Remote access VPN IPsec

Accessing the MRD-3xx Indsutrial 3G router using TheGreenBow IPSec VPN Client

IPsec VPN

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The main purpose of a VPN is to give the company the same capabilities as private leased lines at much lower cost by using the shared public infrastructure. Phone companies have provided private shared resources for voice messages for over a decade. A virtual private network makes it possible to have the same protected sharing of public resources for data.

IPsec is a suite of protocols for providing peer authentication without transmitting the actual keys. Confidentiality using encryption and integrity ensuring that the received data can only come from the authenticated peer and has not been altered in any way.

IPsec Encrypting Security Payload tunnels also provide transparency for all nodes and applications using IP and only the VPN gateways needs to be configured to securely connect geographically separated networks.

Firstly we will describe and determine all the parameters necessary for this configuration. These values will be written into the “IPsec Network setup table”

The numbers and parameter values from the “IPsec Network setup table” will be used throughout this guide while first configuring the responder and then the initiator.

Network setup description

This application note describes how to implement a Remote access IPsec VPN tunnel between TheGreenBow IPsec VPN Client and a Westermo MRD-330 Industrial 3G Router.

TheGreenBow IPsec VPN Client will probably have a dynamically assign IP address and may or may not be behind a Network Address Translation (NAT) device. As such we must assume that we need NAT traversal and TheGreenBow will be the initiator.

In this example the MRD-330 has a 3G subscription that provides a static public IP address. Since we want to access the MRD-330 it has to be the responder.

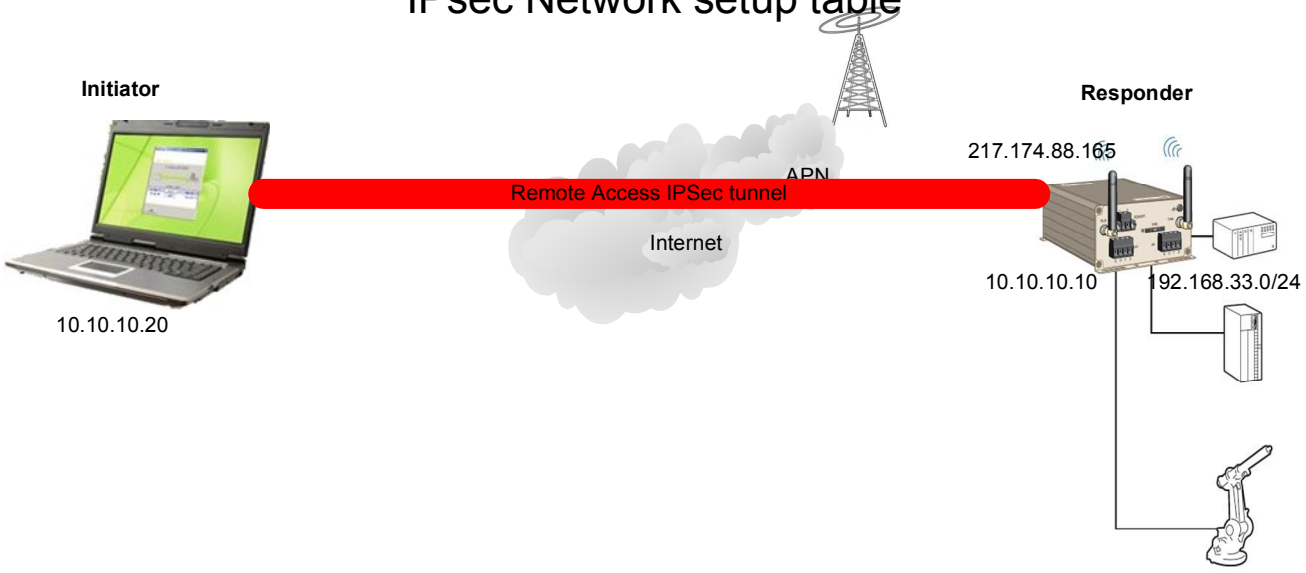
For authentication we will be using Pre-Shared Key (PSK). Simple and practical for initial and small-scale VPN configurations it is however very susceptible to social engineering and large scale or long-term deployment should use certificates for authentication.
This IPsec configuration uses Internet Key Exchange (IKEv1). If the IP addresses of both parties are fixed or certificates are used it is recommended to use IKE main mode which takes longer to establish connection but provides a higher level of security than aggressive mode.
In this example the combination of dynamic IP address and preshared key requires us to use IKE aggressive mode.

