Quick Note 006

Configuring a GRE tunnel within an IPSec tunnel (GRE over IPSec)

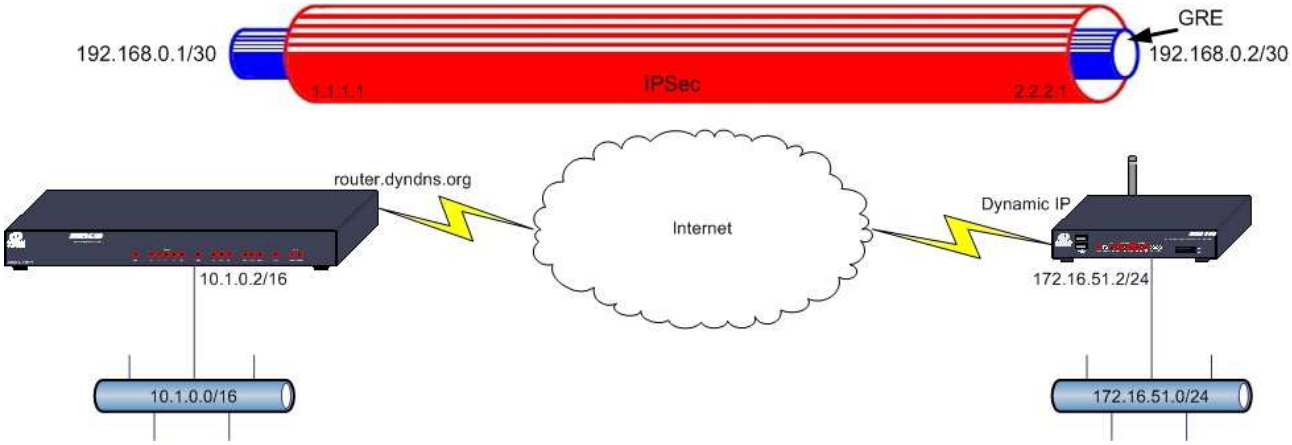
1.0 Version

Version Number	Status
1.0	Published

2.0 Configuration & scenario

This guide has been written for technically competent personnel who are able to configure a standard IPSec tunnel between 2 Sarian routers.

An IPSec tunnel is setup to ensure secure communications between the site HR4110 and the central MW3520. A GRE tunnel is configured to run through the IPSec tunnel to allow point to point communication between the 2 sites. This is used when a process such as a routing protocol needs point to point communication between 2 sites and a point to point link such as leased line is not available.

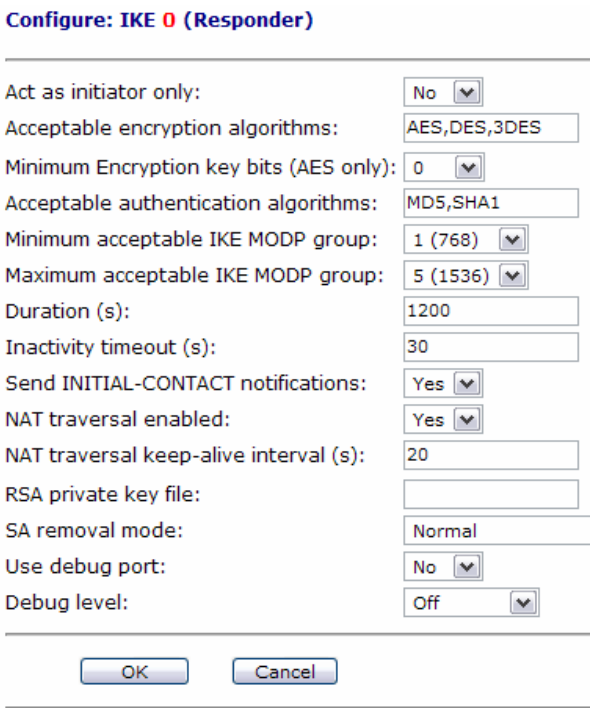


Both routers have been configured with internet connectivity, the MW3520 uses ADSL with a dynamic public IP address but uses the DynDNS service so it can always be reached at router.dyndns.org and the HR4110 has a private IP address supplied by the mobile operator. LAN segments are attached on Eth0.

