Quick Note 45

How to setup the Analyzer to get the IKE/IPsec trace from a Digi TransPort WR

Contents

1 INTRODUCTION

1.1 Outline

When a Digi TransPort WR router is configured to establish an IKE/IPsec connection with another peer, it is often useful, in particular when there are some issues in setting the VPN up, to get the packet trace of the IKE/IPsec negotiation from the device. This Quick Note explains how to configure the TransPort to correctly trace the IKE/IPsec traffic and it shows how to get the files from the device.

The router used in this Quick Note is the TransPort WR44 with ETH 0 as LAN interface and ETH 1 as WAN interface, so the IKE/IPsec trace will be taken on those interfaces, but it is valid also for other scenarios and the parameter that need to be changed is indicated later on.

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router.

This application note applies only to:

Model: DIGI TransPort WR11/21/41/44 with Enterprise firmware if applicable.

Firmware versions: 5169 and later

Configuration: This document assumes that the device has an IKE/IPSEC tunnel configured to a remote peer.

Please note: Please contact tech.support@digi.com if your require assistance in upgrading the firmware of the TransPort router.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com

Requests for new application notes can be sent to the same address.

1.4 Version

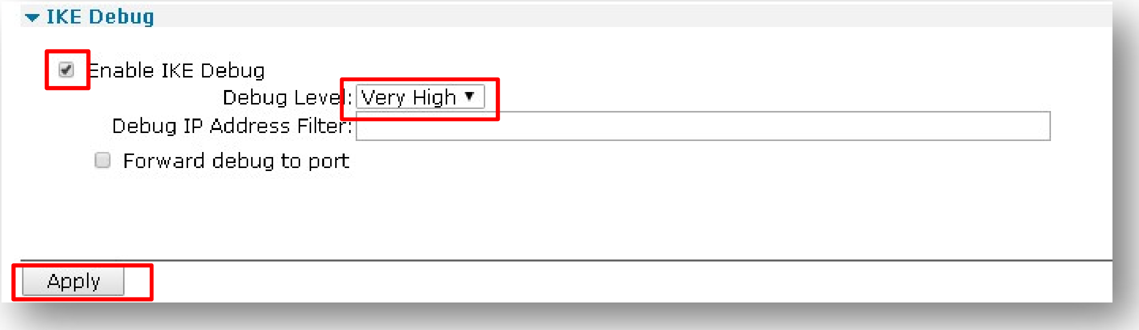
Version Number	Status
1	Published
1.1	Updated Branding and WEB GUIoverall revision and minor fixes (layout, font)

2 DIGI TRANSPORT WR CONFIGURATION

2.1 Enabling IKE debug

Navigate to the TransPort's Web UI that has been configured to setup an IKE/IPsec VPN, browse to the section and select the settings as follows:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE > IKE DEBUG



IKE Debug

☑ Enable IKE Debug

Debug Level: Very High ▼

Debug IP Address Filter:

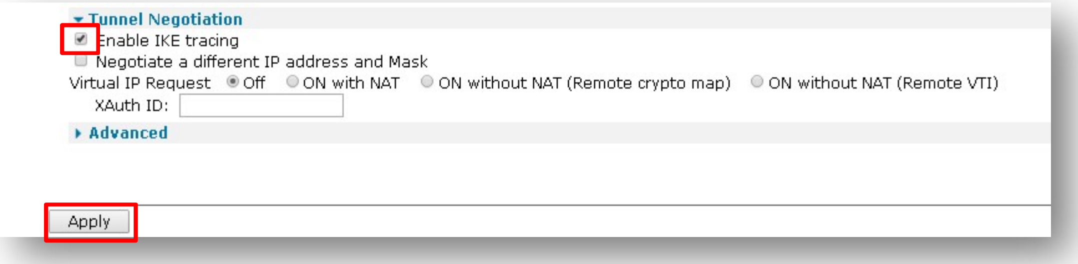
☐ Forward debug to port

Parameter	Setting	Description
Enable IKE Debug	Ticked	Enables IKE debugging to be displayed on the debug port.
Debug Level	Very High	Sets the highest level of IKE debugging

2.2 Enable IPsec tunnel Debug

It is recommended to enable also the debug on the specific Tunnel that needed to be monitored. For every IPSec Tunnel "x" you want to monitor, browse to the following section, enable IKE Tracing and apply. Following an example screenshot for Tunnel 0:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC X > TUNNEL NEGOTIATION



Tunnel Negotiation

☑ Enable IKE tracing

☐ Negotiate a different IP address and Mask

Virtual IP Request ● Off ○ ON with NAT ○ ON without NAT (Remote crypto map) ○ ON without NAT (Remote VTI)

XAuth ID:

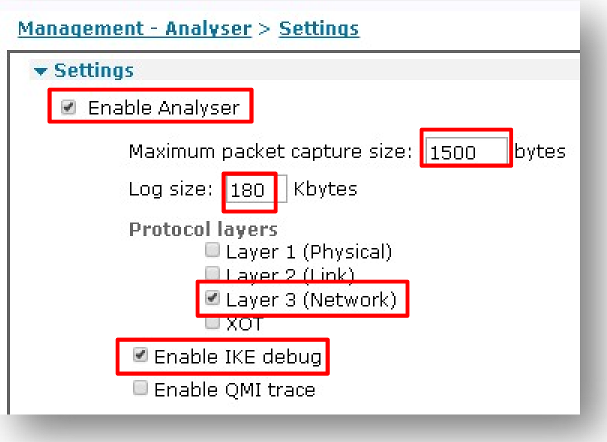
2.3 Configuring Analyser

2.3.1 Enabling Analyzer and basic settings

First of all, analyser needs to be enabled clicking on “Enable Analyser”, this will reveal the other settings.

