Digi Cellular VPN

Setup of a VPN Tunnel between Digi and Sarian

1. VPN Settings of the Digi

1.1 Global Settings

1 .2 VPN Policy Settings

VPN - Tunnel #1 - Configuration

Description: Tunnel 1
Remote VPN Address: 217.91.93.51
VPN Tunnel: ISAKMP
Local Endpoint Type: Local endpoint is a subnet

Identity

Network Interface: mobile0
☑ Negotiate tunnel as soon as interface comes up

◉ Use the following as the identity: pohl@digi.com
○ 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: 10.49.2.0
Subnet Mask: 255.255.255.0

Remote Endpoint

Tunnel Network Traffic to the following Remote Network:
IP Address: 192.168.96.0
Subnet Mask: 255.255.240.0

Pre-Shared Key Settings

Use the following IP address, FQDN, or username for the remote VPN's ID:
217.91.93.51

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

ISAKMP Phase 1 Settings

General Security Settings for Phase 1

Connection Mode: Aggressive
☑ Enable Perfect Forward Secrecy (PFS)

NAT-T Settings

☐ Enable NAT Traversal (NAT-T)
Keep Alive Interval: 20

ISAKMP Phase 1 Policies

Authentication	Encryption	Integrity	SA Lifetime	Diffie-Hellman	
Pre-Shared Key	AES (256-bit)	SHA1	250 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: Group 5

ISAKMP Phase 2 Policies

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

Encryption	Authentication	SA Lifetime	
AES (256-bit)	SHA1	150 secs	Remove
None	None	28200 secs	Add

2. Sarian Settings

2.1 Configure DSL

Operations -> Configure -> DSL -> ADSL

Configure: ADSL 0

Enabled:	Yes
Operational mode:	Multi-mode
Firmware from 'dspfw.bin':	No
Watchdog:	On

Operations -> Configure -> DSL -> ATM PVCs -> PVC 0

Configure: ATM PVC 0

Enabled:	Yes
Encapsulation:	PPPoE LLC
Bridge mode:	No
Bridged ports:	☐ ETH 0
	☐ ETH 1
	☐ ETH 2
	☐ ETH 3
VPI:	1
VCI:	32
Service category:	UBR
Peak cell rate (cells/sec):	0
Sustained cell rate (cells/sec):	0
Maximum burst size (cells):	0
ATM PVC analysis:	Off

Operations -> Configure -> PPP -> PPP 0 – 4 -> PPP 1 -> Standard

Configure: PPP 1 (Standard)

Name:	Digi-DO
IP Analysis:	On
PPP Analysis:	Off
Answering:	Off
Metric:	1
Calling number:	
MSN:	
Sub-address:	
CLI:	
Remote access options:	No restrictions
Dial-out prefix:	
Dial-out number:	
Dial-out number #2:	
Dial-out number #3:	
Dial-out number #4:	
Use GPRS/external modem:	No
Detach GPRS on link failure:	No
Detach GPRS between connection attempts:	No
GPRS SIM:	Any
Username:	feste-ip/6TBXV6HR057J@t-online-
Password (Assigned):	
Confirm password:	
AODI NUA:	
Always on mode:	On
AODI delay (s):	0
AODI delay when other PPPs inhibited by this one are connected (s):	0
Power up AODI delay (s):	0
Go out of service if first AODI connections fail:	No
DNS server:	
Multi-link:	Off
Inactivity timeout (s):	0
Inactivity timeout #2 (s):	0
RX packet Inactivity timeout (s):	0
Traffic activation inactivity timeout (s):	0
Minimum link up-time (s):	0
Maximum link up-time (s):	0
Maximum negotiation time (s):	80
Firewall:	Off
IGMP:	Off
IPSec:	ON-Remove SAs when link down

QOS:	Off
RIP version:	Off
RIP destination IP address list:	
RIP authentication method:	Access list
Only send RIP when interface is in service:	No
DEFLATE compression:	Off
MPPE encryption:	Off
MPPE key size:	Auto
Time band:	
Log event up-time (mins):	0
Max up-time per day (mins):	0
Local IP address:	0.0.0.0
Remote IP address pool minimum:	10.10.10.0
Remote IP address pool range:	5
Remote network address:	0.0.0.0
Remote network mask:	255.255.255.255
NAT mode:	NAT
NAT source IP address:	

OK Cancel

2.2 VPN Settings

Operations -> Configure -> IPSec -> IKE -> IKE0

Configure: IKE 0 (Initiator)

