Application Note 73

How to configure Automatic Failover between two IPsec tunnels on Digi Transport WR Routers

September 2020

Contents

1 Introduction 4

1.1 Outline 4

1.2 Assumptions 4

1.3 Corrections 5

1.4 Version 5

2 Primary Responder Configuration 6

2.1 WAN interface configuration 6

2.2 Local Ethernet Interface configuration 7

2.3 IPsec configuration 8

2.3.1 IPsec Tunnel 8

2.3.2 IKE settings 10

2.3.3 Pre-Shared Key configuration 11

3 Backup Responder Configuration 12

3.1 WAN interface configuration 12

3.2 Local Ethernet Interface configuration 13

3.3 IPsec configuration 14

3.3.1 IPsec Tunnel 14

3.3.2 IKE settings 16

3.3.3 Pre-Shared Key configuration 17

4 Initiator Configuration 18

4.1 WAN Interface configuration 18

4.2 Local Ethernet Interface configuration 19

4.3 IPsec configuration 20

4.3.1 IPsec Tunnel to Primary Responder 20

4.3.2 IPsec Tunnel to Secondary Responder 25

5 Testing The Automatic Failover Between IPsec tunnels 30

5.1 Failure on the primary tunnel (OOS) 30

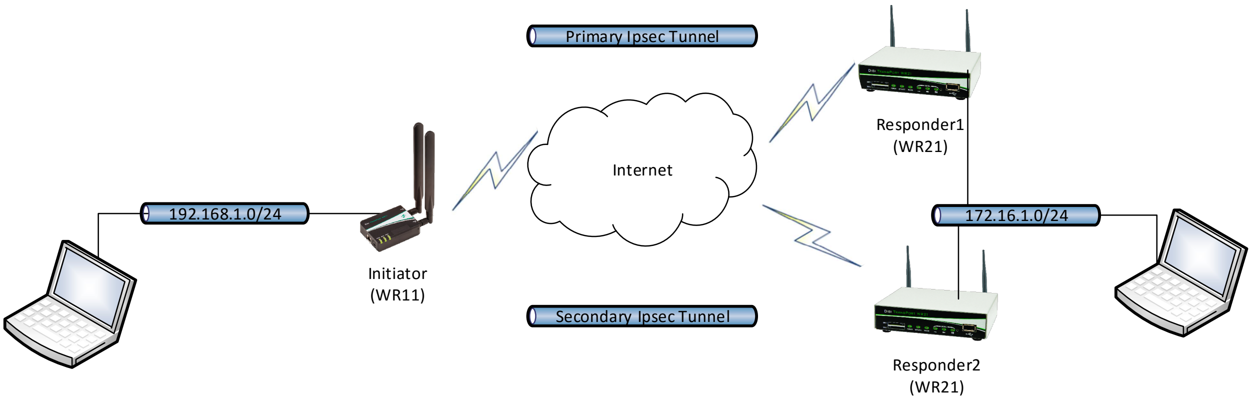
5.2 Failover on Secondary Tunnel 30
5.3 Restore of Primary Tunnel 31
6 CONFIGURATION FILE 32
6.1 Primary Responder Configuration 32
6.2 Backup Responder Configuration 34
6.3 Initiator Configuration 36

1 INTRODUCTION

1.1 Outline

In some IPsec VPN scenarios, it can be useful to have a backup tunnel to failover in case of issues on the primary one, with automatic recovery on the primary once the issue is solved.

This document will describe how to configure this automatic failover between IPsec tunnels, considering the following scenario:



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 and configure it with basic routing functions.

This application note applies to:

Model: Digi Transport WR21 and WR11

Other Compatible Models: All Digi WR Transport models (SarOS)

Firmware versions: 5.077 and later

Configuration: This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

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

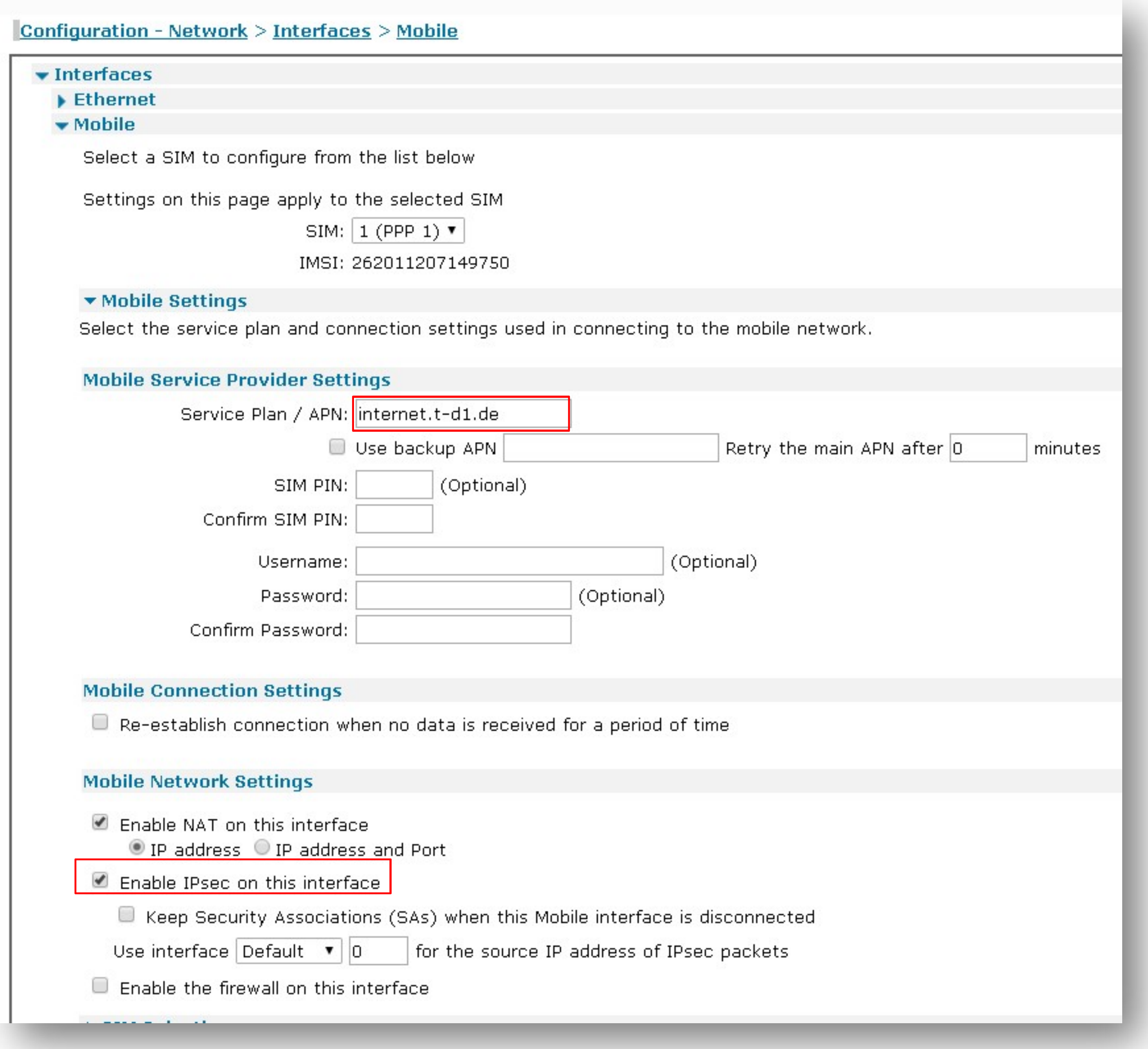
Version Number	Status
1.0	Published (October 2017)
1.1	Added date, corrected links, minor fix (September 2020)

2 PRIMARY RESPONDER CONFIGURATION

2.1 WAN interface configuration

In this example the primary responder has the Mobile interface as the WAN interface and it is configured as follows:

CONFIGURATION - NETWORK > INTERFACES > MOBILE



Configuration - Network > Interfaces > Mobile

▼ Interfaces

▶ Ethernet

▼ Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1) ▾

IMSI: 262011207149750

▼ Mobile Settings

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

Service Plan / APN: internet.t-d1.de

☐ Use backup APN Retry the main APN after 0 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Mobile Connection Settings

☐ Re-establish connection when no data is received for a period of time

Mobile Network Settings

☑ Enable NAT on this interface

● IP address ○ IP address and Port

☑ Enable IPsec on this interface

☐ Keep Security Associations (SAs) when this Mobile interface is disconnected

Use interface Default ▾ 0 for the source IP address of IPsec packets

☐ Enable the firewall on this interface

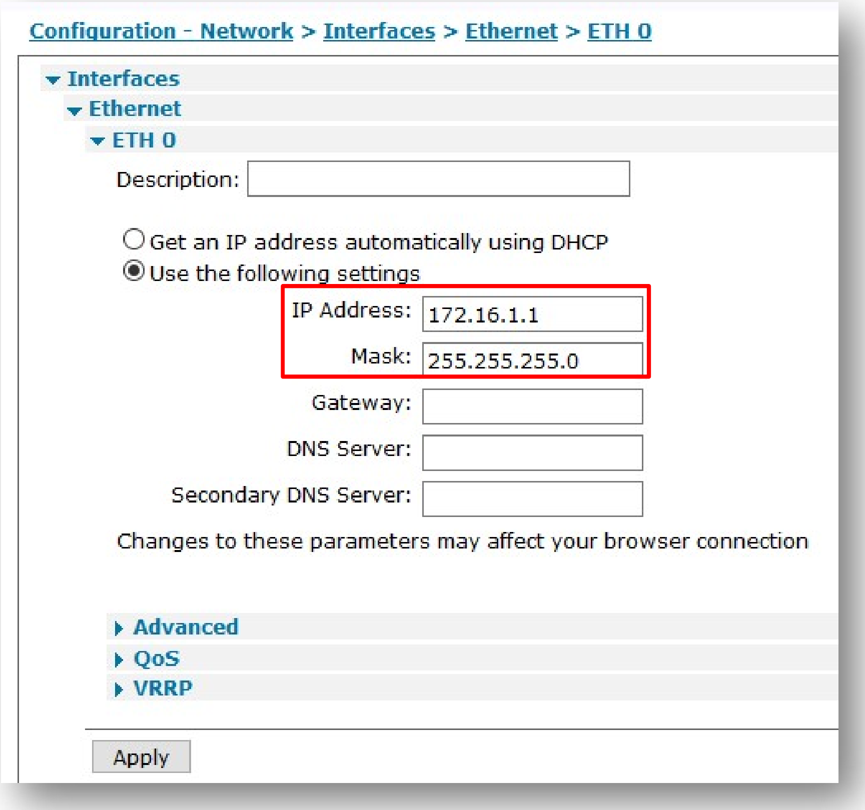
Please note: Depending on provider, a SIM PIN or Username/Password may be required. If needed, enter them in the appropriate fields.

