



# Digi Cellular VPN

## VPN Tunnel between Connect Wan 3G and Transport VC7400

---

### 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

The screenshot shows a configuration page for VPN Global Settings. It is divided into three sections: VPN Global Settings, General Security Settings, and Miscellaneous Settings. The 'Enable Antireplay' checkbox is unchecked. In the 'Miscellaneous Settings' section, 'Suppress SA lifetime during IKE phase 1' is unchecked, 'Suppress Delete Phase 1 SA Message For PFS' is checked, and 'IP addresses of remote VPN peers may change on the fly (Dynamic DNS)' is unchecked. An 'Apply' button is located at the bottom left of the configuration area.

▼ VPN Global Settings

General Security Settings

- Enable Antireplay

Miscellaneous 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)

Apply



# Digi Cellular VPN

## VPN Tunnel between Connect Wan 3G and Transport VC7400

### 2.2 VPN Policy Settings

#### VPN - Tunnel #1 - Configuration

Description:

VPN Tunnel:

Local Endpoint Type:

#### VPN Mode

Initiate client connections to and accept connections from the remote VPN device at:

Accept connections from any VPN device

#### Identity

Network Interface:

Negotiate tunnel as soon as interface comes up

Use the following as the identity:

Use the interface IP address

Use the identity certificate X.509 distinguished name (DN)

#### Local Endpoint

Tunnel Network Traffic from the following Local Network:

IP Address:

Subnet Mask:

#### Remote Endpoint

Tunnel Network Traffic to the following Remote Network:

IP Address:

Subnet Mask:

#### Pre-Shared Key Settings

Use the following IP address, FQDN, or username for the remote VPN's ID:

Use the following pre-shared key to negotiate IKE security settings:

#### ISAKMP Phase 1 Settings

##### General Security Settings for Phase 1

Connection Mode:

Enable Perfect Forward Secrecy (PFS)

#### NAT-T Settings

Enable NAT Traversal (NAT-T)

Keep Alive Interval:

#### ISAKMP Phase 1 Policies

Authentication	Encryption	Integrity	SA Lifetime	Diffie-Hellman	
Pre-Shared Key	AES (256-bit)	MD5	86400 secs	Group 5	Remove
Pre-Shared Key	DES (64-bit)	MD5	86400 secs	Group 2	Add

#### ISAKMP Phase 2 Settings

##### General Security Settings for Phase 2

Diffie-Hellman:

#### ISAKMP Phase 2 Policies

Use the following policies to negotiate security settings --Highest priority listed last:

Encryption	Authentication	SA Lifetime	
AES (256-bit)	MD5	28200 secs	Remove
None	None	28200 secs	Add



# Digi Cellular VPN

## VPN Tunnel between Connect Wan 3G and Transport VC7400

### 3. Digi Transport VC7400 Settings



#### 3.1 VPN Settings

**Configuration - VPN > IPsec > IKE > IKE 0**

**Configure: IKE 0 (Initiator)**

Encryption algorithm:	AES
Encryption key bits (AES only):	256
Authentication algorithm:	MD5
Duration (s):	28800
Aggressive mode:	<input type="checkbox"/>
Dead Peer Detection:	<input type="checkbox"/>
IKE MODP group:	5 (1536)
Minimum IPsec MODP group:	No PFS
RSA private key file:	
Maximum re-transmits:	2
Re-transmit interval (s):	10
Inactivity timeout (s):	30
Send INITIAL-CONTACT notifications:	<input type="checkbox"/>
Retain phase 1 SA after phase 2 negotiation failure:	<input type="checkbox"/>
NAT traversal enabled:	<input checked="" type="checkbox"/>
SA removal mode:	Normal

**Configuration - VPN > IPsec > IKE > Responder**

**Configure: IKE 0 (Responder)**

Act as initiator only:	<input type="checkbox"/>
Acceptable encryption algorithms:	AES,DES,3DES
Minimum Encryption key bits (AES only):	256
Acceptable authentication algorithms:	MD5,SHA1
Minimum acceptable IKE MODP group:	5 (1536)
Maximum acceptable IKE MODP group:	5 (1536)
Duration (s):	28800
Inactivity timeout (s):	30
Send INITIAL-CONTACT notifications:	<input type="checkbox"/>
Send RESPONDER-LIFETIME notifications:	<input type="checkbox"/>
Retain phase 1 SA after phase 2 negotiation failure:	<input type="checkbox"/>
NAT traversal enabled:	<input checked="" type="checkbox"/>
RSA private key file:	
SA removal mode:	Normal
Use debug port:	<input type="checkbox"/>
Debug level:	Very High
Debug IP address filter:	



