

## 1. Purpose

The purpose of this document is to provide instructions in order to correctly configure and establish a VPN tunnel between a Digi Connect Wan 3G and a Digi Transport VC7400.

## 2. VPN Settings of the Digi Connect Wan 3G

### 2.1 Global Settings

Gener	ral Security Settings
	Enable Antireplay
Miscel	llaneous Settings
	Suppress SA lifetime during IKE phase 1
	Suppress Delete Phase 1 SA Message For PFS
	IP addresses of remote VPN peers may change on the fly (Dynamic DNS)



### 2.2 VPN Policy Settings

			juration							
	Description:	Transpo								
	VPN Tunnel:	ISAKMF			-					
Local Er	ndpoint Type:	Local e	ndpoint is a s	ubnet	1	r				
VPN Mo	de									
<ul> <li>Initia</li> </ul>	ate client connec	tions to a	and accept o	onnect	ions from t	he remot	e VPN de	evice at:		
9	4.194.32.202									
	pt connections fi	rom any V	/PN device							
Identity		-:								
	k Interface: mol									
✓ Neg	jotiate tunnel as	soon as	interrace co	mes up	)					
• Use	the following as	the iden	tity: dcwan3	Bg						
O Use	the interface IP	address								
🔿 Use	the identity certi	ificate X.5	i09 distingu	ished n	ame (DN)					
Local Er	ndpoint									
Tunnel I	Network Traffic f	rom the f	ollowing Loo	al Netv	work:					
	IP Address:	10.100.1.0	)							
S	ubnet Mask:	255.255.2	55.0							
Remote	e Endpoint									
	Network Traffic t	to the foll	owing Remo	te Net	work:					
		192.168.2	-							
s	ubnet Mask:	255.255.2								
Pre-Sha	ared Key Setting	S								
Use the	e following IP ad		DN, or usen	name fe	or the rem	ote VPN's	ID:			
Use the			DN, or usen	name fo	or the rem	ote VPN's	ID:			
Use the	e following IP ad vc7400	dress, FQ					ID:			
Use the	e following IP ad	dress, FQ					ID:			
Use the	e following IP ad vc7400 e following pre-sl	dress, FQ					ID:			
Use the Vse the	e following IP ad vc7400 e following pre-sl	dress, FQ hared ke					ID:			
Use the Use the ISAKM	e following IP add vc7400 e following pre-sl digivpn	dress, FQ hared ker ngs	/ to negotia				ID:			
Use the Use the ISAKMI Genera	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Settin	dress, FQ hared key ngs gs for Pha	/ to negotia				ID:			
Use the Use the ISAKMI Genera	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting	dress, FQ hared kee ngs gs for Pha s: Agg	v to negotia nse 1 rressive 💌	te IKE s			ID:			
Use the Use the ISAKMI Genera C	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfec	dress, FQ hared kee ngs gs for Pha s: Agg	v to negotia nse 1 rressive 💌	te IKE s			ID:			
Use the Use the ISAKMI Genera C NAT-T S	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfec	dress, FQ hared kee ngs gs for Pha s: Agg t Forward	v to negotia nse 1 rressive 🍸 d Secrecy (P	te IKE s			ID:			
Use the Use the ISAKMI Genera C NAT-T S	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfect Settings	dress, FQ hared ker ngs gs for Pha e: Agg et Forward	y to negotia nse 1 ressive y d Secrecy (P NAT-T)	te IKE s			ID:			
Use the Use the ISAKMI Genera C NAT-T S	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfect Settings I Enable NAT Tr Keep Alive	dress, FQ hared ker ngs gs for Pha :: Agg :t Forward raversal ( Interval:	y to negotia nse 1 ressive y d Secrecy (P NAT-T)	te IKE s			ID:			
Use the Use the ISAKMI Genera C NAT-T S	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Settling I Security Settling connection Mode Enable Perfect Settlings I Enable NAT Tr Keep Alive P Phase 1 Policies	dress, FQ hared ker ngs gs for Pha :: Agg tt Forward raversal ( Interval: s	y to negotia nse 1 rressive 👻 d Secrecy (P NAT-T) 20	te IKE s	security se	ttings:				
Use the Use the ISAKMI Genera C NAT-T S	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfect Settings I Enable NAT Tr Keep Alive	dress, FQ hared kee ngs gs for Pha est Forware raversal ( Interval: s	y to negotia nse 1 ressive y d Secrecy (P NAT-T)	FS)		ttings:	ID:	Diffie-Helli Group 5		l
Use the Use the Genera C NAT-T S	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting Connection Mode Enable Perfect Settings Cathering Length NAT Tr Keep Alive Phase 1 Policies Authentication	dress, FQ hared kee ngs gs for Pha est Forward raversal ( Interval: s on ey	v to negotia use 1 rressive 🖤 d Secrecy (P NAT-T) 20 Encryption	FS)	security se	ttings:	etime			remove