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
Enable IPSec on this interface	✓	Enable IPSec on PPP 1 interface

2.2 Local Ethernet Interface configuration

In this example, the LAN interface is configured with a static address as follows:

CONFIGURATION - NETWORK > INTERFACES > ETHERNET > ETH 0



Configuration - Network > Interfaces > Ethernet > ETH 0

Description:

○ Get an IP address automatically using DHCP
● Use the following settings

IP Address: 172.16.1.1
Mask: 255.255.255.0
Gateway:
DNS Server:
Secondary DNS Server:

Changes to these parameters may affect your browser connection

Parameter	Setting	Description
IP Address	172.16.1.1	Enter the IP address of the LAN interface for the router
Mask	255.255.255.0	Enter the subnet mask

2.3 IPsec configuration

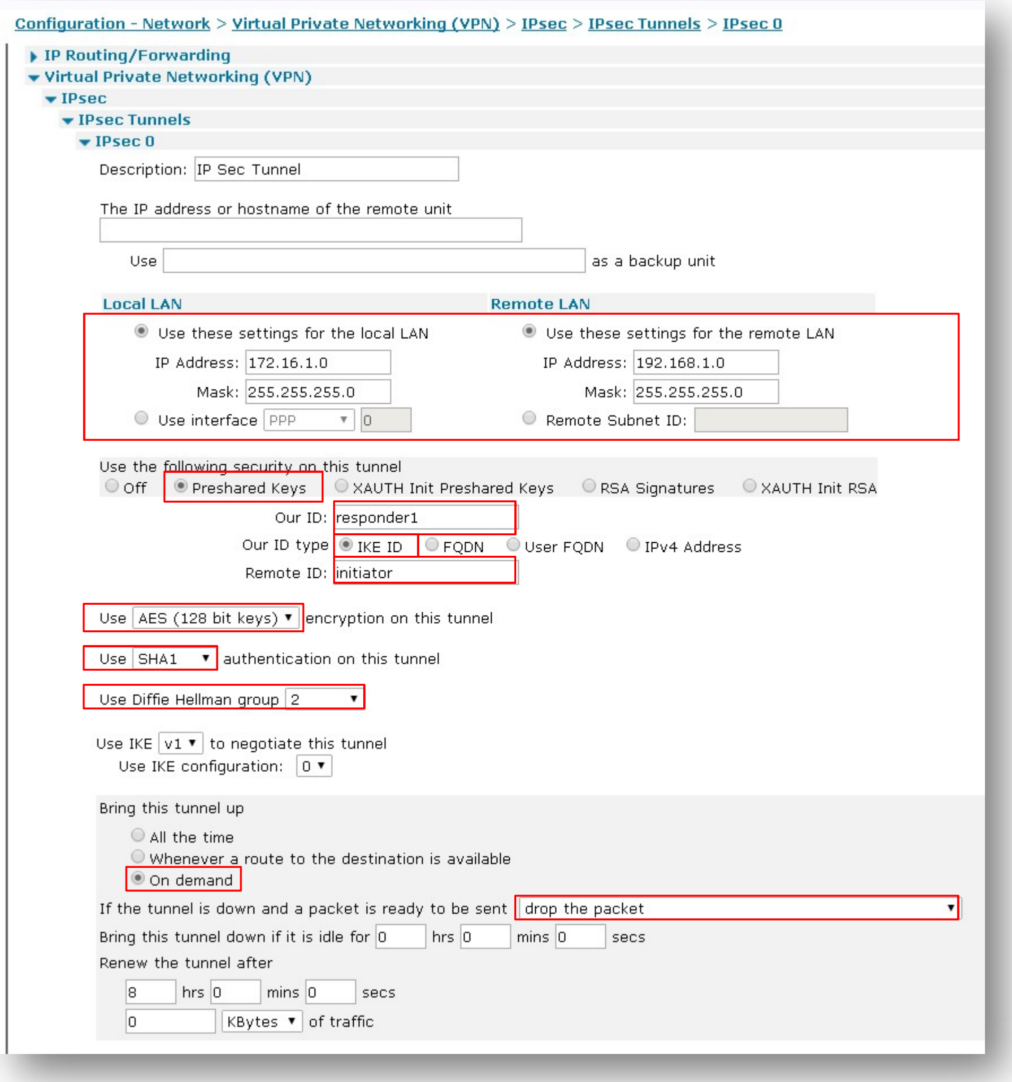
Note: Here will be shown a summary of the configuration on the primary responder, as it is not the main focus of this document. For details about those settings, please check the Application Note:

AN10 - IPSec over Cellular using Digi TransPort Routers with Pre-Shared key authentication.

2.3.1 IPsec Tunnel

The IPsec tunnel is configured as site to site and with Preshared Key using IKE ID. As it is a responder, It is set to be brought up only on demand (so when receive a request from the initiator):

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0



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

▸ IP Routing/Forwarding
▾ Virtual Private Networking (VPN)
▾ IPsec
▾ IPsec Tunnels
▾ IPsec 0

Description: IP Sec Tunnel

The IP address or hostname of the remote unit

Use as a backup unit

Local LAN

● Use these settings for the local LAN
IP Address: 172.16.1.0
Mask: 255.255.255.0
○ Use interface PPP ▾ 0

Remote LAN

● Use these settings for the remote LAN
IP Address: 192.168.1.0
Mask: 255.255.255.0
○ Remote Subnet ID:

Use the following security on this tunnel
○ Off ● Preshared Keys ○ XAUTH Init Preshared Keys ○ RSA Signatures ○ XAUTH Init RSA
Our ID: responder1
Our ID type ● IKE ID ○ FQDN ○ User FQDN ○ IPv4 Address
Remote ID: initiator

Use AES (128 bit keys) ▾ encryption on this tunnel

Use SHA1 ▾ authentication on this tunnel

Use Diffie Hellman group 2 ▾

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

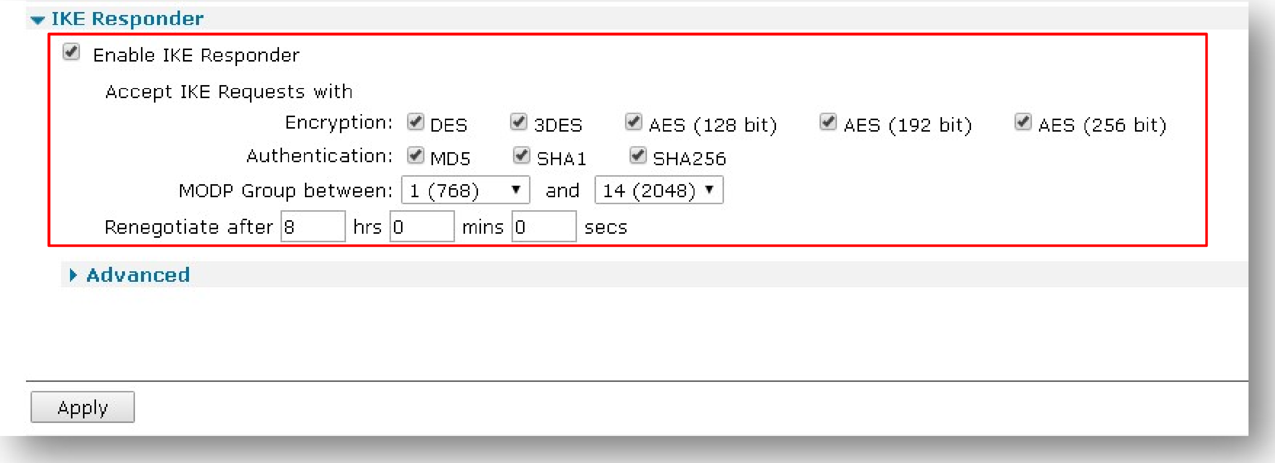
If the tunnel is down and a packet is ready to be sent drop the packet ▾
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 KBytes ▾ of traffic

Parameter	Setting	Description
Local LAN IP Address	172.16.1.0	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface or that of a specific device on the local subnet
Local LAN Mask	255.255.255.0	Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Remote LAN IP Address	192.168.1.0	Use this IP address for the remote LAN subnet. This is usually the IP address of the peer's Ethernet interface or that of a specific device on the local subnet
Remote LAN Mask	255.255.255.0	Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Use the following security on this tunnel	Pre-shared Keys	Pre-shared keys will be used for authentication
Our ID	responder1	Parameter to identify the local peer
Our ID type	IKE ID	Defines how the remote peer is to process the Our ID configuration
Remote ID	initiator	Parameter used to identify the remote peer
Use ( ) encryption on this tunnel	AES (128 bit keys)	The ESP encryption protocol to use with this IPsec tunnel
Use ( ) Authentication on this tunnel	SHA1	The ESP authentication algorithm to use with this IPsec tunnel
Use Diffie Hellman group ( )	2	The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.
Use IKE n to negotiate this tunnel	v1	The IKE version to use to negotiate this IPsec tunnel.
Use IKE configuration	0	The IKE configuration instance to use with this Eroute when the router is configured as an Initiator (so left as default in this case, it makes no difference as this router will no act as initiator)
Bring this tunnel up	On Demand	Controls how the IPsec tunnel is brought up.
If this tunnel is down and a packet is ready to be sent	Drop the packet	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be Sent

2.3.2 IKE settings

The IKE responder settings are set as follows:

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



IKE Responder

☑ Enable IKE Responder

Accept IKE Requests with

Encryption: ☑ DES ☑ 3DES ☑ AES (128 bit) ☑ AES (192 bit) ☑ AES (256 bit)

Authentication: ☑ MD5 ☑ SHA1 ☑ SHA256

MODP Group between: 1 (768) and 14 (2048)

