Email Alert when block/filter contents accessed  
 Email Alert for Hacker Attack

ملتسم إلى مازنل التاليس لاسرال ينورتكلال ديبرل لقي في نيكيتم ددح 1. ةوطخل ينورتكلال ديبرل ربع.

ديبرل مداخل لقي في ديبرل مداخل IP ناونع وأ لاجمال مسا لخدأ 2. ةوطخل.

ةقداصل لقي في ديبرل مداخل ممدختسي يذلا ةقداصلال عون رتخأ 3. ةوطخل.

ةقداصل مةي ديبرل مداخل ممدختسي ال — ال.

يداع صن قيسنتب ةقداصلال ديبرل مداخل ممدختسي — لوخدل ليجستل يداع.

مداخلالو ليمعملل حامسلل (TLS) لقلنل ةقبط نيما ديبرل مداخل ممدختسي — TLS.

معملل حامسلل (SSL) ةنمآل لوصوتل ذآم ةقبط ديبرل مداخل ممدختسي — SSL.

مداخل ممدختسي يذلا (SMTP) طيسبلال ديبرل لقلن لوكتورب ذفنم لخدأ 4. ةوطخل ديبرل لئاسر لاسراب حمسي لوكتورب وه SMTP. SMTP ذفنم لقي في ديبرل IP تاكبش ربع ينورتكلال.

Username:

Password:

Send Email to 1:  Email Address

Send Email to 2:  Email Address(Optional)

Log Queue Length:  entries

Log Time Threshold:  min

Real Time Alert:  Email Alert when block/filter contents accessed

Email Alert for Hacker Attack

5. مَدخْتِ سَم لَم سَا لِق ح ي ف ي ن و ر ت ك ل ل ا ل د ي ر ب ل ل س ر م م د خ ت س م م س ا ل خ د ا . 5 ة و ط خ ل ل

6. ر و ر م ل ا ة م ل ك ل ق ح ي ف ي ن و ر ت ك ل ل ا ل د ي ر ب ل ل س ر م ر و ر م ة م ل ك ل خ د ا . 6 ة و ط خ ل ل

7. ل ق ح ل ا ي ف ي ن و ر ت ك ل ل ا ل د ي ر ب ل ل م ل ت س م ل ي ن و ر ت ك ل ل ا ل د ي ر ب ل ل ن ا و ن ع ل خ د ا . 7 ة و ط خ ل ل  
1. ل ل ي ن و ر ت ك ل ل د ي ر ب ل ل س ر ا

8. د ي ر ب ل ل ل ئ ا س ر ل ل س ر ا ل ي ف ا ض ا ي ن و ر ت ك ل ل د ي ر ب ن ا و ن ع ل خ د ا ( ي ر ا ي ت ا خ ل ا ) . 8 ة و ط خ ل ل  
2. ل ل ي ن و ر ت ك ل ل د ي ر ب ل ل س ر ا ل ق ح ل ا ل ي ل ل ل ج س ل ل ا ب ة ص ا خ ل ل ي ن و ر ت ك ل ل ا ل

9. م ل ت س م ل ل ل ج س ل ل ا ل س ر ا ل ل ب ق ا ه و ا ر ج ا ب ج ي ي ت ل ل ل ج س ل ل ا ل ا خ ا د ا د د ع ل خ د ا . 9 ة و ط خ ل ل  
ل ج س ل ل ر ا ط ت ن ا ة م ئ ا ق ل و ط ل ق ح ي ف ي ن و ر ت ك ل ل ا ل د ي ر ب ل ل

10. ي ن و ر ت ك ل ل ا ل د ي ر ب ل ل ل ل ل ج س ل ل ز ا ه ج ل ا ه ي ف ل س ر ي ي ذ ل ا ي ن م ز ل ل ل ص ا ف ل ل ا ل خ د ا . 10 ة و ط خ ل ل  
ل ج س ل ل ت ق و د ح ل ق ح ي ف

11. د ي ر ب ل ل س ر ا ل ي ل ع ف ل ل ت ق و ل ا ه ي ب ن ت ل ق ح ل ل ي ل و ا ل ا ر ا ي ت ا خ ل ا ل ا ن ا خ د د ح . 11 ة و ط خ ل ل  
ه ج و م ل ا ل ل ل و ص و ل ا ، ه ت ي ف ص ت و ا ه ر ط ح م ت ، ا م ص خ ش ل و ا ح ي ا م د ن ع ر و ف ل ا ل ي ل ع ي ن و ر ت ك ل ل

