

APPLICATION NOTE: AN-029-WUK

# HOW TO CONFIGURE AN IPSEC VPN USING PRE-SHARED KEYS ON MERLIN ROUTERS

LAN to LAN connectivity over an IPSec VPN between a Merlin-4407 4G router and a Merlin-4708 VDSL/ADSL router with fixed public IP address





Introduction:	3
What is an IPSec VPN?	3
Overview	4
Assumptions	4
Merlin 4407 4G Router Configuration (VPN Initiator)	5
LAN IP Address.	5
Mobile 4G Settings	6
IPSec VPN Tunnel Settings (Initiator) – Merlin 4407	7
IKEv2 or IKEv1?	7
IPSec VPN General - IKEv2 (Recommended)	8
IPSec VPN General - Legacy IKEv1 option (Not recommended)	9
IPSec VPN Policy	10
IPSec VPN Proposal	11
IPSec VPN Authentication	11
IPSec VPN Secrets	12
Merlin 4708 VDSL/ADSL Router Configuration (VPN Concentrator)	13
LAN IP Address.	13
VDSL Settings.	14
IPSec VPN Tunnel Settings (Initiator) – Merlin 4708	15
IKEv2 or IKEv1 Options	15
IPSec VPN General - IKEv2 (Recommended)	16
IPSec VPN General - Legacy IKEv1 option (Not recommended)	17
IPSec VPN Policy	18
IPSec VPN Proposal	19
IPSec VPN Authentication	19
IPSec VPN Secrets	20
IPSec VPN Status	21
Browse to System > System Log	21
Revision History	22



### Introduction:

### What is an IPSec VPN?

IPSec VPN's create a secure Virtual Private Network between two or more private LAN networks, over the internet.

The internet is generally accepted as a world wide insecure network, but using IPSec VPN's can make data transfer over the internet much more secure.

IPSec (Internet Protocol Security), utilises a selection of encryption and authentication algorithms which are grouped together under a common banner. Different combinations of these protocols can be used simultaneously to create a secure tunnel between two routers. Despite the fact that business critical data may be traversing over a wireless connection via the internet to your central office, the data itself is both encrypted and encapsulated with secure authentication up to a military grade level of data protection.

It is quite possible to use IPSEC to secure communications between multiple different sites, the diagram below shows three remote sites connecting back to a central location where a number of devices can communicate to the various outstation units.

NB: IPSEC will only provide security for the traffic between the routers. You must not consider the routers themselves to be secure once a VPN is in place. Further security can be afforded through proper username management and implementation of a firewall



### **Overview**

The following pages show how to implement an IPSEC VPN between a pair of Westermo Merlin routers. The Merlin-4407 4G router will be the initiator because this will most likely be given a dynamic and NATed IP address from the network provider. The Merlin-4708, being the DSL broadband router, will be the VPN Concentrator because the DSL IP address can be made static (with the correct package from the ISP). This is therefore ideal for an IPSec VPN concentrator because it has an IP address that never changes. In nearly all cases, an VPN Concentrator, in other words the VPN responder, will be a DSL router located at a central location who's job it is to terminate all VPN connections from remote locations. In all cases the VPN concentrator, will need to have a fixed, publicly accessible IP address. This static IP address will be the destination for all incoming VPN connections.

Thanks to technology within IKE version 2, or the option for an Aggressive mode IPSec VPN with legacy IKE version 1 and NAT-Traversal, the initiating router does not require a fixed, publicly accessible IP address.

**NB:** This application note shows how to configure an IPSec VPN using pre-shared keys (PSK). This is intended as an introduction to IPSec but note either self-signed certificates or preferably certificates generated using SCEP can be used to improve security. These are detailed in the management guides for each router.

### Phase 1: IKE

Internet Key Exchange (IKE) protocol defines what parameters are used to negotiate the initial stage of the VPN connection, and provide security which is used in negotiating the second stage of the VPN. This involves the creation of "IKE SA's".

### Phase 2: IPsec

The IPSec transform defines the negotiation for the second stage of the VPN. This includes exactly what authentication and encryption will be used in the VPN tunnel, along with IP addressing information that allows data to flow from router to router. This involves the creation of "IPSec SA's".

### Assumptions

This application note applies to the Merlin-4407 4G router and the Merlin-4708 VDSL/ADSL router and assumes the routers have a factory default configuration. This application note can be applied to other routers in the Merlin range, providing that the VPN concentrator has a fixed IP address that can be reached from routers initiating the VPN tunnels.

## Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to <u>support.uk@westermo.com</u>

Requests for new Application Notes and Quick Notes can be sent to the same address.

