

اهالصالو WAAS ءاطخأ فاشكتسا ةيلمع ىلع ةماع ةرطن

ةيلاتلا ةماعلا تاداشرالا عبتا ،اهالصالو WAAS ماظن ءاطخأ فاشكتسال

1. نأ بجي ناك اذا WAAS ةزهجأ عيمج ربع هب ىصومو قسانتم جم انرب رادصاب ظافتحالا . مسق عجار . ىلعألا رادصالو وه Central Manager نوكي نأ بجي ، تارادصالو فلتخت م. مدختسمل رادصالو ديدحتل "[WAAS ةروص نم ققحتلا](#)".
2. ، تازيمل اشدحا ىلع لوصحلل كب صاخلا جم انربلا رادصالو [WAAS رادصا تاطحالم](#) عجار . CLI رمأ تاريغيغتو ، تاريذحتلاو ، ليغشتلا تارابتعاو
3. خسنلا ةزيم مدختسا ، WAAS ل ةيزكرمل ةرادالا ىلع نيوكتلا تاريغيغت لاخدا لب ق . ، ديدجل نيوكتلا عم لكاشم تهجاو اذا . كب صاخلا نيوكتلا ظفحل CMS ل يطايتحالا ، ايطايتح [WAAS ماظن خسن](#) مسق عجار . قباسلا نيوكتلا ةداعتسا كنكميف ءاطخأ فاشكتسا . Cisco نم ةعساو [تاقببطللا تامدخ نيوكت ليلا](#) ف هتداعتساو ةرشابم اهؤارج دعب اهالصالو ةديجل نيوكتلا تاريغيغت
4. ةبولطم تاريغيغت يا ءارجاب مق . ةكبشلا قيببطلل كب صاخلا نيوكتلا ةحص نم ققحت فلم يف هظفح مقف ، ايضرم ناك اذا . نيوكتلا ربتخا مث ، running-config فلم ىلع startup-config رملأ مادختساب [copy running-config startup-config](#).
5. "[WAAS ليچست نيكمت](#)" مسق عجار . ماظنلا لئاسر لوخد ليچست نيكمت .
6. عجار . هب لاصتالا ةيناكم او زاهجال فئاظو نم ققحتلل صيخشتلا ةادا ليغشتب مق "[تاصيخشتلا ليغشت](#)" مسق
7. [نم ققحتلا](#)" مسق عجار . قيببطللا مداوخو WAAS نارقأ نيبي ىلعفلا لاصتالا نم ققحت "[تاقببطللا مداوخو ةريظنلا WAAS ةزهجأ نيبي ىلعفلا لاصتالا](#)".
8. [WAAS ءاطخأ فاشكتسا تامولعم](#)" مسق عجار . ةددحمل ضارعال ددحت يتلا تامولعمل عمجا "[اهالصالو](#)".
9. لوصحلل اذه WAAS اهالصالو ءاطخأ فاشكتسا ليلا ىف ىرخألا تالاقملا يدحا ىلا عجارا :
 - [فاشكتسا](#) ةلاقم عجارف ، صارقالا وأ ةزهجالاب تالكشم نم يناعي ماظنلا نأ ادب اذا [اهالصالو تانوكمل او صارقالا ءاطخأ](#).
 - [فاشكتسا](#) ةلاقم عجارف ، رورملا ةكرح لابقستسا يف ةلكشم هجاوي ماظنلا ناك اذا . ةيامحلا رادج يف ةلكشم ببسب اضيا ةلكشملا هذه نوكت دق . [اهالصالو WCCP](#)
 - لكاشم هجاوي ناك وأ اهنيسحت نم الدب تانايبلا رورم ةكرح ربع رمي ماظنلا ناك اذا ، (كلذىلا مو ، SSL ، MAPI ، HTTP) تاقببطللا رورم ةكرح نم ةنيعم عاونأ نيسحت يف اهالصالو [قيببطللا عيرستو اهالصالو ءاطخأ فاشكتسا نيسحت](#) يتلاقم عجارف .
 - ةلاقملا عجارف ، اهنيسحت نم الدب عقوتمل نم رثكأ رورم ةكرح رمي ماظنلا ناك اذا [اهالصالو ءاطخأ فاشكتسا دئاز ليحمت طورش](#).
10. زكرمب لصلتا ، ةلكشملا لحت مل اهالصالو ءاطخأ فاشكتسا تالواجم نأ ديدحت دعب . مسق عجار . كب صاخلا ىنفل معدلا لثمم وأ Cisco نم (TAC) ةينقتلا ةدعاسملا "[ينفلا Cisco معدب لاصتالا](#)".