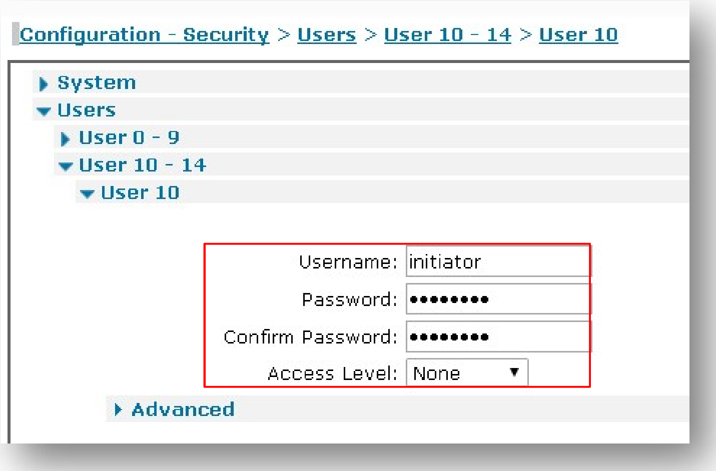
Renegotiate after 8 hrs 0 mins 0 secs

Parameter	Setting	Description
Enable IKE Responder	✓	Allows the router to respond to incoming IKE requests
Encryption	ALL ✓	The acceptable encryption algorithms
Authentication	ALL ✓	The acceptable authentication algorithms
MODP Group between x and y	1(768) and 14(1536)	The acceptable range for MODP group
Renegotiate after h hrs m mins s secs	8 hrs	How long the initial IKE Security Association will stay in force. When the IKE Security Association expires, any attempt to send packets to the remote system will result in IKE attempting to establish a new SA

2.3.3 Pre-Shared Key configuration

For the Pre-Shared key, a user needs to be configured with the Username as the ID of the initiator and the password as the Pre-Shared key:

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10



Username: initiator
Password: ••••••••
Confirm Password: ••••••••
Access Level: None ▼

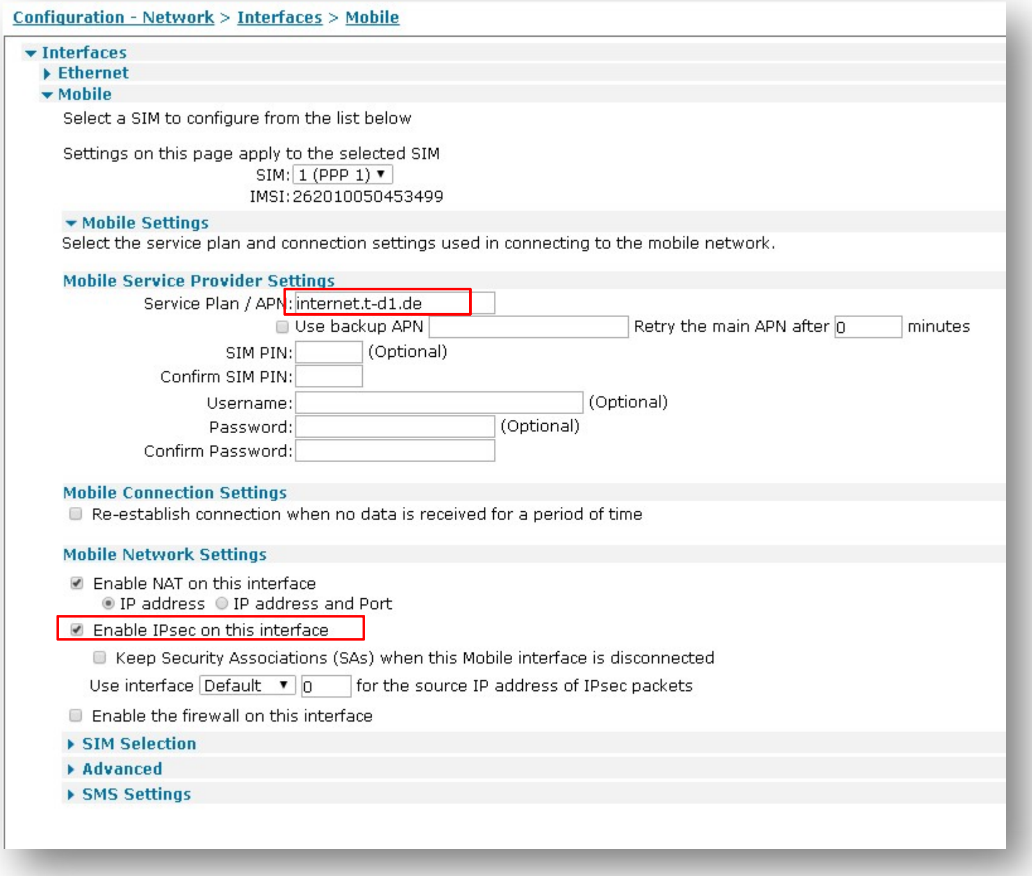
Parameter	Setting	Description
Username	initiator	Name should match the Peer ID: value from Eroute 0
Password	****	Enter a password
Confirm Password	****	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key

3 BACKUP RESPONDER CONFIGURATION

3.1 WAN interface configuration

In this example the Initiator has the Mobile interface as the WAN interface and it is configured as follows:

CONFIGURATION - NETWORK > INTERFACES > MOBILE



Configuration - Network > Interfaces > Mobile

▾ Interfaces

▸ Ethernet

▾ Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM
SIM: 1 (PPP 1) ▾
IMSI: 262010050453499

▾ Mobile Settings

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

Service Plan / APN: internet.t-d1.de
□ Use backup APN Retry the main APN after 0 minutes
SIM PIN: (Optional)
Confirm SIM PIN:
Username: (Optional)
Password: (Optional)
Confirm Password:

Mobile Connection Settings

□ Re-establish connection when no data is received for a period of time

Mobile Network Settings

☑ Enable NAT on this interface
● IP address ○ IP address and Port
☑ Enable IPsec on this interface
□ Keep Security Associations (SAs) when this Mobile interface is disconnected
Use interface Default ▾ 0 for the source IP address of IPsec packets
□ Enable the firewall on this interface

▸ SIM Selection

▸ Advanced

▸ SMS Settings

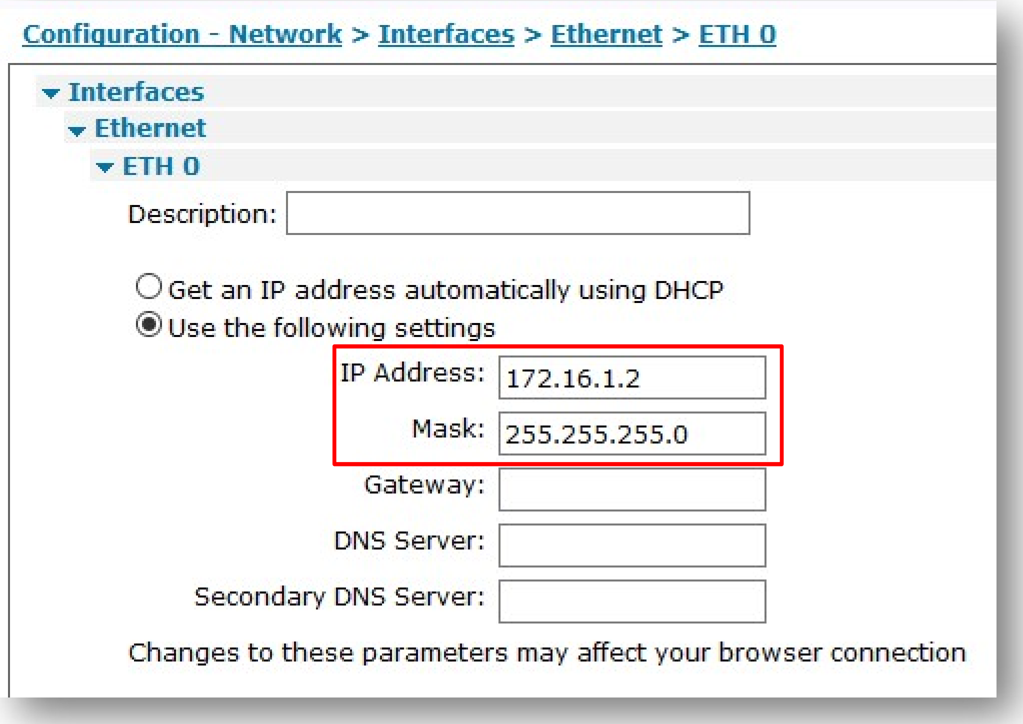
Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
Enable IPSec on this interface	✓	Enable IPSec on PPP 1 interface

Please note: Depending on provider, a SIM PIN or Username/Password may be required. If needed, enter them in the appropriate fields.

3.2 Local Ethernet Interface configuration

In this example, the LAN interface is configured with a static address as follows:

CONFIGURATION - NETWORK > INTERFACES > ETHERNET > ETH 0



Configuration - Network > Interfaces > Ethernet > ETH 0

Description:

○ Get an IP address automatically using DHCP
● Use the following settings

IP Address: 172.16.1.2
Mask: 255.255.255.0
Gateway:
DNS Server:
Secondary DNS Server:

Changes to these parameters may affect your browser connection

Where:

Parameter	Setting	Description
IP Address	172.16.1.2	Enter the IP address of the LAN interface for the router
Mask	255.255.255.0	Enter the subnet mask

3.3 IPsec configuration

Note: Here will be shown a summary of the configuration on the backup responder, as it is not the main focus of this document. For details about those settings, please check the Application Note:

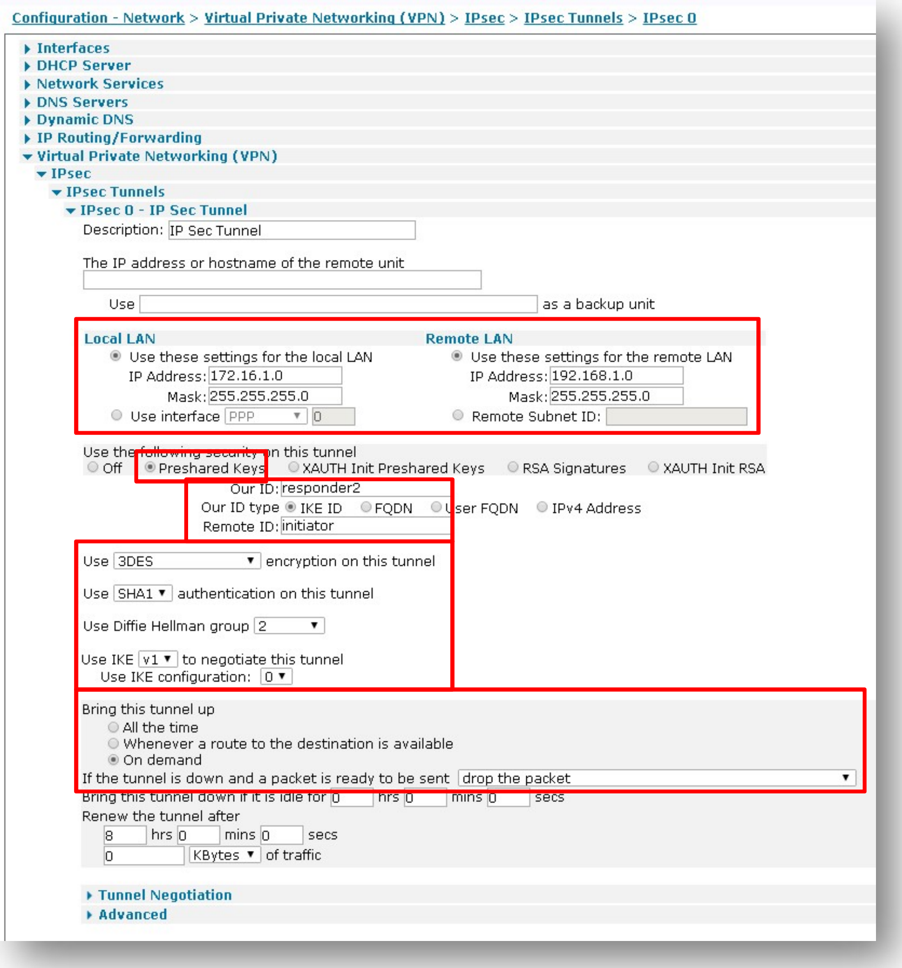
AN10 - IPSec over Cellular using Digi TransPort Routers with Pre-Shared key authentication

3.3.1 IPsec Tunnel

The IPsec tunnel is configured as site to site and with Pre-Shared Key using IKE ID. As it is a responder, It is set to be brought up only on demand (so when receive a request from the initiator).

Some security parameters are different than the primary responder ones.

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0


Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0
Interfaces
DHCP Server
Network Services
DNS Servers
Dynamic DNS
IP Routing/Forwarding
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec 0 - IP Sec Tunnel

Description: IP Sec Tunnel

The IP address or hostname of the remote unit

Use as a backup unit

Local LAN
● Use these settings for the local LAN
IP Address: 172.16.1.0
Mask: 255.255.255.0
○ Use interface PPP 0

Remote LAN
● Use these settings for the remote LAN
IP Address: 192.168.1.0
Mask: 255.255.255.0
○ Remote Subnet ID:

Use the following security on this tunnel
○ Off ● Preshared Keys ○ XAUTH Init Preshared Keys ○ RSA Signatures ○ XAUTH Init RSA

Our ID: responder2
Our ID type ● IKE ID ○ FQDN ○ User FQDN ○ IPv4 Address
Remote ID: initiator

Use 3DES encryption on this tunnel

Use SHA1 authentication on this tunnel

Use Diffie Hellman group 2

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

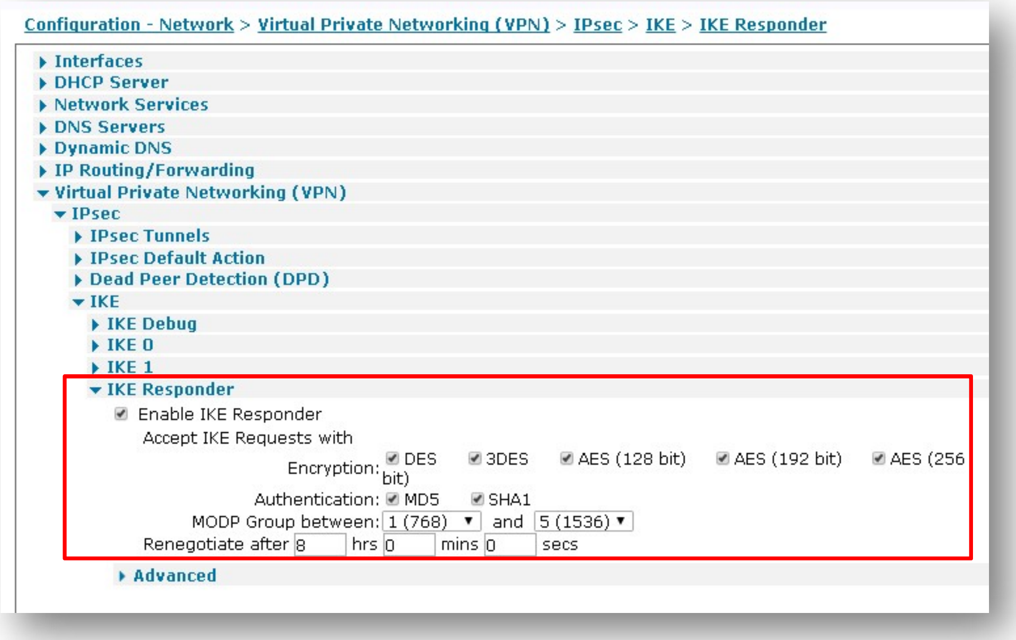
Where:

Parameter	Setting	Description
Local LAN IP Address	172.16.1.0	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface or that of a specific device on the local subnet
Local LAN Mask	255.255.255.0	Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Remote LAN IP Address	192.168.1.0	Use this IP address for the remote LAN subnet. This is usually the IP address of the peer's Ethernet interface or that of a specific device on the local subnet
Remote LAN Mask	255.255.255.0	Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Use the following security on this tunnel	Pre-shared Keys	Pre-shared keys will be used for authentication
Our ID	responder2	Parameter to identify the local peer
Our ID type	IKE ID	Defines how the remote peer is to process the Our ID configuration
Remote ID	initiator	Parameter used to identify the remote peer
Use ( ) encryption on this tunnel	3DES	The ESP encryption protocol to use with this IPsec tunnel
Use ( ) Authentication on this tunnel	SHA1	The ESP authentication algorithm to use with this IPsec tunnel
Use Diffie Hellman group ( )	2	The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.
Use IKE n to negotiate this tunnel	v1	The IKE version to use to negotiate this IPsec tunnel.
Use IKE configuration	0	The IKE configuration instance to use with this Eroute when the router is configured as an Initiator (so left as default in this case, it makes no difference as this router will no act as initiator)
Bring this tunnel up	On Demand	Controls how the IPsec tunnel is brought up.
If this tunnel is down and a packet is ready to be sent	Drop the packet	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent

3.3.2 IKE settings

The IKE responder settings are set as follows:

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



☑ Enable IKE Responder

Accept IKE Requests with

Encryption: ☑ DES ☑ 3DES ☑ AES (128 bit) ☑ AES (192 bit) ☑ AES (256 bit)

Authentication: ☑ MD5 ☑ SHA1

MODP Group between: 1 (768) and 5 (1536)

Renegotiate after 8 hrs 0 mins 0 secs

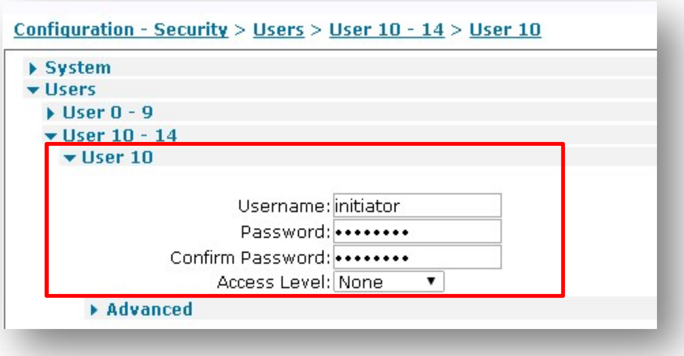
Where:

Parameter	Setting	Description
Enable IKE Responder	✓	Allows the router to respond to incoming IKE requests
Encryption	ALL ✓	The acceptable encryption algorithms
Authentication	ALL ✓	The acceptable authentication algorithms
MODP Group between x and y	1(768) and 5(1536)	The acceptable range for MODP group
Renegotiate after h hrs m mins s secs	8 hrs	How long the initial IKE Security Association will stay in force. When the IKE Security Association expires, any attempt to send packets to the remote system will result in IKE attempting to establish a new SA

3.3.3 Pre-Shared Key configuration

For the Pre-Shared key, a user needs to be configured with the Username as the ID of the initiator and the password as the Pre-Shared key:

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10



Username: initiator
Password: ••••••••
Confirm Password: ••••••••
Access Level: None

Where:

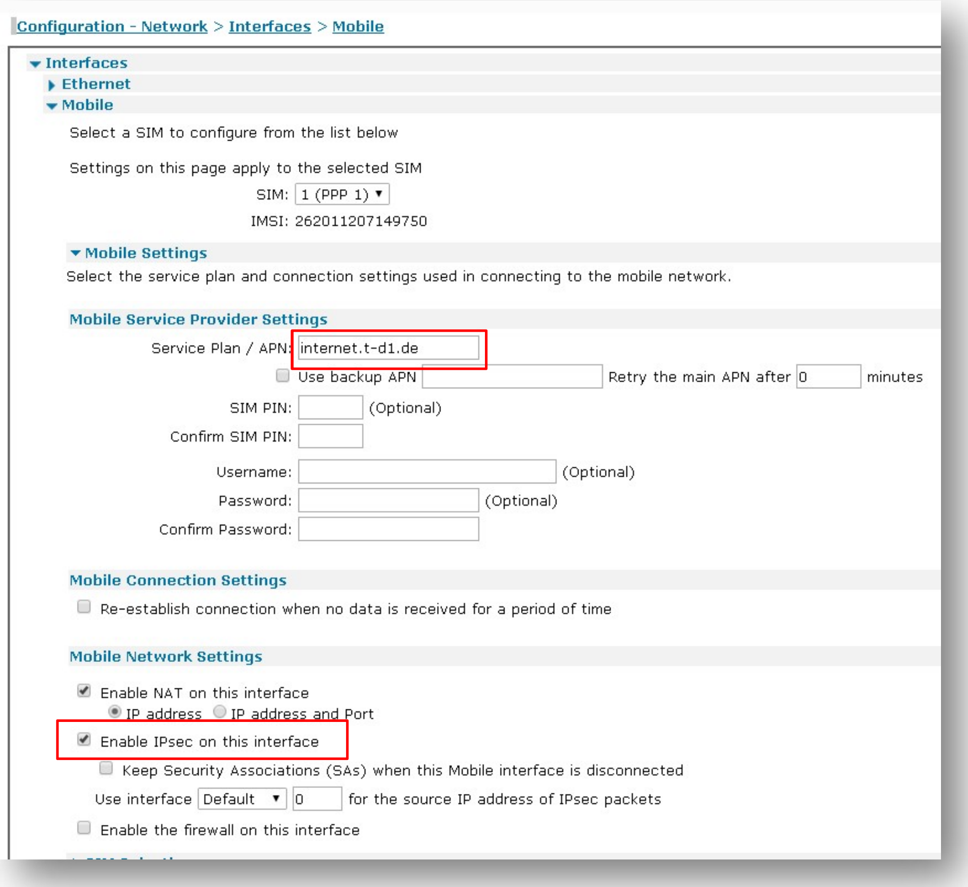
Parameter	Setting	Description
Username	initiator	Name should match the Peer ID: value from Eroute 0
Password	****	Enter a password
Confirm Password	****	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key

