

LAN to LAN IPsec VPN

Between MRD-3xx 3G routers and Cisco ASA 5500 series



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 secondly the initiator.

Network setup description

This application note describes how to implement a LAN to LAN IPsec VPN tunnel between a Westermo MRD-310 3G Router and a Cisco 5500 series Adaptive Security Appliance.

It is important to decide which of the two routers will be the initiator and which will be the responder. In nearly all cases, the responder will be a VPN gateway, which is located at a central location, such as company headquarters. In all cases the responder must have a publicly accessible IP address to connect across internet.

In this example the MRD-310 has a 3G subscription that dynamically assigns a private IP address and is hidden behind a Network Address Translation (NAT) device. As such it can only be the initiator.

The ASA 5505 has a fixed public IP address. The ASA 5505 will 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. 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 gateways 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.

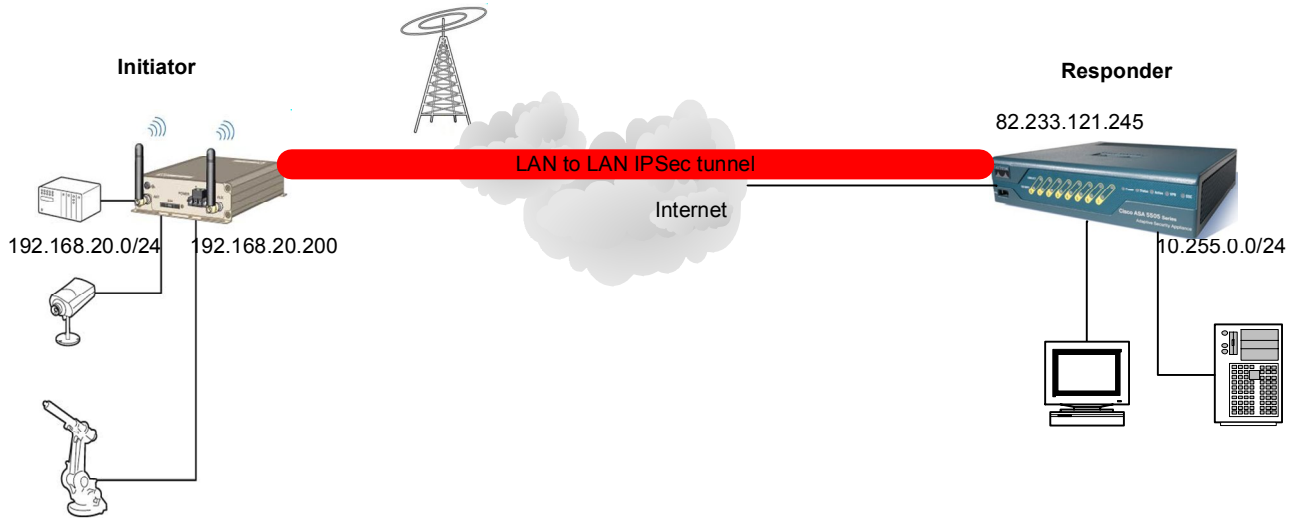
IKE supports many different types of identifiers (ID) for this example we have chosen type 2 FQDN.

Please review RFC 2407 for further details.

Encapsulated Security Payload (ESP) is the final encrypted tunnel joining the two LAN together. A 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:
Westermo MRD-310 firmware version 1.11
Cisco ASA 5500 series 8.0(2)

IPsec Network setup table



	Initiator		Responder	
General				
External Address IP or FQDN	1	any	2	82.233.121.245
Internal IP address	3	192.168.20.0	4	10.255.0.0
Internal subnet mask	5	255.255.255.0	6	255.255.255.0
ID type	7	2	8	2
ID value	9	mrdsa	10	vidar
PSK			11	secret
Certificate	12		13	
NAT Traversal			14	YES
NAT-T keepalive			15	20s
Dead Peer Detection			16	NO
DPD delay & timeout			17	120s/10s
MTU	18		19	
IKE phase 1				
Mode			20	Aggressive
Encryption			21	AES (128)
Authentication			22	SHA1
Diffie Hellman Group			23	2
IKE SA Lifetime			24	28800s
IKE phase 2				
ESP encryption			25	AES (128)
ESP authentication			26	SHA1
SA Lifetime			27	28800s
Perfect Forward Secrecy			28	

Cisco ASA 5505 Responder VPN configuration

First configure access-lists to exempt the protected networks from network address translation.