## Merlin 4407 4G Router Configuration (VPN Initiator)

### LAN IP Address.

Log in to the Merlin web configuration UI and browse to Network > Interfaces.

In the LAN section, click the **EDIT** button.

westermo	FC-We-Merlin4	407	image1/config1 AUTO REFRESH ON 00E0C819399E / SXL-25.04.16.000
	LAN MOBILE		
🖗 Status 🕨 🕨			
△ System ►	Interfaces		
🖲 Security 🕨 🕨			
Management	Interface Overv	iew	
T Nistanski T	Network	Status	Actions
Interfaces	LAN	Uptime: 23h 14m 42s MAC Address: 00:E0:C8:19:39:9E PX: 7 67 MB (101739 Ptre.)	
BFD	br-LAN	<b>TX:</b> 6.67 MB (16090 Pkts.)	
BGP		IPv4: 172.30.1.201/24	

Next enter the new LAN IP address and subnet mask:

Protocol: Static address

IPv4 address: 172.30.1.201

IPv4 netmask: 255.255.255.0

westermo	FC-We-Merlin4407
	LAN MOBILE
₽ Status ►	_
△ System ►	Interfaces - LAN
🖲 Security 📃 🕨	On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several
• Management	network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLAWIR (e.g.: eth0.1).
♣ Network ▼	General Setup Advanced Settings Physical Settings Firewall Settings
Interfaces BFD BGP	Uptime: 23h 17m 36s MAC Address: 00:E0:C8:19:39:9E MTU: 1500 Br. 7.97 MB (102721 Pkts, 0 Errors, 0 Drops, 0 Overruns, 0 Frame) br-LAN Status IPv4: 172.30.1.201/24 IPv4: 172.30.1.201/24
DHCP and DNS	
DHCP-Forwarder	Protocol Static address
Diagnostics	
Hostnames	IPv4 address 172.30.1.201
ISDN PRI	
Multi-WAN	IPv4 netmask 255 255 255 0

Scroll to the bottom of the page and click **Save & Apply**.





## **Mobile 4G Settings**

Browse to **Network > Interfaces**.

In the MOBILE section, click the EDIT button.



Enter the appropriate APN (Access Point Name) provided by your mobile network provider.

westermo		FC-We-Merlin4407
		LAN MOBILE
Status	•	
<ul> <li>System</li> </ul>	•	Interfaces - MOBILE
Security	•	On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" fi
• Management	•	Common Configuration
🐣 Network	•	General Setup Advanced Settings Firewall Settings
Interfaces		Uptime: 23h 39m 28s
BFD		RX: 2.41 MB (17080 Pkts, 0 Errors, 0 Drops
BGP		rmnet_data0 TX: 2.42 MB (17127 Pkts, 0 Errors, 0 Drops Status IPv4: 10.184.203.184/32
DHCP and DNS		Status
DHCP-Forwarder		Protocol 5G/LTE/UMTS/GPRS/EV-DO V
Diagnostics		
Hostnames		Assigned mobile device WAN-1 (Sierra Wireless WP7607)
ISDN PRI		
Multi-WAN		Service Preference LTE
OSPF		UMTS
RIP		GPRS
Static Routes		Auto
VRRP		
Л SCADA		SIM 1 *
<ul> <li>Services</li> </ul>	•	Operator DI MN code
		- Specify this if you want to face connection to particular carrier
U VPIN	1	ореслу чла в уюч ини колосе соплесают ю раз исыле сакте
් Reboot		APN your_APN_goes_here
× Logout		APN username
		APN password 🔤 😴

#### APN: Enter your APN here

APN Username: Only if applicable

APN Password: Only if applicable



Scroll to the bottom of the page and click Save and Apply.

## **IPSec VPN Tunnel Settings (Initiator) – Merlin 4407** Browse to **VPN > IPSec > General Section**.

westerm		FC-We-Merlin4407
Status	•	Virtual Private Network - IPsec
△ System	•	Strongswan is IPsec-based VPN solution supporting IKEv1 and IKEv2 key exchange.
🔋 Security	•	General Section
Management	Þ	General Section - Configure global parameters for all IPsec connections
💑 Network	F	
Л SCADA	F	General Advanced Certificates
<ul> <li>Services</li> </ul>	•	
U VPN	•	
DMVPN		Debug
IPsec	_	- Set modules' debug levels e.g. 'ike 2, lib 0', or use 'none' for minimal debug

Tick Enable IPSec.

### **IKEv2 or IKEv1?**

In the next section, you will find two options for configuring the IPSec VPN: IKEv2 and IKEv1. Both are protocols used to set up a secure, encrypted communication channel between two routers, but they have distinct differences that could influence your choice.