Use the Sector S	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Settin Security Setting Connection Mode Enable Perfect Settings Chable NAT Tr Keep Alive P hase 1 Policies Authenticatio Pre-Shared Keep	dress, FQ hared key ngs gs for Pha :: Agg tt Forward raversal ( Interval: s on ey / _ D	v to negotia use 1 rressive 🖤 d Secrecy (P NAT-T) 20 Encryption AES (256-bi	FS)	security se	SA Life 86400	etime ) secs	Group 5	R	
Use the State of State of State Stat	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfect Settings ✓ Enable NAT Tr Keep Alive Phase 1 Policies Authentication Pre-Shared Key	dress, FQ hared kee ngs gs for Pha :: Agg tt Forward raversal ( Interval: s on ay / _ D ngs	y to negotia nse 1 ressive y d Secrecy (P NAT-T) 20 Encryption AES (256-bi ES (64-bit)	FS)	security se	SA Life 86400	etime ) secs	Group 5	R	
Use the Use the Use the Use the Use the Ise the Ise Control Ise Co	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfect Settings ✓ Enable NAT Tr Keep Alive P Phase 1 Policies Authenticatio Pre-Shared Key P Phase 2 Setting	dress, FQ hared kee ngs gs for Pha :: Agg tt Forward raversal ( Interval: s on ay / _ D ngs	/ to negotia nse 1 ressive v d Secrecy (P NAT-T) 20 Encryption AES (256-bi ES (64-bit) ase 2	FS)	security se	SA Life 86400	etime ) secs	Group 5	R	
Use the Use the C C C C C C C C C C C C C C C C C C C	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Settlin I Security Settling Connection Mode Enable Perfect Settlings ✓ Enable NAT Tr Keep Alive P Phase 1 Policies P Phase 1 Policies P Phase 1 Policies Pre-Shared Key P Phase 2 Settlin I Security Settling Diffie-Hellman:	dress, FQ hared kee ngs gs for Pha :: Agg tt Forward raversal ( Interval: s on ay f _ D ngs gs for Pha Group E	/ to negotia nse 1 ressive v d Secrecy (P NAT-T) 20 Encryption AES (256-bi ES (64-bit) ase 2	FS)	security se	SA Life 86400	etime ) secs	Group 5	R	
Use the Use the C Use the C ISAKM P ISAKMP ISAKMP ISAKMP	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfect Connection Mode Enable Perfect Connection Mode Enable Perfect Connection Mode Perfect Connection Mode Phase 1 Policies Authenticatio Pre-Shared Key P Phase 2 Setting Offie-Hellman: P Phase 2 Policies	dress, FQ hared key ngs gs for Pha :: Agg tt Forward raversal ( Interval: s n raversal ( Interval: s n gs for Pha gs for Pha gs for Pha gs for Pha s	v to negotia nse 1 ressive v d Secrecy (P NAT-T) 20 NAT-T) 20 Encryption AES (256-bi ES (64-bit) ase 2 i v	FS)	security se	<b>SA Li</b> 86400 86400	etime ) secs secs	Group 5 Group 2	R	
Use the Use the C Use the C ISAKM P ISAKMP ISAKMP ISAKMP	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfect Connection Mode Enable Perfect Connection Mode Enable Perfect Connection Mode Phase 1 Policies P Phase 1 Policies Pre-Shared Key P Phase 2 Setting Security Setting Offici-Hellman: P Phase 2 Policies e following policies	dress, FQ hared ker ngs gs for Pha :: Agg tt Forward raversal ( Interval: s on ay / D D ngs gs for Pha gs for Pha gs for Pha gs for Pha gs for Pha s s s to neg	v to negotia ise 1 ressive v d Secrecy (P NAT-T) 20 Encryption AES (256-bi ES (64-bit) ise 2 i v otiate secur	FS)	Integrity MD5 MD5 SingsHigh	<b>SA Li</b> 86400 86400	etime ) secs secs	Group 5 Group 2	R	
Use the Use the C Use the C ISAKM P ISAKMP ISAKMP ISAKMP	e following IP add vc7400 e following pre-sl digivpn P Phase 1 Setting I Security Setting Connection Mode Enable Perfect Connection Mode Enable Perfect Connection Mode Enable Perfect Connection Mode Perfect Connection Mode Phase 1 Policies Authenticatio Pre-Shared Key P Phase 2 Setting Offie-Hellman: P Phase 2 Policies	dress, FQ hared key ags for Pha s for Pha raversal ( Interval: s ay y v D ags for Pha gs for Pha gs for Pha gs for pha gs s to neg Auth	v to negotia nse 1 ressive v d Secrecy (P NAT-T) 20 NAT-T) 20 Encryption AES (256-bi ES (64-bit) ase 2 i v	FS) FS)	security se	<b>SA Li</b> 86400 86400	etime ) secs ] secs ] secs	Group 5 Group 2	R	