IKE supports many different types of identifiers (ID). For this example we have chosen type 2 FQDN. Please review RFC 2407 for further options.

Encapsulated Security Payload (ESP) is the final encrypted tunnel joining initiator/responder together. An ESP tunnel is unidirectional so two tunnels are used for full duplex communication. Advanced Encryption Standard (AES) is the recommended encryption standard to use since it is more secure and more efficient than the older 3DES encryption.

This configuration is valid for:
TheGreenBow IPsec VPN Client 4.5
Westermo MRD-310/330 firmware version 1.11

IPsec Network setup table



			Initiator				Responder
General							
	External Address IP or FQDN	1	0.0.0.0			2	217.174.88.165
	Internal IP address	3	10.10.10.20			4	10.10.10.10
	Internal subnet mask	5	255.255.255.255			6	255.255.255.255
	ID type	7	2		RFC2407	8	2
	ID value	9	greenbow			10	mrd330
	PSK			11	54321		
	Certificate	12				13	
	NAT Traversal			14	YES		
	NAT-T keepalive			15	20s		
	Dead Peer Detection			16	YES		
	DPD delay & timeout			17	30s/15s		
	MTU	18				19	
IKE phase 1							
	Mode			20	Aggressive		
	Encryption			21	AES (128)		
	Authentication			22	MD5		
	Diffie Hellman Group			23	2		
	IKE SA Lifetime			24	3600s		
IKE phase 2							
	ESP encryption			25	AES (128)		
	ESP authentication			26	MD5		
	SA Lifetime			27	28800s		
	Perfect Forward Secrecy			28	2		

Responder configuration

Make sure you have configured your MRD-3xx router as described in the User Guide.
The firewall on the MRD-330 will deny all connection attempts by default. In order for us to connect with IPsec we must open the firewall to IKE udp ports 500 and 4500 aswell as allow ESP (IP protocol 50)

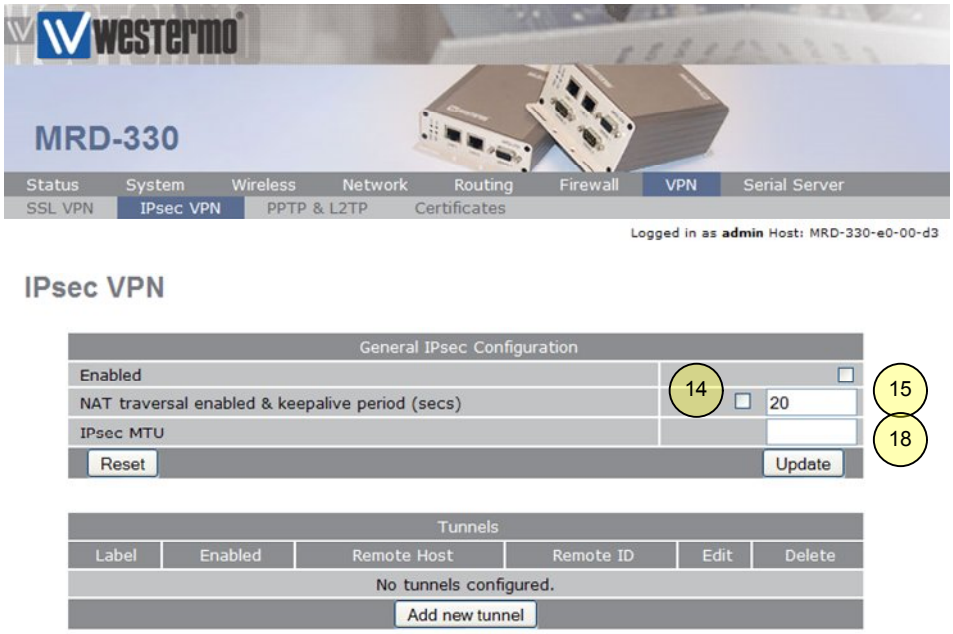
Select Firewall in the top most menu followed by Access Control in the submenu.
Select allow for IPsec VPN on the wireless interface (WLS) and press update.

IPsec VPN Configuration

Make sure you have configured your MRD-3xx router as described in the User Guide. Access the routers web interface and select VPN in the top menu followed by ”IPsec VPN” in the submenu.