IKEv2 (Internet Key Exchange version 2) is a more modern protocol, offering several advantages over its predecessor, IKEv1. It includes improved security features, faster connection setup, and better stability. IKEv2 supports Mobility and Multihoming Protocol (MOBIKE), making it particularly effective for users who frequently switch between different networks (e.g., DSL to 4G, or switching between 4G networks etc). Its ability to handle changing network conditions smoothly without dropping the VPN connection is a significant benefit, especially for connections with dynamic IP addresses. Additionally, IKEv2 is more efficient in terms of bandwidth usage and provides stronger encryption methods.

On the other hand, IKEv1, while still in use, is an older protocol that may not support some of the advanced features available in IKEv2. It is less efficient and can be slower in establishing connections. Although it remains a viable option for some legacy systems, it lacks the robust security and performance enhancements found in IKEv2.

Given these considerations, we strongly encourage users to opt for IKEv2 when setting up their IPSec VPN. The enhanced security, speed, and adaptability of IKEv2 will provide a more reliable and secure VPN experience, particularly in dynamic networking environments.

## IPSec VPN General - IKEv2 (Recommended)

Browse to VPN > IPSec > IPSec Connection > General tab.

Westermo		IPsec Connection
		Configure parameters for individual IPsec connection.
൙ Status	•	
△ System	- F	
Security	->	General Policy Proposal Authentication FlexVPN DPD Advanced
• Management	•	Enabled 🗹
💑 Network	•	Name MerlinIPSecAppNote
Л SCADA	•	- Local name of IPsec Connection
<ul> <li>Services</li> </ul>	•	WAN Interface MOBILE
C VPN		- Interfaces tunnel is controlled by, i.e. when any of interfaces goes down, tunnel is reevaluated
DMVPN	_	
IPsec	- 1	Remote node address 81.x.x.
OpenVPN		- Could be IP address or FQDN or '%any'
(5 D L L		Autostart Action always -
C Reboot		- How the tunnel is initiated:
<ul> <li>Logout</li> </ul>		start: on startup always: like start, but connection is restarted whenever it goes down for any reason
		route: when traffic routes this way add: not initiated, just added
		ignove: don't add. Only used for template connection
		Connection Type funnel
	- 1	
		- Version of IKE protocol to use.
		Inherit SA
		- Inherit CHILD SA when IKE SA is rekeyed
		- Sends in the Contract nouncearon when its connection attempt
		Aggressive mode Use IKEv1 aggressive mode

Tick Enabled.

Name: Enter a label to help you identify what the VPN is for.

WAN Interface: MOBILE

**Remote Node Address:** This is the remote static outside IP address of the VPN Concentrator router (in this case the Merlin-4708 VDSL/ADSL router).

Autostart Action: Always

Connection Type: tunnel

IKE Version: 2

Inherit SA: Tick to inherit CHILD SA's when IKE SA is rekeyed.

**INIT CONT:** Tick to enable send Initial Contact.

If you are using IKEv2 (recommended), skip to the **IPSec VPN Policy** section.

## IPSec VPN General - Legacy IKEv1 option (Not recommended) Browse to VPN > IPSec > IPSec Connection > General tab.

westermo		General Policy Proposal Authentication FlexVPN DPD Advanced
		Enabled
൙ Status	•	
△ System	•	Name MeriniPSecAppNote
Security	•	
Management	•	WAN Interface MOBILE -
A Network	•	- Interfaces tunnel is controlled by, i.e. when any of interfaces goes down, tunnel is reevaluated
Л SCADA	•	Remote node address 81.x.x.x
<ul> <li>Services</li> </ul>	•	- Could be IP address or FQDN or '%any'
U VPN	▼	Autostart Action always
DMVPN IPsec		- How the tunnel is initiated: start: on startup
OpenVPN	_	always: like start, but connection is restarted whenever it goes down for any reason route: when traffic routes this way
WeConnect		<b>add</b> : not initiated, just added <b>ignore</b> : don't add. Only used for template connection
් Reboot		
× Logout		Connection type
		IKE version 1
		- Version of IKE protocol to use.
		Inherit SA
		- Inherit CHILD SA when IKE SA is rekeyed
		INIT CONT
		Aggressive mode

### Tick Enabled.

Name: Enter a label to help you identify what the VPN is for.

WAN Interface: MOBILE

**Remote Node Address:** This is the remote static outside IP address of the VPN Concentrator router (in this case the Merlin-4708 VDSL/ADSL router).

Autostart Action: Always

Connection Type: tunnel

IKE Version: 1

**INIT CONT:** Tick to enable send Initial Contact.

Aggressive Mode: Tick to enable Aggressive Mode.