WAAS ةروص نم ققحتلا

يلاتلا رملأ لاخدا ، WAAS زاهج يف ايلاح اهليغشت متي يتلا جم انربلا ةروص رادصا ضرعل

```
wae# show version
```

```
Cisco Wide Area Application Services Software (WAAS)
```

```
Copyright (c) 1999-2009 by Cisco Systems, Inc.
```

```
Cisco Wide Area Application Services Software Release 4.1.3a (build b25 May 23 2 <-----
```

009)

Version: oe7341-4.1.3a.25

Compiled 10:10:47 May 23 2009 by cnbuild

System was restarted on Wed May 27 14:45:28 2009.

The system has been up for 6 weeks, 2 hours, 35 minutes, 48 seconds.

الاثم ل ل ي ب س ي ل ع ، ي ر خ أ ة د ي ف م ت ا م و ل ع م ر م أ ل ا ذ ه ر ف و ي :

- زار ط م ق ر ر ا د ص إ ل ا ة ل س ل س ر ي ف ش ت ن م ل و أ ل ا ع ز ج ل ا ي ف ة د و ج و م ل ا م ا ق ر أ ل ا ز ا ه ج ل ا ز ا ر ط (. ا ن ه WAE-7341 ض ر ع م ت ي ؛ ز ا ه ج ل ا ل ي غ ش ت ل ا ت ق و WAE)

ر م أ ل ا ل خ د أ ، (ز ا ه ج ل ا د ي ه م ت ة د ا ع إ ر ا ط ت ن ا ي ف) ج م ا ر ب ل ل ة ق ل ع م ة ي ق ر ت د و ج و م د ع ن م ق ق ح ت ل ل ي ل ا ت ل :

```
wae# show version pending
No pending version
```

" ق ل ع م ر ا د ص إ د ج و ي ا ل " ة ل ا س ر ل ا ي ر ت ن أ ب ج ي .

W A A S ل ي ج س ت ن ي ك م ت

ل ك ش ب /local1/syslog.txt ص ر ق ل ا ف ل م ي ل ا م ا ظ ن ل ا ي ف م ا ع ل ا أ ط خ ل ل ل ي ج س ت ل ا ن ي ك م ت م ت ي ي ل ا ت ل ر م أ ل ا ل ا خ د ا ل ا ل خ ن م ل ي ج س ت ل ا ن ي ك م ت ن م ق ق ح ت ل ا ك ن ك م ي . ي ض ا ر ت ف ا

```
wae# show logging
Syslog to host is disabled.

Syslog to console is disabled
Priority for console logging is set to: warning

Syslog to disk is enabled
Priority for disk logging is set to: notice
Filename for disk logging is set to: /local1/syslog.txt

Syslog facility is set to *

Syslog disk file recycle size is set to 10000000
```

ي ل ا ت ل م ا ع ل ا ن ي و ك ت ل ا ر م أ ل خ د أ ، م ك ح ت ل ا ة د ح و ي ل ل ي ج س ت ل ا ن ي ك م ت ل :

```
wae(config)# logging console enable
```

ة د ح و ل ا ف ث ك م ر ا ع ش إ ل ا ن م ل ق أ ي و ت س م ي ل ع ل ي ج س ت ل ا ة ي و ل و أ ن ي ي ع ت ن و ك ي ن أ ن ك م ي : ة ط ح ا ل م ي ف ل ي ل ق و و ة م ك ح ب ا ه و ل م ع ت س ا . ج ا ر خ إ ل ا ن م ة ر ي ب ك ة ي م ك ج ت ن ي ن أ ن ك م ي و ة ي ز ك ر م ل ا ة ج ل ا ع م ل ا ج ا ت ن ا ة ي ب .