12. د ي ر ب ل ل س ر ا ل ي ل ع ف ل ل ت ق و ل ا ه ي ب ن ت ل ق ح ل ل ي ن ا ث ل ل ا ر ا ي ت ا خ ل a ل ا ن ا خ د د ح . 12 ة و ط خ ل ل  
م و ج ه ل ل ا ل خ ن م ه ج و م ل ا ل ل ل ل و ص و ل ا ن ي ق ر ت خ م ل د ح ا ل و ا ح ي ا م د ن ع ر و ف ل ا ل ي ل ع ي ن و ر ت ك ل ل  
(DOS) ة م د خ ل ا ض ف ر

ر و ف ل ا ل ي ل ع ل ج س ل ل ا ل س ر ا ل ن ا ل ا ي ن و ر ت ك ل ل ا ل د ي ر ب ل ل ل ج س ق و ف ر ق ن ا : ة ط ح ا ل م

ي ن و ر ت ك ل ل ا ل د ي ر ب ل ل ر ب ع م ا ط ن ل ل ا ل ج س ن ي و ك ت م ت . ط ف ح ة ق ط ق ط . 13 ة و ط خ ل ل

## ل ج س ل ل ا د ا د ع ا

**Log**

Alert Log:  Syn Flooding  IP Spoofing  Unauthorized Login Attempt

Ping Of Death  Win Nuke

General Log:  Deny Policies  Authorized Login  System Error Messages

Allow Policies  Kernel  Configuration Changes

IPSec & PPTP VPN  SSL VPN  Network

- لجس لاخدا لئغش تب موقتس يتلا ثادخالل راي تخالال تاناخ دح 1. ةوطخال
- موجه ةلواحم وأ موجه ثودح دنع تالجالسلا هذه عاشنإ متي — هي بننتلا لجس:
- اهتجالعم يلع هجوملا ةردق نم ربكأ ةعرسب SYN ب لطي قلت متي — Syn Flooding
- ردملل ةروزم IP نيوانعب IP مزح RV320 يقلت — IP لاحتنا
- لجس تل اهضفر مت ةلواحم تلشف — اهب حرصملا ريغ لوخدلا لجس ت ةلواحم - ةكبشلا يلا لوخدلا
- يف ةهجاو يلا يعبط ريغ مجحب لاصتا رابتخا لاسرا مت — توملا لاصتا رابتخا - فدهتسملا زاهجال ميطحتل ةلواحم
- مساب فورعملا (DDOS) دعب نع عزوملا ةمدخل اضفر موجه لاسرا مت — Win Nuke WinNuke، فدهال زاهجال ميطحتل ةلواحم يف ةهجاو يلا
- ةماع ةكبش تاءارجا ثودح دنع تالجالسلا هذه عاشنإ متي — ماع لجس:
- يتلا تاسايسلا يلا اذانتسا مدختسم يلا لوصول اضفر مت — تاسايسلا اضفر - هجوملل اهنويوكت مت
- ةكبشلا يلا لوصول مدختسملا ليوخت مت — دمتعملا لوخدلا لجس ت
- ماطنلا يف أطخ ثدح — ماطنلا أطخ لئاسر -
- تاسايسلا يلا اذانتسا مدختسملا لوصول قح حنم مت — تاسايسلاب حامسلا - هجوملل اهنويوكت مت يتلا
- ماطن نم لوألا عزجال يه ةاونلا .لجسلا يف kernel لئاسر عي مج ني مضت — Kernel يه kernel لئاسر .لئغش تلا ادب دنع ةركاذلا يف هلي محت متي يذلا لئغش تلا ةاونلاب ةنرتقم تالجالس
- هجوملا نيوكت لئدعت مت — نيوكتلا تاريغيغ ت
- لاصتا عطق وأ لاصتا وأ PPTP VPN و IPsec ضوافت ثدح — IPSec و PPTP VPN
- لاصتا عطق وأ لاصتا وأ SSL VPN ضوافت ثدح — SSL VPN
- DMZ وأ WAN تاهجاو يلع هنادقف وأ يلعف لاصتا عارجا مت — ةكبشلا
- لجسلا تادادعا نيوكت مت .ظفح ةقطق 2. ةوطخال
- يلا لجالسلا حسمل لجسلا حسم يلع رقنا :ةظحالم

## مماظنلا لجس ضرع

**Log**

Alert Log:  Syn Flooding  IP Spoofing  Unauthorized Login Attempt

Ping Of Death  Win Nuke

General Log:  Deny Policies  Authorized Login  System Error Messages

Allow Policies  Kernel  Configuration Changes

IPsec & PPTP VPN  SSL VPN  Network

**View System Log...**

لودج ةذفان رهظت .ماظنلا لجس لودج ضرعل ماظنلا لجس ضرع قوف رقنا 1. ةوطخل ماظنلا لجس