## **IPSec VPN Policy**

Browse to VPN > IPSec > IPSec Connection > Policy tab.

westermo		General	Policy	Proposal	Authentication	FlexVPN	DPD	Advanced	
൙ Status	•				Local I	d initiator-me	erlin4407 to use d	efault (local inte	erface IP address) or Leave blank when using Certificates
△ System	•				Local Certificat	e			
Security	•					- Configure w	ith local	certificate name	e. When using SCEP append '.pem' to SCEP's section name.
Management					Remote I	d responder-	merlin47	08	
🖧 Network	•					- Leave blank	to use d	efault (remote g	gateway IP address) or configure with Remote Certificate DN parameters
Л SCADA	•			1	ocal I AN IP Addres	s 172 30 1 0	1		
<ul> <li>Services</li> </ul>	▶					- Specifies Id	acal 'inter	resting' traffic a	rdd I AN Network IP
O VPN						opecifies in		cooring cromo, o	
DMVPN				Local L	AN IP Address Mas	k 255.255.25	55.0		
OpenVPN	-					- Specifies lo	ocal 'inter	resting' traffic, a	dd LAN Network Mask
WeConnect				Ren	note LAN IP Addre	s 192.168.1.	0		
് Reboot						- Specifies r	emote 'in	teresting' traffic	c, add remote LAN Network IP
× Logout				Remote L	AN IP Address Mas	k 255.255.2	55.0		
						- Specifies n	emote 'in	teresting' traffic	c, add remote Network Mask

Local Id: initiator-merlin4407

Remote Id: responder-merlin4708

Local LAN IP Address: 172.30.1.0

Local LAN IP Address Mask: 255.255.255.0

Remote LAN IP Address Mask: 192.168.1.0

Remote LAN IP Address Mask: 255.255.255.0

**NB:** When using Aggressive Mode IPSec the local and remote ID's are free text and is the initial method that each router will use to identify each other. It's useful for the purposes of managing your VPN connections to make the ID something meaningful like a site name for example. Just as long as it is consistent and is accurately reflected on the other router.

## **IPSec VPN Proposal**

Browse to VPN > IPSec > IPSec Connection > Proposal tab.

🔒 Security		General Policy Proposal Authentication FlexVPN DPD Advanced
Management	•	IKE Key algorithm aes256-sha256-modp2048
🐣 Network	•	- Phase 1 - Proposal algorithms
Л SCADA	•	IVE Key lifetime
<ul> <li>Services</li> </ul>	•	- How long the keying channel of a connection should last before being renegotiated.
O VPN		
DMVPN		IPsec Key algorithm aes256-sha256-modp2048
OpenVPN	-	- Phase 2 - Transformset algorithms
WeConnect		IPsec Key lifetime 3600s
් Reboot		- How long a particular instance of a connection should last, from successful negotiation to expiry.

IKE Key algorithm: aes256-sha256-modp2048

IKE Key lifetime: 28800s

IPSec Key algorithm: aes256-sha256-modp2048

IPSec Key Lifetime: 3600s

**NB:** Choose the strongest encryption and authentication algorithms supported by both routers and ensure they match at both ends.

## **IPSec VPN Authentication**

Browse to VPN > IPSec > IPSec Connection > Authentication tab.

westermo		General	Policy	Proposal	Authentication	FlexVPN DPD	Advanced			
					Local Auth Method	psk		•		
Status						- Use this auth meth	nod locally to pr	esent this system	to peer. Methods:	
△ System	•					secret or psk for pro pubkey for public k	e-shared secrets ey signatures	i,		
Security	•					rsasig for RSA digita ecdsasig for Elliptic	al signatures (pr Curve DSA sign	efered). Digital si atures	gnatures are superior in every	way to shared secrets!
Management	•					never can be used it xauthpsk and xauth	f negotiation is i hrsasig(IKEv1 or	never to be atten nly) that will enal	npted or accepted (useful for s ble eXtended Authentication (X	hunt-only conns). (Auth)
💑 Network						eap-radius(IKEV1 on	nly) for auth agai nly) for auth aga	nst external RAL inst external RAL	NUS server NUS server	
Л SCADA				F	emote Auth Method	nsk				
<ul> <li>Services</li> </ul>	•					Domand this outh	method from re	moto poor Moth	ode	
						secret or psk for pr	e-shared secrets	, ,	005.	
DMVPN	_					rsasig for RSA digita	al signatures (pr	efered). Digital si	gnatures are superior in every	way to shared secrets!
IPsec	_					ecdsasig for Elliptic never can be used i	Curve DSA sign f negotiation is i	atures never to be atter	npted or accepted (useful for s	hunt-only conns).
OpenVPN	_					xauthpsk and xauth xauth-eap(IKEv1 on	h <b>rsasig</b> (IKEv1 or Ily) for auth agai	nly) that will enab nst external RAD	ole eXtended Authentication (X IUS server	(Auth)
WeConnect						eap-radius(IKEv2 or	nly) for auth aga	inst external RAI	DIUS server	

Local Auth Method: PSK

Remote Auth Method: PSK

### **IPSec VPN Secrets**

Browse to VPN > IPSec > Secrets > General tab.