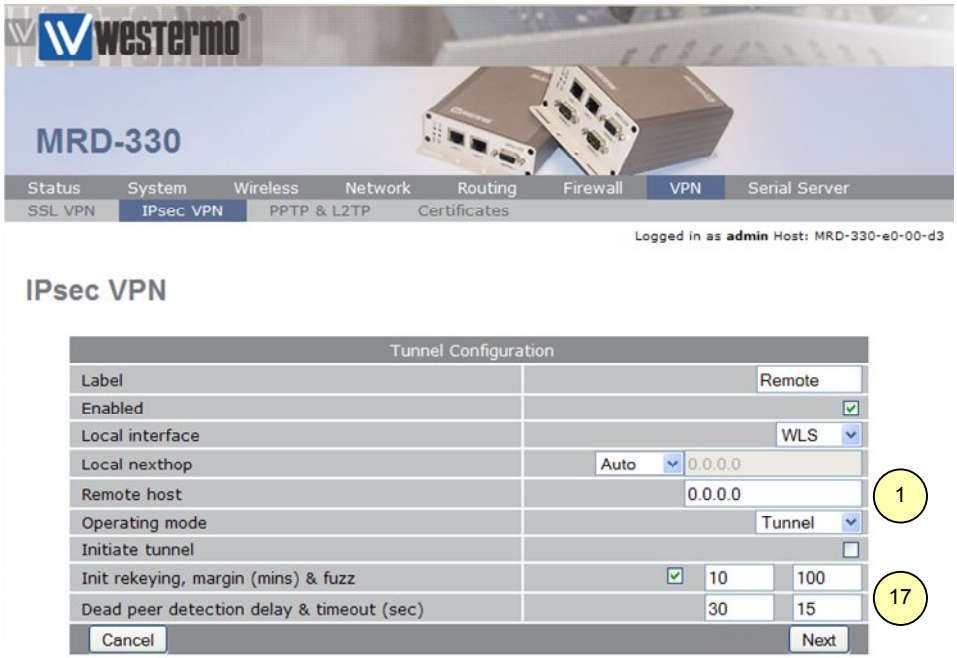
Select ”Enabled” and NAT traversal followed by update.

To create a new tunnel click the Add new tunnel button.



The web interface requires a Remote host to move to the next step but since we can not know the address we use 0.0.0.0 to indicate that the remote host can have any IP address.

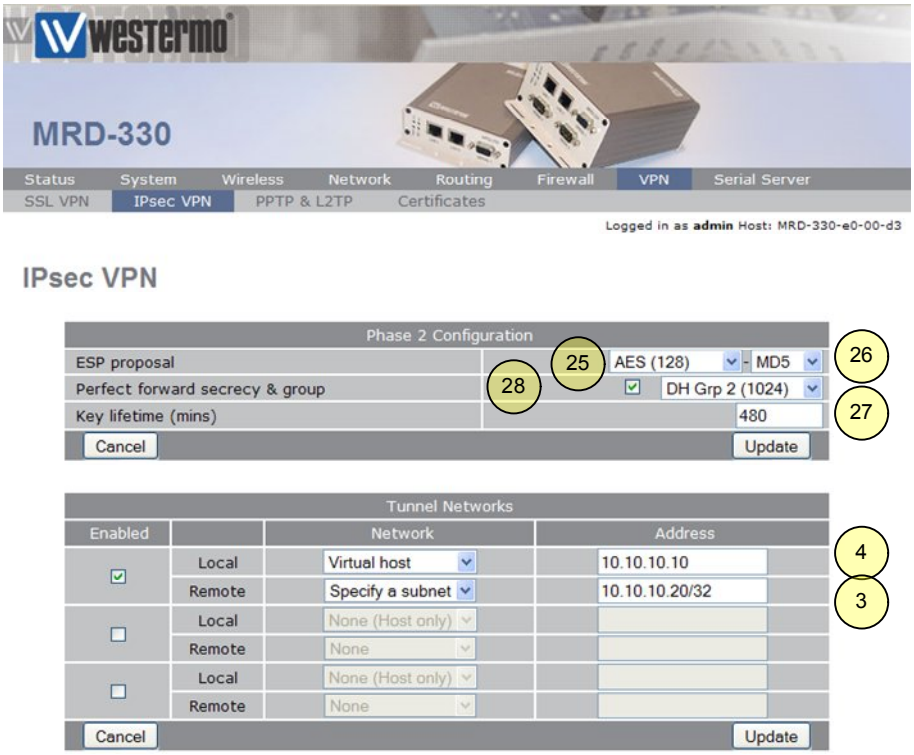
We cannot access the private IP address of the initiator and as such the responder should not ”Initiate tunnel”



