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 smallscale VPN configurations it is however very susceptible to social engineering and large scale or longterm 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



			Initiator				Responder
General							
External Addres	s IP or FQDN 1		0.0.0.0			2	217.174.88.165
Internal IP addre	ess 3	3	10.10.10.20			4	10.10.10.10
Internal subnet	mask 5	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	2				13	
NAT Traversal				14	YES		
NAT-T keepalive	2			15	20s		
Dead Peer Dete	ection			16	YES		
DPD delay & tir	neout	_		17	30s/15s		
MTU	18	8				19	
IKE phase 1	_						
Mode				20	Aggressive	_	
Encryption				21	AES (128)		
Authentication				22	MD5		
Diffie Hellman G	Group			23	2		
IKE SA Lifetime	•			24	3600s		
IKE phase 2	_						
ESP encryption				25	AES (128)		
ESP authentica	tion			26	MD5		
SA Lifetime				27	28800s		
Perfect Forward	Secrecy			28	2		

Wester



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.

W	western	no		1	1000	6.8.1	122222
MR	0-330						
Status	System	Wireless	Network	Routing	Firewall	VPN	Serial Server
Setup	Access Cor	ntrol DoS	Filters	Custom Filters	Port For	wards	Custom NAT

Logged in as admin Host: MRD-330-e0-00-d3

Access Control

External Access Control	Incoming Interface						
External Access Control		WLS		VPN			
Default policy	D	eny 🔽	A	llow 💌			
Services	Allow						
Web Server		80		80			
Secure Web Server		443		443			
Telnet Server		23		23			
SSH		22		22			
SNMP		162		161			
DNP3							
Serial Server							
IPsec VPN		1					
Respond to ICMP (Ping)							
Reset				Update			
Allow IPsec VPN access							



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.

No tunnels configured.

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



TheGreenBow[™] IPsec VPN Client

www.westermo.com

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.

	vesterma	j	12	A Second	0.4	131	122222	
MRD)-330						•	
Status	System	Wireless	Network	Routing F	Firewall	VPN	Serial Server	
			Pha	se 1 Configuration				
Aut	thentication met	thod		se i comgaration	_		Preshared key	~
Pre	-shared key			Not se	t New:	5432	1 (1	1)
Cer	tificate					No ce	rtificates loaded. >	\prec
Ren	note ID					@gre	eenbow (9)
Loc	al ID				(10) @mr	d330	\prec
Neg	gotiation mode			\frown		Ag	gressive mode 💌 🤇 2	20)
IKE	proposal	(2	1)(22)	(23) AES (128) 🗸 - MD	5 🔽 - DH	Grp 2 (1024)	\prec
IKE	lifetime (mine)						Construction of the second	
	meane (mins)	-		\smile			60 2	24)

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[™] IPsec VPN Client

www.westermo.com

TheGreenbow VPN client configuration

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

TheGreenBow VPN CI	ient 📃 🗖 🔀
Eile VPN Configuration Viev	I Tools 2
THEGREENBOU	IPSec VPN Client
Console Parameters Connections Root Gateway1	Phase 1 (Authentication) Name MRD330 Interface Any Remote Gateway 217.174.88.165 Preshared Key 2 Preshared Key 11 Confirm: 11 Certificate Certificates Import Image: Key P1 Advanced Authentication MD5 Image: Very State 2
VPN ready	Key Group DH2 (1024)

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

	Phase1 Advanced	
		53)
	Advanced features	
	Config Mode Redund.GW	
	20	Automatic 🔹 🚺
	X-Auth	
I	TX-Auth Popup Login	
	Hybrid Mode Password	
	Local and Remote ID	
ł	Choose the type of ID:	Set the value for the ID:
	Local ID DNS	greenbow
	Remote ID DNS	mrd330 (10
		OK Cancel

TheGreenBow[™] IPsec VPN Client

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"

TheGreenBow VPN Clie	ent	
Eile VPN Configuration View	Tools 2	
THEGREENBOW	6	IPSec VPN Client
😣 Console	Phase 2 (IPSec Configuration)
Parameters	Name Tunnel	
S Connections	VPN Client address 10 . 10	. 10 . 20 3
Root Stybtest Stybtest Stybtest Styptest	Address type Single address Remote host address 10 . 10 Subnet Mask 255 . 255	10 . 10 255 . 0
	Encryption AES 128	P2 Advanced
	26) Authentication MD5 💌	Scripts
	Mode Tunnel 🔽	
	28 FFS Group DH2 (1024)	Open Tunnel
		Save & Apply
VPN ready		Tunnel 🥑

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

HEGREENBOL	J IPSec VPN Clien
💫 Console	Parameters
ParametersConnections	Lifetime (sec.) Default Minimal Maximal Authentication (IKE) [3600 [60 [28800
Root	Encryption (IPSec) 3600 300 28800
Gradiente G	Dead Peer Detection (DPD) Check interval (sec.) 30 Max.number of retries 5
	Delay between retries (sec.) 15
	Miscellaneous IKE Port Retransmissions 2 Delay between retries (sec.) 15 X-Auth timeout 60
	Block non-ciphered connection
	Save & Apply

TheGreenBow[™] IPsec VPN Client

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

TheGreenBov	v VPN Client	
	T	IEGREENBOW
MRD	330-Tur	nnel
TT.		
	funnel onened	
tgbtest-tgbtest	Open	closed
MRD330-Tunnel	Close	O opened
Configuration		Close

VPN Conse	ole ACTIVE			
Save	Stop	Clear	Reset IKE	
20081103 15192 20081103 15193 20081103 15193 20081103 15193 20081103 15193 20081103 15193 20081103 15193 20081103 15193	28 Default (SA 31 Default (SA 31 Default (SA 31 Default phas 31 Default (SA 32 Default (SA 32 Default (SA 32 Default (SA	MRD 330-P1) SEN MRD 330-P1) REC MRD 330-P1) SEN se 1 done: initiator i MRD 330-T unnel-P MRD 330-T unnel-P MRD 330-T unnel-P MRD 330-P1) SEN	D phase 1 Aggr V phase 1 Aggr D phase 1 Aggr d greenbow, re 2) SEND phase 2) RECV phase 2) SEND phase D Informational	essive Mode [SA] [KEY_EXCH] [NONCE] [ID] [VID] [VID] [VID] [VID] [VID] essive Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [NAT_D] [NAT_D] [VID] essive Mode [HASH] [NAT_D] [NAT_D] sponder id mrd330 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID] 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]





	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	e 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	

TheGreenBow[™] IPsec VPN Client

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

United Kingdom

Web: <u>www.westermo.co.uk</u> technical@westermo.co.uk Telephone: +44 (0)1489 580585 Fax: +44 (0)1489 580586

Germany

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

France

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

Singapore

www.westermo.com sales@westermo.com.sg Phone +65 6743 9801 Fax +65 6745 0670