Create a access-list to be used by for the tunnel networks (inside_cryptomap_65535.11)

```
access-list inside_nat0_outbound extended permit 10.255.0.0 255.255.255.0 \
192.168.20.0 255.255.255.0
access-list inside_cryptomap_65535.11 extended permit ip 10.255.0.0 \
255.255.255.0 192.168.20.0 255.255.255.0
```

Add the access-list to the NAT of the outside interface

```
nat-control
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.255.0.0 255.255.255.0
```

Configure the crypto parameters

```
crypto ipsec transform-set mrdset esp-aes esp-sha-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 11 match address
inside_cryptomap_65535.11
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 11 set transform-set mrdset
crypto map outside_map interface outside
crypto isakmp identity hostname
crypto isakmp enable outside
```

Configure the IKE phase 1

```
crypto isakmp policy 10
  authentication pre-share
  encryption aes
  hash sha
  group 2
  lifetime 28800
```

Configure a group policy to use in the following tunnel-group

```
group-policy westermo internal
group-policy westermo attributes
  vpn-tunnel-protocol IPSec
  vpn-group-policy westermo
```

Finally configure the tunnel group

```
tunnel-group mrdasa type ipsec-l2l
tunnel-group mrdasa general-attributes
  default-group-policy westermo
tunnel-group mrdasa ipsec-attributes
  pre-shared-key *
  isakmp keepalive threshold 120 retry 10
  peer-id-validate nocheck
```

MRD-310 Initiator VPN configuration

Make sure you have configured your MRD-3xx 3G 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 sub menu. Press **Add new tunnel** to start configuring a new VPN tunnel. The local interface should be WLS for the wireless 3G/GPRS interface.



IPsec VPN

Tunnel Configuration	
Label	MRD2ASA
Enabled	<input checked="" type="checkbox"/>
Local interface	WLS
Local nexthop	Auto 0.0.0.0
Remote host	82.233.121.245
Operating mode	Tunnel
Initiate tunnel	<input checked="" type="checkbox"/>
Init rekeying, margin (mins) & fuzz	<input checked="" type="checkbox"/> 10 100
Dead peer detection delay & timeout (sec)	120 10
<input type="button" value="Cancel"/> <input type="button" value="Next"/>	

2

17

Press **Next**

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



IPsec VPN

Phase 1 Configuration	
Authentication method	Preshared key
Pre-shared key	Not set New: <input checked="" type="checkbox"/> secret
Certificate	No certificates loaded.
Remote ID	@vidar
Local ID	@mrdasa
Negotiation mode	Aggressive mode
IKE proposal	AES (128) SHA1 DH Grp 2 (1024)
IKE lifetime (mins)	480
<input type="button" value="Cancel"/> <input type="button" value="Next"/>	

11

10

9

20

24

21

22

23

Press **Next**

MRD-310 Initiator Phase 2

Configures two ESP tunnels for the actual protected traffic.
LAN to LAN IPsec must know which IP packets to protect so these must be specified in tunnel networks address with subnet address/subnet mask. LAN subnet will apply the subnet and mask configured on the Ethernet ports of the MRD-310



IPsec VPN

Phase 2 Configuration

ESP proposal: AES (128) - SHA1 (26)

Perfect forward secrecy & group: DH Grp 2 (1024) (28)

Key lifetime (mins): 480 (27)

Buttons: Cancel, Update

Tunnel Networks

Enabled	Local	Network	Address
<input checked="" type="checkbox"/>	Local (3)	LAN subnet	
	Remote	Specify a subnet	10.255.0.0/24 (4)
<input type="checkbox"/>	Local	None (Host only)	
	Remote	None	
<input type="checkbox"/>	Local	None (Host only)	
	Remote	None	

Buttons: Cancel, Update

Press

Finally we set NAT traversal since our MRD-310 has a private IP address dynamically assigned from the 3G provider.

Set Enabled, Press to start the IPsec VPN connection.



IPsec VPN

General IPsec Configuration

Enabled:

NAT traversal enabled & keepalive period (secs): 20 (14) (15)

IPsec MTU: 18

Buttons: Reset, Update

Tunnels

Label	Enabled	Remote Host	Remote ID	Edit	Delete
MRD2ASA	Yes	82.233.121.245	@vidar		

Buttons: Add new tunnel

Diagnostics

To debug the Ipsec negotiation on the Cisco ASA 5505 enter the following commands in privileged mode