Westermo	_	Secrets
	_	Configure Passwords/Certificates used to secure IPsec Connections
൙ Status		
△ System	•	
💼 Security	•	General Certificates
• Management	•	Enabled 🗹
🖧 Network		ID selector Initiator-merlin4407 responder-merlin4708
Л SCADA		- To match local and remote ip enter local ip followed by space followed by remote ip
<ul><li>Services</li></ul>	•	
O VPN		Secret Type psk 🗸
DMVPN	_	- Available secret types:
IPsec	_	<b>RSA</b> defines an RSA private key
OpenVPN	_	ECDSA defines an ECDSA private key P12 defines a PKCS#12 container
WeConnect	_	EAP defines EAP credentials NTLM defines NTLM credentials
් Reboot	_	XAUTH defines XAUTH credentials (IKEv1 only) PIN defines a smartcard PIN
× Logout	_	TOKEN defines a label of a private key on a TPM or a PKCS #11 token
		Secret
		- Provide secret's string or certificate name (Max 30 CHAR)

Enabled: Tick to enable.

ID selector: initiator-merlin4407 responder-merlin4708

Secret Type: psk

Secret: topsecret

**NB:** The pre-shared secret "topsecret" is just an example. Choose an appropriate secret and match it on the other router.

**Hint:** Treat your pre-shared secret as you would with a strong password for additional difficulty to guess.



Click Save and Apply.

## Merlin 4708 VDSL/ADSL Router Configuration (VPN Concentrator)

### LAN IP Address.

Log in to the Merlin web configuration UI and browse to Network > Interfaces.

In the LAN section, click the **EDIT** button.

westermo	FC-We-Merlin47	08	AUTO REFRESH ON 00E0C8197333 / DRS-25.04.16.000
	LAN MOBILE PPPoA	dsi PPPoVdsi WANETH	
🖉 Status 🕨 🕨			
△ System ►	Interfaces		
🕯 Security 🕨 🕨			
Management	Interface Overvie	W	
Notwork	Network	Status	Actions
Interfaces BFD	LAN Ø (222) br-LAN	Uptime: 2h 3m 42s MAC Address: 00:E0:C8:19:73:33 RX: 2.41 MB (17324 Pkts.) TX: 16:53 MB (23061 Pkts.) IPv4: 192.168.100.1/24	CONNECT STOP EDIT DELETE

Next enter the new LAN IP address and subnet mask:

Protocol: Static address

IPv4 address: 192.168.1.1

IPv4 netmask: 255.255.255.0

westermo	FC-We-Merlin4708
	LAN MOBILE PPPoAdsi PPPoVdsi WANETH
🖻 Status 🕨	
△ System ►	Interfaces - LAN
🔹 Security 🔹 🕨	On this page you can configure the network interfaces. You can bridge several interfaces by ticking the
Management	network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: eth0.1
⊷ Network 🛛 🔻	General Setup Advanced Settings Physical Settings Firewall Settings
Interfaces BFD	Uptime: 2h 9m 3s MAC Address: 00:E0:C8:19:73:33 MTU: 1500 RX: 2.47 MB (17912 Pkts, 0 Errors, 0 Drops, 0 br-LAN TX: 16.86 MB (23694 Pkts, 0 Errors, 0 Drops, C
BGP DHCP and DNS	Status IPv4: 192.168.100.1/24
DHCP-Forwarder	Protocol Static address
Diagnostics	
Hostnames	IPv4 address 192.168.1.1
Multi-WAN	
OSPF	IPv4 netmask 255.255.255.0

Scroll to the bottom of the page and click Save & Apply.



### **VDSL Settings.**

Browse to **Network > Interfaces**.

In the PPPoVDSL section, click the **EDIT** button.



Enter the appropriate VDSL/ADSL details provided by your ISP.



Protocol: PPPoE

PAP/CHAP Username: Enter your VDSL username here (provided by your ISP).

PAP/CHAP Password: Enter your VDSL password here (provided by your ISP).



Scroll to the bottom of the page and click Save and Apply.