When the other settings are revealed, configure the following settings (please refer for the table below for details:

MANAGEMENT - ANALYSER > SETTINGS



Management - Analyser > Settings

▾ Settings

☑ Enable Analyser

Maximum packet capture size: 1500 bytes

Log size: 180 Kbytes

Protocol layers

☐ Layer 1 (Physical)

☐ Layer 2 (Link)

☑ Layer 3 (Network)

☐ XOT

☑ Enable IKE debug

☐ Enable QMI trace

Parameter	Setting	Description
Enable Analyser	Ticked	Turn on the analyser
Max packet capture size	1500	Capture any packet up to 1500 Bytes
Log Size	180	The maximum size of the pseudo file “ana.txt” that is used to store the captured data packets. Once the maximum size is reached, the oldest captured data packets are overwritten when new packets are captured. The maximum value is 180 and it is the one recommended.
Protocol Layers > Layer 3 (Network)	Ticked	This setting specify that the Network Layer (Layer 3) protocol will be captured and included in the analyser trace
Enable IKE Debug	Ticked	Enable this setting in order to see IKE debug in the trace

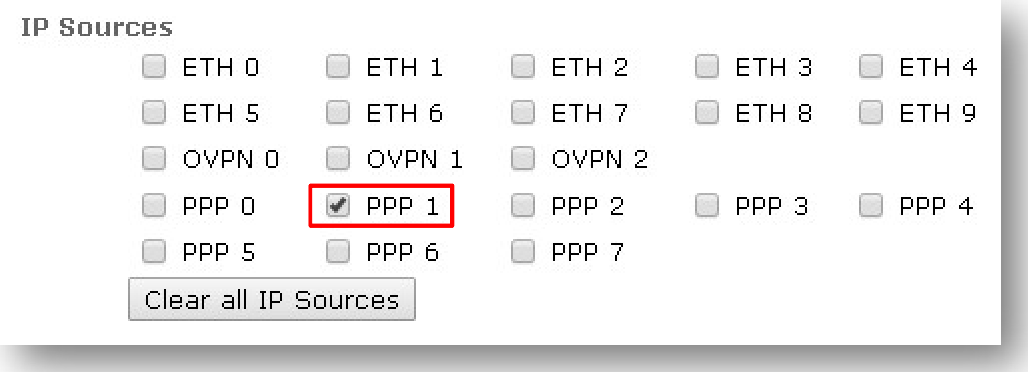
2.3.2 IP Source

This setting is used to select the source interfaces of IP packets to be captured and included in the analyser trace. As for the VPN troubleshooting in the IKE/IPsec packets exchanged between the two peers, the WAN interface should be selected as IP Source.

Following two example screenshot for the most common WAN interfaces used

MANAGEMENT - ANALYSER > SETTINGS

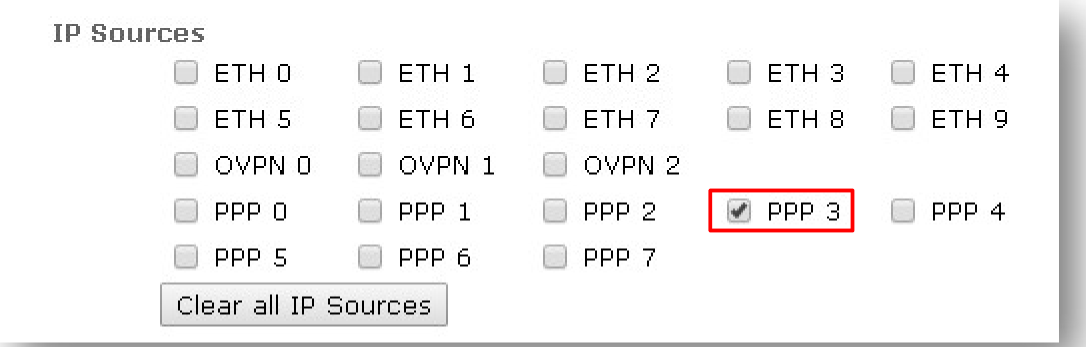
Cellular: If the cellular connection is used as WAN connection, the IP source should be set on "PPP 1":



IP Sources

☐ ETH 0	☐ ETH 1	☐ ETH 2	☐ ETH 3	☐ ETH 4
☐ ETH 5	☐ ETH 6	☐ ETH 7	☐ ETH 8	☐ ETH 9
☐ OVPN 0	☐ OVPN 1	☐ OVPN 2		
☐ PPP 0	☑ PPP 1	☐ PPP 2	☐ PPP 3	☐ PPP 4
☐ PPP 5	☐ PPP 6	☐ PPP 7		

DSL: IS the DSL is used as WAN connection, the IP source should be set on "PPP 3":



IP Sources

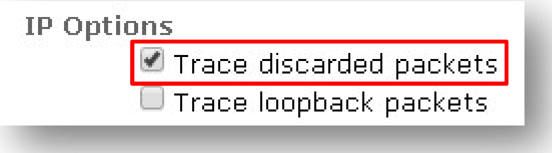
☐ ETH 0	☐ ETH 1	☐ ETH 2	☐ ETH 3	☐ ETH 4
☐ ETH 5	☐ ETH 6	☐ ETH 7	☐ ETH 8	☐ ETH 9
☐ OVPN 0	☐ OVPN 1	☐ OVPN 2		
☐ PPP 0	☐ PPP 1	☐ PPP 2	☑ PPP 3	☐ PPP 4
☐ PPP 5	☐ PPP 6	☐ PPP 7		

Please also note that if the WAN interface is one of the Ethernet interfaces (ETH x), the IP source should be set as "ETH x".

2.3.3 IP options

Under the IP options section, the “Trace discarded packets” should be enabled, in order to allow the capture of packets that are discarded by an interface along with a reason for why the packet was discarded. Enable this setting is useful in troubleshooting as it can shows that an IKE/IPsec packet is discarded for some reason.