ل ج س ل ا ت ا ف ل م ل W A A S ل ب ق ن م ة ي ل ا ت ل ل ا ل د ل ا م ا د خ ت س ا م ت ي :

- /local1/syslog.txt ع ق و م و ل ج س ل ا ت ا ف ل م ع ي م ج ل ر ذ ج ل ل ي ل د ل ا — /local1
- /local1/log — ة م د خ ل ل ل ج س ت ا ف ل م — /local1
- /local1/errorlog — ة م د خ ل ل ل ج س ت ا ف ل م — /local1

قريظننل WAAS ةزهجأ نيب يلعفل لاصتال نم ققحتل قيبطتال مداوخو

ةيلال تاوطخل عبتا، قريظننل WAAS زاوجل يلعفل لاصتال نم ققحتل:

1. WAAS زاوجل يلع رثؤي دق يذلا هجوملا وأ لوجملا يلع تالبكل تالاصتاي عيمج نم ققحت.
2. قريظننل WAE يلى ICMP يدص بلط لاسرل ping رمال مدختسأ.

```
wae# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=37 time=83.9 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=37 time=80.6 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=37 time=79.2 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=37 time=79.3 ms
64 bytes from 10.1.1.2: icmp_seq=5 ttl=37 time=79.4 ms

--- 10.1.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 79.274/80.538/83.904/1.793 ms
```

لاصتاي رابتخا كليلع، زاوجل يلى لوصولي نم نكمتت ملو ةدحاو ةوطخ دعب يلع زاوجل ناك اذا ققحتو `show ip route` رمال لخدا، لوصولل ةلباق ةباوبل نكت مل اذا. طيسول ةرابع لخدا، لاثملا ليبس يلع. ححصلا راسملا ضرع نم دكأتل

```
wae# show ip routes
Destination      Gateway           Netmask
-----
10.10.10.1       0.0.0.0          255.255.255.255
10.43.62.4       0.0.0.0          255.255.255.255
10.43.62.0       0.0.0.0          255.255.255.192
10.10.10.0       0.0.0.0          255.255.255.0
0.0.0.0          10.43.62.1      0.0.0.0
```

ةرابعلل اثبات اراسم لخدا، رمال مزل اذا.

WAAS تانايب زكرم زاوجل نيب لاصتال نم ققحتل لثامم لاصتاي رابتخا رمأ مادختسإ كنكمي قيبطتال مداوخو.

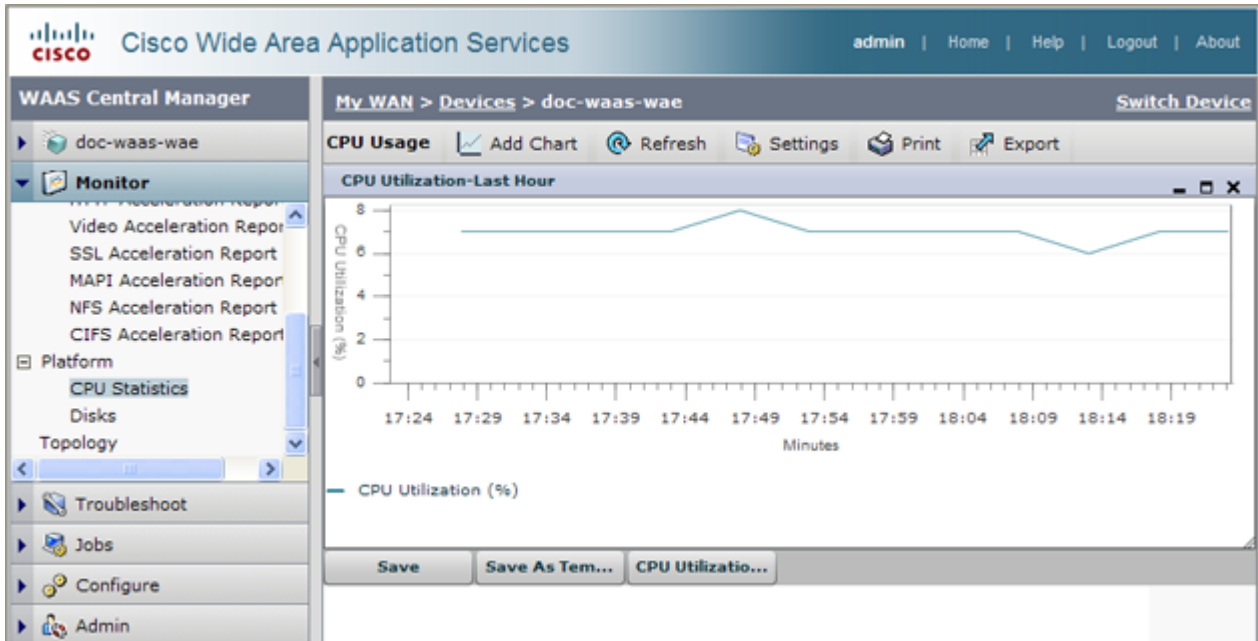
هيجوت ةداعا راسم ICMP رورم ةكرح عبتت الو ICMP رورم ةكرح عنمت دق ةيامحل نارجل نأ ظحال كنكمي، ليدبك. عيرستل وأ هيجوتل ةداعا ققدي ال ping رمال مادختسإ نإ كلذل WCCP، TCP يلى دنستس ي لاصتاي رابتخا ذيفنتب موقت ةيجراخ ةه ةادأ مادختسإ.