# 3. Digi Transport VC7400 Settings



#### 3.1 VPN Settings

al Private Networking (VPN)		
iec IDeos Tunnols		
Psec Tunnels Psec Default Action		
IPsec Groups		
Dead Peer Detection (DPD)		
IKE		
▶ IKE Debug		
▼ IKE 0		
Use the following settings for negotiation		
Encryption: O None O DES O 3DES AES (128	oit) O AES (192 bit)	AES (256 bit)
Authentication:  None  Authentication:		(
Mode: @ Main @ Aggressive		
MODP Group for Phase 1: 5 (1536)		
MODP Group for Phase 2: 5 (1536)		
Renegotiate after 8 hrs 0 mins 0 secs		
Advanced		
▶ IPsec Tunnels	<u>esponder</u>	
	<u>esponder</u>	
	<u>esponder</u>	
<ul> <li>&gt; IPsec Tunnels</li> <li>&gt; IPsec Default Action</li> <li>&gt; IPsec Groups</li> </ul>	esponder	
) IPsec Tunnels ) IPsec Default Action ) IPsec Groups ) Dead Peer Detection (DPD)	esponder	
<ul> <li>▶ IPsec Tunnels</li> <li>▶ IPsec Groups</li> <li>▶ Dead Peer Detection (DPD)</li> <li>▼ IKE</li> </ul>	esponder	
) IPsec Tunnels ) IPsec Default Action ) IPsec Groups ) Dead Peer Detection (DPD)	esponder	
<ul> <li>&gt; IPsec Tunnels</li> <li>&gt; IPsec Default Action</li> <li>&gt; IPsec Groups</li> <li>&gt; Dead Peer Detection (DPD)</li> <li>&gt; KE</li> <li>&gt; IKE Debug</li> </ul>	esponder	
<ul> <li>&gt; IPsec Tunnels</li> <li>&gt; IPsec Groups</li> <li>&gt; Dead Peer Detection (DPD)</li> <li>&gt; IKE</li> <li>&gt; IKE 0</li> <li>&gt; IKE 1</li> <li>&gt; IKE 2</li> </ul>	esponder	
<ul> <li>▶ IPsec Default Action</li> <li>▶ IPsec Default Action</li> <li>▶ IPsec Groups</li> <li>▶ Dead Peer Detection (DPD)</li> <li>▼ IKE</li> <li>▶ IKE Debug</li> <li>▶ IKE 0</li> <li>▶ IKE 1</li> <li>▶ IKE 2</li> <li>▶ IKE 3</li> </ul>	esponder	
<ul> <li>) IPsec Tunnels</li> <li>&gt; IPsec Default Action</li> <li>&gt; IPsec Groups</li> <li>&gt; Dead Peer Detection (DPD)</li> <li>&gt; IKE</li> <li>&gt; IKE Debug</li> <li>&gt; IKE 0</li> <li>&gt; IKE 1</li> <li>&gt; IKE 2</li> <li>&gt; IKE 3</li> <li>&gt; IKE 4</li> </ul>	esponder	
<ul> <li>&gt; IPsec Tunnels</li> <li>&gt; IPsec Groups</li> <li>&gt; Dead Peer Detection (DPD)</li> <li>&gt; IKE</li> <li>&gt; IKE 0</li> <li>&gt; IKE 1</li> <li>&gt; IKE 2</li> <li>&gt; IKE 3</li> <li>&gt; IKE 4</li> <li>&gt; IKE 5</li> </ul>	esponder	
<ul> <li>) IPsec Tunnels</li> <li>&gt; IPsec Default Action</li> <li>&gt; IPsec Groups</li> <li>&gt; Dead Peer Detection (DPD)</li> <li>&gt; IKE</li> <li>&gt; IKE Debug</li> <li>&gt; IKE 0</li> <li>&gt; IKE 1</li> <li>&gt; IKE 2</li> <li>&gt; IKE 3</li> <li>&gt; IKE 4</li> </ul>	esponder	
<ul> <li>&gt; IPsec Tunnels</li> <li>&gt; IPsec Groups</li> <li>&gt; Dead Peer Detection (DPD)</li> <li>&gt; IKE</li> <li>&gt; IKE Debug</li> <li>&gt; IKE 0</li> <li>&gt; IKE 1</li> <li>&gt; IKE 2</li> <li>&gt; IKE 3</li> <li>&gt; IKE 4</li> <li>&gt; IKE 5</li> <li>&gt; IKE 6</li> <li>&gt; IKE 7</li> <li>&gt; IKE 8</li> </ul>	esponder	
<pre>&gt; IPsec Tunnels &gt; IPsec Default Action &gt; IPsec Groups &gt; Dead Peer Detection (DPD)</pre>	esponder	