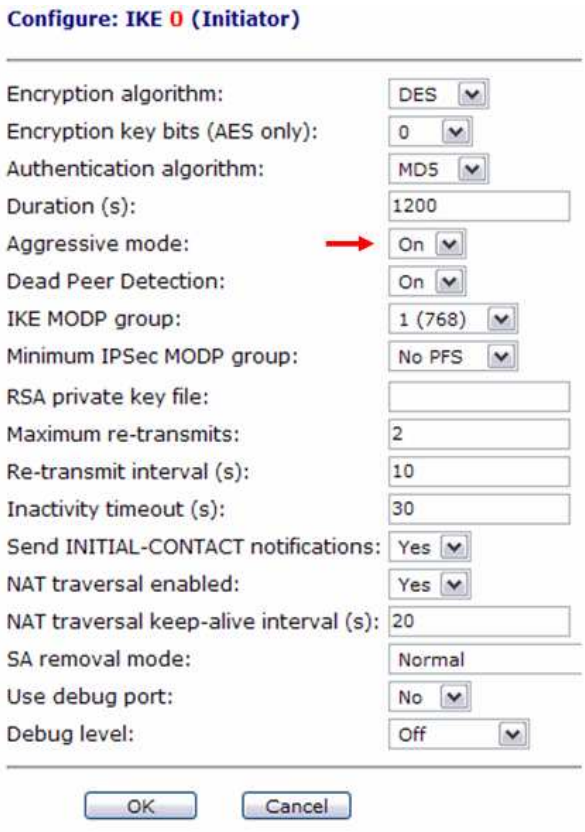
Configure IKE

Configure > IPSec > IKE > IKE 0

MW3520 (IPSec responder)



HR4110 (Initiator)

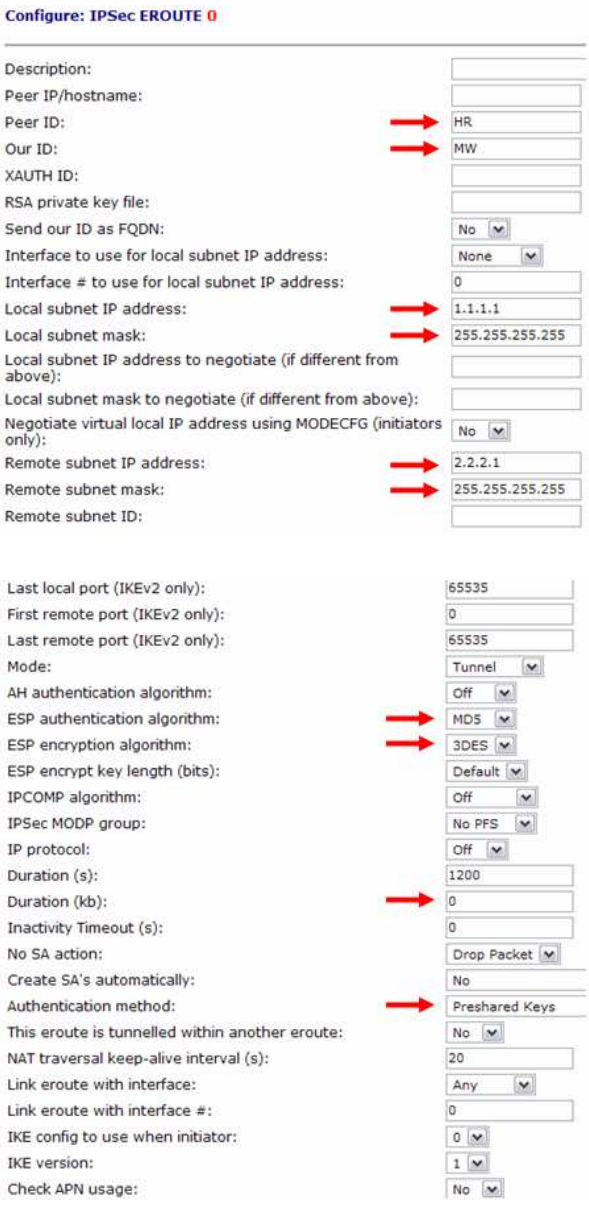


The IKE configuration is default except for enabling aggressive mode on the HR4110 IPSec initiator.