MANAGEMENT - ANALYSER > SETTINGS



IP Options

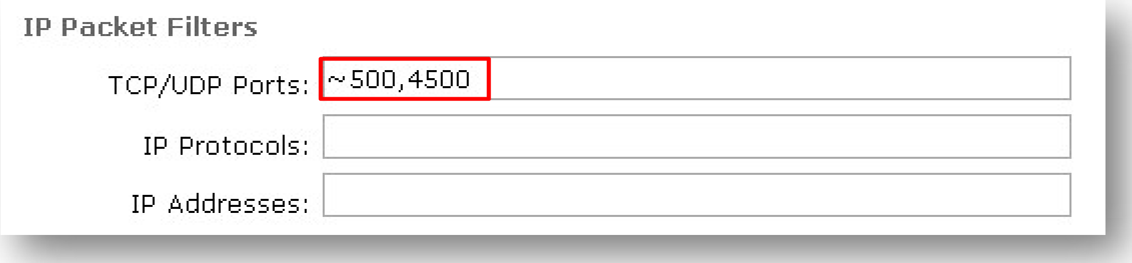
☑ Trace discarded packets

□ Trace loopback packets

2.3.4 IP Packet Filters

Under the IP Packet Filters section, the TCP/UDP Ports section should be configured in order to have only IKE (500) Float (4500) packets captured and included in the trace. The format of this parameter is a tilde (~) symbol followed by comma-separated list of port numbers you want to include in the trace. In our case this will be “~500,4500” as in the following screenshot:

MANAGEMENT - ANALYSER > SETTINGS



IP Packet Filters

TCP/UDP Ports: ~500,4500

IP Protocols:

IP Addresses:

Please note, that if you want to exclude the capture of certain TCP/UDP ports, the field should be filled only with the ports list, without the tilde (~) symbol.

3 CAPTURING THE TRAFFIC

In order to have the trace filled with significant traffic that permits to analyse issues in the IKE/IPsec negotiation phases, the capture of the traffic should be performed following the steps below:

3.1 Disabling the VPN to start negotiation

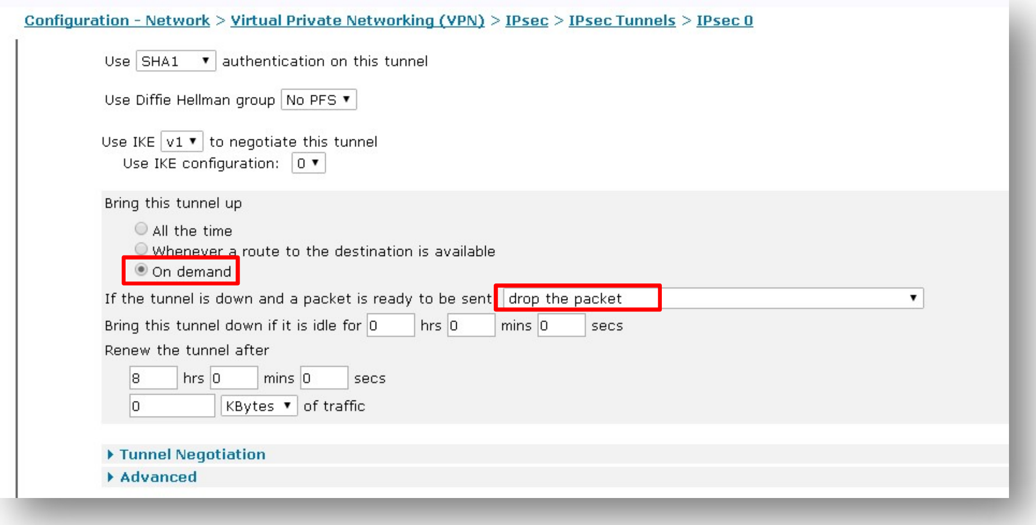
If the issue is about a VPN negotiation failure and the TransPort is the Initiator, configure the IPsec tunnel as NOT trying to go up

```
eroute x autosa 0
eroute x nosa drop
```

So for example, for tunnel 0 you should issue the command "eroute 0 autosa 0".

This can be also configured on WEB UI browsing, for every tunnel x you need to troubleshoot, and select "bring this tunnel up: on demand", as in the following example for Tunnel 0:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC X



Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0

Use SHA1 ▾ authentication on this tunnel

Use Diffie Hellman group No PFS ▾

Use IKE v1 ▾ to negotiate this tunnel
Use IKE configuration: 0 ▾

Bring this tunnel up

○ All the time
○ Whenever a route to the destination is available
● On demand

If the tunnel is down and a packet is ready to be sent drop the packet ▾

Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs

Renew the tunnel after

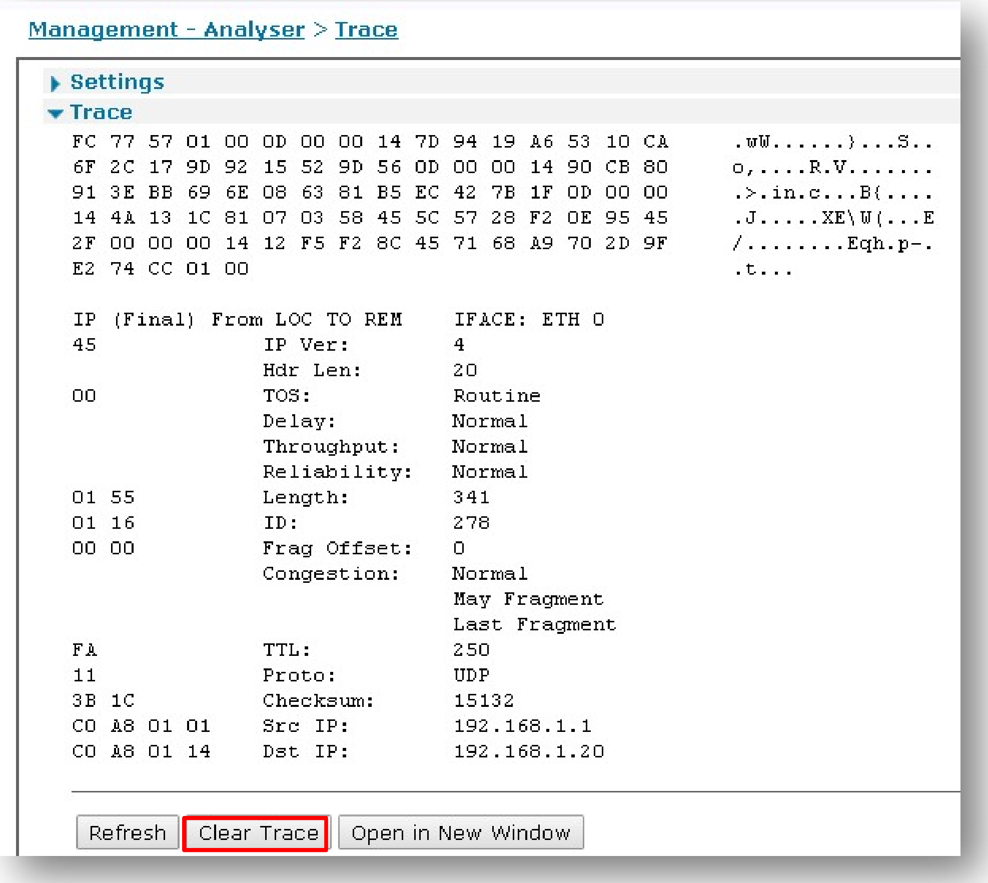
8 hrs 0 mins 0 secs
0 KBytes ▾ of traffic

Skip this step if the issue happens while the VPN is already up (for example VPN systematic disconnections for some reason and, after that, negotiation failures) or the TransPort is not the initiator of the IPsec tunnel.