ةيزكرملا ةجلعمل ةدحو لمح نم ققحتل

ةيلال تاوطخل عبتا، WAAS زاوجل ةيزكرملا ةجلعمل ةدحو لمح نم ققحتل:

1. WAAS Central Manager ب صاخلا (GUI) ةيموسرلا مدختسملا ةهجاو يلقننل اعزج نم ةزهجالا ةرادا > يب صاخلا WAN رتخأ.
2. ةدحو ليمحت نم ققحتل ديرت يذلا زاوجل مسا راوجب دوجوملا ريرحت زمر قوف رونا. هيلع ةيزكرملا ةجلعمل.
3. (CPU) ةيزكرملا ةجلعمل ةدحو تايئاصح > ةصنم > ةشاش رتخأ، حصتال حول ي.

جلعمل تايئاصح | 1 لكش



ةعاسل"ا" هه ةيضا رتف الال ةمي قلا نال ارطن ،ططخ ملل ةي نزل ةرتف الال طبض ي ف بغرت دق اراطا رتخاو ماهم الال طيرش ي ف تاداع الال ةنوق ي قوف رقنا ،ةي نزل ةرتف الال طبضل . "ريخ الال" "يضا م الال عوبس الال" و "ريخ الال موي الال" لثم افلتخ م اي نزم

ةجلال عملال ةدحو مادختس الال لوطا تارتف ي تح و ةداح الال تا عافترا الال راهظا WAAS زا هجل عئاشل الال نم ةجلال عملال ةدحو لظت ام دنع . ةي لال الال مدختس م لاطاشن تارتف ةانثا ي لال الال (CPU) ةي زك رمل الال ةليوط تارتف الال (CPU) ةي زك رمل الال ةجلال عملال ةدحو نم عفترم يوتسم ي ف (CPU) ةي زك رمل الال زا هجلال م ح ر ي ي غ ت و ا ه ح ال ص و ا ط ا خ الال ف ا ش ك ت س ا نم د ي ز م ي ل ا ة ر ا ش الال م ت ت د ق ، ة ي ا غ ل ل

اهح ال ص و ا WAAS ءاطخا فاش ك ت س ا تام و ل عملال عي م ح ت

ي ت ل و ا و ث د ح ت ي ت ل ا ة ل ك ش م ل ا ب ة ل ص ل ا ت ا ذ ت ا م و ل عملال عي م ح ت ق ر ط ب ة ي ل ا ت الال م ا س ق الال ي ص و ت Cisco نم (TAC) ةي ن ق ت ل ا ة د ع ا س م ل ا ز ك ر م ب ل ا ص ت الال ل ب ق ة ي ر و ر ض ن و ك ت

WAAS زا هجل لي غ ش ت ة د ا ع ا

تام و ل عملال ض ع ب ن ك م ت ت ال د ق . ا م ا م ت ا ي ر و ر ض ن ا ك ا ذ ا الال WAAS زا هجل لي غ ش ت ة د ا ع ا ب م ق ت ال ر د ق ر ب ك ا ع م ج ل و ا ح . ل ي غ ش ت ل ا ة د ا ع ا ة ي ل م ع ز و ا ج ت نم ا ه ح ال ص و ا ت ا ل ك ش م ل ا ف ا ش ك ت س ا ل ة م ا ه ل ل ل ي غ ش ت ل ا ة د ا ع ا ل ب ق ت ا م و ل عملال نم ن ك م .