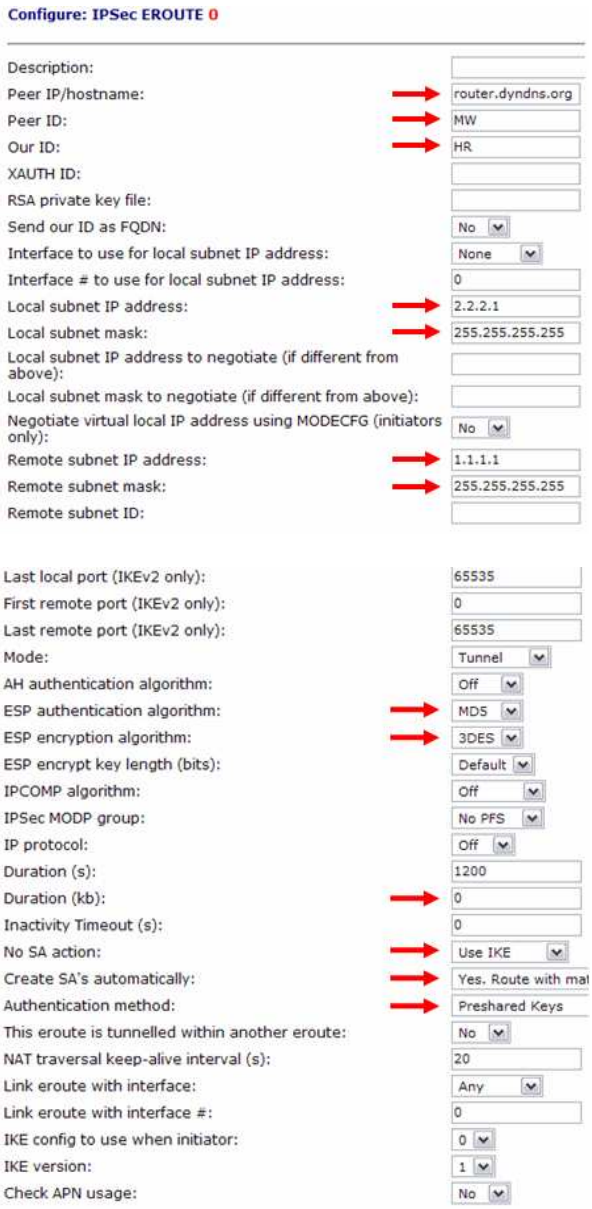
2.1 Configure IPSec

Configure > IPSec > IPSec Eroutes > Eroute 0

MW3520 (IPSec responder)



HR4110 (Initiator)

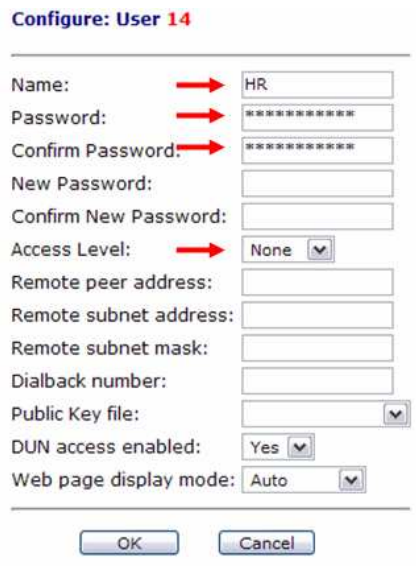


This Eroute config is exactly the same as a regular IPSec tunnel except for the following fields: Local subnet IP address, Local subnet mask, Remote subnet IP address, Remote subnet mask These fields are configured with a host IP address that does not actually exist (use an unused IP address from an unused subnet, it doesn't matter what is used). These are the end points of the IPSec tunnel. In this example 1.1.1.1 is used on the MW3520 and 2.2.2.1 is used on the HR4110, both with the subnet mask 255.255.255.255