4 INITIATOR CONFIGURATION

4.1 WAN Interface configuration

In this example the Initiator has the Mobile interface as WAN and it is configured as follows, with an APN set and IPsec enabled:

CONFIGURATION - NETWORK > INTERFACES > MOBILE



Configuration - Network > Interfaces > Mobile

▾ Interfaces

▸ Ethernet

▾ Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1) ▾

IMSI: 262011207149750

▾ Mobile Settings

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

Service Plan / APN: internet.t-d1.de

□ Use backup APN Retry the main APN after 0 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Mobile Connection Settings

□ Re-establish connection when no data is received for a period of time

Mobile Network Settings

☑ Enable NAT on this interface

● IP address ○ IP address and Port

☑ Enable IPsec on this interface

□ Keep Security Associations (SAs) when this Mobile interface is disconnected

Use interface Default ▾ 0 for the source IP address of IPsec packets

□ Enable the firewall on this interface

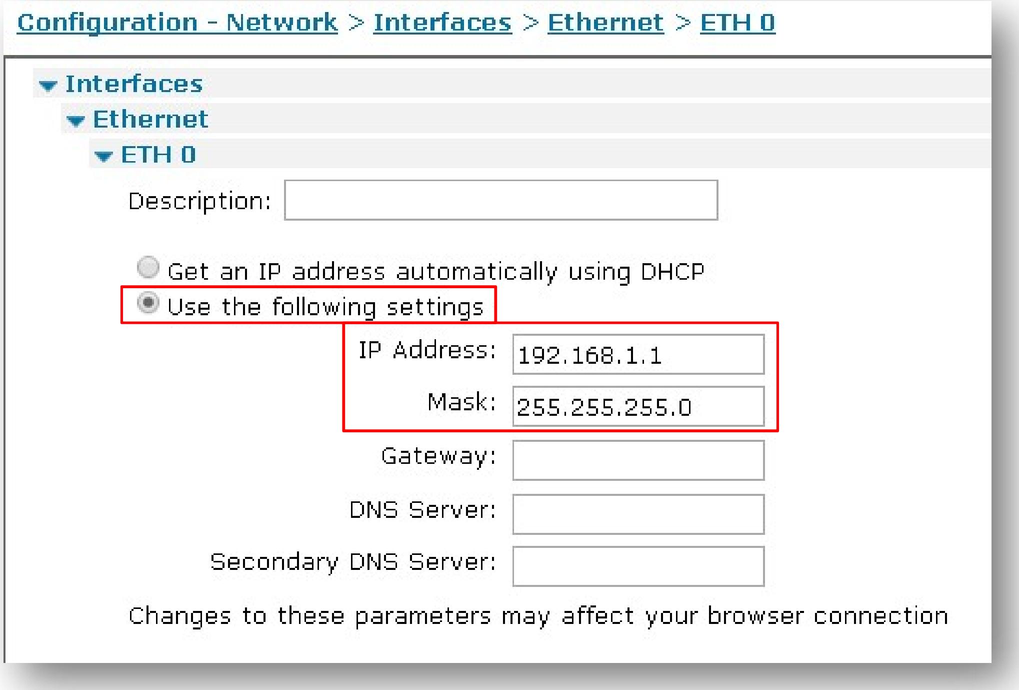
Where:

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
Enable IPSec on this interface	✓	Enable IPSec on PPP 1 interface

4.2 Local Ethernet Interface configuration

In this example, the LAN interface is configured with a static address as follows:

CONFIGURATION - NETWORK > INTERFACES > ETHERNET > ETH 0



Configuration - Network > Interfaces > Ethernet > ETH 0

Description:

○ Get an IP address automatically using DHCP
● Use the following settings

IP Address: 192.168.1.1
Mask: 255.255.255.0
Gateway:
DNS Server:
Secondary DNS Server:

Changes to these parameters may affect your browser connection

Where:

Parameter	Setting	Description
IP Address	192.168.1.1	Enter the IP address of the LAN interface for the router
Mask	255.255.255.0	Enter the subnet mask

4.3 IPsec configuration

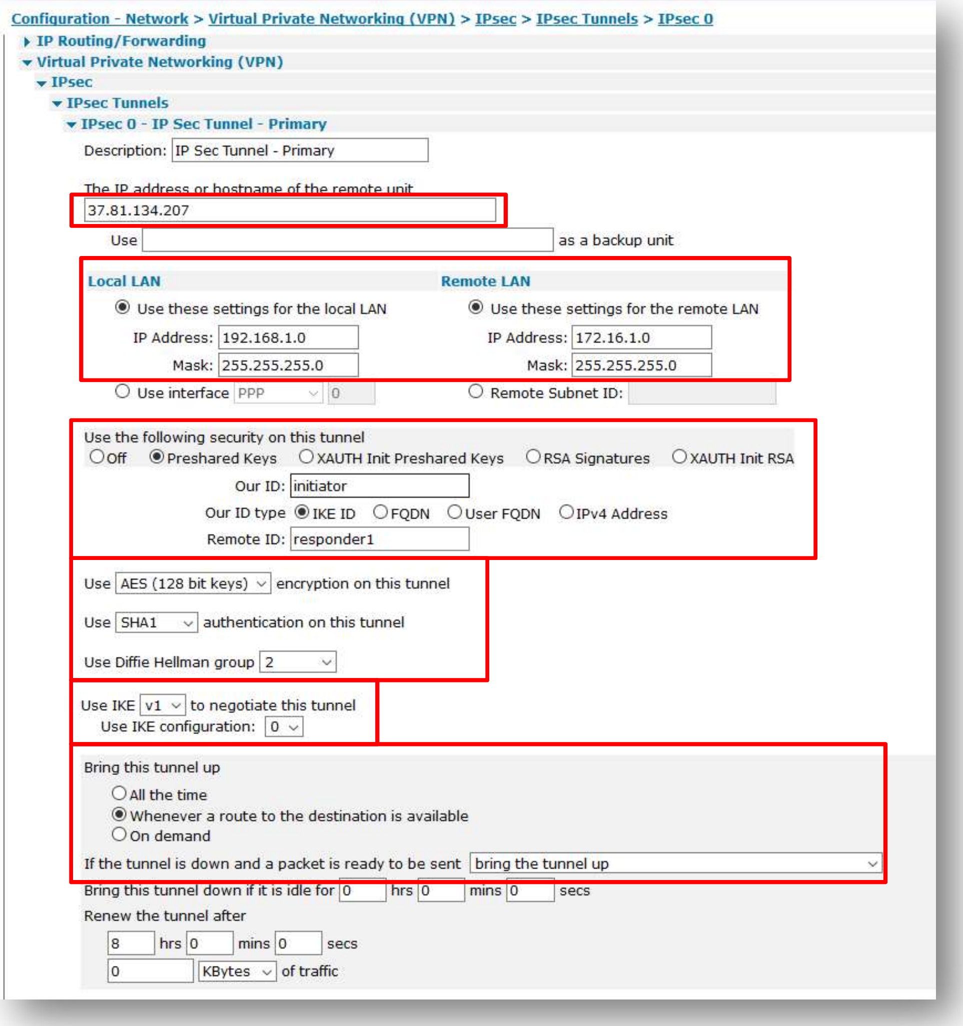
On the initiator two tunnels will be configured, one to the Primary responder and one to the Backup one.

4.3.1 IPsec Tunnel to Primary Responder

4.3.1.1 IPsec Tunnel

The IPsec tunnel is configured as site to site and with Preshared Key using IKE ID. As it is the initiator, It is set to be brought up whenever a route is available to the destination:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0



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

▸ IP Routing/Forwarding
▾ Virtual Private Networking (VPN)
▾ IPsec
▾ IPsec Tunnels
▾ IPsec 0 - IP Sec Tunnel - Primary

Description: IP Sec Tunnel - Primary

The IP address or hostname of the remote unit
37.81.134.207
Use [ ] as a backup unit

Local LAN
● Use these settings for the local LAN
IP Address: 192.168.1.0
Mask: 255.255.255.0
○ Use interface PPP 0

Remote LAN
● Use these settings for the remote LAN
IP Address: 172.16.1.0
Mask: 255.255.255.0
○ Remote Subnet ID:

Use the following security on this tunnel
○ Off ● Preshared Keys ○ XAUTH Init Preshared Keys ○ RSA Signatures ○ XAUTH Init RSA
Our ID: initiator
Our ID type ● IKE ID ○ FQDN ○ User FQDN ○ IPv4 Address
Remote ID: responder1

Use AES (128 bit keys) encryption on this tunnel
Use SHA1 authentication on this tunnel
Use Diffie Hellman group 2