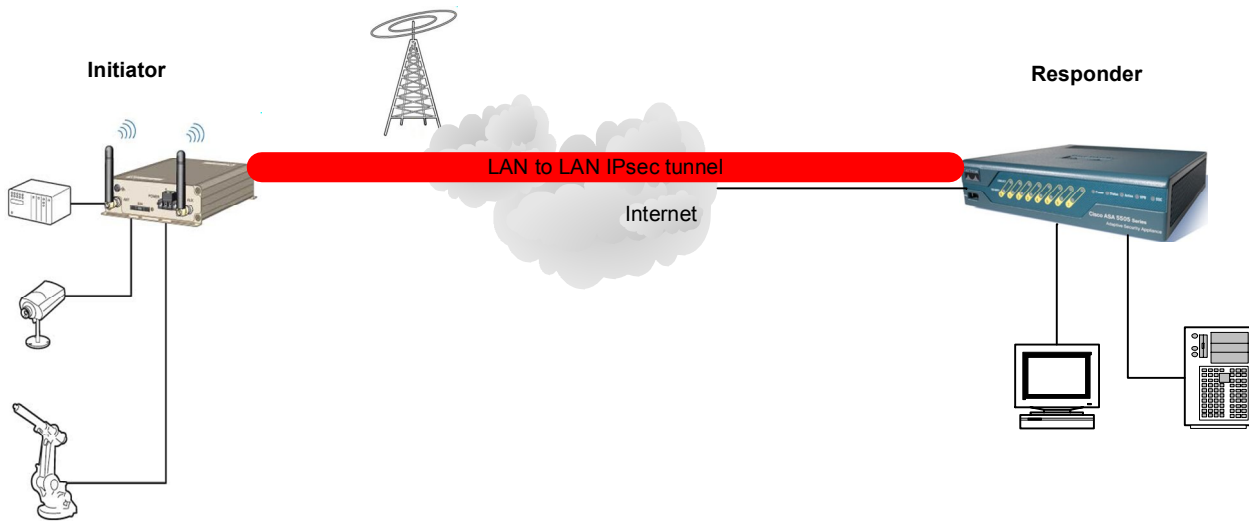
```
#terminal monitor
#debug crypto isakmp
```

```
IP = 87.253.85.130, processing SA payload
IP = 87.253.85.130, processing ke payload
IP = 87.253.85.130, processing ISA_KE payload
IP = 87.253.85.130, processing nonce payload
IP = 87.253.85.130, processing ID payload
IP = 87.253.85.130, ID_FQDN ID received, len 6
0000: 6D726461 7361                                mrdasa

IP = 87.253.85.130, processing VID payload
IP = 87.253.85.130, Received DPD VID
IP = 87.253.85.130, processing VID payload
IP = 87.253.85.130, Received NAT-Traversal RFC VID
IP = 87.253.85.130, processing VID payload
IP = 87.253.85.130, Received NAT-Traversal ver 03 VID
IP = 87.253.85.130, processing VID payload
IP = 87.253.85.130, processing VID payload
IP = 87.253.85.130, Received NAT-Traversal ver 02 VID
IP = 87.253.85.130, processing VID payload
IP = 87.253.85.130, Connection landed on tunnel_group mrdasa
Group = mrdasa, IP = 87.253.85.130, processing IKE SA payload
Group = mrdasa, IP = 87.253.85.130, IKE SA Proposal # 1, Transform # 0 acceptable
Matches global IKE entry # 2
Group = mrdasa, IP = 87.253.85.130, constructing ISAKMP SA payload
Group = mrdasa, IP = 87.253.85.130, constructing ke payload
Group = mrdasa, IP = 87.253.85.130, constructing nonce payload
Group = mrdasa, IP = 87.253.85.130, Generating keys for Responder...
Group = mrdasa, IP = 87.253.85.130, constructing ID payload
Group = mrdasa, IP = 87.253.85.130, constructing hash payload
Group = mrdasa, IP = 87.253.85.130, Computing hash for ISAKMP
Group = mrdasa, IP = 87.253.85.130, constructing Cisco Unity VID payload
Group = mrdasa, IP = 87.253.85.130, constructing xauth V6 VID payload
Group = mrdasa, IP = 87.253.85.130, constructing dpd vid payload
Group = mrdasa, IP = 87.253.85.130, constructing NAT-Traversal VID ver 02 payload
Group = mrdasa, IP = 87.253.85.130, constructing NAT-Discovery payload
Group = mrdasa, IP = 87.253.85.130, computing NAT Discovery hash
Group = mrdasa, IP = 87.253.85.130, constructing NAT-Discovery payload
Group = mrdasa, IP = 87.253.85.130, computing NAT Discovery hash
Group = mrdasa, IP = 87.253.85.130, constructing Fragmentation VID + extended
capabilities payload
Group = mrdasa, IP = 87.253.85.130, constructing VID payload
Group = mrdasa, IP = 87.253.85.130, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
IP = 87.253.85.130, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) +
KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) total
length : 451
IP = 87.253.85.130, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + NAT-D
(130) + NAT-D (130) + HASH (8) + NONE (0) total length : 100
Group = mrdasa, IP = 87.253.85.130, processing NAT-Discovery payload
Group = mrdasa, IP = 87.253.85.130, computing NAT Discovery hash
Group = mrdasa, IP = 87.253.85.130, processing NAT-Discovery payload
Group = mrdasa, IP = 87.253.85.130, computing NAT Discovery hash
Group = mrdasa, IP = 87.253.85.130, processing hash payload
Group = mrdasa, IP = 87.253.85.130, Computing hash for ISAKMP
```

```
Group = mrdasa, IP = 87.253.85.130, Automatic NAT Detection Status: Remote end IS
behind a NAT device This end is NOT behind a NAT device
Group = mrdasa, IP = 87.253.85.130, PHASE 1 COMPLETED
IP = 87.253.85.130, Keep-alive type for this connection: DPD