) IPsec Tunnels ) IPsec Default Action ) IPsec Groups > Dead Peer Detection (DPD) <b>IKE</b> > IKE Debug > IKE 1 > IKE 1 > IKE 2 > IKE 3 > IKE 4 > IKE 5 > IKE 5 > IKE 6 > IKE 7 > IKE 8 > IKE 8 > IKE 9 > IKE 8 > IKE 8 > IKE 9 > IKE 8	esponder	
<pre>&gt; IPsec Tunnels &gt; IPsec Default Action &gt; IPsec Groups &gt; Dead Peer Detection (DPD)</pre>	esponder	
) IPsec Tunnels ) IPsec Default Action ) IPsec Groups > Dead Peer Detection (DPD) * IKE > IKE Debug > IKE 0 > IKE 1 > IKE 1 > IKE 2 > IKE 3 > IKE 4 > IKE 5 > IKE 6 > IKE 7 > IKE 8 > IKE 8 > IKE 9 > IKE 9 > IKE 8 > IKE 9 > IKE 8 > IKE 9 > IKE 8 > IKE 9 > IKE 9 > IKE 8 > IKE 9 > IKE 8 > IKE 9 > IKE 9 > IKE 8 > IKE 9 > IKE 8 > IKE 9 > IKE 8 > IKE 9	esponder	
<ul> <li>IPsec Tunnels</li> <li>IPsec Default Action</li> <li>IPsec Groups</li> <li>Dead Peer Detection (DPD)</li> <li>IKE</li> <li>IKE Debug</li> <li>IKE 0</li> <li>IKE 1</li> <li>IKE 1</li> <li>IKE 2</li> <li>IKE 3</li> <li>IKE 4</li> <li>IKE 5</li> <li>IKE 6</li> <li>IKE 7</li> <li>IKE 8</li> <li>IKE 9</li> <li>IKE 8</li> <li>IKE 9</li> <li>IKE 9</li></ul>		✓ AES (256 bit)
> IPsec Tunnels > IPsec Default Action > IPsec Groups > Dead Peer Detection (DPD) ▼ IKE > IKE Debug > IKE 0 > IKE 1 > IKE 1 > IKE 2 > IKE 3 > IKE 4 > IKE 5 > IKE 6 > IKE 6 > IKE 7 > IKE 8 > IKE 9 ▼ IKE Responder ✓ Accept IKE Requests with		☑ AES (256 bit)
<ul> <li>JPsec Tunnels</li> <li>JPsec Default Action</li> <li>JPsec Groups</li> <li>Dead Peer Detection (DPD)</li> <li>TKE</li> <li>IKE Debug</li> <li>IKE 0</li> <li>IKE 1</li> <li>IKE 2</li> <li>IKE 3</li> <li>IKE 3</li> <li>IKE 4</li> <li>IKE 5</li> <li>IKE 6</li> <li>IKE 6</li> <li>IKE 6</li> <li>IKE 8</li> <li>IKE 9</li> <li>TKE Reguests with Accept IKE Requests with Encryption: Des U aces (128)</li> </ul>		☑ AES (256 bit)
) IPsec Tunnels ) IPsec Default Action ) IPsec Groups > Dead Peer Detection (DPD) / IKE > IKE Debug > IKE 1 > IKE 1 > IKE 2 > IKE 3 > IKE 4 > IKE 5 > IKE 6 > IKE 7 > IKE 8 > IKE 8 > IKE 9 ✓ IKE Responder ✓ Cept IKE Requests with Encryption: ⑦ DES ⑦ 2DES ⑦ AES (128 Authentication: ⑦ MD5 ⑦ SHA1 MODP Group between: 1(758) ♥ and \$ 5(1536) ♥	bit) 🛛 AES (192 bit)	⊠AES (256 bit)
IPsec Tunnels IPsec Default Action IPsec Groups Dead Peer Detection (DPD) IKE IKE Debug IKE 1 IKE 1 IKE 2 IKE 3 IKE 4 IKE 5 IKE 6 IKE 7 IKE 8 IKE 8 IKE 9 KE Responder ZE Enable IKE Requests with Encryption: ♥ DES ♥ 3DES ♥ AES (128 Authentication: ♥ MD5 ♥ SHA1 MODP Group between: 1(768) ♥ and 5(1536) ♥ Renegotiate after ⓐ hrs 0 mins 0 secs		I AES (256 bit)
) IPsec Default Action ) IPsec Groups > Dead Peer Detection (DPD) > IKE > IKE Debug > IKE 1 > IKE 1 > IKE 2 > IKE 3 > IKE 4 > IKE 5 > IKE 6 > IKE 7 > IKE 8 > IKE 8 > IKE 8 > IKE 8 > IKE Responder Accept IKE Requests with Encryption: ♥ DES ♥ 2DES ♥ AES (128 Authentication: ♥ MD5 ♥ SHA1 MODP Group between: 1(758) ♥ and \$ 5(1556) ♥	bit) 🛛 AES (192 bit)	🛛 AES (256 bit)



Configuration - Network > Virtual Private Networking (VPN) > IPs	<u>ec &gt; IPsec Tunnels &gt; IPsec 0 - 9</u> > <u>IPsec 0</u>
▼ IPsec 0	
Description: vc7400	
The IP address or hostname of the remote unit	
Use	as a backup unit
ose	as a backup unic
Local LAN R	emote LAN
Ose these settings for the local LAN	Ose these settings for the remote LAN
IP Address: 192.168.252.0	IP Address: 10.100.1.0
Mask: 255.255.255.0	Mask: 255.255.255.0
🔘 Use interface PPP 🖵 0	Remote Subnet ID:
Use the following security on this tunnel Off  Preshared Keys  XAUTH Init Preshar	ed Keys 🔘 RSA Signatures 🔘 XALITH Init RSA
Our ID: vc7400	
	N 🖲 User FQDN 💿 IPv4 Address
Remote ID: dcwan3g	
Kentote ID. adwanbg	
Use AES (256 bit keys) 💌 encryption on this tunnel	
Use MD5 💌 authentication on this tunnel	
Use Diffie Hellman group 5	
Use IKE vi v to negotiate this tunnel Use IKE configuration: 0 v	
Bring this tunnel up	
<ul> <li>All the time</li> </ul>	
Whenever a route to the destination is availal On demand	ble
If the tunnel is down and a packet is ready to be ser	nt 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 v of traffic	
o Noyces 💌 of claime	
iguration - Network > <u>Virtual Private Networking (VPN) &gt; IPse</u>	ec > IPsec Default Action
Interfaces     Ethermot	
Ethernet     GRE	
> Serial	
Advanced	

Ethernet	
▶ GRE	
▶ Serial	
Advanced	
DHCP Server	
Network Services	
DNS Servers	
Dynamic DNS	
IP Routing/Forwarding	
<ul> <li>Virtual Private Networking (VPN)</li> </ul>	
▼ IPsec	
IPsec Tunnels	
▼ IPsec Default Action	
When a packet is received which does not match	any IPsec tunnel
<ul> <li>Pass the packet</li> <li>Drop the packet</li> </ul>	
When a packet is to be transmitted which does r	not match any IPsec tunnel
Pass the packet Drop the packet	$\triangleright$
Apply	



Configuration - Security	y > <u>Users</u> > <u>User 0 - 9</u> > <u>User 8</u>
User 3	
User 4	
User 5	
User 6	
User 7	
▼ User 8	
► Advanced	Username: dcwan3g I Password: ••••••• Confirm Password: •••••• Access Level: Super 💌
Advanced	

Note : username = remote identity , password = preshared-key

# 4. VPN Connection Status and Debug

4.1 Digi Connect Wan 3G Status

	ctions Mana	(VPN) Connections		
Action	Description	Remote Address	Local Address	Status
	Transport	94.194.32.202	80.187.240.163	Connected

4.2 Digi Transport VC7400 Status

<u>Management</u>	- Connecti	ons >	• <u>Virtual Pr</u> i	vate Netw	orking (VPN)	) >	• <u>IPs</u>	<u>ec</u> >	<u>IPsec</u>	c Tunne	<u>els</u> >	<u>IPse</u>	c Tunne	<u>ls 0 - 9</u>	> <u>IPsec</u>	Tunnel	<u>5 0 - 9</u>
▶ IP Conn	ections																
► PPP Cor	nnections	;															
▼ Virtual	Private N	etwo	rking (VPN	I)													
▼ IPse	C																
▼ IP:	sec Tunne	els															
-	IPsec Tur	nels	0 - 9														
	▼ IPsec 1	Funne	els 0 - 9														
	Outbour	d V1 S	As														
	SPI	Eroute	Peer IP	Rem. selector	Loc. selector	АН	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface				
	cd5b0baf	0	80.187.240.163	10.100.1.0/24	192.168.252.0/24	N/A	MD5	AES (256)	N/A	0	0	23576	ETH 5				
	Remov	e All															
	Inbound	V1 SA	s														
	SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	Auth	ESP Enc	IPCOMP	KBytes Delivered	KByte: Left	s Time Left	Interface				
	8c2c64d5	0	80.187.240.163	10.100.1.0/24	192.168.252.0/24	N//	A MD5	AES (256)	N/A	0	0	23576	ETH 5				
	Remov	e All															
	Refres	h															



4.3 Transport Debug Settings

<u>Management - Analyser</u> > <u>Settings</u>
▼ Settings
Enable Analyser
Maximum packet capture size: 1500 bytes
Log size: 180 Kbytes
Protocol layers Layer 1 (Physical) Layer 2 (Link) Variable Layer 3 (Network) XOT
🗹 Enable IKE debug