3.2 Clear the trace

Clear the Trace to have an clear start:

MANAGEMENT - ANALYSER > TRACE



```
FC 77 57 01 00 0D 00 00 14 7D 94 19 A6 53 10 CA     .wW......}...S..
6F 2C 17 9D 92 15 52 9D 56 0D 00 00 14 90 CB 80     o,....R.V.......
91 3E BB 69 6E 08 63 81 B5 EC 42 7B 1F 0D 00 00     .>.in.c...B{....
14 4A 13 1C 81 07 03 58 45 5C 57 28 F2 0E 95 45     .J.....XE\W(...E
2F 00 00 00 14 12 F5 F2 8C 45 71 68 A9 70 2D 9F     /........Eqh.p-.
E2 74 CC 01 00                                      .t...

IP (Final) From LOC TO REM    IFACE: ETH 0
45              IP Ver:       4
                Hdr Len:      20
00              TOS:          Routine
                Delay:        Normal
                Throughput:   Normal
                Reliability:  Normal
01 55           Length:       341
01 16           ID:           278
00 00           Frag Offset:  0
                Congestion:   Normal
                              May Fragment
                              Last Fragment
FA              TTL:          250
11              Proto:        UDP
3B 1C           Checksum:     15132
C0 A8 01 01     Src IP:       192.168.1.1
C0 A8 01 14     Dst IP:       192.168.1.20
```

3.3 Trigger/Wait for the issue

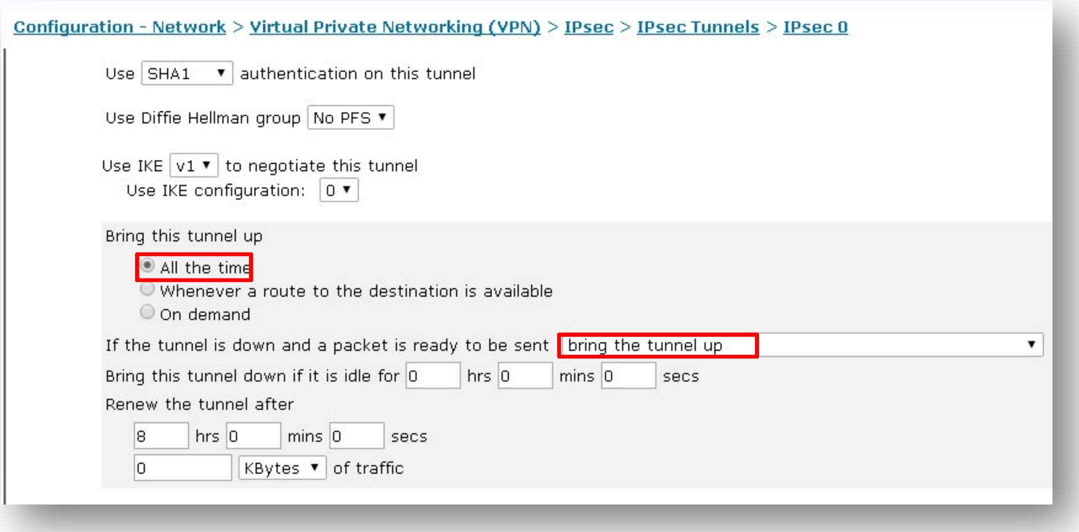
If the issue is about a VPN negotiation failure and the TransPort is the Initiator, configure the IPsec tunnel TO TRY to go UP, browsing to Administration - Execute a command and type one by one those command for every Tunnel “x” you need to troubleshoot:

```
eroute x autosa 2
eroute x nosa TRY
```

So for example, for tunnel 0 you should issue the command “eroute 0 autosa 2”.

This can be also configured on WEB UI browsing for every tunnel x you need to troubleshoot, and select “bring this tunnel up: All the time”, as in the following example for Tunnel 0:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC X



Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0

Use SHA1 ▾ authentication on this tunnel

Use Diffie Hellman group No PFS ▾

Use IKE v1 ▾ to negotiate this tunnel
Use IKE configuration: 0 ▾

Bring this tunnel up
● All the time
○ Whenever a route to the destination is available
○ On demand

If the tunnel is down and a packet is ready to be sent bring the tunnel up ▾
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 KBytes ▾ of traffic