Current Time: Sat Apr 6 10:59:40 2013

All Log

System Log Table		
Time	Event-Type	Message
Apr 6 10:59:34 2013	Kernel	kernel: tr_enable=0, smartqos=0, period=0
Apr 6 10:59:34 2013	Kernel	kernel: wrong ip[0],not_list[0]

اهضرع ديرت يتال تالجالسلا عون رتخأ ةلدس نمل ةمئاقلا نم (يراي تخا). 2. ةوطخل

لجسلا لئاسر عيمج نمضتت — تالجالسلا عيمج

طقف ماظنلا أطخ لئاسر نمضتي — ماظنلا لجس

طقف هيبننتال تالجالس نمضتي — ةي/DoS ةي/ماحل راج لامعأ لجس

طقف SSL VPN و PPTP VPN و IPsec تالجالس نمضتي — VPN لجس

ةكبشلا تالجالس ال نمضتي ال — ةكبشلا لجس

طقف Kernel لئاسر نمضتي — Kernel لجس

لجسو ، تاسايسلاب حمسيو ، طقف ضفرل تاسايس نمضتي — مدختس مالا لجس  
نيوكتال ريغت تالجالسو ، دمتمع مالا لودخل

طقف SSL VPN تالجالس نمضتي — SSL لجس

ةيلاتال تامولعمل ماظنلا لجس لودج ضرعي

لجسلا عاشن تقو — تقولا

لجسلا عون — ثدحلا عون

ردصم ال IP ناوونو جهنلا عون نمضتي اذهو .لجس لل ةقباطملا تامولعمل — ةلاسرلا  
ردصم ال MAC ناوونو

تالجالس لودج ثي دحتل ثي دحت قوف رقنا :ةطحالم

**رداصلال لجسلا لودج ضرع**



**Log**

Alert Log:  Syn Flooding  IP Spoofing  Unauthorized Login Attempt  
 Ping Of Death  Win Nuke

General Log:  Deny Policies  Authorized Login  System Error Messages  
 Allow Policies  Kernel  Configuration Changes  
 IPSec & PPTP VPN  SSL VPN  Network

مزجلاب طقف قلعتي يذلا لجسلا لودج ضرعل رداصلا لجسلا لودج قوف رقنا 1. ةوطخل رداصلا لجسلا لودج ةذفان رهظت. ةرداصلا

Current Time: Sat Apr 6 10:57:28 2013

Outgoing Log Table		
Time	Event-Type	Message
Apr 6 10:57:22 2013	Connection Accepted	IN=eth0 OUT=eth1 SRC=192.168.1.150 DST=156.26.180.254 DMAC=... SMAC=... LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=15306 DF PROTO=TCP SPT=63865 DPT=80 WINDOW=8192 RES=0x00 SYN URGP=0
Apr 6 10:57:24 2013	Connection Accepted	IN=eth0 OUT=eth1 SRC=192.168.1.150 DST=156.26.180.254 DMAC=... SMAC=... LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=15312 DF PROTO=TCP SPT=63868 DPT=80 WINDOW=8192 RES=0x00 SYN URGP=0

ةيلاتلا تامولعمل رداصلا لجسلا لودج ضرعي.

لجسلا ءاشنإ تقو — تقولا.

لجسلا عون — شذحلا عون.

ردصم ال IP ناو نوجهنلا عون نمضتي اذهو. لجسلل ةقباطملا تامولعمل — ةلاسرلا. ردصم ال MAC ناو نوجو.

تالجسلا لودج شيذحتل شيذحت قوف رقنا: ةظحالم.

## ةدراولا تالجسلا لودج ضرع

**Log**

Alert Log:  Syn Flooding  IP Spoofing  Unauthorized Login Attempt  
 Ping Of Death  Win Nuke

General Log:  Deny Policies  Authorized Login  System Error Messages  
 Allow Policies  Kernel  Configuration Changes  
 IPSec & PPTP VPN  SSL VPN  Network

مزجلاب طقف قلعتي يذلا لجسلا لودج ضرعل دراولا لجسلا لودج قوف رقنا 1. ةوطخل دراولا لجسلا لودج ةذفان رهظت. ةدراولا



Current Time: Fri Apr 5 11:59:55 2013

Incoming Log Table		
Time ▾	Event-Type	Message
Apr 5 09:04:23 2013	Kernel	kernel: i2c i2c-0: Can't create device at 0x32
Apr 5 09:04:23 2013	Kernel	kernel: gre: can't add protocol

ةيلال تامولعمل دراوال تالجال لودج ضرعي

لجال عاشن تقو — تقولا

لجال عون — ثدجال عون

ردصم ال IP ناووعو جهن ال عون نمضتي اذهو. لجال لة قباطم ال تامولعمل — ةلاس رلا  
ردصم ال MAC ناووعو

تالجال لودج ثيديحتل ثيديحت قوف رقنا: ةطحالم

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 ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل