

# Vodafone MachineLink

---

## IPSec Configuration Guide



## Document history

This guide covers the following products:

- Vodafone MachineLink 3G (NWL-10)
- Vodafone MachineLink 3G Plus (NWL-12)
- Vodafone MachineLink 4G (NWL-22)

Ver.	Document description	Date
v. 1.0	Initial document release.	March 2013
v. 2.0	Revised content based on current firmware.	September 2016

*Table i - Document revision history*



**Note** – Before performing the instructions in this guide, please ensure that you have the latest firmware version installed on your router.

Visit <http://vodafone.netcommwireless.com> to download the latest firmware.



**Note** – The functions described in this document require that the router is assigned with a publicly routable IP address.

Please ensure that your mobile carrier has provided you with a publicly routable IP address before performing the instructions in this document.

## Copyright

Copyright© 2016 NetComm Wireless Limited. All rights reserved.

Copyright© 2016 Vodafone Group Plc. All rights reserved.

The information contained herein is proprietary to NetComm Wireless and Vodafone. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless and Vodafone.

Trademarks and registered trademarks are the property of NetComm Wireless Limited or Vodafone Group or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.



**Note** – This document is subject to change without notice.

# Contents

<b>Introduction .....</b>	<b>4</b>
<b>Concepts and Basics.....</b>	<b>5</b>
Site-to-site IPsec VPN pre-conditions.....	5
IKE Phase 1 and Phase 2 .....	6
<b>IPsec VPN Web Interface.....</b>	<b>8</b>
Dead Peer Detection (DPD) mechanism .....	9
RSA Key mode.....	9
Digital Certificate mode.....	10
<b>IPsec VPN Configuration Examples .....</b>	<b>11</b>
<b>IPsec VPN Tunnel (Cisco router/Pre-shared key mode).....</b>	<b>11</b>
IPsec VPN configuration.....	12
Verify IPsec VPN connection status .....	14
<b>IPsec VPN Tunnel (Pre-shared Key mode) .....</b>	<b>14</b>
IPsec VPN configuration for local router.....	16
IPsec VPN configuration for remote router.....	17
Verify IPsec VPN connection status .....	18
<b>IPsec VPN tunnel (RSA Key mode).....</b>	<b>18</b>
IPsec VPN RSA configuration for local router .....	21
IPsec VPN RSA configuration for remote router .....	22
Verify IPsec VPN connection status.....	23
<b>IPsec VPN Tunnel (Digital Certificate mode).....</b>	<b>24</b>
IPsec VPN Digital Certificate configuration for local router .....	26
IPsec VPN Digital Certificate configuration for remote router .....	27
Verify IPsec VPN connection status .....	28

## Notation

The following symbols are used in this user guide:



The following note requires attention.



The following note provides a warning.



The following note provides useful information.

## Introduction

A VPN (Virtual private network) is a secure connection between two or more endpoints. It can also be seen as an extension to a private network.

There are two key types of VPN scenarios:

- Site-to-site VPN
- Remote Access VPN

In a site-to-site VPN, data is encrypted from one VPN gateway to the other, providing a secure link between two sites over an insecure third party network like the Internet.

In a remote access VPN scenario, a secure connection is made from an individual computer to a VPN gateway. This enables users to access their e-mail, files and other resources at work from wherever they may be, providing they have an Internet connection.

The Vodafone MachineLink router supports three types of Virtual Private Network (VPN) technologies:

- Point-to-Point Tunnelling Protocol (PPTP) VPN
- OpenVPN
- Internet Protocol Security (IPsec) VPN

### Point-to-Point Tunnelling Protocol (PPTP) VPN

PPTP works on a client server model. The Vodafone MachineLink router has a built-in PPTP client. Further details on how to set up a PPTP VPN tunnel connection is described in a separate document.

### OpenVPN

OpenVPN is an open source virtual private network (VPN) program for creating point-to-point or server-to-multi-client encrypted tunnels between host computers. The Vodafone MachineLink router supports three different OpenVPN modes:

- OpenVPN Server
- OpenVPN Client
- OpenVPN Peer-to-Peer VPN connection.

Further details on how to set up an OpenVPN tunnel connection is described in a separate document.

## Internet Protocol Security (IPsec) VPN

IPSec operates on Layer 3 and as such can protect higher layer protocols.

IPSec is used for both Site-to-site VPN and Remote Access VPN.

The Vodafone MachineLink router supports IPsec end points and can be configured with Site-to-site VPN tunnels with other MachineLink routers or third party VPN routers.

Further configuration instructions for IPsec VPN tunnels on the M2M Series Router are provided in this document.

# Concepts and Basics

## Site-to-site IPsec VPN pre-conditions

When setting up a Site to Site VPN with IPsec, firstly check the following pre-conditions.

- Make sure that there is connectivity between the two end points/VPN routers before you configure an IPsec VPN tunnel between them.

For example, you may do a simple 'Ping' test between the two VPN end points/Routers to verify connectivity.