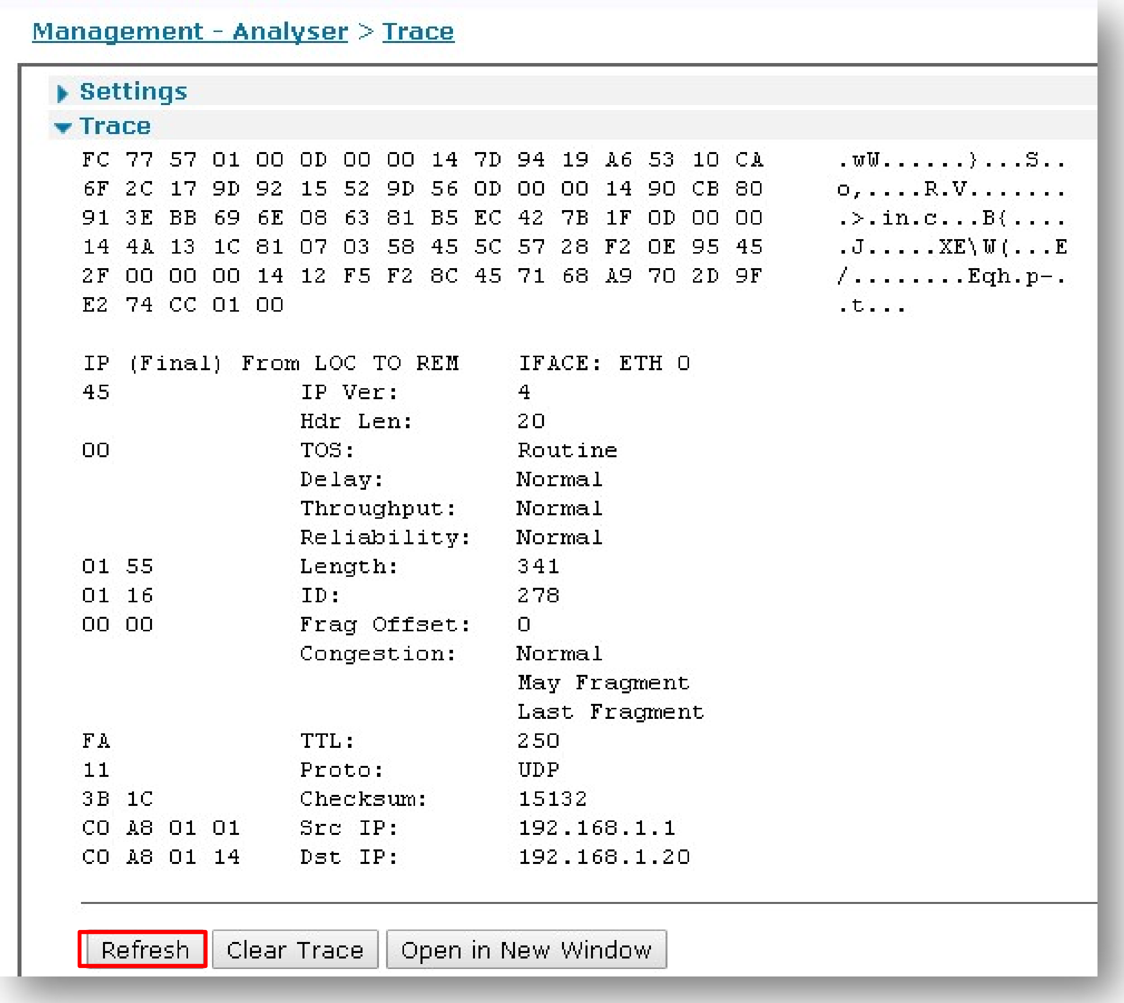
If there is some other event/action that triggers the issue, do that in order to reproduce it.

If, instead, the issue cannot be triggered (so it is an issue that occurs periodically but without any evident event causing it) wait for the issue to occur (for example if there is a VPN that, sometimes, goes down unexpectedly).

3.4 Refresh the trace

Refresh the trace to see the collected packets:

MANAGEMENT - ANALYSER > TRACE

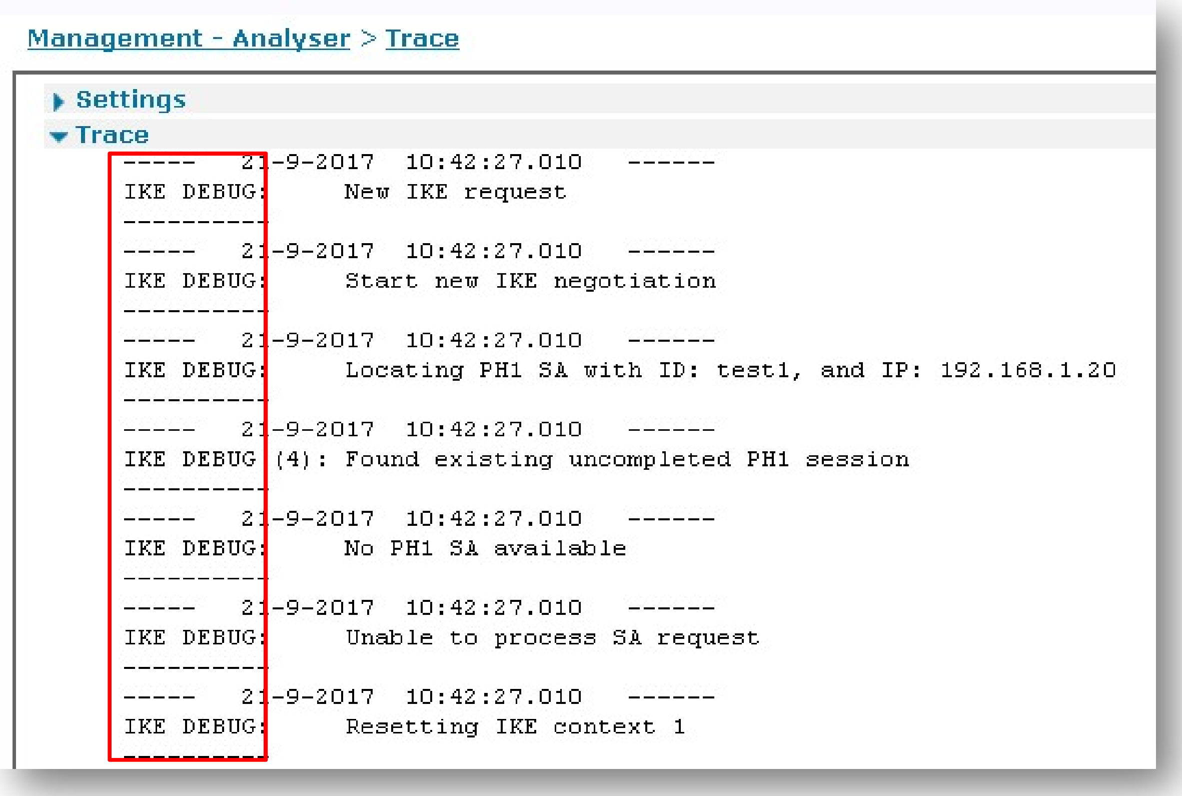


```
FC 77 57 01 00 0D 00 00 14 7D 94 19 A6 53 10 CA     .wW......}...S..
6F 2C 17 9D 92 15 52 9D 56 0D 00 00 14 90 CB 80     o,....R.V.......
91 3E BB 69 6E 08 63 81 B5 EC 42 7B 1F 0D 00 00     .>.in.c...B{....
14 4A 13 1C 81 07 03 58 45 5C 57 28 F2 0E 95 45     .J.....XE\W(...E
2F 00 00 00 14 12 F5 F2 8C 45 71 68 A9 70 2D 9F     /........Eqh.p-.
E2 74 CC 01 00                                      .t...

IP (Final) From LOC TO REM    IFACE: ETH 0
45              IP Ver:        4
                Hdr Len:       20
00              TOS:           Routine
                Delay:         Normal
                Throughput:    Normal
                Reliability:   Normal
01 55           Length:        341
01 16           ID:            278
00 00           Frag Offset:   0
                Congestion:    Normal
                               May Fragment
                               Last Fragment
FA              TTL:           250
11              Proto:         UDP
3B 1C           Checksum:      15132
C0 A8 01 01     Src IP:        192.168.1.1
C0 A8 01 14     Dst IP:        192.168.1.20
```