# Digi Cellular VPN

## VPN Tunnel between Connect Wan 3G and Transport VC7400

**Configuration - VPN > IPsec > IPsec Eroutes > Eroute 0 - 9 > Eroute 0**

**Configure: IPsec EROUTE 0**

Description:	vc7400
Peer IP/hostname:	
Backup peer IP:	
Peer ID:	dcwan3g
Our ID:	vc7400
XAUTH ID:	
RSA private key file:	
Our ID type:	User FQDN
Interface to use for local subnet IP address:	None 0
Local subnet IP address:	192.168.252.0
Local subnet mask:	255.255.255.0
Local subnet IP address to negotiate (if different from above):	
Local subnet mask to negotiate (if different from above):	
Negotiate virtual local IP address using MODECFG (initiators only):	<input type="checkbox"/>
Remote subnet IP address:	10.100.1.0
Remote subnet mask:	255.255.255.0
Remote subnet ID:	
Local port:	0
Remote port:	0
TX packets with these TOS values through this eroute:	
First local port (IKEv2 only):	0
Last local port (IKEv2 only):	65535
First remote port (IKEv2 only):	0
Last remote port (IKEv2 only):	65535
Mode:	Tunnel
AH authentication algorithm:	Off
ESP authentication algorithm:	MD5
ESP encryption algorithm:	AES (Recommended)
ESP encrypt key length (bits):	256
IPCOMP algorithm:	Off
IPsec MODP group:	No PFS
IP protocol:	Off
Duration (s):	28800
Duration (kb):	0
Inactivity Timeout (s):	0
No SA action:	Drop Packet
Create SA's automatically:	No
Go out of service if automatic establishment fails:	<input type="checkbox"/>
Disconnect interface after this many consecutive auto-negotiation failures:	0
Authentication method:	Preshared Keys
This eroute is tunnelled within another eroute:	<input type="checkbox"/>
NAT traversal keep-alive interval (s):	20
Link eroute with interface:	Any 0
IKE config to use when initiator:	0
IKE version:	1
Use Secondary IP address as source address:	<input type="checkbox"/>
Get source address from this interface:	N/A 5
Delete SAs when eroute goes out of service:	<input type="checkbox"/>
Inhibit this eroute when these eroutes are not OOS:	
Inhibit unless this eroute is UP:	
Delete SAs if not VRRP Master:	<input type="checkbox"/>
Display IKE lookup debug info:	<input checked="" type="checkbox"/>

OK Cancel



# Digi Cellular VPN

## VPN Tunnel between Connect Wan 3G and Transport VC7400

---

**Configuration - VPN > IPsec > IPsec Eroutes > Default Eroute**

**Configure: Default IPsec Eroute**

No inbound SA action:

No outbound SA action:

**Configuration - Security > Users > User 0 - 9 > User 8**

**Configure: User 8**

Name:

Password:

Confirm Password:

Alternate Key:

Confirm Alternate Key:

Access Level:

Remote peer address:

Remote subnet address:

Remote subnet mask:

Dialback number:

Public Key file:

DUN access enabled:

Web page display mode:

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



# Digi Cellular VPN

## VPN Tunnel between Connect Wan 3G and Transport VC7400

### 4. VPN Connection Status and Debug

#### 4.1 Digi Connect Wan 3G Status

Connections Management				
Virtual Private Network (VPN) Connections				
Action	Description	Remote Address	Local Address	Status
<input type="checkbox"/>	Transport	94.194.32.202	80.187.240.163	Connected

Refresh    Disable

#### 4.2 Digi Transport VC7400 Status

**Diagnostics - Status > IPsec > IPsec SAs > Eroute 0 - 9 > View 0 - 9**

IPsec Status: Eroutes 0 -> 9

**Outbound V1 SAs**

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	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

Remove All

**Inbound V1 SAs**

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	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

Remove All

#### 4.3 Transport Debug Settings

**Diagnostics - Analyser > Settings**

Configure: Analyser

Analyser:

Protocol layers:

- Layer 1 (physical)
- Layer 2 (link)
- Layer 3 (network)
- XOT (link)

IKE:

- IKE debug