- When a firewall or filtering router exists between IPsec peers, it must be configured to forward IPsec traffic on UDP source and destination port 500, IP protocol 50 (Encryption Service Payload: ESP), or IP protocol 51 (Authentication Header: AH). If you are using IPsec NAT-T, the firewall or filtering router must also be configured to forward IPsec traffic on UDP source and destination port 4500.
- If there is no firewall or filtering router between the IPsec end points, the MachineLink router will automatically create internal firewall rules to allow VPN tunnel connections to be established once an IPsec VPN is configured on the management interface. This behaviour will occur regardless of whether the firewall setting is 'Enabled' under the web management interface > system > administration page.

The next step is to select an authentication method for use on the VPN Tunnel. This defines what authentication key mode that you are going to use, either:

- Pre-shared key
- RSA key
- Install a digital certificate



Please note that both VPN routers must use the same type of credentials (either both using pre-shared keys or both using digital certificates).

If pre-shared keys are used, then both routers' keys would have to match each other.

In general, the pre-shared key method is the simplest to configure. Digital certificates require more complex configuration however they provide a more scalable solution, better suited for enterprise use.

## IKE Phase 1 and Phase 2

IPsec VPN's are configured and processed in two phases, Phase 1 and 2. They are also called the Internet Key Exchange (IKE) phase 1 and IKE phase 2. In the Vodafone MachineLink router VPN web-based graphical user interface, the IKE phase 2 parameters are named IPsec parameters.

IKE phase 1 focuses on establishing authentication and a secure tunnel for IKE phase 2 (IPsec tunnel) exchange. There are two modes in IKE phase 1: the main mode or aggressive mode. The Main mode is more secure, but slower than the aggressive mode. In Main mode, peers exchange identities with encryption whereas in aggressive mode, peers exchange identities without encryption.

IKE phase 1 requires the following elements to be configured. Attributes of the points 2-6 below must match on both VPN peers/routers before establishing an IKE phase 1 connection.

- Remote peer IP or hostname
- Key distribution method and authentication method: Pre-shared Key, RSA Key or Digital Certificates. If you use a digital certificate you could generate all the required files using OpenSSL, an open source Certificate Authority (CA).
- Encryption Algorithm for confidentiality: DES, 3DES or AES, AES 128, 192, 256 bit key strength. AES is the strongest protocol.
- Hashing Algorithm for Data Integrity and authentication: SHA1 or MD5. SHA1 is the stronger authentication algorithm.
- Diffie-Hellman Group Level: This is a method of the establishment of a shared key over an insecure medium. DH1, 2, 5, 14, 15, 16, 17 and 18 are available on the Vodafone MachineLink router.
- IKE Security Association (SA) Lifetime in seconds: As a general rule, a shorter lifetime provides more secure IKE negotiations. In the MachineLink router series routers, it is named the IKE rekey interval time in seconds.

IKE Phase 2 (IPsec) focuses on establishing secure IPsec tunnel for data transfer. IKE Phase 2 or IPsec requires the following elements.

### Transform set

This includes the encapsulation negotiation protocol to be used, either selecting Authentication Header (AH) or Encryption Security Payload (ESP). The Authentication Header only provides authentication and data integrity. The Encryption Security Payload provides authentication, data integrity and encryption. If you select ESP, you

need to specify authentication (SHA1 or MD5) and encryption (DES, 3DES or AES 128, 192, or 256-bit key strength). The transform set is used to transfer the clear text data to cipher text going across the IPsec tunnel. Attributes in the transform set on both VPN routers and SA life time are required to be matched across both ends of the tunnel.

### Peer information

The IP address of the VPN routers.

### Interesting traffic designation

Defines what traffic is to be sent encrypted to the remote VPN router and what traffic is expected to be encrypted from the remote VPN router and vice versa. This is to specify what traffic will go across the VPN. An IP address, Network address, or IP address range needs to be specified.

### IPsec SA life time

The IPsec Security Association lifetime in the MachineLink router VPN configuration page is named the 'SA Life' Time.

There is another optional security parameter to the IPsec phase, which basically performs a Diffie-Hellman exchange of the key when requesting a new IPsec SA. It is called Perfect Forward Secrecy (PFS). It ensures that a given IPsec SA key was not derived from any other secret. If PFS is not enabled, someone can potentially break the IKE SA secret key, copy all the IPsec protected data, and then use knowledge of the IKE SA secret in order to compromise the IPsec SAs setup by this IKE SA. With PFS, breaking IKE does not give an attacker immediate access to IPsec. The attacker needs to break each IPsec SA individually.