show رم او ا م ا د خ ت س ا

ض ا ر ع الال ة ص ا خ ت ا م و ل عملال عي م ح ت ل EXEC ع ض و ي ف ض ر ع الال رم او ا نم د ي د ع الال م ا د خ ت س ا ك ن ك م ي ا ه ي ل ا ج ا ت ح ت ي ت ل ا ت ا م و ل عملال عي م ح ت ك ن ك م ي ، ت ا ل ا ح الال م ط ع م ي ف . زا هجل ي ف ا ه ا ر ت ي ت ل ا ر م الال ا ذ ه م و ق ي . **copy tech-support** ر م الال ل ا خ د ا ل ل ا خ نم ا ه ح ال ص و ا زا هجل الال ءاطخا فاش ك ت س ا ل ت ا ج ر خ م ل ا ع م ج ي و ا ه ح ال ص و ا ءاطخا الال ف ا ش ك ت س ا ل ة د ي ف م ل ا ض ر ع الال رم او ا نم د ي د ع الال ل ي غ ش ت ب و ا FTP م د ا خ و ا ص ر ق ف ل م ي ل ا **copy tech-support** ر م الال ج ا ر خ ا ه ي ج و ت ة د ا ع ا ك ن ك م ي . د ح و ف ل م ي ف ي ل ي ا م ك ي ه ر م الال ة غ ا ي ص . TFTP م د ا خ

`ftp {hostname | ip-address} remoteDirectory
remoteFilename | tftp {hostname | ip-address} remoteFilename` ف ل م م س ا خ س ن

ن ي ي ع ت ب م ق ، ي ل ح م ل ا م ا ظ ن ل ا ي ل ع ص ر ق ف ل م ي ل ا ر م الال ت ا ج ر خ م خ س ن ل ، ل ا ث م ل ا ل ي ب س ي ل ع ي ل ي ا م ك ر م الال

wae# copy tech-support disk ts-report.txt

ييلي ام ىرألأا ةديفملا ضرعلا رماو نمضتت

- تاهي بنتللا ضرع: تاهي بنتللا راهظا|
- قيبطتللا عرسم ةلاح ضرعي: عرسملا راهظا|
- صيخرتللا ةلاح ضرعي: صيخرتللا ضرع
- TCP تالاصتلا عيمجل تايئاصح| ضرعي: تايئاصحالا لاصتلا راهظا|
- TFO تايئاصح| ضرعي: tfo تايئاصحالا راهظا|
- show interface: اهتلاحو ةهجاوولا تامولعم ضرعي: لاسرالاو ةعرسللا قباطت نم ققحت. لوحملا عم هاجتالا يئانث
- WAE ىلع ةيلاتللا رماوألأا مدختسا، WCCP رشن تايلاعمل ةبسنلاب
 - show wccp gre
 - show wccp routers
 - show wccp wide-area-engine
 - WCCP تاقفدت راهظا|
 - جورخللا بيلالسا راهظا|
- لولحلا وأ هجوملا ىلع ةيلاتللا رماوألأا مدختسا، WCCP رشن تايلاعمل ةبسنلاب (كلذ لولحلا قبطني امثيح، تامدخ ةعومجم):
 - show ip wccp
 - show ip wccp تاهجاوولي صافات
 - show ip wccp ةمدخ
 - show ip wccp ليصفت ةمدخ
- دنع لولحلا وأ هجوملا ىلع ةيلاتللا رماوألأا مدختسا، WCCP رشن تايلاعمل ةبسنلاب (ئزجتلا مادختسا):
 - show tcam count
 - mls ةلاح راهظا|
 - show mls netflow لودج ليصافات
 - show mls NetFlow ip count
 - show mls netflow ip sw-install count
 - ةتبتمل MLS NetFlow IP ليصافات ضرع
 - FM interface_name ةهجاوولا راهظا|
- دنع لولحلا وأ هجوملا ىلع ةيلاتللا رماوألأا مدختسا، WCCP رشن تايلاعمل ةبسنلاب (عانقلا مادختسا):
 - show ip wccp عانقلا ةمدخ
 - show ip wccp جمدةمدخ
 - show tcam interface interface_name acl {in | out} ip
 - show tcam interface interface_name acl {in | out} ليصافات IP

ماظن ريرقت عاشن|

ييفل Cisco معدب لاصتالا لبق هيلي| جاتحتسا الماش اريرقت (sysreport) ماظنلا ريرقت دعي
ماظنلا ريرقت يوتحي. [copy sysreport](#) رمالا ليغشت قيرط نع sysreport ريرقت عاشن| كنكمي
تايئاصحاو ضرعلا رماوألأا كلذ يفا ماب، ماظنلا ىلع تالاجسللاو رماوألأا نم ديدعلا نم تاجرخم ىلع
كلذ ىلا امو تايئاصحالاو نيوكتللا تادادعاو لاجسللا تايوتحمو ةيئانبالا تاموسرلاو ةكبشلا