IKE phase configuration

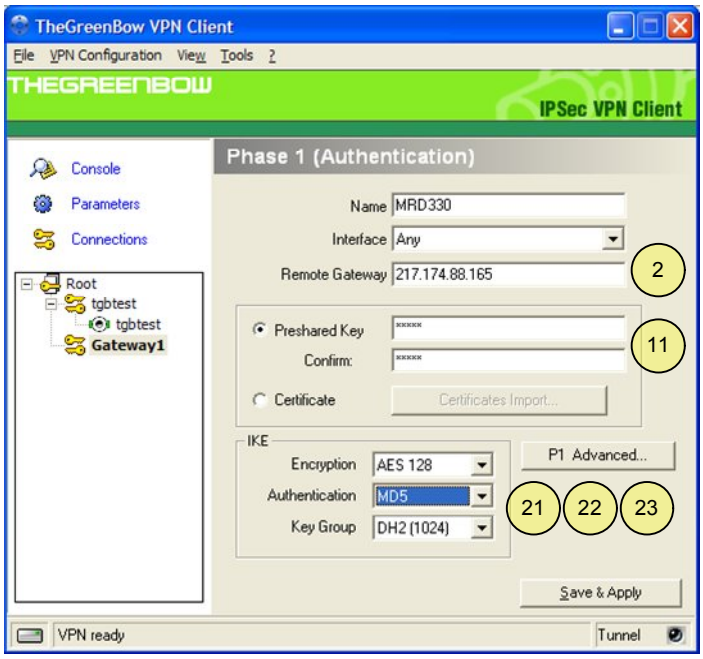
Next we configure the authentication and proposal for Internet Key Exchange (IKE)
The ID must be preceeded with a @ sign to indicate a type 2 or 3 ID (RFC2407) string.

Phase 2 configures two ESP tunnels for the actual protected traffic. The newer less CPU intensive AES encryption should be preferred before 3DES.
For Remote access we are using endpoint addresses or virtual hosts where the MRD-330 will have the internal address 10.10.10.10 and the client 10.10.10.20

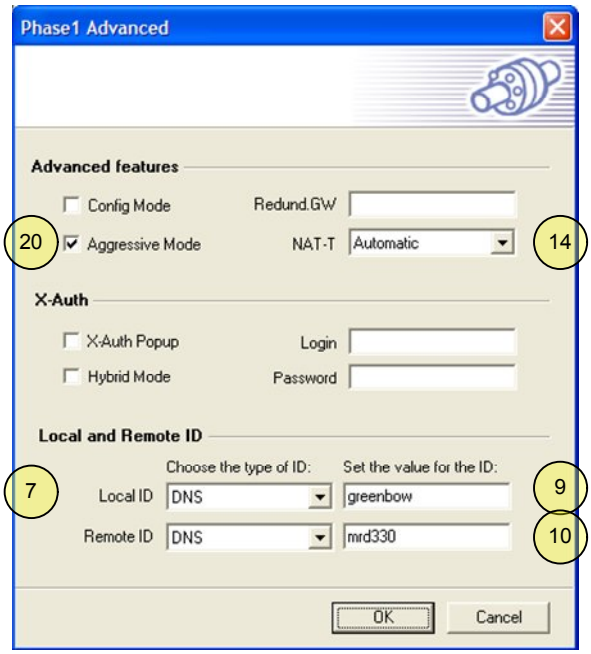


TheGreenbow VPN client configuration

TheGreenBow VPN client is available on trial from http://www.thegreenbow.com/vpn_down.html
Once installed open the configuration window and start a new phase 1.