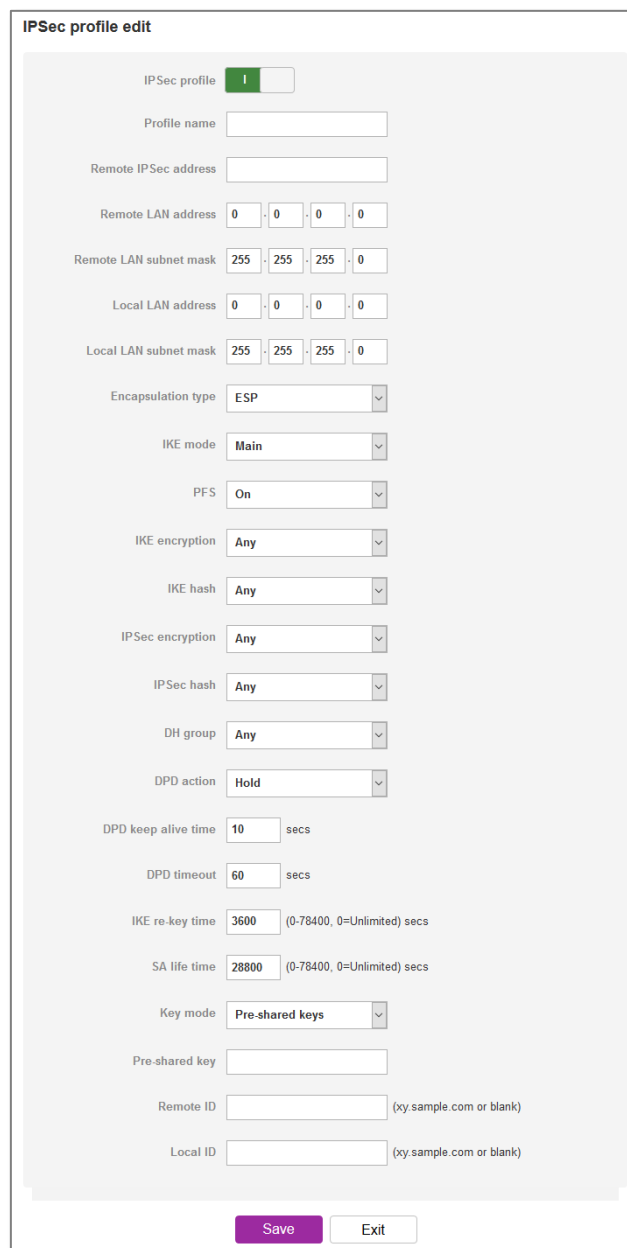


Note that these are the general steps in configuring your IPsec VPN router, and when you configure the peer VPN router, remember to configure it with the exact same settings as you configured your local router or else the VPN tunnel will not form successfully.

## IPsec VPN Web Interface

On the Vodafone MachineLink router, both the IKE phase 1 and phase 2 parameters are shown in one single configuration page (Figure 1). Open the IPsec configuration page by clicking the **Networking** toolbar item, then open the **VPN** menu item on the left and select **IPSec**.

The IPSEC tunnel list page appears, click the **+Add** button to open a new IPsec profile configuration edit page.



**IPSec profile edit**

IPSec profile:

Profile name:

Remote IPsec address:

Remote LAN address:  ·  ·  ·

Remote LAN subnet mask:  ·  ·  ·

Local LAN address:  ·  ·  ·

Local LAN subnet mask:  ·  ·  ·

Encapsulation type:

IKE mode:

PFS:

IKE encryption:

IKE hash:

IPSec encryption:

IPSec hash:

DH group:

DPD action:

DPD keep alive time:  secs

DPD timeout:  secs

IKE re-key time:  (0-78400, 0=Unlimited) secs

SA life time:  (0-78400, 0=Unlimited) secs

Key mode:

Pre-shared key:

Remote ID:  (xy.sample.com or blank)

Local ID:  (xy.sample.com or blank)

Figure 1 - IPsec Configuration Page of Web User Interface



## Dead Peer Detection (DPD) mechanism

The Vodafone MachineLink router supports Dead Peer Detection: A Traffic-Based method of detecting dead IKE peers.

DPD works using a keepalive system, when a tunnel is idle. Both sides attempt to exchange “hello” messages until the DPD timeout value has elapsed. If there still hasn't been any traffic received, the peer is declared to be dead, and the Security Association (SA) deleted, and related route removed from the table.

There are four DPD Action options:

- None - the DPD mechanism is disabled. This is the default setting
- Clear
- Hold
- Restart

The DPD Action parameter determines what the router does when a peer is determined to be dead. If set to "hold", the router will place the entire tunnel into a “hold” status, and wait for the peer to return. If set to "clear" it will remove the connection entirely. Lastly, Restart will recreate the tunnel after the dead peer is detected once again.

It is recommended that "Hold" be used for statically defined tunnels, and "Clear" be used for roadwarrior tunnels. Use “Restart” if you want the tunnel connection to restart after dead peer detected.

There are two timer options:

- DPD Keep Alive Time
- DPD Timeout

Thus, the mechanism works as follows:

During idle periods, the router sends R\_U\_THERE packets every **DPD\_Keep\_Alive\_Time** seconds.