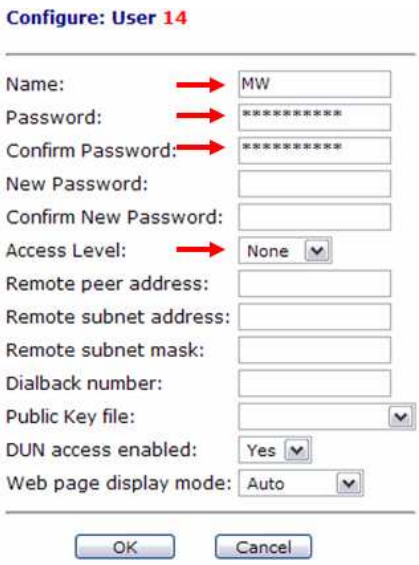
2.2 Configure Pre-Shared Key

Configure > Users > Users 10 - 14 > User 14

MW3520 (IPSec responder)



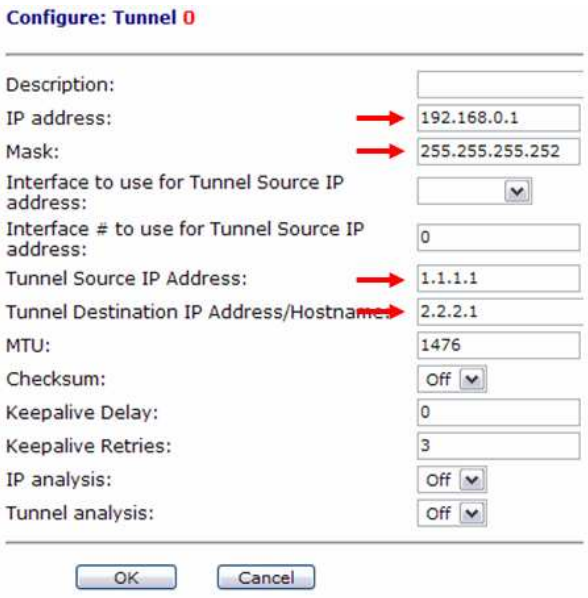
HR4110 (Initiator)



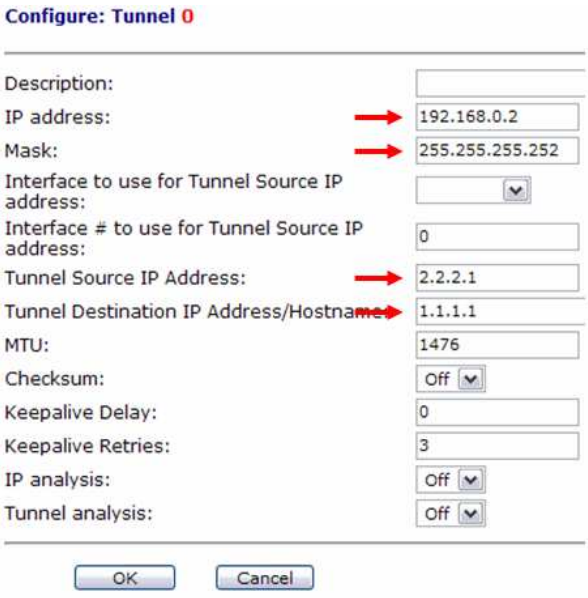
2.3 Configure GRE tunnels

Configure > Tunnel (GRE) > Tunnel 0

MW3520 (IPSec responder)



HR4110 (Initiator)

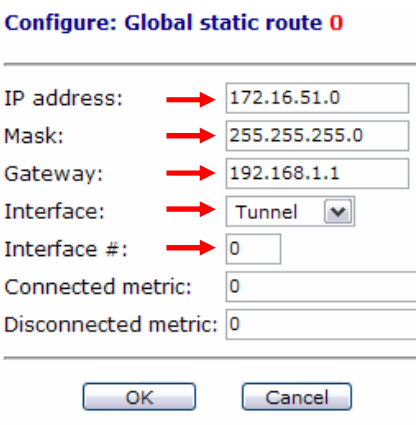


The GRE tunnel is configured as a point to point connection using the 192.168.0.0/30 subnet. Note the usage of the previously configured addresses 1.1.1.1 and 2.2.2.1 from within the Eroute settings, these are the source and destination IP addresses of the IPSec tunnel that GRE will tunnel through.