Encryption algorithm:	AES
Encryption key bits (AES only):	256
Authentication algorithm:	SHA1
Duration (s):	86400
Aggressive mode:	On
Dead Peer Detection:	On
IKE MODP group:	5 (1536)
Minimum IPSec MODP group:	5 (1536)
RSA private key file:	
Maximum re-transmits:	2
Re-transmit interval (s):	10
Inactivity timeout (s):	30
Send INITIAL-CONTACT notifications:	Yes
NAT traversal enabled:	No
NAT traversal keep-alive interval (s):	20
SA removal mode:	Remove IKE SA when last IPsec SA removed
Use debug port:	No
Debug level:	Very High

Operations -> Configure -> IPSec -> IKE -> Reponder

Configure: IKE 0 (Responder)

Act as initiator only:	No
Acceptable encryption algorithms:	AES
Minimum Encryption key bits (AES only):	256
Acceptable authentication algorithms:	SHA1
Minimum acceptable IKE MODP group:	5 (1536)
Maximum acceptable IKE MODP group:	5 (1536)
Duration (s):	86400
Inactivity timeout (s):	30
Send INITIAL-CONTACT notifications:	Yes
Send RESPONDER-LIFETIME notifications:	Yes
NAT traversal enabled:	No
NAT traversal keep-alive interval (s):	20
RSA private key file:	
SA removal mode:	Remove IKE SA when last IPsec SA removed
Use debug port:	No
Debug level:	Very High

Operations -> Configure -> IPSec -> IPSec Eroutes -> Eroutes 0 – 9 -> Eroute 0

Configure: IPSec EROUTE 0

Description:	Digi-DO
Peer IP/hostname:	
Backup peer IP:	
Peer ID:	pohl@digi.com
Our ID:	
XAUTH ID:	
RSA private key file:	
Send our ID as FQDN:	No
Interface to use for local subnet IP address:	None
Interface # to use for local subnet IP address:	0
Local subnet IP address:	192.168.96.0
Local subnet mask:	255.255.240.0
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):	No
Remote subnet IP address:	10.49.2.0
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:	SHA1
ESP encryption algorithm:	AES
ESP encrypt key length (bits):	256
IPCOMP algorithm:	Off
IPSec MODP group:	5 (1536)
IP protocol:	Off
Duration (s):	86400
Duration (kb):	1000000
Inactivity Timeout (s):	0
No SA action:	Use IKE
Create SA's automatically:	No
Go out of service if automatic establishment fails:	No
Authentication method:	Preshared Keys
This eroute is tunnelled within another eroute:	No

NAT traversal keep-alive interval (s):	20
Link eroute with interface:	Any
Link eroute with interface #:	0
IKE config to use when initiator:	0
IKE version:	1
Check APN usage:	No
Interface must use this APN:	Main APN
Use Secondary IP address as source address:	No
Get source address from this interface:	N/A
Get source address from this interface #:	0
Delete SAs when eroute goes out of service:	No
Inhibit this eroute when these eroutes are not OOS:	
Inhibit unless this eroute is UP:	
Delete SAs if not VRRP Master:	No
Display IKE lookup debug info:	Yes

Operations -> Configure -> IPSec -> IPSec Eroutes -> Default Eroute

Configure: Default IPSec Eroute

No inbound SA action:	pass packet
No outbound SA action:	pass packet

OK Cancel

Operations -> Configure -> Users -> Users 0 – 9 -> User 8

Operations -> Configure -> Users -> Users 0 – 9 -> User 9

3. VPN Connection Status and Debug

3.1 Digi Status

Connections Management

Virtual Private Network (VPN) Connections

Action	Description	Remote Address	Local Address	Status
☐	Tunnel 1	217.91.93.51	80.187.234.81	Connected

3.2 Sarian Status

Operations -> Status -> IPSec -> IPSec SAs -> Eroute 0 – 9 -> Eroute 0

IPSec Status: Eroutes 0 -> 0

Outbound V1 SAs

SPI	Eroute	Peer IP	Rem. IP	Rem. Mask	Loc. IP	Loc. Mask	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KByte Left
fffafb01	0	80.187.234.81	10.49.2.0	255.255.255.0	192.168.96.0	255.255.240.0	N/A	SHA1	AES (256)	N/A	0	10000

Remove All

Inbound V1 SAs

SPI	Eroute	Peer IP	Rem. IP	Rem. Mask	Loc. IP	Loc. Mask	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBy Le
e835c153	0	80.187.234.81	10.49.2.0	255.255.255.0	192.168.96.0	255.255.240.0	N/A	SHA1	AES (256)	N/A	0	1000

Remove All

3.3 Sarian Debug Settings

Operations -> Configure -> Analyser