

## MR-200/250 and DR-250

### The IPsec VPN Configuration



#### Technical Support

If you require assistance with any of the instructions in this application note you can contact Westermo as follows:

##### Sweden

www.westermo.com  
support@westermo.se  
Phone: +46 (0)16 42 80 00  
Fax: +46 (0)16 42 80 01

##### France

www.westermo.fr  
support@westermo.fr  
Tél : +33 1 69 10 21 00  
Fax : +33 1 69 10 21 01

##### United Kingdom

Web: www.westermo.co.uk  
Technical e-mail: technical@westermo.co.uk  
Telephone: +44 (0)1489 580585  
Fax: +44 (0)1489 580586

##### Singapore

www.westermo.com  
E-mail: sales@westermo.com.sg  
Phone +65 6743 9801  
Fax +65 6745 0670

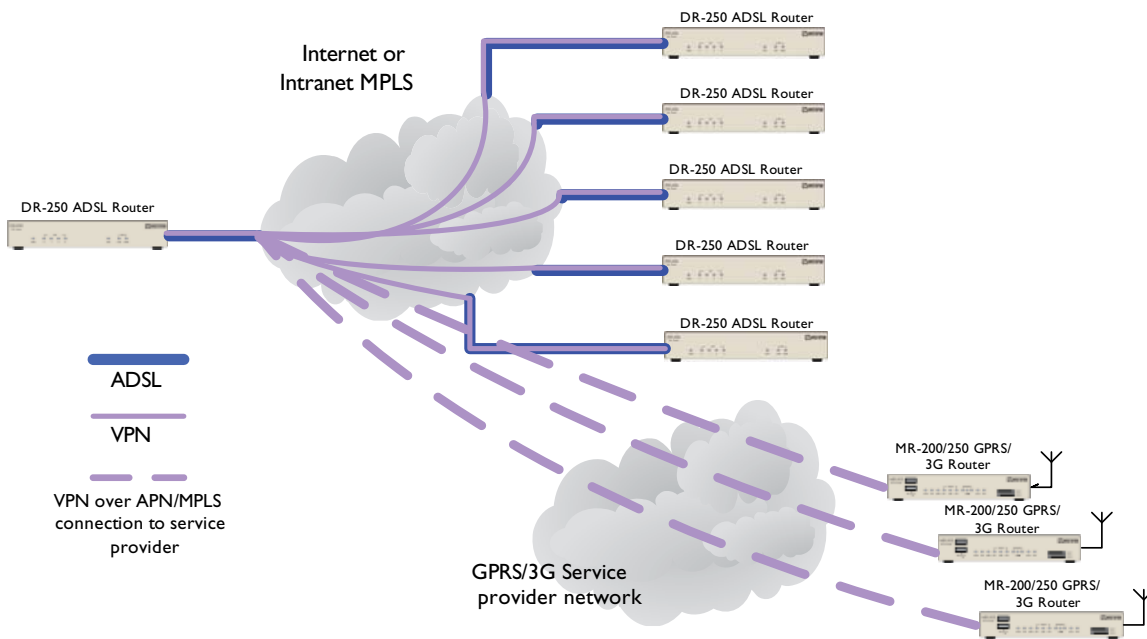
##### Germany

www.westermo.de  
support@westermo.de  
Tel: +49(0)7254 95400-0  
Fax: +49(0)7254-95400-9

## Introduction

This application note describes how to implement an IPsec VPN between two Westermo MR or DR series routers. When creating a VPN between an MR and DR series router the MR should always be the Initiator and the DR the Responder. Applications where there are many remote location with VPN's to a single location (see diagram below) the Remote router should be the Initiator and the central location the Responder. To create VPN's from a Westermo MR or DR router to a third party router please contact your local Westermo support organization for advice.

## VPN configuration over WAN network



## Encapsulation using PPOE or PPOA

**Configure: PPP 1 (Standard)**

Name: ADSL  
Username: 1489579936\_csl@dslconnect.co.u  
Password (Assigned):  
Confirm password:  
IPsec: ON-Remove SAs when link down

OK  
Load answering defaults

To allow the IPSEC packets over the PPP interface the Ipsec must be set to on. Note changes to the PPP interface will require the interface to be dropped and restarted.

## Encapsulation using Bridge mode

**Configure: Ethernet 4**

Physical port: ATM PVC 0  
Description:  
DHCP client: Enabled  
Mask:  
NAT mode: NAT  
IPsec: ON-Remove SAs when link down

OK Cancel

## IKE 0 Initiator

**Configure: IKE 0 (Initiator)**

Encryption algorithm: DES  
Encryption key bits (AES only): 0  
Authentication algorithm: MD5  
Duration (s): 1200  
Aggressive mode: On  
NAT traversal enabled: Yes  
Debug level: Off

OK Cancel

The IKE responder can be left at default

The duration value controls the length of time the key will be valid. On GPRS and 3G based system it is a good idea to have a longer duration (Max 28800).