## **IPSec VPN Tunnel Settings (Initiator) – Merlin 4708** Browse to **VPN > IPSec > General Section**.

westerm	0	FC-We-Merlin4708
൙ Status	•	Virtual Private Network - IPsec
△ System	•	Strongswan is IPsec-based VPN solution supporting IKEv1 and IKEv2 key exchange.
🕯 Security	•	General Section
Management	•	General Section - Configure global parameters for all IPsec connections
🐣 Network	•	
Л SCADA		General Advanced Certificates
<ul> <li>Services</li> </ul>	•	
ି VPN		Enable iPsec
DMVPN		Debug
IPsec	_	- Set modules' debug levels e.g. 'ike 2, lib 0', or use 'none' for minimal debug
OpenVPN		

Tick Enable IPSec.

## **IKEv2 or IKEv1 Options**

The next section gives options for both IKEv2 (recommended) and legacy IKEv1. Please refer to the section "<u>IKEv2 or IKEv1?</u>". Note that the same IKE version needs to be used on both routers.

## IPSec VPN General - IKEv2 (Recommended)

Browse to VPN > IPSec > IPSec Connection > General tab.

westermo			IPsec Connection							
			Configure parameters for individual IPsec connection.							
æ	Status									
۵	System									
	Security		General Policy Proposal Authentication	FlexVPN DPD Advanced						
0	Management		Enabled							
8	Network		Name	MerlinIPSecAppNote						
Л	SCADA			- Local name of IPsec Connection						
۲	Services		WAN Interface	PPPoVdsl ·						
۵	VPN	•		Interface tunnel is controlled by in when any of interfaces goes down, tunnel is reactly total						
	DMVPN			- Interfaces currier is controlled by, i.e. when any of interfaces goes down, currier is reevaluated						
	IPsec	_	Remote node address	%any						
	OpenVPN			- Could be IP address or FQDN or '%any'						
	WeConnect		Autostart Action	add						
U	Reboot			- How the tunnel is initiated:						
×	Logout			start: on startup always: like start, but connection is restarted whenever it goes down for any reason						
				route: when traffic routes this way add: not initiated, just added						
				ignore: don't add. Only used for template connection						
			Connection Type	tunnel						
			IKE version	2						
				- Version of IKE protocol to use.						
			Inherit SA							
				- Inherit CHILD SA when IKE SA is rekeyed						
			INIT CONT							
				- Sends INITIAL CONTACT notification when first connection attempt						
			Aggressive mode							

Tick Enabled.

Name: Enter a label to help you identify what the VPN is for.

WAN Interface: PPPoVdsl

Remote Node Address: %any

Autostart Action: Add

Connection Type: tunnel

**IKE Version:** 2

Inherit SA: Tick to inherit CHILD SA's when IKE SA is rekeyed.

## IPSec VPN General - Legacy IKEv1 option (Not recommended) Browse to VPN > IPSec > IPSec Connection > General tab.

westermo		IPsec Connection						
		Configure parameters for individual IPsec connection.						
൙ Status	•							
△ System	•							
Security	•	General Policy Proposal Authentication FlexVPN DPD Advanced						
Management	•	Enabled						
Network	•	Name MerlinIPSecAppNote						
Л SCADA	•	- Local name of IPsec Connection						
<ul> <li>Services</li> </ul>	•	WAN Interface DDPol/dol						
ି VPN	T	WAY IIIdenate						
DMVPN		- Interfaces tunnel is controlled by, i.e. when any of interfaces goes down, tunnel is reevaluated						
IPsec	_	Remote node address %any						
OpenVPN		- Could be IP address or FQDN or '%any'						
WeConnect		Autostart Action add						
් Reboot		- How the tunnel is initiated:						
imes Logout		start: on startup always: like start, but connection is restarted whenever it goes down for any reason						
		route: when traffic routes this way add: not initiated, iust added						
		ignore: don't add. Only used for template connection						
		Connection Type tunnel						
		IKE version 1						
		- Version of IKE protocol to use						
		Inherit SA						
		- Innerit CHILU SA when IKE SA Is rekeyed						
		- Sends INITIAL CONTACT notification when first connection attempt						
		Aggressive mode - Use IKEv1 aggressive mode						

Tick Enabled.

Name: Enter a label to help you identify what the VPN is for.

WAN Interface: PPPoVdsl

Remote Node Address: %any

Autostart Action: Add

Connection Type: tunnel

**IKE Version:** 1

Aggressive Mode: Tick to enable Aggressive Mode.

## **IPSec VPN Policy**

Browse to VPN > IPSec > IPSec Connection > Policy tab.