وأنتي اياجي م 100 الى 30 نم همجج حوارتي دقو تقولا ضع ب ماظن ريرقت عاشن ا قرغت سي دق رم ال اي ف اهنيمضت متي يتل نم ريثك ب رثك ا رصانع يلع ماظنل ريرقت يوتحي .رثك ا ينفل Cisco معدب لاصتال دنع ماع لكش ب بولطم وهو ،copy tech-support

متي شي حبة صيغش التل تارابتخال لايغش تل test رم ال مدختس ا ،ماظن ريرقت عاشن ا لب ق (وا) "يزكرم ريدم" يلع ماظن ريرقت عاشن ا دنع .ماظنل ريرقت ي ف تامولع م ا هذه ني مضت CMS رم ال مادختساب تاناي بل ا دعاق ل يطايتح ا خسن ارج ا ال ا ب جي ،("ي طايتح ا يزكرم ريدم" Database Backup

sysreport خسن ا :يل التل رم ال ج ذومن مدختس ا ، FTP مداخ يل ا هنيزختو sysreport ريرقت عاشن ا ل دع ب نع فللمل مس ا directory-دع ب نع ftp server-ip

لالتل ليبس يلع

```
wae# copy sysreport ftp 10.10.10.5 /reports wae1report
```

،ددم ةني نمز ةرتف يل ريرقتل نم دحت رم او ا تارايخ ي ا مدختست ال ،ماظن ريرقت عاشن ا دنع ،ةني مزل ا ةرتف لالتل خيتح تامولع م ا ني مضت مدع ي ف ببست ي دق كلذ ن ا شيح

اهل ليحتو مزحل طاق التل

فاشكتس ا ي ف ةدي فم ةدعاسم وه ("TCP غيرفت" مساب انايخ ا اهل ا راشي) مزحل طاق التل زاوجل نكمي .ببرملا طاشنل ا ب قارم ل و WAAS زاغ مادختساب ا ا حالص ا و لاصتال ا ا طاخ ا مزحل تامس دي دحت متي .اهل الخ رم ت يتل ا ةكبش ل رورم ةك رحل ةمزحل تامولع م بقع ت WAAS خسن كنكمي و ،ةطقتل لم مزحل WAAS زاغ ننخي .(ACL) لوصول ي ف مكحت ةمئاق ةطساوب ةمزحل تامولع م ضرع اضي ا كنكمي .ديعب مداخ يل ا و فلم يل ا اتقوم نزنم ل ا تايوتحم ل ا .ك ب ةصاخ ل ا ةيفرطال ا ةدحو ل ا و مكحتل ا ةدحو يلع ةطقتل لم ل ا

ل. لوؤس م ا تازايتم ا رم او ال ا هذه بلطتت .tcpdump gtethereal :مزحل طاق التل ا ةدعاسم ا تاد ا دجوت

S- را ي خ مادختساب ي صون .ةمزح لك نم تي اب 64 لو ا رم او ال ا هذه طقتلت ،يضا رتف ا لكش ب .ةلمك ل ا ةمزحل ا تاناي ب طاق التل ال 1600

طاق التل ا تاي لمع عاشن ا ل tcpdump مدختس ا ف ،ةري ب ك عبتت تاي لمع يلع لصحتس تنك ا ذا موق ي و KB ي ف طقتل لم فلم لكل مجج ي صق ا C- را ي خ طبضي .ةددمت تافل م ي ف ةجومت مزح .اهل اشن ا متيل ني و دتل ا تافل نم ددع ي صق ا ني يعبت M- را ي خ

.ةعارق ل ل R- حشرم را ي خ عم را ي خ ل ا مدختس ا ف ،ةطقتل لم مزحل ا ةيفصت يل ا ةجاحب تنك ا ذا فلم ل ا لباقم tethereal مادختس ا م ث ،ةري ب ك ةمزح طاق التل عاشن ا ل tcpdump مادختس ا كنكمي .ةيفصت ل ا ذي فننتل طقتل لم ل ا

لخاد ثحبت ال tcpdump ةيفصت لم اوع ن ا ل WCCP ةئي ب ي ف tcpdump مادختس ا دنع ارذح نك .كلذب مايق ل ا يل ا ةجاحب تنك ا ذا فورحل ا مادختس ا يل ا جاتحت فوس .GRE ني مضت جمانرب