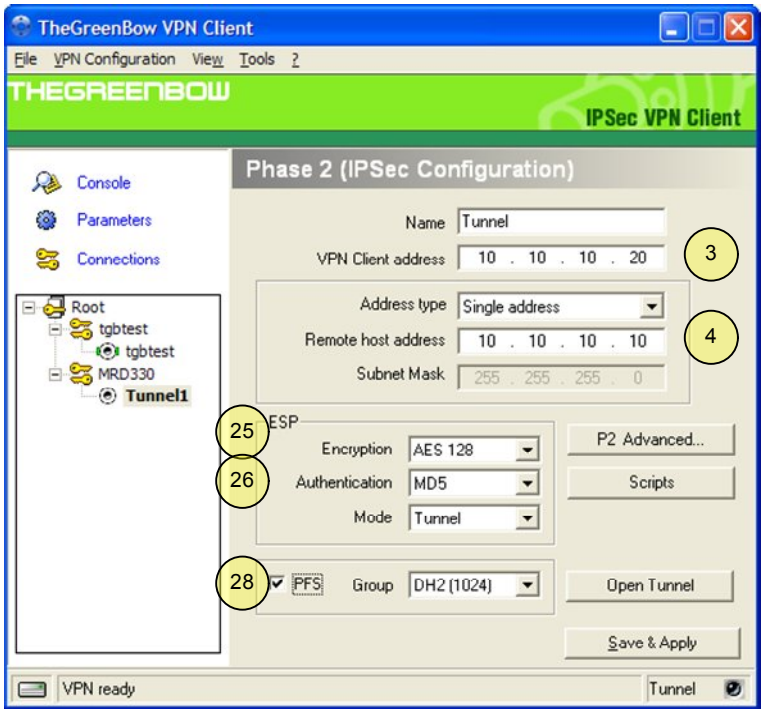


Enter a gateway name and the Responder address. Preshared key and IKE encryption, authentication and Diffie Hellman group must match what has been entered in the MRD330.
Remember to Save & Apply
Next open the ”P1 Advanced…" window and enter Local and Remote ID type and value. Select Aggressive Mode and click OK
Remember to Save & Apply

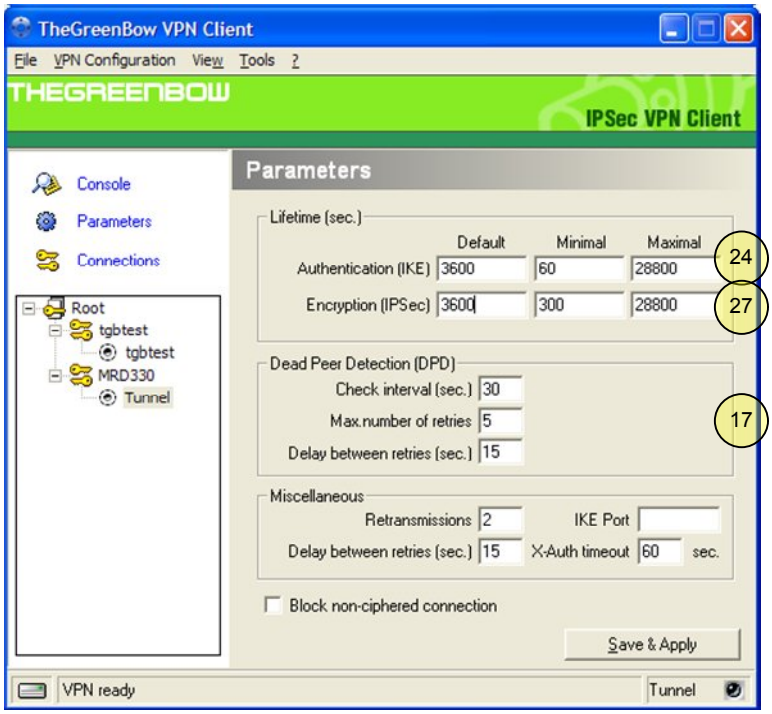


Tunnel configuration

Right click on the Phase 1 entry ”MRD330" and select ”add Phase 2".
Choose a name for the tunnel and enter the virtual host IP address of both client(Initiator) and Remote host(Responder). Select the correct Encryption, authentication and mode (tunnel).
Press ”Save & Apply”