Turn Aggressive Mode On

## Eroute Setup

The tunnel parameters must be the same at both ends of the tunnel or the negotiation will fail

Initiator Eroute

Responder Eroute

The image shows two configuration windows side-by-side. The left window is titled 'Configure: IPsec ERROUTE 0' and the right is 'Configure: IPsec ERROUTE 1'. Both windows have the following fields: Description, Peer IP/hostname, Peer ID, Our ID, Local subnet IP address, Local subnet mask, Remote subnet IP address, Remote subnet mask, Mode, AH authentication algorithm, ESP authentication algorithm, ESP encryption algorithm, ESP encrypt key length (bits), Duration (s), Duration (kb), No SA action, Create SA's automatically, and Authentication method. Blue callouts point to the Peer IP/hostname field in the Initiator window, stating 'IP Address or Host Name for the termination point of the VPN tunnel'. Another callout points to the Duration (s) field in the Responder window, stating 'The duration value controls the length of time the SA will be valid.' A large callout in the center, spanning both windows, states 'These parameters must be the same at both end of the tunnel' and has arrows pointing to the Peer ID, Local subnet IP address, Remote subnet IP address, Mode, and Authentication method fields in both windows.

## Preshared Key Setup

Preshared key entry Initiator

The screenshot shows the 'Configure: User 14' window. Fields include Name (Eagle), Password (masked with dots), Confirm Password (masked with dots), Access Level (Low), and Web page display mode (Auto). Callouts point to the Name field (stating 'The user number is not important') and the Password field (stating 'Password should be entered here').

The user number is not important

The user name will be the Peer ID. The password must be the same on both sides of the VPN

Password should be entered here

Preshared key entry Responder

The screenshot shows the 'Configure: User 13' window. Fields include Name (hawk), Password (empty), Confirm Password (empty), Access Level (Low), and Web page display mode (Auto). A callout points to the Password field (stating 'Password should be entered here').

Password should be entered here

## Config.da0 files shown are for a DR-250

Config.da0 Initiator	Config.da0 Responder
CFG]	[CFG]
config last_saved "10:27:49, 19 Feb 2008"	config last_saved "10:27:49, 19 Feb 2008"
config last_saved_changes "1"	config last_saved_changes "1"
config last_saved_user "username"	config last_saved_user "username"
eth 0 IPAddr "192.168.83.1"	eth 0 IPAddr "197.67.51.1"
lapb 0 ans OFF	lapb 0 ans OFF
lapb 2 dtemode 2	lapb 2 dtemode 2
lapb 3 dtemode 2	lapb 3 dtemode 2
def_route 0 ll_ent "PPP"	def_route 0 ll_ent "PPP"
def_route 0 ll_add 1	def_route 0 ll_add 1
eroute 0 descr "Demo Eroute Initiator"	eroute 1 descr "Demo Eroute Responder"
eroute 0 peerip "80.34.56.91"	eroute 1 peerid "Hawk"
eroute 0 peerid "Eagle"	eroute 1 ourid "Eagle"
eroute 0 ourid "Hawk"	eroute 1 locip "197.67.51.0"
eroute 0 locip "192.168.83.0"	eroute 1 locmsk "255.255.255.0"
eroute 0 locmsk "255.255.255.0"	eroute 1 remip "192.168.83.0"
eroute 0 remip "197.67.51.0"	eroute 1 remmsk "255.255.255.0"
eroute 0 remmsk "255.255.255.0"	eroute 1 ESPauth "MD5"
eroute 0 ESPauth "MD5"	eroute 1 ESPenc "3DES"
eroute 0 ESPenc "3DES"	eroute 1 ltime 6000
eroute 0 ltime 6000	eroute 1 authmeth "PRESHARED"
eroute 0 authmeth "PRESHARED"	ppp 1 IPAddr "0.0.0.0"
eroute 0 nosa "TRY"	ppp 1 username "Enter ADSL Username"
eroute 0 autosa 2	ppp 1 timeout 0
ppp 1 IPAddr "0.0.0.0"	ppp 1 aodion 1
ppp 1 username "Enter ADSL Username"	ppp 1 autoassert 1
ppp 1 timeout 0	ppp 1 ipsec 1
ppp 1 aodion 1	ppp 1 echo 10
ppp 1 autoassert 1	ppp 1 echodropcnt 5
ppp 1 ipsec 1	ppp 1 l1iface "AAL"
ppp 1 echo 10	ana 0 anon ON
ppp 1 echodropcnt 5	ana 0 lapdon 0
ppp 1 l1iface "AAL"	ana 0 lapbon 0

Config.da0 Initiator	Config.da0 Responder
ana 0 anon ON	ana 0 maxdata 200
ana 0 lapdon 0	ana 0 logsize 45
ana 0 lapbon 0	cmd 0 unitid "DR-250"
ana 0 maxdata 200	cmd 0 cmdnua "99"
ana 0 logsize 45	cmd 0 hostname "SS.6000r"
cmd 0 unitid "DR-250"	cmd 0 asyled_mode 1
cmd 0 cmdnua "99"	cmd 0 tremto 1200
cmd 0 hostname "SS.6000r"	user 0 name "username"
cmd 0 asyled_mode 1	user 0 access 0
cmd 0 tremto 1200	user 1 name "westermo"
user 0 name "username"	user 1 access 0
user 0 access 0	user 2 access 0
user 1 name "Westermo"	user 3 access 0
user 1 access 0	user 4 access 0
user 2 access 0	user 5 access 0
user 3 access 0	user 6 access 0
user 4 access 0	user 7 access 0
user 5 access 0	user 8 access 0
user 6 access 0	local 0 transaccess 2
user 7 access 0	[ENDCFG]
user 8 access 0	
user 14 name "Eagle"	
local 0 transaccess 2	
[ENDCFG]	