جمانرب لمع تاسلج و ا ،تاهجاول ا عي مج طاق التل ا ي ا -i را ي خ مدختس ا ،ني رم ال ا لك مادختس ا ب طاق التل ا فاق ي ل ا CTRL+c) ^c مدختس ا .ةلصفنم ل ا تاهجاول ا يلع طاق التل ل ا ل لصفنم ل a telnet ةمزحل ا

مزحل طاق التل ا تافل م لي لحتل ا مادختس ا كنكمي ي تل ا مزحل ا لي لحتل ا او دا نم دي دعل ا كانه ب :مه فاطتخاب تمق ن ا دع ب

- (مزالل نم رثك ا نسحتسم) ةعساو ل ا تاردق ل ا عم ةني ن ا ج م ل ا مزحل ا لي لحتل ا ةادا :Wireshark
- .ةلماش تانك م ا عم ةني ن ا ج م ل ا مزحل ا لي لحتل ا ي رخ ا ةادا :كلذل
- Microsoft Netmon: جمانرب عم نمضم
- sniffer pro

TCPDUMP غي رقت مادختسا

تاقى ببطتلا تامدخ رم او عجرم يف [tcpdump](#) عجار ،ةلماكللا غايص يلع لوصحلل Cisco نم ةعسا اول

يلى امك يه ةدئاف TCPDUMP غي رقت تاراخي رثكأ:

- **-i interface:** طبر ضبق يلع نأ ديرت تنأ ثيح نراقلا
 - يلمح : ول
 - th0: GigabitEthernet 1/0
 - eth1: GigabitEthernet 2/0
 - th2: InlinePort 1/1/WAN ذفنم
 - eth3: InlinePort 1/1/lan
 - eth4: InlinePort 1/0/WAN ذفنم
 - eth5: InlinePort 1/0/lan
 - اهنكمي ال "any" ةهجاو لا ناب ملمع يلع نك . ةرفوتملا تنرثيإ ذفانم ةفاك : يأ نم ديزملا . ةرداصللا مزحلا ضعب دقت دقت لك لذل ، ةطلتخملا عضولا يف طاقتلالا يلع راخلا اذه رفوتي ال : ةظحالم . (8) tcpdump يلع Linux لجة ةحفص عجار ، تامولعمللا . ثدحألا تارادصللا او WAAS نم 4.1.5 رادصللا .
 - ةيدامللا تاهجاو لا عيمج نيب عمجت يتلا ةيقطنملا ةهجاو لا : ةطبارلا .
- **-s Snaplen:** ةمزح لك هطاقتلا متي مجح ي صقأ
- **-w file:** ماخلا اهل كش يف هي ةطقتلملا مزحلا ةباتك متيس يذل فلملا مسا
- **-C count:** -M راخلا ديدحت مت اذا . تيابلا فالآب ددحلا ، طاقتلالا فلم مجح ي صقألا دحلا . اهائاشن متي ةيفاضا طاقتلا تافلما نإف ، اضيأ دنع يقوفلا رورملا ةطساوب اهؤاشن مت يتلا لجلسلا تافلما ددعل ي صقألا دحلا .
- **-m num:** اهللمع بجي يتلا طاقتلالا تافلما ددع ددحي اذه . فلملا مجح ي صقألا دحلا يلى لوصولا . طاقتلالا فاقيا لبق
- **-D:** طاقتلالا ةحاتملا تاهجاو لا ةمئاق غي رقت .

1.cap تافللملا مزح يلى مزحلا عيمج يلاتلا لاثملا طقتلي

```
wae# tcpdump -i bond0 -s 1600 -w packets1.cap
```

فرحمل مادختسا

نم ةعسا اول تاقى ببطتلا تامدخ رم او عجرم يف [ةغايصللا](#) عجار ،ةلماكللا غايصللا يلع لوصحلل Cisco .