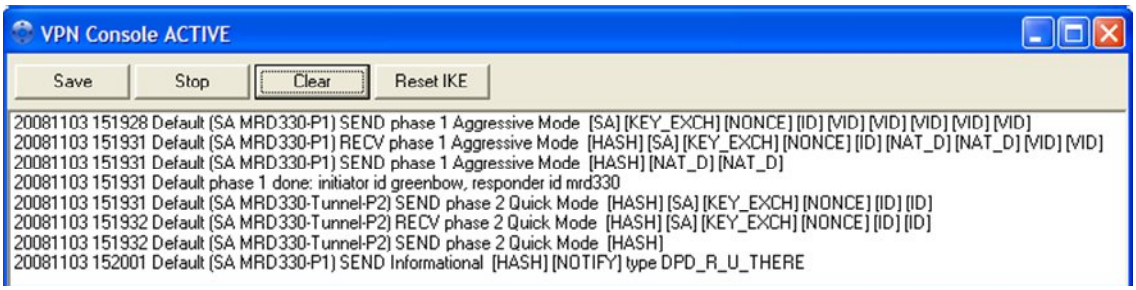


Select ”Parameters” from the left side menu and enter the correct Lifetime and Dead Peer Detection values.
Press ”Save & Apply”

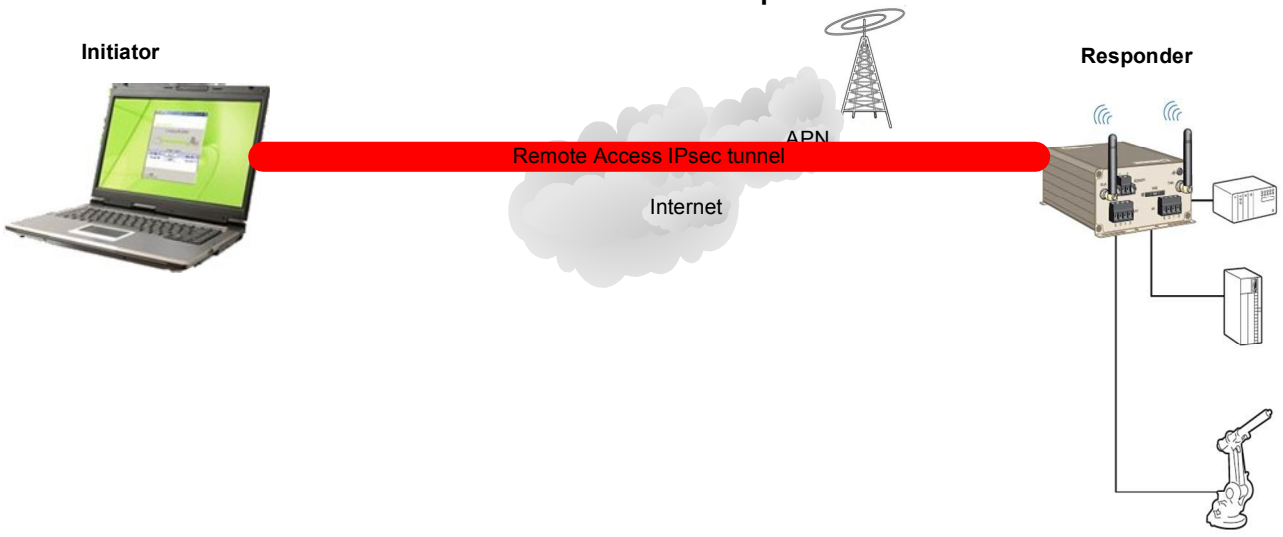


Diagnostics

Open TheGreenBow VPN client connection panel and press ”Open” on the MRD330-Tunnel.
Progress or errors can be viewed in TheGreenBow Console and the MRD-330 Status > Syslog.
Once connected you should be able to open the MRD-330 web interface on address 10.10.10.10



IPsec Network setup table



		Initiator			Responder	
General						
	External Address IP or FQDN	1			2	
	Internal IP address	3			4	
	Internal subnet mask	5			6	
	ID type	7			8	
	ID value	9			10	
	PSK			11		
	Certificate	12			13	
	NAT Traversal			14		
	NAT-T keepalive			15		
	Dead Peer Detection			16		
	DPD delay & timeout			17		
	MTU	18			19	
IKE phase 1						
	Mode			20		
	Encryption			21		
	Authentication			22		
	Diffie Hellman Group			23		
	IKE SA Lifetime			24		
IKE phase 2						
	ESP encryption			25		
	ESP authentication			26		
	SA Lifetime			27		
	Perfect Forward Secrecy			28		

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

Sweden
www.westermo.se
support.sverige@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@westermo.co.uk
Telephone: +44 (0)1489 580585
Fax: +44 (0)1489 580586

Singapore
www.westermo.com
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