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

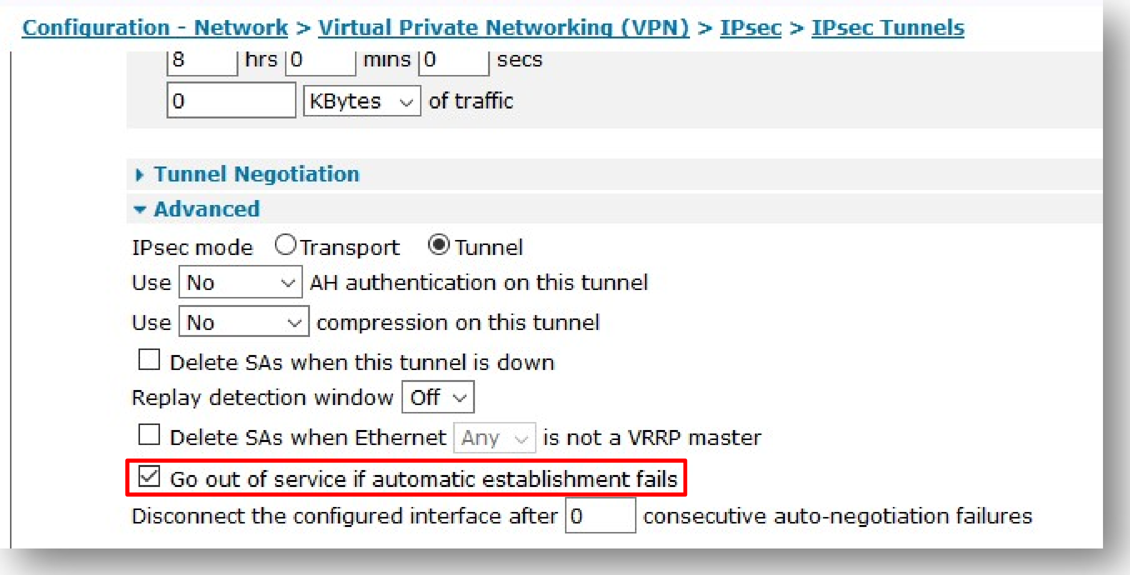
Bring this tunnel up
○ All the time
● Whenever a route to the destination is available
○ On demand
If the tunnel is down and a packet is ready to be sent bring the tunnel up
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 KBytes of traffic

Where:

Parameter	Setting	Description
The IP address or hostname of the remote unit	37.81.134.207	The IP address or hostname of the remote IPsec peer that a VPN will be initiated to. In this case, is the responder 1 WAN address
Local LAN IP Address	192.168.1.0	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface or that of a specific device on the local subnet
Local LAN Mask	255.255.255.0	Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Remote LAN IP Address	172.16.1.0	Use this IP address for the remote LAN subnet. This is usually the IP address of the peer's Ethernet interface or that of a specific device on the local subnet
Remote LAN Mask	255.255.255.0	Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Use the following security on this tunnel	Pre-shared Keys	Pre-shared keys will be used for authentication
Our ID	initiator	Parameter to identify the local peer
Our ID type	IKE ID	Defines how the remote peer is to process the Our ID configuration
Remote ID	responder1	Parameter used to identify the remote peer
Use ( ) encryption on this tunnel	AES 128	The ESP encryption protocol to use with this IPsec tunnel
Use ( ) Authentication on this tunnel	SHA1	The ESP authentication algorithm to use with this IPsec tunnel
Use Diffie Hellman group ( )	2	The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.
Use IKE n to negotiate this tunnel	v1	The IKE version to use to negotiate this IPsec tunnel.
Use IKE configuration	0	The IKE configuration instance to use with this Eroute when the router is configured as an Initiator (so left as default in this case, it makes no difference as this router will no act as initiator)
Bring this tunnel up	Whenever a route to the destination is available	Controls how the IPsec tunnel is brought up.
If this tunnel is down and a packet is ready to be sent	Bring the tunnel Up	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent

For the automatic failover to work, the primary tunnel needs to be set as Out of Service when the automatic establishment fails. This setting can be configured in the Advanced section of the tunnel section:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0 > ADVANCED



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

8 hrs 0 mins 0 secs

0 KBytes of traffic

▸ Tunnel Negotiation

▾ Advanced

IPsec mode ○ Transport ● Tunnel

Use No AH authentication on this tunnel

Use No compression on this tunnel

□ Delete SAs when this tunnel is down

Replay detection window Off

□ Delete SAs when Ethernet Any is not a VRRP master

☑ Go out of service if automatic establishment fails

Disconnect the configured interface after 0 consecutive auto-negotiation failures

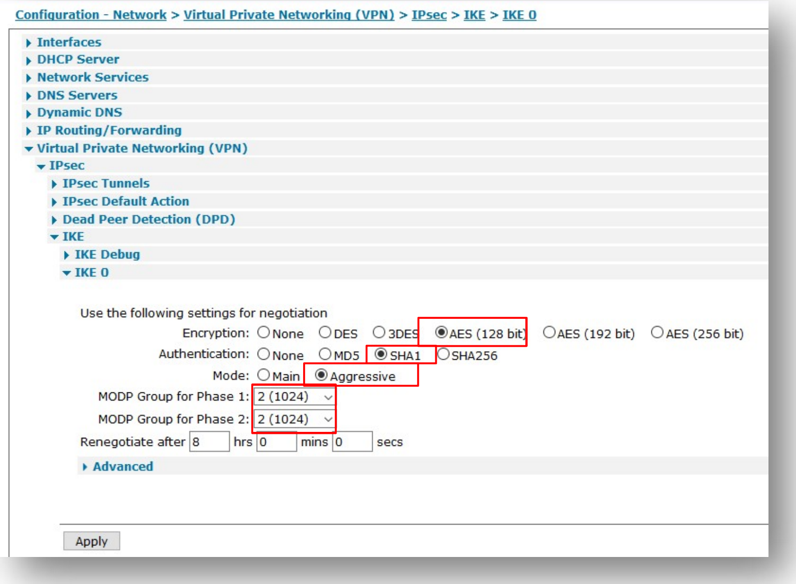
Where:

Parameter	Setting	Description
Go out of service if automatic establishment fails	✓	The router will take the IPsec tunnel out of service if the automatic establishment fails. Selecting this, will allow the tunnel 1 to be brought up when tunnel 0 goes OOS

4.3.1.2 IKE settings

The IKE settings are set as follows (note that for the secondary tunnel, a different IKE configuration will be used):

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE 0



Use the following settings for negotiation

Encryption: ○ None ○ DES ○ 3DES ● AES (128 bit) ○ AES (192 bit) ○ AES (256 bit)

Authentication: ○ None ○ MD5 ● SHA1 ○ SHA256

Mode: ○ Main ● Aggressive

MODP Group for Phase 1: 2 (1024)

MODP Group for Phase 2: 2 (1024)

Renegotiate after 8 hrs 0 mins 0 secs

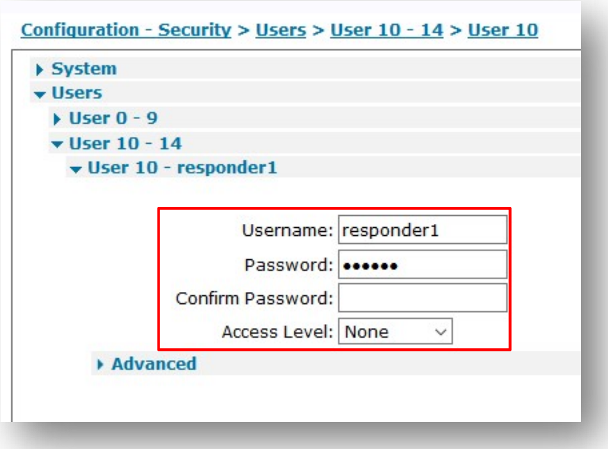
Where:

Parameter	Setting	Description
Encryption	AES (128 bit)	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	SHA1	The algorithm used to authenticate the IKE session
Mode	Aggressive	Aggressive mode is used in this example
MODP Group for Phase 1	2 (1024)	The key length used in the IKE Diffie-Hellman exchange
MODP Group for Phase 2	2 (1024)	The minimum width of the numeric field used in the calculations for phase 2 of the security exchange.

4.3.1.3 Pre-Shared Key configuration

For the Pre-Shared key, a user needs to be configured with the Username as the ID of the primary responder and the password as the Pre-Shared key:

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10



Username: responder1
Password: ••••••
Confirm Password:
Access Level: None

Where:

Parameter	Setting	Description
Username	responder1	Name should match the Peer ID: value from Eroute 0
Password	****	Enter a password
Confirm Password	****	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key

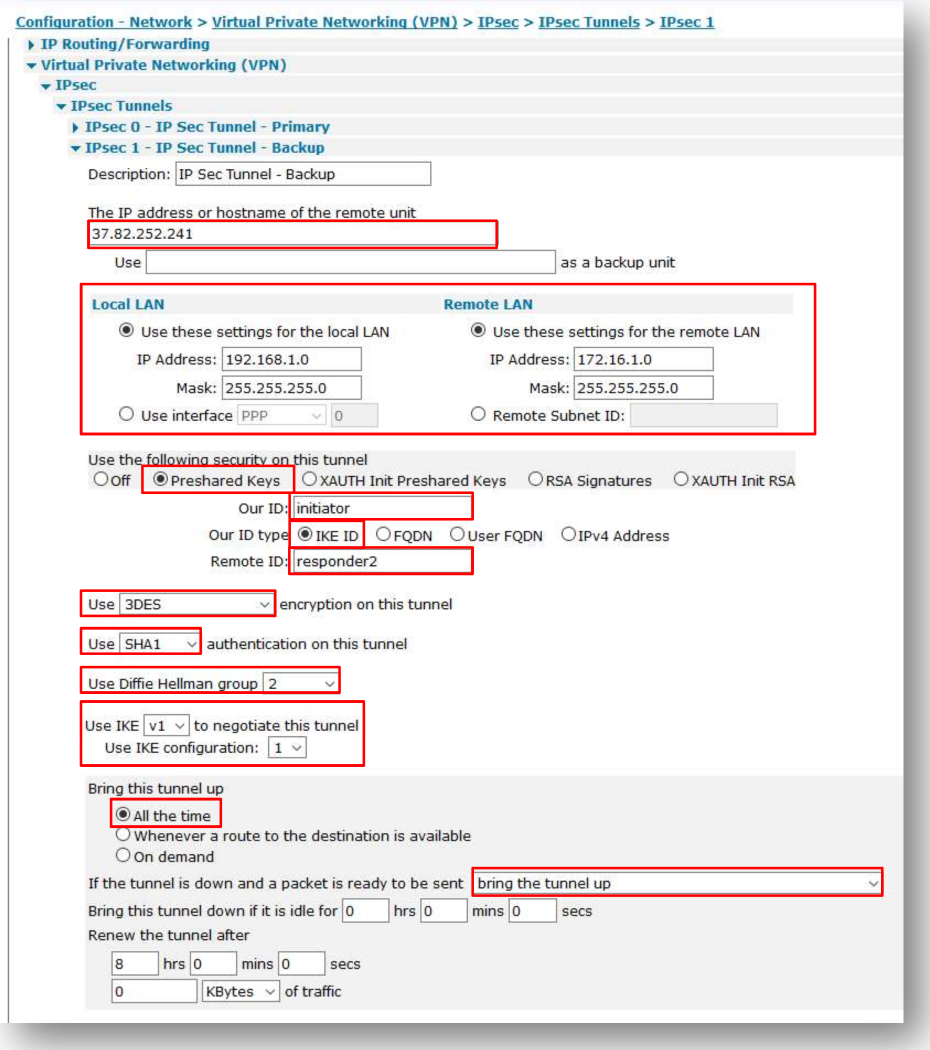
4.3.2 IPsec Tunnel to Secondary Responder

4.3.2.1 IPsec Tunnel

The IPsec tunnel is configured as site to site and with Preshared Key using IKE ID. Even if this will be the backup tunnel, it needs to be set as brought up ALL the time. That means that, thanks to another parameter in the advanced section explained late ron this section, this tunnel will try to go UP all the time but only when the primary one is detected as Out of Service.