3.5 Check the trace

Once the trace is refreshed, check that it is valid for troubleshooting using the scroll bar in the trace window, you should see "IKE DEBUG" lines in it. Please find below an example of a valid IKE trace:



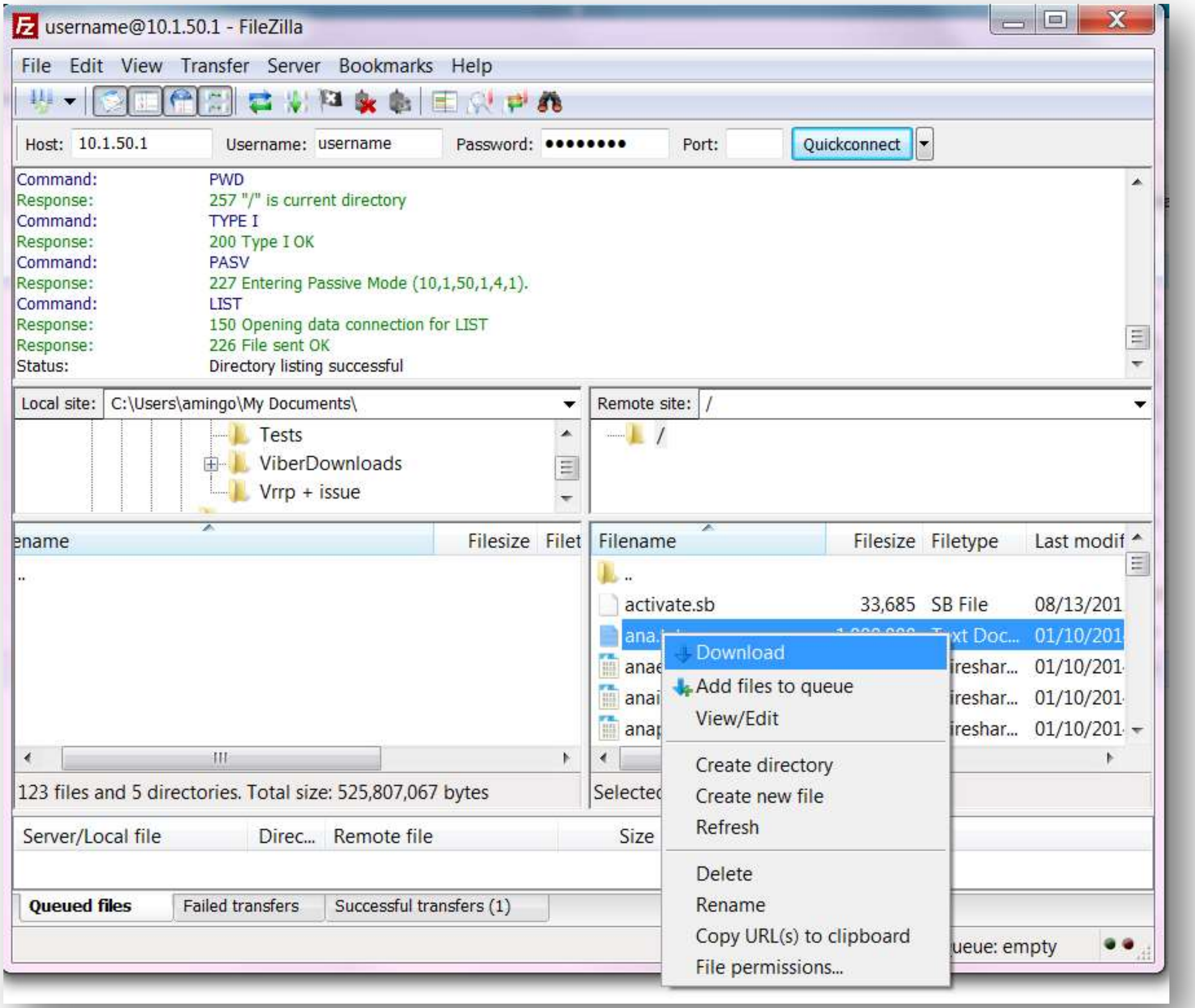
```
-----   21-9-2017  10:42:27.010   ------
IKE DEBUG:     New IKE request
----------
-----   21-9-2017  10:42:27.010   ------
IKE DEBUG:     Start new IKE negotiation
----------
-----   21-9-2017  10:42:27.010   ------
IKE DEBUG:     Locating PH1 SA with ID: test1, and IP: 192.168.1.20
----------
-----   21-9-2017  10:42:27.010   ------
IKE DEBUG (4): Found existing uncompleted PH1 session
----------
-----   21-9-2017  10:42:27.010   ------
IKE DEBUG:     No PH1 SA available
----------
-----   21-9-2017  10:42:27.010   ------
IKE DEBUG:     Unable to process SA request
----------
-----   21-9-2017  10:42:27.010   ------
IKE DEBUG:     Resetting IKE context 1
----------
```

If there are no IKE DEBUG lines in the refreshed trace, try to refresh again after some minutes or check that all the steps are executed correctly.