If the tunnel is idle and the router hasn't received an R\_U\_THERE\_ACK from our peer in **DPD\_Timeout** seconds, the router declares the peer dead, and clears the Security Association (SA). Hence the entire tunnel is removed. Note that both sides must have either DPD Keep Alive Time or DPD Time out set for DPD to be proposed or accepted.

If one directive is set but not the other, the defaults are used (DPD Keep Alive Time=30, DPD Time Out =120).

## RSA Key mode

RSA is an acronym composed of the first letter of each of its inventors' last names (Ronald **R**ivest, Adi **S**hamir, and Leonard **A**dleman).

The RSA algorithm is a public-key cryptosystem that offers both encryption and digital signatures authentication. The Vodafone MachineLink router has a built-in RSA key generator. The RSA public key of your router can be generated by

clicking on the 'Generate' button under its web GUI interface: **Networking > VPN > IPsec** Configuration page where RSA key mode is selected. It then can be downloaded by clicking the 'Download' button on the same IPsec configuration page.

When using RSA key mode for IPsec VPN authentication between two MachineLink routers, it is important that the left RSA public key for the left VPN device is uploaded to its peer VPN device as remote RSA key via the 'Remote RSA Key Upload' button. Similarly the right key for the right VPN device should be uploaded to its peer VPN device as remote RSA key via the 'Remote RSA Key Upload' button. Further details can be found in the configuration examples section of this white paper.

## Digital Certificate mode

The Vodafone MachineLink router supports IPsec VPN tunnels using self signed x.509 Digital Certificates generated by OpenSSL. Details on how to install and generate digital certificates using the OpenSSL Certificate Authority (CA) server is not covered in this document.

The following files are compulsory when using Digital Certificate mode in the Vodafone MachineLink router:

- **Local Private Key** in .pem or .key format
- **Local Public Certificate** in .crt format
- **Remote Public Certificate** in .crt format
- **Certificate Authority (CA) Certificate** in .crt format

The certificate revocation list (CRL) in .crt format is an optional file. The CRL file provides the router with a means of determining whether a certificate that is within its valid time range has been revoked by its issuing Certificate Authority (CA).

It is important that both the local and remote public certificates are signed by the same Certificate Authority. Additionally, the system date and time of the cellular routers matter when using digital certificates as this affects the time validity of the router's certificates for making a successful VPN connection.

# IPsec VPN Configuration Examples

## IPsec VPN Tunnel (Cisco router/Pre-shared key mode)

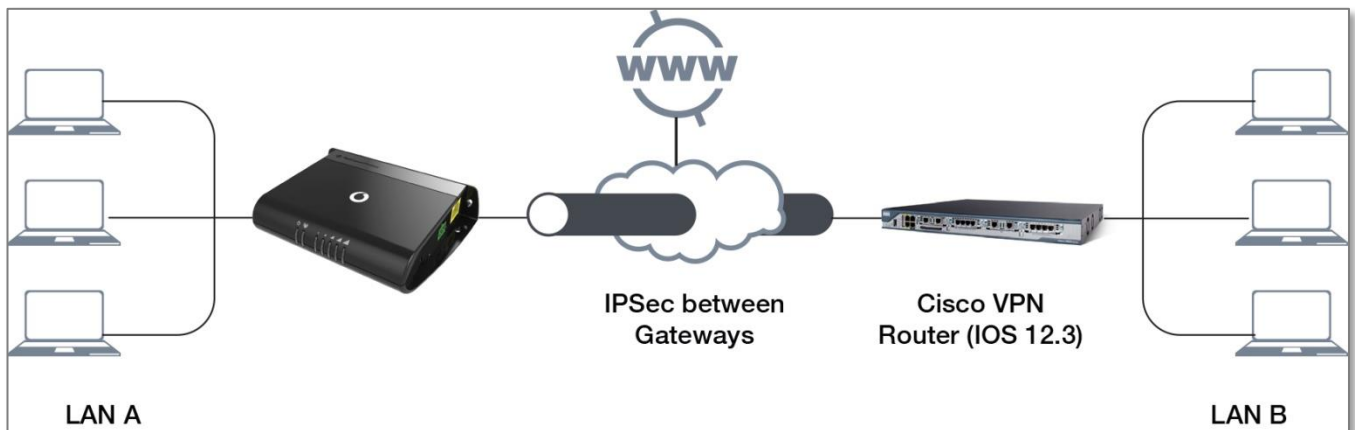


Figure 2 – Vodafone MachineLink router to Cisco VPN Router Site-to-site network diagram

	Local VPN Router (MachineLink 3G)	Remote VPN router (Cisco VPN Router running ios 12.3)
LAN IP Address	192.168.20.1	192.168.1.80
WAN IP Address	123.209.156.240	115.166.45.22
IPSec	Enabled	Enabled
Local Secure Group Network Address	192.168.20.0 / 255.255.255.0	192.168.1.0 / 255.255.255.0
Remote Secure Group Network Address	192.168.1.0 / 255.255.255.0	192.168.20.0 / 255.255.255.0
IPSec Gateway	123.209.182.205	60.242.24.140
IKE Mode	Main	Main
IKE Encryption	3DES	3DES
IKE Hash	MD5	MD5
IKE Reh		
IKE Rekey Time (sec)	3600	3600
IPSec Encapsulation Protocol	ESP	ESP
IPSec Encryption	3DES	3DES
IPSec Hash	MD5	MD5
SA Life Time (sec)	28800	28800
DH Group	Group 2 (1024)	Group 2 (1024)
PFS	ON	ON

	Local VPN Router (MachineLink 3G)	Remote VPN router (Cisco VPN Router running ios 12.3)
IKE Key Mode	Pre-shared Key	Pre-shared Key
Pre-shared Key	testing123	testing123
DPD Action	Hold	Hold
DPD Keep Alive Time (sec)	10	10
DPD Time Out (sec)	60	60

Figure 3 – Vodafone MachineLink router to Cisco VPN Router Site-to-site configuration details

## IPSec VPN configuration

**IPSec profile edit**

IPSec profile: **1**

Profile name:

Remote IPsec address:

Remote LAN address:  ·  ·  ·

Remote LAN subnet mask:  ·  ·  ·

Local LAN address:  ·  ·  ·

Local LAN subnet mask:  ·  ·  ·

Encapsulation type:

IKE mode:

PFS:

IKE encryption:

IKE hash:

IPSec encryption:

IPSec hash:

DH group:

DPD action:

DPD keep alive time:  secs

DPD timeout:  secs

IKE re-key time:  (0-78400, 0=Unlimited) secs

SA life time:  (0-78400, 0=Unlimited) secs

Key mode:

Pre-shared key:

Remote ID:  (xy.sample.com or blank)

Local ID:  (xy.sample.com or blank)

Figure 4: IPsec Example VPN Configuration on the Vodafone MachineLink router

## IPsec VPN configuration for Cisco router (IOS 12.3)



**Note** – This partial configuration is provided as an example only.  
NetComm Wireless does not offer further assistance with Cisco configuration.

```
-----  
!  
crypto isakmp policy 1  
  encr 3des  
  hash md5  
  authentication pre-share  
  group 2  
  lifetime 28800  
crypto ipsec security-association lifetime seconds 600  
crypto ipsec transform-set NWL10set esp-3des esp-md5-hmac  
crypto dynamic-map dynmapNWL 1  
  description NWL-10  
  set transform-set NWL10set  
  set pfs group2  
  match address 101  
  reverse-route  
crypto map mymap 1 ipsec-isakmp dynamic dynmapNWL  
interface FastEthernet0/1  
  ip address 192.168.1.80 254 255.255.255.0  
  ip nat inside  
  ip virtual-reassembly  
  duplex auto  
  speed auto  
interface Dialer1  
.  
.  
.  
.  
crypto map mymap  
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.20.0 0.0.0.255
```

## Verify IPsec VPN connection status

Ping the remote IPsec gateway and its secure group to verify VPN tunnel connectivity. Refer to screen shot shown below.

**Packet data connection status**

Profile name: Profile1  
 Status: Connected  
 Default profile: Yes

WWAN IP: 123.209.182.205  
 DNS server: 10.4.81.103, 10.4.182.20

```

Command Prompt - ping 60.242.24.140 -t
Reply from 60.242.24.140: bytes=32 time=114ms TTL=239
Reply from 60.242.24.140: bytes=32 time=165ms TTL=239
Reply from 60.242.24.140: bytes=32 time=114ms TTL=239
Reply from 60.242.24.140: bytes=32 time=114ms TTL=239
Reply from 60.242.24.140: bytes=32 time=124ms TTL=239
Reply from 60.242.24.140: bytes=32 time=129ms TTL=239
Reply from 60.242.24.140: bytes=32 time=113ms TTL=239
Reply from 60.242.24.140: bytes=32 time=124ms TTL=239
Reply from 60.242.24.140: bytes=32 time=113ms TTL=239
Reply from 60.242.24.140: bytes=32 time=164ms TTL=239
Reply from 60.242.24.140: bytes=32 time=114ms TTL=239
    
```

#	Name	Interface	Local LAN	Remote gateway	Remote LAN	Status
1	IPsec Demo	rmnet1	192.168.20.0	60.242.24.140	192.168.1.0	Connected

Figure 5: Testing the IPsec VPN Connection Status

The IPsec VPN tunnel between the Vodafone MachineLink router and the Cisco router is now up and running.

## IPsec VPN Tunnel (Pre-shared Key mode)

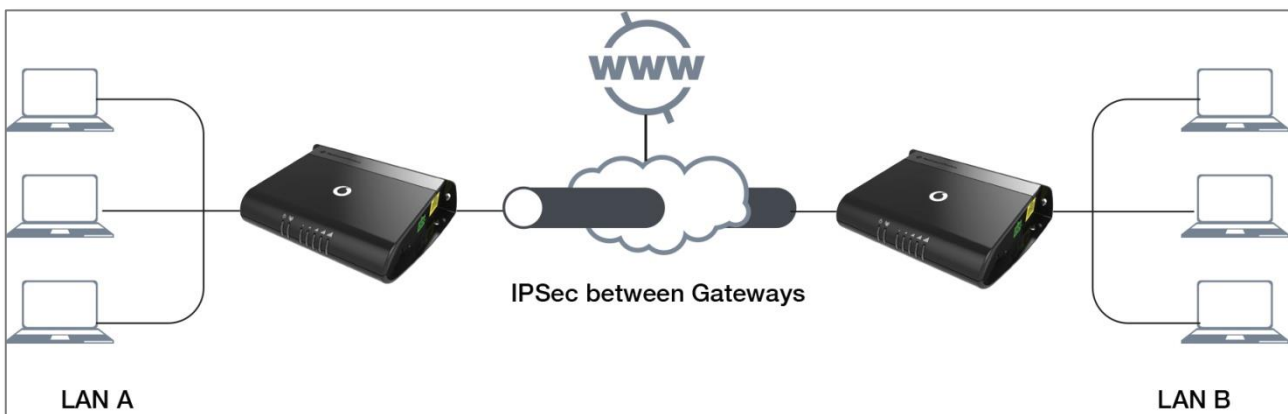


Figure 6 – MachineLink router to MachineLink router Site-to-site network diagram

	Local VPN Router (MachineLink 3G)	Remote VPN router (MachineLink 3g)
LAN IP Address	192.168.1.1	192.168.20.1
WAN IP Address	123.209.37.6	123.209.177.239
IPSec	Enabled	Enabled
Local Secure Group Network Address	192.168.1.0 / 255.255.255.0	192.168.20.0 / 255.255.255.0
Remote Secure Group Network Address	192.168.20.0 / 255.255.255.0	192.168.1.0 / 255.255.255.0
IPSec Gateway	123.209.37.6	123.209.177.239
IKE Mode	Main	Main
IKE Encryption	AES	AES
IKE Hash	SHA1	SHA1
IKE Reh		
IKE Rekey Time (sec)	3600	3600
IPSec Encapsulation Protocol	ESP	ESP
IPSec Encryption	AES	AES
IPSec Hash	SHA1	SHA1
SA Life Time (sec)	28800	28800
DH Group	Group 2 (1024)	Group 2 (1024)
PFS	ON	ON
IKE Key Mode	Pre-shared Key	Pre-shared Key
Pre-shared Key	testkey	testkey
DPD Action	Restart	Restart
DPD Keep Alive Time (sec)	10	10
DPD Time Out (sec)	60	60

*Table 1 – MachineLink router to MachineLink router Site-to-site configuration details*

## IPsec VPN configuration for local router

### IPsec VPN Configuration using Pre-shared key mode (Local Router)

**IPSec profile edit**

IPSec profile: 1

Profile name:

Remote IPSec address:

Remote LAN address:  ·  ·  ·

Remote LAN subnet mask:  ·  ·  ·

Local LAN address:  ·  ·  ·

Local LAN subnet mask:  ·  ·  ·

Encapsulation type:

IKE mode:

PFS:

IKE encryption:

IKE hash:

IPSec encryption:

IPSec hash:

DH group:

DPD action:

DPD keep alive time:  secs

DPD timeout:  secs

IKE re-key time:  (0-78400, 0=Unlimited) secs

SA life time:  (0-78400, 0=Unlimited) secs

Key mode: Pre-shared keys

Pre-shared key:

Remote ID:  (xy.sample.com or blank)

Local ID:  (xy.sample.com or blank)

Figure 7 – IPsec VPN Configuration in the MachineLink router (Local Router)



## IPsec VPN configuration for remote router

### IPsec VPN Configuration using Pre-shared key mode (Remote Router)

**IPSec profile edit**

IPSec profile: 1

Profile name:

Remote IPSec address:

Remote LAN address:  ·  ·  ·

Remote LAN subnet mask:  ·  ·  ·

Local LAN address:  ·  ·  ·

Local LAN subnet mask:  ·  ·  ·

Encapsulation type:

IKE mode:

PFS:

IKE encryption:

IKE hash:

IPSec encryption:

IPSec hash:

DH group:

DPD action:

DPD keep alive time:  secs

DPD timeout:  secs

IKE re-key time:  (0-78400, 0=Unlimited) secs

SA life time:  (0-78400, 0=Unlimited) secs

Key mode:

Pre-shared key:

Remote ID:  (xy.sample.com or blank)

Local ID:  (xy.sample.com or blank)

Figure 8 – IPsec VPN Configuration in Vodafone MachineLink routers (Remote Router)

## Verify IPsec VPN connection status

Ping a device in the remote secure group to verify VPN tunnel connectivity. Refer to screen shot shown below.

**Packet data connection status**

Profile name: Profile1  
 Status: Connected  
 Default profile: Yes

WWAN IP: 123.209.37.6  
 DNS server: 10.4.182.20, 10.4.81.103

**IPsec VPN status**

#	Name	Interface	Local LAN	Remote gateway	Remote LAN	Status
1	ML3G-to-ML3G	rmnet1	192.168.1.0	123.209.177.239	192.168.20.0	Connected

Command Prompt - ping 192.168.20.93 -t

```

Reply from 192.168.20.93: bytes=32 time=959ms TTL=126
Reply from 192.168.20.93: bytes=32 time=918ms TTL=126
Reply from 192.168.20.93: bytes=32 time=1095ms TTL=126
Reply from 192.168.20.93: bytes=32 time=996ms TTL=126
Reply from 192.168.20.93: bytes=32 time=935ms TTL=126
Reply from 192.168.20.93: bytes=32 time=908ms TTL=126
Reply from 192.168.20.93: bytes=32 time=913ms TTL=126
Reply from 192.168.20.93: bytes=32 time=864ms TTL=126
Reply from 192.168.20.93: bytes=32 time=906ms TTL=126
    
```

Figure 9 – Verifying the IPsec VPN Connection Status

The IPsec VPN tunnel between the two MachineLink routers is now up and running.

## IPsec VPN tunnel (RSA Key mode)

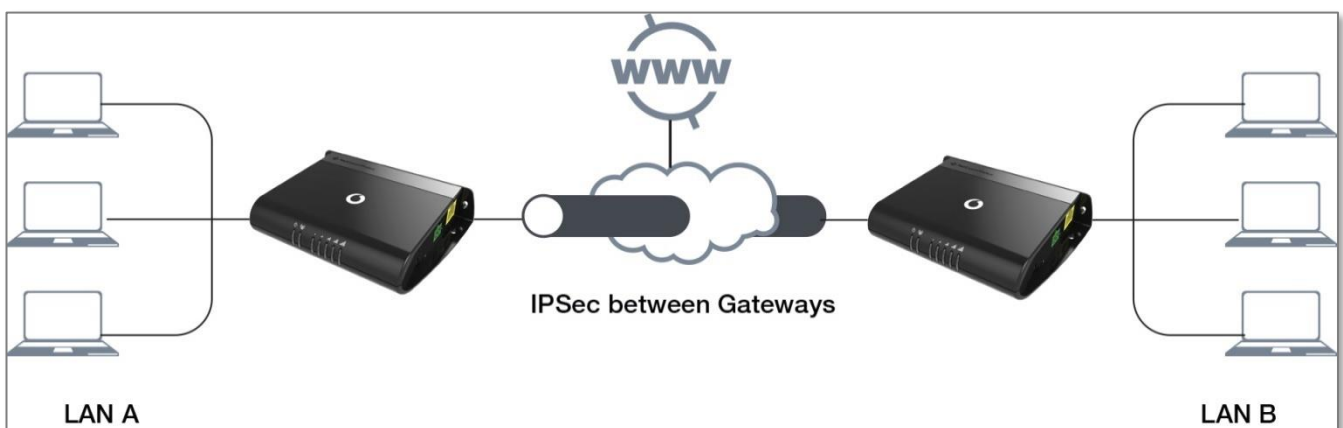


Figure 10 – MachineLink router to MachineLink router RSA key mode Site-to-site network diagram

	Local VPN Router (MachineLink 3G)	Remote VPN router (MachineLink 3g)
LAN IP Address	192.168.1.1	192.168.20.1
WAN IP Address	123.209.156.240	123.209.43.246
IPSec	Enabled	Enabled
Local Secure Group Network Address	192.168.1.0 / 255.255.255.0	192.168.20.0 / 255.255.255.0
Remote Secure Group Network Address	192.168.20.0 / 255.255.255.0	192.168.1.0 / 255.255.255.0
IPSec Gateway	123.209.156.240	123.209.43.246
IKE Mode	Main	Main
IKE Encryption	3DES	3DES
IKE Hash	SHA1	SHA1
IKE Rehash		
IKE Rekey Time (sec)	3600	3600
IPSec Encapsulation Protocol	ESP	ESP
IPSec Encryption	3DES	3DES
IPSec Hash	SHA1	SHA1
SA Life Time (sec)	28800	28800
DH Group	Group 2 (1024)	Group 2 (1024)
PFS	ON	ON
IKE Key Mode	RSA Key	RSA Key
Local RSA Key Upload	Not required*	Not required*
Remote RSA Key Upload	Upload the peer's RSA key)**	Upload the peer's RSA key)**
DPD Action	Hold	Hold
DPD Keep Alive Time (sec)	10	10
DPD Timeout (sec)	60	60

*Table 2 –MachineLink 3G to MachineLink 3G RSA Key Mode Site-to-site configuration details*

**Important Notes:**



\* The local RSA key in this sample scenario is not required to be uploaded because when the RSA key **'Generate'** button on the IPSec configuration page is pressed, the router's own local RSA key is generated and saved in its IPSec VPN directory.

The router's local RSA key file can be downloaded by clicking on the **'Download'** button. The RSA key file can be renamed as long as the extension **'.key'** remains unchanged.