Please also note that in this case, a different IKE configuration is used ("Use IKE configuration 1").

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 1



Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 1

▸ IP Routing/Forwarding
▾ Virtual Private Networking (VPN)
▾ IPsec
▾ IPsec Tunnels
▸ IPsec 0 - IP Sec Tunnel - Primary
▾ IPsec 1 - IP Sec Tunnel - Backup

Description: IP Sec Tunnel - Backup

The IP address or hostname of the remote unit
37.82.252.241
Use [ ] as a backup unit

Local LAN	Remote LAN
● Use these settings for the local LAN	● Use these settings for the remote LAN
IP Address: 192.168.1.0	IP Address: 172.16.1.0
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 Preshared Keys ○ RSA Signatures ○ XAUTH Init RSA
Our ID: initiator
Our ID type ● IKE ID ○ FQDN ○ User FQDN ○ IPv4 Address
Remote ID: responder2

Use 3DES encryption on this tunnel

Use SHA1 authentication on this tunnel

Use Diffie Hellman group 2

Use IKE v1 to negotiate this tunnel
Use IKE configuration: 1

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

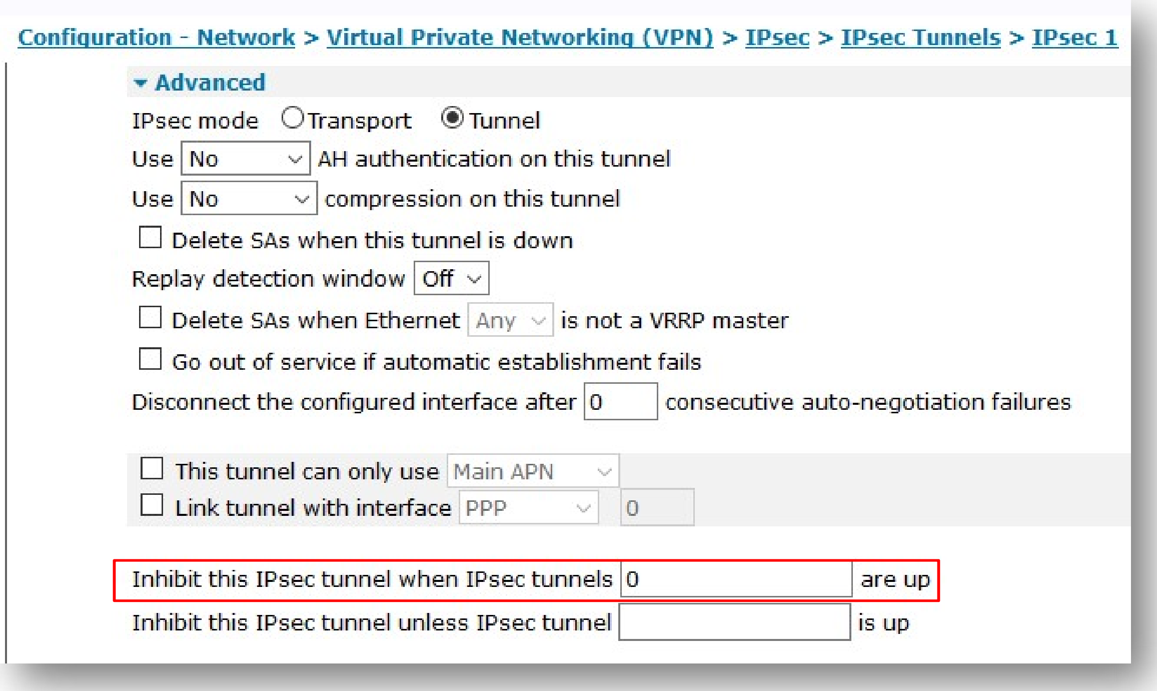
Renew the tunnel after
8 hrs 0 mins 0 secs
0 KBytes of traffic

Where:

Parameter	Setting	Description
The IP address or hostname of the remote unit	37.82.252.241	The IP address or hostname of the remote IPsec peer that a VPN will be initiated to. In this case, is the responder 1 WAN address
Local LAN IP Address	192.168.1.0	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface or that of a specific device on the local subnet
Local LAN Mask	255.255.255.0	Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Remote LAN IP Address	172.16.1.0	Use this IP address for the remote LAN subnet. This is usually the IP address of the peer's Ethernet interface or that of a specific device on the local subnet
Remote LAN Mask	255.255.255.0	Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Use the following security on this tunnel	Pre-shared Keys	Pre-shared keys will be used for authentication
Our ID	initiator	Parameter to identify the local peer
Our ID type	IKE ID	Defines how the remote peer is to process the Our ID configuration
Remote ID	responder2	Parameter used to identify the remote peer
Use ( ) encryption on this tunnel	3DES	The ESP encryption protocol to use with this IPsec tunnel
Use ( ) Authentication on this tunnel	SHA1	The ESP authentication algorithm to use with this IPsec tunnel
Use Diffie Hellman group ( )	2	The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.
Use IKE n to negotiate this tunnel	v1	The IKE version to use to negotiate this IPsec tunnel.
Use IKE configuration	1	The IKE configuration instance to use with this Eroute when the router is configured as an Initiator. In this case, the inititaor will use the configuration instance 1 (and not the default 0) for the tunnel to the responder 2
Bring this tunnel up	All the time	Controls how the IPsec tunnel is brought up.
If this tunnel is down and a packet is ready to be sent	Bring the tunnel Up	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent

As noted before, in order to have the automatic failover working, in the advanced section of the tunnel, a parameter needs to be configured so that the secondary tunnel is inhibited when the primary one is UP:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0 > <u>ADVANCED</u>



Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 1

Advanced

IPsec mode ○ Transport ● Tunnel

Use No AH authentication on this tunnel

Use No compression on this tunnel

□ Delete SAs when this tunnel is down

Replay detection window Off

□ Delete SAs when Ethernet Any is not a VRRP master

□ Go out of service if automatic establishment fails

Disconnect the configured interface after 0 consecutive auto-negotiation failures

□ This tunnel can only use Main APN

□ Link tunnel with interface PPP 0

Inhibit this IPsec tunnel when IPsec tunnels 0 are up

Inhibit this IPsec tunnel unless IPsec tunnel is up

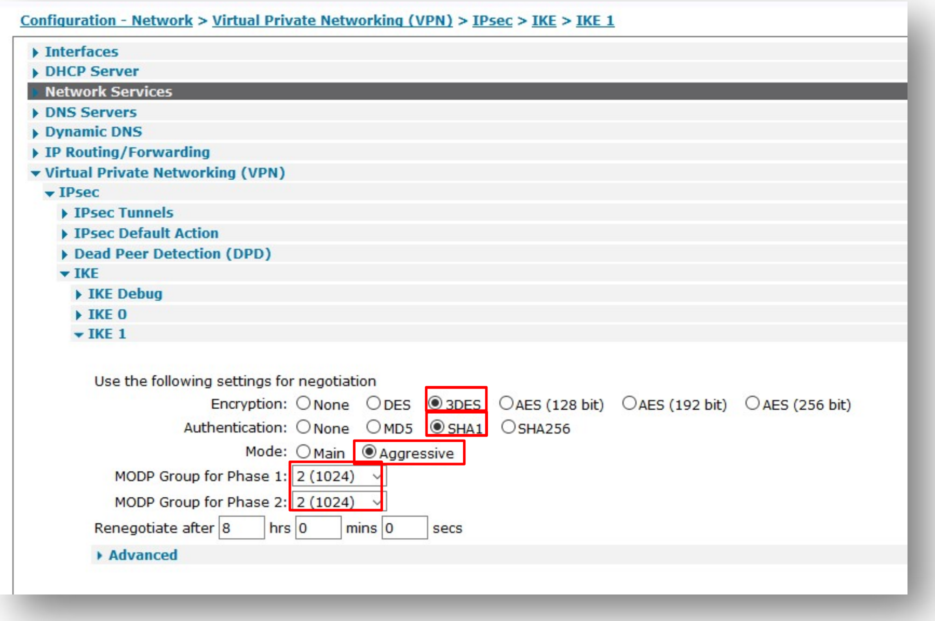
Where:

Parameter	Setting	Description
Inhibit this IPsec tunnel when IPsec tunnels n are up	0	A list of IPsec tunnels that can inhibit this IPsec tunnel from being used as long as they are up. In this case, the primary tunnel is the number “0”

4.3.2.2 IKE settings

For the backup tunnel, IKE1 configuration section will be configured, as this is the one used in the tunnel.