4 EXTRACTING THE ANA.TXT FILE

4.1 Extracting the file via FTP

Using Filezilla or similar FTP client, make an FTP connection to the router and download the “ana.txt” file to the PC:



username@10.1.50.1 - FileZilla

Host: 10.1.50.1 Username: username Password: •••••••• Port:

```
Command:    PWD
Response:   257 "/" is current directory
Command:    TYPE I
Response:   200 Type I OK
Command:    PASV
Response:   227 Entering Passive Mode (10,1,50,1,4,1).
Command:    LIST
Response:   150 Opening data connection for LIST
Response:   226 File sent OK
Status:     Directory listing successful
```

Local site: C:\Users\amingo\My Documents\

Tests
ViberDownloads
Vrrp + issue

Remote site: /

Filename	Filesize	Filetype	Last modif
..			
activate.sb	33,685	SB File	08/13/201
ana.		Text Doc...	01/10/201
anae		ireshar...	01/10/201
anai		ireshar...	01/10/201
anap		ireshar...	01/10/201

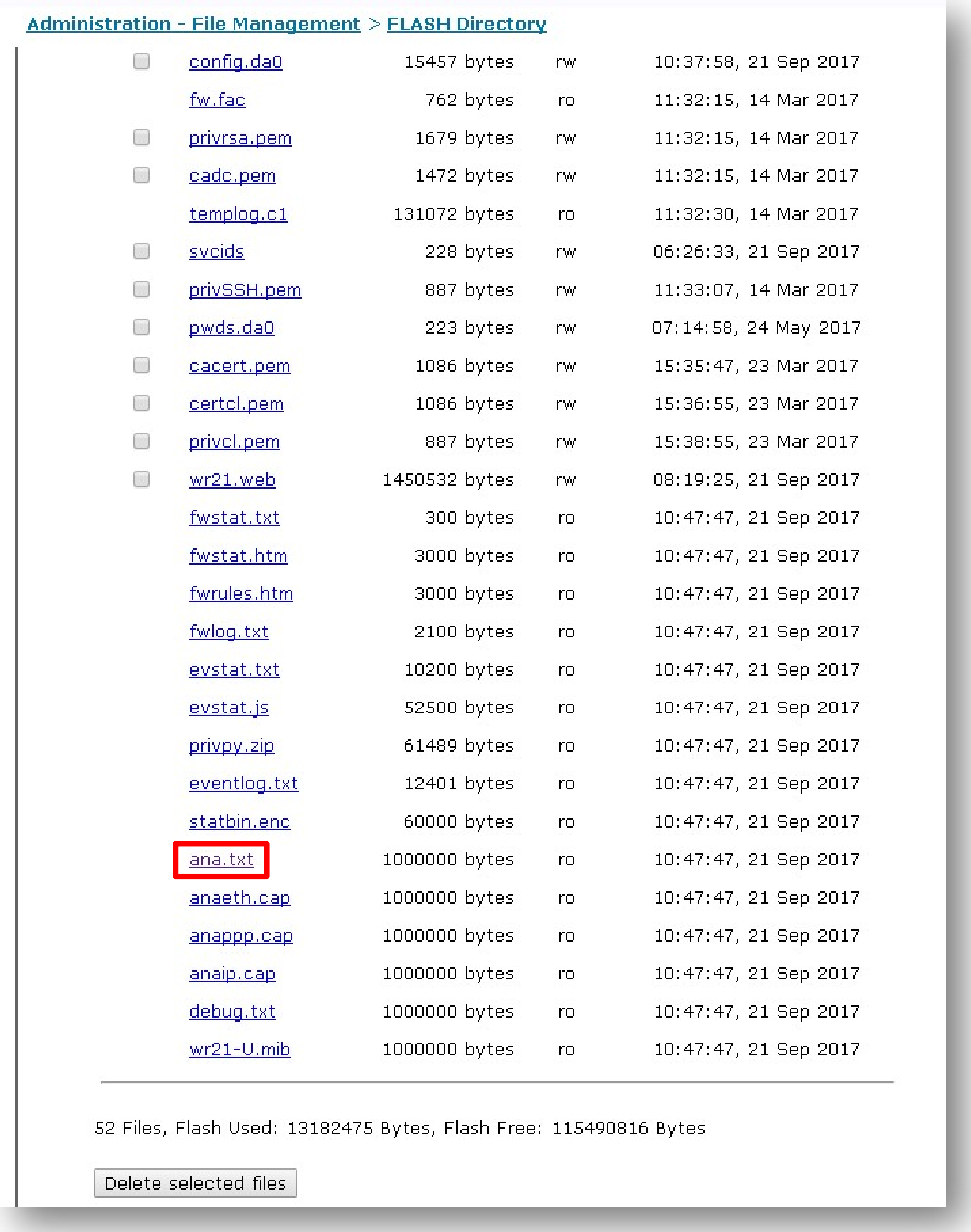
123 files and 5 directories. Total size: 525,807,067 bytes

4.2 Extracting the file via WEB UI

Administration - File Management > FLASH Directory

Browse to the router’s IP address.

Right click on “ana.txt”:

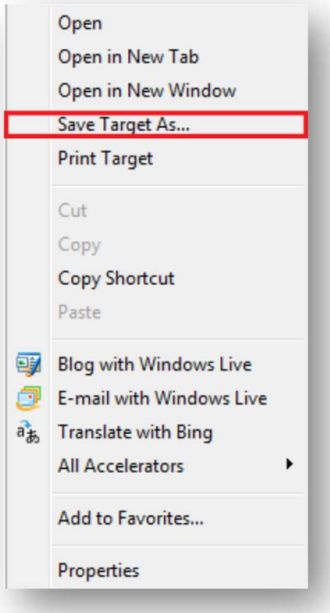


Administration - File Management > FLASH Directory

□	config.da0	15457 bytes	rw	10:37:58, 21 Sep 2017
	fw.fac	762 bytes	ro	11:32:15, 14 Mar 2017
□	privrsa.pem	1679 bytes	rw	11:32:15, 14 Mar 2017
□	cadc.pem	1472 bytes	rw	11:32:15, 14 Mar 2017
	templog.c1	131072 bytes	ro	11:32:30, 14 Mar 2017
□	svcids	228 bytes	rw	06:26:33, 21 Sep 2017
□	privSSH.pem	887 bytes	rw	11:33:07, 14 Mar 2017
□	pwds.da0	223 bytes	rw	07:14:58, 24 May 2017
□	cacert.pem	1086 bytes	rw	15:35:47, 23 Mar 2017
□	certcl.pem	1086 bytes	rw	15:36:55, 23 Mar 2017
□	privcl.pem	887 bytes	rw	15:38:55, 23 Mar 2017
□	wr21.web	1450532 bytes	rw	08:19:25, 21 Sep 2017
	fwstat.txt	300 bytes	ro	10:47:47, 21 Sep 2017
	fwstat.htm	3000 bytes	ro	10:47:47, 21 Sep 2017
	fwrules.htm	3000 bytes	ro	10:47:47, 21 Sep 2017
	fwlog.txt	2100 bytes	ro	10:47:47, 21 Sep 2017
	evstat.txt	10200 bytes	ro	10:47:47, 21 Sep 2017
	evstat.js	52500 bytes	ro	10:47:47, 21 Sep 2017
	privpy.zip	61489 bytes	ro	10:47:47, 21 Sep 2017
	eventlog.txt	12401 bytes	ro	10:47:47, 21 Sep 2017
	statbin.enc	60000 bytes	ro	10:47:47, 21 Sep 2017
	ana.txt	1000000 bytes	ro	10:47:47, 21 Sep 2017
	anaeth.cap	1000000 bytes	ro	10:47:47, 21 Sep 2017
	anappp.cap	1000000 bytes	ro	10:47:47, 21 Sep 2017
	anaip.cap	1000000 bytes	ro	10:47:47, 21 Sep 2017
	debug.txt	1000000 bytes	ro	10:47:47, 21 Sep 2017
	wr21-U.mib	1000000 bytes	ro	10:47:47, 21 Sep 2017

52 Files, Flash Used: 13182475 Bytes, Flash Free: 115490816 Bytes

Click “Save Target As”:

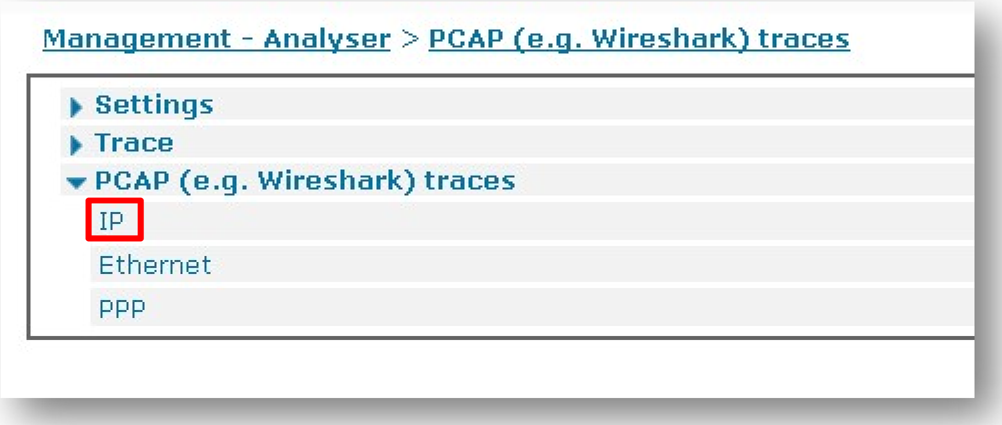


NOTE: In other browsers the menu may be slightly different, for example, Chrome uses “Save Link As”.

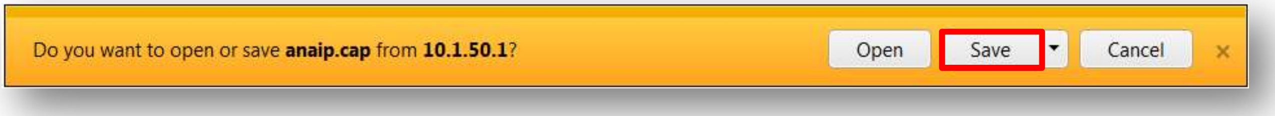
5 EXTRACTING THE PCAP FILES

Management - Analyser > PCAP (e.g. Wireshark) traces

It can be required to get also the PCAP files from the device. That files could be of four types: IP, ETH, PPP, and WIFI (if present). Depending on which is requested (usually is the IP one), browse to the section and left click on “IP” (or “PPP” or “ETH” if requested):


Management - Analyser > PCAP (e.g. Wireshark) traces
Settings
Trace
PCAP (e.g. Wireshark) traces
IP
Ethernet
PPP

The browser (in the example below is IE) will show up a window asking for save/open the PCAP file, click save in order to save the file on your PC:


Do you want to open or save **anaip.cap** from **10.1.50.1**?

6 CONFIGURATION FILE

This is the configuration used for the purpose of this Quick Note. The CLI commands relevant for the configuration of the IKE debug and Analyser settings are highlighted:

```
eth 0 IPaddr "10.1.63.254"
eth 0 ipanon ON
eth 1 IPaddr "10.1.50.1"
eth 1 ipsec 1
eth 1 ipanon ON
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
def_route 0 ll_ent "eth"
def_route 0 ll_add 1
eroute 0 peerip "10.1.50.2"
eroute 0 peerid "responder"
eroute 0 ourid "initiator"
eroute 0 locip "10.1.63.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "10.1.89.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "3DES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 debug ON
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
ppp 0 timeout 300
ppp 1 name "W-WAN (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 encalg "3DES"
ike 0 ikegroup 2
ike 0 deblevel 4
ike 0 delmode 1
modemcc 0 info_asy_add 6
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Your.APN.goes.here"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_replies OFF
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "none"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_interval_2 1
modemcc 0 sms_access_2 1
ana 0 anon ON
ana 0 l1on ON
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ipfilt "~500,4500"
ana 0 ikeon ON
ana 0 discardson ON
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 1
cmd 0 tremto 1200
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
user 10 name "10.1.50.2"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
idigi 0 ssl ON
idigi 0 sms_optin ON

Power Up Profile: 0
OK
```