

Quick Note 006

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



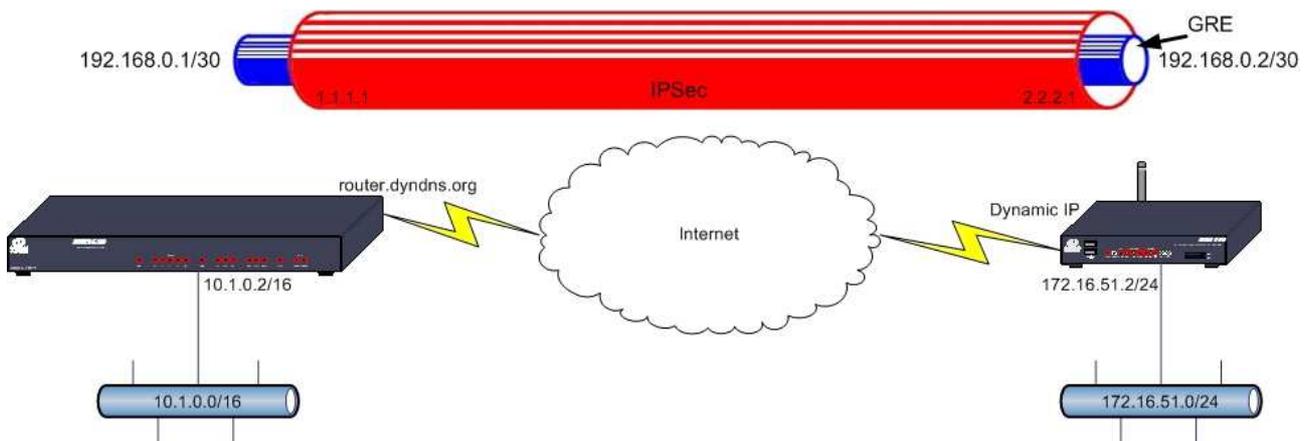
1.0 Version

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)

Configure: IKE 0 (Responder)

Act as initiator only:	No
Acceptable encryption algorithms:	AES,DES,3DES
Minimum Encryption key bits (AES only):	0
Acceptable authentication algorithms:	MD5,SHA1
Minimum acceptable IKE MODP group:	1 (768)
Maximum acceptable IKE MODP group:	5 (1536)
Duration (s):	1200
Inactivity timeout (s):	30
Send INITIAL-CONTACT notifications:	Yes
NAT traversal enabled:	Yes
NAT traversal keep-alive interval (s):	20
RSA private key file:	
SA removal mode:	Normal
Use debug port:	No
Debug level:	Off

Configure: IKE 0 (Initiator)

Encryption algorithm:	DES
Encryption key bits (AES only):	0
Authentication algorithm:	MD5
Duration (s):	1200
Aggressive mode:	On
Dead Peer Detection:	On
IKE MODP group:	1 (768)
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:	Yes
NAT traversal enabled:	Yes
NAT traversal keep-alive interval (s):	20
SA removal mode:	Normal
Use debug port:	No
Debug level:	Off

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)

Configure: IPsec EROUTE 0

Description:	
Peer IP/hostname:	
Peer ID:	HR
Our ID:	MW
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:	1.1.1.1
Local subnet mask:	255.255.255.255
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:	2.2.2.1
Remote subnet mask:	255.255.255.255
Remote subnet ID:	
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:	MDS
ESP encryption algorithm:	3DES
ESP encrypt key length (bits):	Default
IPCOMP algorithm:	Off
IPsec MODP group:	No PFS
IP protocol:	Off
Duration (s):	1200
Duration (kb):	0
Inactivity Timeout (s):	0
No SA action:	Drop Packet
Create SA's automatically:	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

Configure: IPsec EROUTE 0

Description:	
Peer IP/hostname:	router.dyndns.org
Peer ID:	MW
Our ID:	HR
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:	2.2.2.1
Local subnet mask:	255.255.255.255
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:	1.1.1.1
Remote subnet mask:	255.255.255.255
Remote subnet ID:	
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:	MDS
ESP encryption algorithm:	3DES
ESP encrypt key length (bits):	Default
IPCOMP algorithm:	Off
IPsec MODP group:	No PFS
IP protocol:	Off
Duration (s):	1200
Duration (kb):	0
Inactivity Timeout (s):	0
No SA action:	Use IKE
Create SA's automatically:	Yes. Route with mal
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

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)

Configure: User 14

Name:	→	HR
Password:	→	*****
Confirm Password:	→	*****
New Password:		
Confirm New Password:		
Access Level:	→	None
Remote peer address:		
Remote subnet address:		
Remote subnet mask:		
Dialback number:		
Public Key file:		
DUN access enabled:		Yes
Web page display mode:		Auto

OK Cancel

HR4110 (Initiator)

Configure: User 14

Name:	→	MW
Password:	→	*****
Confirm Password:	→	*****
New Password:		
Confirm New Password:		
Access Level:	→	None
Remote peer address:		
Remote subnet address:		
Remote subnet mask:		
Dialback number:		
Public Key file:		
DUN access enabled:		Yes
Web page display mode:		Auto

OK Cancel

2.3 Configure GRE tunnels

Configure > Tunnel (GRE) > Tunnel 0

MW3520 (IPSec responder)

Configure: Tunnel 0

Description:		
IP address:	→	192.168.0.1
Mask:	→	255.255.255.252
Interface to use for Tunnel Source IP address:		
Interface # to use for Tunnel Source IP address:		0
Tunnel Source IP Address:	→	1.1.1.1
Tunnel Destination IP Address/Hostname:	→	2.2.2.1
MTU:		1476
Checksum:		Off
Keepalive Delay:		0
Keepalive Retries:		3
IP analysis:		Off
Tunnel analysis:		Off

OK Cancel

HR4110 (Initiator)

Configure: Tunnel 0

Description:		
IP address:	→	192.168.0.2
Mask:	→	255.255.255.252
Interface to use for Tunnel Source IP address:		
Interface # to use for Tunnel Source IP address:		0
Tunnel Source IP Address:	→	2.2.2.1
Tunnel Destination IP Address/Hostname:	→	1.1.1.1
MTU:		1476
Checksum:		Off
Keepalive Delay:		0
Keepalive Retries:		3
IP analysis:		Off
Tunnel analysis:		Off

OK Cancel

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)

Configure: Global static route 0

IP address:	→	172.16.51.0
Mask:	→	255.255.255.0
Gateway:	→	192.168.1.1
Interface:	→	Tunnel
Interface #:	→	0
Connected metric:		0
Disconnected metric:		0

OK Cancel

Configure: Global static route 0

IP address:	→	10.1.0.0
Mask:	→	255.255.0.0
Gateway:	→	192.168.1.2
Interface:	→	Tunnel
Interface #:	→	0
Connected metric:		0
Disconnected metric:		0

OK Cancel

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

Save Config

Save current config to Config

0 (power up)

OK

Cancel

The SaveAll button will save the following
Save the current config to config 0.
Save the current firewall.
Save all the sregisters on all ports to profile 0.
Save all PAD parameters on all PADs to profile 0.

SaveAll

3.0 Check the global static routing table

Execute a command

```
route print
```

Execute a command

Command to execute:

Execute

Cancel

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)

Execute a command

Command to execute:

Execute

Cancel

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)

Execute a command

Command to execute:

Execute

Cancel

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