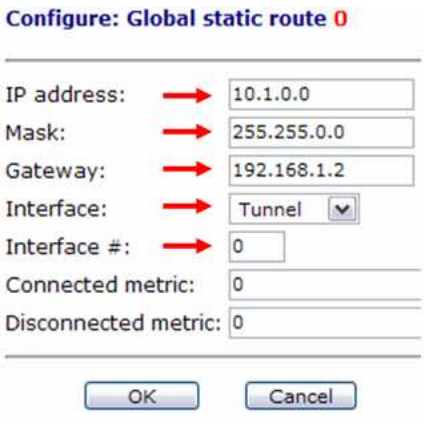
2.4 Configure routes

Configure > IP Routes > Global static routing table > Route 0 – 9 > Route 0

MW3520 (IPSec responder)



HR4110 (Initiator)



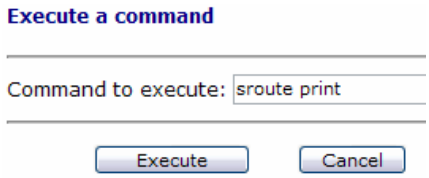
Routes are added for the remote LAN segments, notice that the interface in use is Tunnel 0 and the gateway is the local IP address of the GRE tunnel as previously configured in the Tunnel 0 settings.

2.5 Save your config changes to profile 0

3.0 Check the global static routing table

Execute a command

```
sroute print
```



MW3520 (IPSec responder)

```
flags: I = Interface, S = Static, H = Host,  D = Dynamic, O = Out of Service
flags             destination          gateway         protocol interface
---I-            10.1.0.0/16         10.1.51.2             TCP   ETH 0
-----          62.3.82.17/32     88.96.215.246             TCP   PPP 1
---I-       88.96.215.246/32     88.96.215.246             TCP   PPP 1
-S---         172.16.51.0/24       192.168.1.1             TCP   TUN 0
OK
```

HR4110 (Initiator)

```
flags: I = Interface, S = Static, H = Host,  D = Dynamic, O = Out of Service
flags             destination          gateway         protocol interface
-S---            10.1.0.0/16       192.168.1.2             TCP   TUN 0
---I-       10.182.17.131/32     10.182.17.131             TCP   PPP 1
---I-         172.16.51.0/24       172.16.51.2             TCP   ETH 0
OK
```

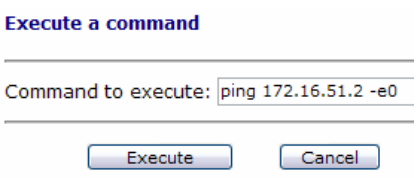
Viewing the global static routing table shows:
The local LAN segment will be available via ETH 0.
The internet facing interface will be PPP 1.
The remote LAN will be routed via TUN 0 and its gateway will be the local address of the GRE tunnel.

3.1 Test connectivity

Execute a command

```
ping <IP address of Eth0 on other router> <source port of ping>
```

MW3520 (IPSec responder)



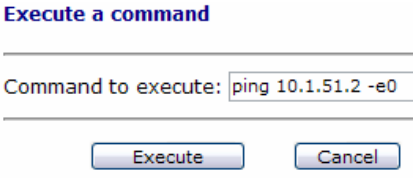
Command: ping 172.16.51.2 -e0
Command result

```
Pinging Addr [172.16.51.2]

sent PING # 1
PING receipt # 1 : response time 0.17 seconds
Iface: TUN 0
Ping Statistics
Sent         : 1
Received     : 1
Success      : 100 %
Average RTT : 0.17 seconds

OK
```

HR4110 (Initiator)



Command: ping 10.1.51.2 -e0
Command result

```
Pinging Addr [10.1.51.2]

sent PING # 1
PING receipt # 1 : response time 0.14 seconds
Iface: TUN 0
Ping Statistics
Sent         : 1
Received     : 1
Success      : 100 %
Average RTT : 0.14 seconds

OK
```