Group = mrdasa, IP = 87.253.85.130, Starting P1 rekey timer: 21600 seconds.
IP = 87.253.85.130, IKE Responder starting QM: msg id = 7683c925
IP = 87.253.85.130, IKE_DECODE RECEIVED Message (msgid=7683c925) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 156
Group = mrdasa, IP = 87.253.85.130, processing hash payload
Group = mrdasa, IP = 87.253.85.130, processing SA payload
Group = mrdasa, IP = 87.253.85.130, processing nonce payload
Group = mrdasa, IP = 87.253.85.130, processing ID payload
Group = mrdasa, IP = 87.253.85.130, ID_IPV4_ADDR_SUBNET ID received--192.168.20.0--
255.255.255.0
Group = mrdasa, IP = 87.253.85.130, Received remote IP Proxy Subnet data in ID Payload:
Address 192.168.20.0, Mask 255.255.255.0, Protocol 0, Port 0
Group = mrdasa, IP = 87.253.85.130, processing ID payload
Group = mrdasa, IP = 87.253.85.130, ID_IPV4_ADDR_SUBNET ID received--10.255.0.0--
255.255.255.0
Group = mrdasa, IP = 87.253.85.130, Received local IP Proxy Subnet data in ID Payload:
Address 10.208.0.32, Mask 255.255.255.224, Protocol 0, Port 0
Group = mrdasa, IP = 87.253.85.130, QM IsRekeyed old sa not found by addr
Group = mrdasa, IP = 87.253.85.130, Static Crypto Map check, checking map = outside_map,
seq = 20...
Group = mrdasa, IP = 87.253.85.130, Static Crypto Map Check by-passed: Crypto map entry
incomplete!
Group = mrdasa, IP = 87.253.85.130, Selecting only UDP-Encapsulated-Tunnel and UDP-
Encapsulated-Transport modes defined by NAT-Traversal
Group = mrdasa, IP = 87.253.85.130, IKE Remote Peer configured for crypto map:
SYSTEM_DEFAULT_CRYPTOMAP
Group = mrdasa, IP = 87.253.85.130, processing IPsec SA payload
Group = mrdasa, IP = 87.253.85.130, IPsec SA Proposal # 0, Transform # 0 acceptable
Matches global IPsec SA entry # 11
Group = mrdasa, IP = 87.253.85.130, IKE: requesting SPI!
Group = mrdasa, IP = 87.253.85.130, IKE got SPI from key engine: SPI = 0x0c84204c
Group = mrdasa, IP = 87.253.85.130, oakley constructing quick mode
Group = mrdasa, IP = 87.253.85.130, constructing blank hash payload
Group = mrdasa, IP = 87.253.85.130, constructing IPsec SA payload
Group = mrdasa, IP = 87.253.85.130, constructing IPsec nonce payload
Group = mrdasa, IP = 87.253.85.130, constructing proxy ID
Group = mrdasa, IP = 87.253.85.130, Transmitting Proxy Id:
Remote subnet: 192.168.20.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.255.0.0 mask 255.255.255.0 Protocol 0 Port 0
Group = mrdasa, IP = 87.253.85.130, constructing qm hash payload
Group = mrdasa, IP = 87.253.85.130, IKE Responder sending 2nd QM pkt: msg id = 7683c925
IP = 87.253.85.130, IKE_DECODE SENDING Message (msgid=7683c925) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
IP = 87.253.85.130, IKE_DECODE RECEIVED Message (msgid=7683c925) with payloads : HDR +
HASH (8) + NONE (0) total length : 52
Group = mrdasa, IP = 87.253.85.130, processing hash payload
Group = mrdasa, IP = 87.253.85.130, loading all IPSEC SAs
Group = mrdasa, IP = 87.253.85.130, Generating Quick Mode Key!
Group = mrdasa, IP = 87.253.85.130, Generating Quick Mode Key!
Group = mrdasa, IP = 87.253.85.130, Security negotiation complete for LAN-to-LAN Group
(mrdasa) Responder, Inbound SPI = 0x0c84204c, Outbound SPI = 0xdc68831e
```

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		RFC2407	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