Westermo		IPsec Connection							
acsicing		Configure parameters for individual IPsec connection.							
Status									
△ System									
<ul> <li>Security</li> </ul>	•	General Policy Proposal Authentication	FlexVPN DPD Advanced						
Management	•	Local Id	responder-merlin4708						
💑 Network	•		- Leave blank to use default (local interface IP address) or Leave blank when using Certificates						
Л SCADA	×	Local Certificate	- Configure with local certificate name. When using SCEP annend ' nem' to SCEP's section name.						
Services	<b>F</b>								
C VPN		Remote Id	initiator-merlin4407						
DMVPN			- Leave blank to use default (remote gateway IP address) or configure with Remote Certificate DN parameters						
IPsec	- 1	Local LAN IP Address	192.168.1.0						
OpenVPN			- Specifies local 'interesting' traffic, add LAN Network IP						
© Reboot		Local LAN IP Address Mask	255,255,255,0						
× Logout			- Specifies local 'interesting' traffic, add LAN Network Mask						
	- 1	Remote LAN IP Address	172.30.1.0						
			- Specifies remote 'interesting' traffic, add remote LAN Network IP						
		Remote LAN IP Address Mask	255.255.255.0						
			- Specifies remote 'interesting' traffic, add remote Network Mask						

Local Id: responder-merlin4708

Remote Id: initiator-merlin4407

Local LAN IP Address: 192.168.1.0

Local LAN IP Address Mask: 255.255.255.0

Remote LAN IP Address Mask: 172.30.1.0

### Remote LAN IP Address Mask: 255.255.255.0

**NB:** When using Aggressive Mode IPSec the local and remote ID's are free text and is the initial method that each router will use to identify each other. It's useful for the purposes of managing your VPN connections to make the ID something meaningful like a site name for example. Just as long as it is consistent and is accurately reflected on the other router.

## **IPSec VPN Proposal**

Browse to VPN > IPSec > IPSec Connection > Proposal tab.

🔒 Security		General Policy Proposal Authentication FlexVPN DPD Advanced
Management	•	IKE Key algorithm aes256-sha256-modp2048
🐣 Network	•	- Phase 1 - Proposal algorithms
Л SCADA	•	IVE Key lifetime
<ul> <li>Services</li> </ul>	•	- How long the keying channel of a connection should last before being renegotiated.
O VPN		
DMVPN		IPsec Key algorithm aes256-sha256-modp2048
OpenVPN	-	- Phase 2 - Transformset algorithms
WeConnect		IPsec Key lifetime 3600s
් Reboot		- How long a particular instance of a connection should last, from successful negotiation to expiry.

IKE Key algorithm: aes256-sha256-modp2048

IKE Key lifetime: 28800s

IPSec Key algorithm: aes256-sha256-modp2048

IPSec Key Lifetime: 3600s

**NB:** Choose the strongest encryption and authentication algorithms supported by both routers and ensure they match at both ends.

## **IPSec VPN Authentication**

Browse to VPN > IPSec > IPSec Connection > Authentication tab.

Illestermo		General	Policy	Proposal	Authentication	FlexVPN DPD	Advanced			
					Local Auth Method	psk		•		
൙ Status	•					- Use this auth met	hod locally to pre	ent this system to peer. Methods:		
△ System	•					secret or psk for pr pubkey for public k	e-shared secrets, ey signatures			
Security	•					rsasig for RSA digit ecdsasig for Elliptic	al signatures (pre Curve DSA signa	ered). Digital signatures are super ures	ior in every way to shared secrets!	
Management	•					never can be used if negotiation is never to be attempted or accepted (useful for shunt-only conns). xauthpsk and xauthrsasig(IKEv1 only) that will enable eXtended Authentication (XAuth) with sample cartificity of the same statement is a same as a same statement is a same statement in the same statement in the same statement is a same statement in the same statement in the same statement is a same statement in the same statement is a same statement in the same statement in the same statement is a same statement in the same statement is a same statement in the same statement in the same statement is a same statement in the same statement is a same statement in the same statement in the same statement is a same statement in the same statement is a same statement in the same statement in the same statement is a same statement in the same statement is a same statement in the same statement in the same statement is a same statement in the same statement i				
🖏 Network	•					eap-radius(IKEv2 only) for auth against external RADIUS server				
Л SCADA	•				Remote Auth Method	nsk				
<ul><li>Services</li></ul>	•					Demand this outh	mothed from ren	ata naar Mathada		
C VPN						secret or psk for public k	re-shared secrets,	ote peel, metrious.		
DMVPN	_					rsasig for RSA digit	al signatures (pre	ered). Digital signatures are super	ior in every way to shared secrets!	
IPsec	_					never can be used i	if negotiation is n	ver to be attempted or accepted	(useful for shunt-only conns).	
OpenVPN	_					xautnpsk and xaut xauth-eap(IKEv1 or	nrsasig(IKEv1 onl nly) for auth again	y that will enable eXtended Authe st external RADIUS server	intication (XAuth)	
WeConnect						eap-radius(IKEv2 o	nly) for auth agair	st external RADIUS server		