يلى امك يه ةديفملا ةيوناتلا تاراخيلا

- **R read_filter:** ةغايص س فن مدختسا . ةياغلل ةديفم ةيفصتلا نوكت نأ نكمي . كلت يدح مادختسا كنكمي ثيح ب ، Wireshark أو EtherAI عم اهمدختست يتلا ةيفصتلا فلم ليوحتل اضيأ اديفم TetherAI دعي . ةيفصت لماع نيوكت يف ك تدعاسمل تاودألا (tcpdump نم ، لاثملا لىبس يلع) لع فالاب هطاقتلا مت ةمزح طاقتلالا فلم ةيفصتو تاراخيلا رفوتت ، كلذ عمو ؛ libpcap فلم وه يضا رتفاللا فلملا عون :
 - LIBPCAP - libpcap (tcpdump، ethereal، خل)
 - rh6_1libpcap - RedHat Linux 6. 1 libpcap (tcpdump) ليغشتلا ماظن
 - suse6_3libpcap - SuSE Linux 6.3 libpcap (tcpdump) ليغشتلا ماظن

- MODLIBPCAP - tcpdump لدمج ربييل فرح
- tcpdump بباكبيل ايكون - بباكبيل ايكون
- Novell LANalyzer - رزيل انال
- Network Associates Sniffer (DOS) (دنتسم)
- سمشال بوونس - بوونس
- Microsoft Network Monitor 1.x - NetMon1
- Microsoft Network Monitor 2.x - Netmon2
- Network Associates Sniffer (Windows) 1.1 - ngwsniffer_1_1
- Network Associates Sniffer (Windows) 2.00x - ngwsniffer_2_0
- HP-UX ةكبش عبتت
- رورم ةكرح طاقتل - ئيرم
- Accellent 5Views طاقتل - ضرع 5
- Network Instruments Observer، رادصال 9 - NetVerv9

ليوحتلاو ةيفصتلل مدختست ةفلتخم تاراخي ةيلالتل ةلثمالا حضوت:

يولي امل لثامم رما مدختسا، رخا يلى فلم قيسنت نم ليوحتلل

```
wae# tethereal -r test-netmon.cap -F libpcap -w test-libpcap.cap
```

يولي امل لثامم رما مدختسا، SYN ةمالعل ةءارق حشرم مادختسال

```
wae# tethereal -R "tcp.flags.syn eq 1"
```

امل لثامم رما مدختسا، (GRE مزح لخد رطانوا) نينيعم نينيفيضم ةءارق حشرم مادختسال يولي:

```
wae# tethereal -s 1600 -w dump1.cap -R "ip.addr eq 2.43.183.254 and ip.addr eq 2.43.182.165"
```

ةيارد يلع نوكت نا بجي يتل مادختسال تاريذحت ضعب يلع tethereal رمالا يوتحي: **مظالم**
 اها:

- -w رايخال عم هجمد دنع -R رايخال مادختساب هفيرعت مت يذلا ةيفصتلا لماع لهاجت متي ةباتكلاو ةطقتلمل رورملا ةكرح ةيفصتل 4.1.3 و 4.1.1 WAAS في (فلم يلى ةباتكلا) ةغصي في رادصال اذه تللح. طاقتلال حشرم ديدحتل -f رايخال مدختسا، صرق فلم يلى 4.1.5.
- نكمي هنا، ةشاشلا يلع ةفيثكلا تانايبلا رورم ةكرح ةءابطل -a رايخال مادختسا دنع يلع تامولعمل ضرعل يئاقلتل فاقيلال ةدم نم ريثكب لوطا اتقو قرغتسي نا لوطا اتقو مكحتلا ةدحو يلى جارخال ضرع قرغتسي دق. رمالا يهتني يتح رظتنا. ةشاشلا مكحتلا ةدحو ضرعب ي صوي ال كلذل، SSH و Telnet جم انرب لال خ نم ريثكب.
- نكمي، "فيضملا ريغ" و "فيضملا" ةيفصتلا لماع ريبعت عم -f رايخال مادختسا دنع رورم ةكرح عم. VLAN رورم ةكرح و WCCP GRE نيمضت عم أطخال رورملا ةكرح طاقتلال مزحلا لخد يلى صأل IP ناو نع سي لو، يجارخال ناو نعلا طقف قيرفال يري، WCCP GRE لا ضبق يلى نا ريبعت حشرم -f لا لخد حاتملا ةملكلا "proto 47" لا تفضا. ةفلغملا "vlan" ةيساسالا ةملكلا فضا، VLAN رورم ةكرح، كلذ يلى ل ةفاضال ابو. رورم ةكرح حصي VLAN ةكبش تانايب رورم ةكرح ليحلحتب رمالا ل حامس لل -f ةيفصتلا لماع ريبعت في ححص لكشب.
- عقوتم ريغ لكشب زاوجل فقوتي دق، -R رايخ عم ةيفصتلا ل -a رايخ مادختسا دنع