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE > IKE 1



Use the following settings for negotiation

Encryption: ○None ○DES ●3DES ○AES (128 bit) ○AES (192 bit) ○AES (256 bit)

Authentication: ○None ○MD5 ●SHA1 ○SHA256

Mode: ○Main ●Aggressive

MODP Group for Phase 1: 2 (1024)

MODP Group for Phase 2: 2 (1024)

Renegotiate after 8 hrs 0 mins 0 secs

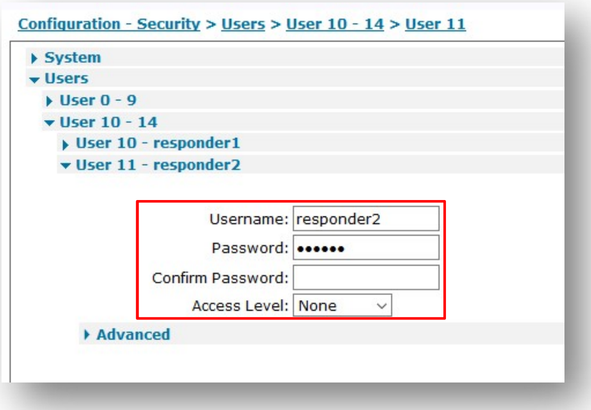
Where:

Parameter	Setting	Description
Encryption	3DES	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	SHA1	The algorithm used to authenticate the IKE session
Mode	Aggressive	Aggressive mode is used in this example
MODP Group for Phase 1	2 (1024)	The key length used in the IKE Diffie-Hellman exchange
MODP Group for Phase 2	2 (1024)	The minimum width of the numeric field used in the calculations for phase 2 of the security exchange.

4.3.2.3 Pre-Shared Key configuration

For the Pre-Shared key, another user needs to be configured with the Username as the ID of the backup responder and the password as the Pre-Shared key:

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 11



Configuration - Security > Users > User 10 - 14 > User 11

Username: responder2

Password: ••••••

Confirm Password:

Access Level: None

Where:

Parameter	Setting	Description
Username	responder2	Name should match the Peer ID: value from Eroute 0
Password	****	Enter a password
Confirm Password	****	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key

5 TESTING THE AUTOMATIC FAILOVER BETWEEN IPSEC TUNNELS

In this section will be explained how to test the automatic failover between IPsec tunnel functionality. In order to see what happens, the events from the eventlog section will be shown.

5.1 Failure on the primary tunnel (OOS)

Having the primary tunnel correctly established:

```
09:56:04, 12 May 2017,(2) IKE SA Removed. Peer: responder1,Successful Negotiation
09:55:37, 12 May 2017,Eroute 0 VPN up peer: responder1
09:55:37, 12 May 2017,New IPSec SA created by responder1
09:55:37, 12 May 2017,(2) IKE Notification: Initial Contact,RX
09:55:37, 12 May 2017,(3) IKE Notification: Responder Lifetime,RX
09:55:37, 12 May 2017,(2) New Phase 2 IKE Session 37.81.134.207,Initiator
09:55:36, 12 May 2017,(1) IKE Keys Negotiated. Peer: responder1
09:55:34, 12 May 2017,(1) New Phase 1 IKE Session 37.81.134.207,Initiator
09:55:34, 12 May 2017,IKE Request Received From Eroute 0
```

A failure needs to be simulated on the primary responder (for example a WAN disconnection) so that the tunnel can be set as OOS:

```
09:57:49, 12 May 2017,Eroute 0 Out Of Service,No SAs
09:57:49, 12 May 2017,Eroute 0 VPN down peer: responder1
09:57:49, 12 May 2017,IPSec SA Deleted ID responder1,Dead Peer Detected
```

5.2 Failover on Secondary Tunnel

Once the primary tunnel is marked as OOS, the secondary on will immediately start to try the establishment and will go UP:

```
09:57:50, 12 May 2017,Eroute 1 VPN up peer: responder2
09:57:50, 12 May 2017,New IPSec SA created by responder2
09:57:50, 12 May 2017,(11) IKE Notification: Initial Contact,RX
09:57:50, 12 May 2017,(12) IKE Notification: Responder Lifetime,RX
09:57:50, 12 May 2017,(11) New Phase 2 IKE Session 37.82.252.241,Initiator
09:57:50, 12 May 2017,(9) IKE Keys Negotiated. Peer: responder2
09:57:49, 12 May 2017,(1) IKE SA Removed. Peer: responder1,Dead Peer Detected
09:57:49, 12 May 2017,(9) New Phase 1 IKE Session 37.82.252.241,Initiator
09:57:49, 12 May 2017,IKE Request Received From Eroute 1
```

5.3 Restore of Primary Tunnel

As the primary tunnel is configured to be always brought up, it will continue to try the establishment even if the tunnel 1 is UP. Once the failure on the primary responder is solved (so for example, reconnecting the WAN interface), the primary Tunnel will be correctly established:

```
09:59:21, 12 May 2017,Eroute 0 VPN up peer: responder1
09:59:21, 12 May 2017,New IPSec SA created by responder1
09:59:21, 12 May 2017,(15) IKE Notification: Initial Contact,RX
09:59:21, 12 May 2017,(16) IKE Notification: Responder Lifetime,RX
09:59:21, 12 May 2017,(15) New Phase 2 IKE Session 37.81.134.207,Initiator
09:59:21, 12 May 2017,(14) IKE Keys Negotiated. Peer: responder1
09:59:19, 12 May 2017,IKE Request Received From Eroute 0
09:59:09, 12 May 2017,IKE Request Received From Eroute 0
09:58:59, 12 May 2017,(14) New Phase 1 IKE Session 37.81.134.207,Initiator
09:58:59, 12 May 2017,IKE Request Received From Eroute 0
09:58:59, 12 May 2017,(13) IKE SA Removed. Peer: ,Negotiation Failure
09:58:59, 12 May 2017,(13) IKE Negotiation Failed. Peer: ,Retries Exceeded
09:58:49, 12 May 2017,IKE Request Received From Eroute 0
09:58:39, 12 May 2017,IKE Request Received From Eroute 0
09:58:29, 12 May 2017,(13) New Phase 1 IKE Session 37.81.134.207,Initiator
09:58:29, 12 May 2017,IKE Request Received From Eroute 0
09:58:20, 12 May 2017,(11) IKE SA Removed. Peer: responder2,Successful Negotiation
09:58:19, 12 May 2017,(8) IKE SA Removed. Peer: ,Negotiation Failure
09:58:19, 12 May 2017,(8) IKE Negotiation Failed. Peer: ,Retries Exceeded
09:58:19, 12 May 2017,IKE Request Received From Eroute 0
09:58:09, 12 May 2017,IKE Request Received From Eroute 0
09:57:59, 12 May 2017,IKE Request Received From Eroute 0
```

At the same time, due to the “inhibit” setting, the secondary one will be brought down:

```

09:59:21, 12 May 2017,Eroute 1 VPN down peer: responder2
09:59:21, 12 May 2017,IPSec SA Deleted ID responder2,Eroute inhibited
```

6 CONFIGURATION FILE

6.1 Primary Responder Configuration

This is the config.da0 file used on the primary responder for the purpose of this Application Note

```
eth 0 IPaddr "172.16.1.1"
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 "ppp"
def_route 0 ll_add 1
eroute 0 descr "IP Sec Tunnel"
eroute 0 peerid "initiator"
eroute 0 ourid "responder1"
eroute 0 locip "172.16.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "192.168.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
eroute 0 dhgroup 2
eroute 0 enckeybits 128
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
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
web 0 prelogin_info ON
modemcc 0 asy_add 4
modemcc 0 info_asy_add 2
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet.t-d1.de"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
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 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 l1on ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
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 "initiator"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
local 0 transaccess 2
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
templog 0 mo_autooff ON
cloud 0 ssl ON
```

6.2 Backup Responder Configuration

This is the config.da0 file used on the backup responder for the purpose of this Application Note

```
eth 0 IPaddr "172.16.1.2"
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 "ppp"
def_route 0 ll_add 1
eroute 0 descr "IP Sec Tunnel"
eroute 0 peerid "initiator"
eroute 0 ourid "responder2"
eroute 0 locip "172.16.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "192.168.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "3DES"
eroute 0 authmeth "PRESHARED"
eroute 0 dhgroup 2
eroute 0 enckeybits 128
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN (LTE)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 firewall ON
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
web 0 prelogin_info ON
web 0 showgswiz ON
modemcc 0 info_asy_add 4
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet.t-d1.de"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
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 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 l1on ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
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 "initiator"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
local 0 transaccess 2
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
templog 0 mo_autooff ON
cloud 0 ssl ON
```

6.3 Initiator Configuration

This is the config.da0 file used on the initiator for the purpose of this Application Note

```
eth 0 IPaddr "192.168.1.1"
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 "ppp"
def_route 0 ll_add 1
eroute 0 descr "IP Sec Tunnel - Primary"
eroute 0 peerip "37.81.134.207"
eroute 0 peerid "responder1"
eroute 0 ourid "initiator"
eroute 0 locip "192.168.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "172.16.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 1
eroute 0 nosaoos ON
eroute 0 dhgroup 2
eroute 0 enckeybits 128
eroute 1 descr "IP Sec Tunnel - Backup"
eroute 1 peerip "37.82.252.241"
eroute 1 peerid "responder2"
eroute 1 ourid "initiator"
eroute 1 locip "192.168.1.0"
eroute 1 locmsk "255.255.255.0"
eroute 1 remip "172.16.1.0"
eroute 1 remmsk "255.255.255.0"
eroute 1 ESPauth "SHA1"
eroute 1 ESPenc "3DES"
eroute 1 authmeth "PRESHARED"
eroute 1 nosa "TRY"
eroute 1 autosa 2
eroute 1 ikecfg 1
eroute 1 dhgroup 2
eroute 1 inhibitno "0"
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
```

```
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 ipsec 1
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
web 0 prelogin_info ON
ftpcli 0 hostname "ftp1.digi.com"
ftpcli 0 username "anonymous"
ftpcli 0 epassword "OTF5VFxBSElB"
ftpcli 0 directory "support/firmware/transport/radio_module_firmware/he910d"
ike 0 encalg "AES"
ike 0 keybits 128
ike 0 authalg "SHA1"
ike 0 aggressive ON
ike 0 ikegroup 2
ike 0 ipsecgroup 2
ike 1 encalg "3DES"
ike 1 authalg "SHA1"
ike 1 aggressive ON
ike 1 ikegroup 2
ike 1 ipsecgroup 2
modemcc 0 info_asy_add 3
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet.t-d1.de"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
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 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 l1on ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 1200
cmd 0 rcihttp ON
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 "responder1"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
user 11 name "responder2"
user 11 epassword "PDZxU0FFQFU="
user 11 access 4
local 0 transaccess 2
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
templog 0 mo_autooff ON
cloud 0 ssl ON
```