#### Local Auth Method: PSK

Remote Auth Method: PSK

### **IPSec VPN Secrets**

Browse to VPN > IPSec > Secrets > General tab.

westermo		Secrets
		Configure Passwords/Certificates used to secure IPsec Connections
൙ Status		
△ System	•	
🗴 Security	•	General Certificates
Ø Management	•	Enabled 🧹
🖧 Network		ID selector responder merlin 4708 initiator, merlin 4407
Л SCADA	•	- To match local and remote in enter local in followed by space followed by remote in
<ul><li>Services</li></ul>	•	to match rocal and remote ip enter rocal ip remoted by space romoted by remote ip
U VPN	V	Secret Type psk -
DMVPN		- Available secret types:
IPsec		RSA defines a pre-snared key
OpenVPN	_	ECDSA defines an ECDSA private key P12 defines a PKCS#12 container
WeConnect		EAP defines EAP credentials NTLM defines NTLM credentials
් Reboot		XAUTH defines XAUTH credentials (IKEv1 only) PIN defines a smartcard PIN
imes Logout		TOKEN defines a label of a private key on a TPM or a PKCS #11 token
		Secret
		- Provide secret's string or certificate name (Max 30 CHAR)

**Enabled:** Tick to enable.

**ID selector:** responder-merlin4708 initiator-merlin4407

Secret Type: psk

Secret: topsecret

**NB:** The pre-shared secret "topsecret" is just an example. Choose an appropriate secret and match it on the other router.

**Hint:** Treat your pre-shared secret as you would with a strong password for additional difficulty to guess.



Click Save and Apply.



## **IPSec VPN Status**

### Browse to Status > IPSec.

This status page will show any active IPSec SA's (security associations) indicating that the VPN tunnel(s) are established.

Merlin 4407

westermo	FC-We-Merlin4	1407	-+++		1	$\leq$			image1/cc 00E0C819	onfig1 399E / SXL-25.04.16.000
Status     ▼	IPsec Connectio	ons								
Overview	Nama	IKE				SA				
802.1x	Name	Status	Remote	Established	Status	Policy	Encryption	Integrity	Data In/Out	Rekey in
ARP Table	MerlinIPSecAppNote	ESTABLISHED	81.143.212.121	38 minutes (2306s)	INSTALLED	172.30.1.0/24 <===>	AES_CBC_256	HMAC_SHA2_256_128	0/0	20 minutes
Active Routes				690		TOLET OST TOLET				(12133)
Firewall										
GPS Information										
IPsec										
Mobile IP										

#### Merlin 4708

westermo	FC-We-Merlin4	4708	-Ht			$\leq$			image1/cor 00E0C8197	nfig1 333 / DRS-25.04.16.000
P Status	IPsec Connection	ons								
Overview	News	IKE			5A					
802.1x	name.	Status	Remote	Established	Status	Policy	Encryption	Integrity	Data In/Out	Rekey in
ARP Table Active Routes	MerlinIPSecAppNote	ESTABLISHED	initiator- merlin4407	32 minutes (1964s) ago	INSTALLED	192.168.1.0/24 <===> 172.30.1.0/24	AES_CBC_256	HMAC_SHA2_256_128	0/0	26 minutes (1585s)
Firewall										
IPsec Mobile Information										

### Browse to System > System Log

#### The system log will indicate that the VPN tunnel has been established.

Nov 14 09:29:30 daemon.info 00E0C819399E ipsec: 11[IKE] <MerlinIPSecAppNote|1> initiating IKE\_SA MerlinIPSecAppNote[1] to 81.143.212.121

Nov 14 09:29:32 daemon.info 00E0C819399E ipsec: 12[IKE] <MerlinIPSecAppNote|1> establishing CHILD\_SA MerlinIPSecAppNote

Nov 14 09:29:32 daemon.info 00E0C819399E ipsec: 10[IKE] <MerlinIPSecAppNote[1] established between 10.250.118.10[initiator-merlin4407]...81.143.212.121[responder-merlin4708]

Nov 14 09:29:32 daemon.info 00E0C819399E ipsec: 10[IKE] <MerlinIPSecAppNote|1> CHILD\_SA MerlinIPSecAppNote{1} established with SPIs c36ace46\_i cb9b497e\_o and TS 172.30.1.0/24 === 192.168.1.0/24

## **Revision History**

Revision	Rev by	Revision Notes	Date
00	GJM		06/01/2025
01			
02			
03			
04			
05			
06			
07			