\*\* "Remote RSA Key" refers to the peer's RSA key in .key format. It is the RSA key file where you downloaded, saved and transferred from its peer router to this router. In other words, a router's local RSA key is the remote RSA key for its peer VPN router.

In this sample scenario, the following files names were used to identify the local RSA key file and remote RSA key file.

	Local VPN Router (MachineLink 3G)	Remote VPN router (MachineLink 3g)
Local RSA key file	leftrsa7_local.key	leftrsa7_remote.key
Remote RSA key file	leftrsa7_remote.key	leftrsa7_local.key

*Table 3 – Local and remote RSA key names*

## IPsec VPN RSA configuration for local router

### IPsec VPN RSA Key Mode Configuration using RSA key mode (Local Router)

**IPSec profile edit**

IPSec profile:

Profile name:

Remote IPSec address:

Remote LAN address:  ·  ·  ·

Remote LAN subnet mask:  ·  ·  ·

Local LAN address:  ·  ·  ·

Local LAN subnet mask:  ·  ·  ·

Encapsulation type:

IKE mode:

PFS:

IKE encryption:

IKE hash:

IPSec encryption:

IPSec hash:

DH group:

DPD action:

DPD keep alive time:  secs

DPD timeout:  secs

IKE re-key time:  (0-78400, 0=Unlimited) secs

SA life time:  (0-78400, 0=Unlimited) secs

Key mode:

Remote ID:   
(xy.sample.com or blank)

Local ID:   
(xy.sample.com or blank)

Update time:

Local RSA key upload:

Remote RSA key upload:

Figure 11 – IPsec VPN RSA Key Mode Configuration in MachineLink 3G (Local Router)

**Important Note**


It is important to 'Enable' and 'Save' the IPsec RSA key mode configuration profile before the router generates its own RSA key. This will ensure that the MachineLink router's IPsec main program is running. Once the router finishes generating its RSA key, you will need to click on the 'Save' button again at the bottom of its configuration page to make it effective.

## IPsec VPN RSA configuration for remote router

The following is an example of an IPsec VPN using RSA Key mode on the remote router.

**IPSec profile edit**

IPSec profile: 1

Profile name:

Remote IPsec address:

Remote LAN address:

Remote LAN subnet mask:

Local LAN address:

Local LAN subnet mask:

Encapsulation type: Any

IKE mode:

PFS:

IKE encryption:

IKE hash:

IPsec encryption:

IPsec hash:

DH group:

DPD action:

DPD keep alive time:  secs

DPD timeout:  secs

IKE re-key time:  (0-78400, 0=Unlimited) secs

SA life time:  (0-78400, 0=Unlimited) secs

Key mode:

Remote ID:

(xy.sample.com or blank)

Local ID:

(xy.sample.com or blank)

Update time:

Local RSA key upload:

Remote RSA key upload:

Figure 12 – IPsec VPN RSA Key Mode Configuration in MachineLink router (Remote Router)

**Important Note**

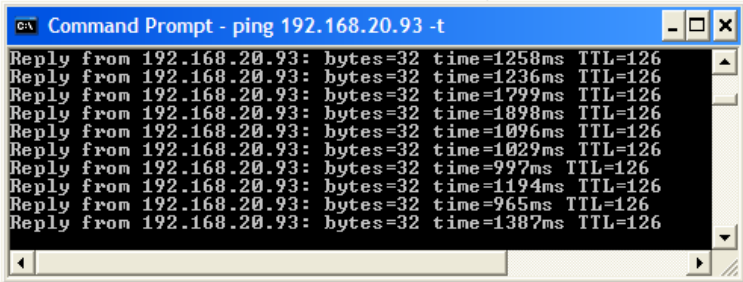

It is important to 'Enable' and 'Save' the IPsec RSA key mode configuration profile before the router generates its own RSA key. This will ensure that the MachineLink router's IPsec main program is running. Once the router finishes generating its RSA key, you will need to click on the 'Save' button again at the bottom of its configuration page to make it effective.

## Verify IPsec VPN connection status

Ping a device in the remote secure group to verify VPN tunnel connectivity. Refer to screen shot shown below.

**^ Packet data connection status**

<b>Profile name</b>	<b>Profile1</b>
<b>Status</b>	<b>WWAN IP</b>
<b>Connected</b>	<b>123.209.156.240</b>
<b>Default profile</b>	<b>DNS server</b>
<b>Yes</b>	<b>10.4.81.103</b>
	<b>10.4.182.20</b>



**^ IPsec VPN status**

#	Name	Interface	Local LAN	Remote gateway	Remote LAN	Status
1	ML3G-to-ML3G	rmnet1	192.168.1.0	123.209.43.246	192.168.20.0	Connected

The IPsec VPN tunnel between the two MachineLink routers using RSA key mode is now up and running.

## IPsec VPN Tunnel (Digital Certificate mode)

This diagram illustrates a IPsec Site to Site VPN Tunnel using the digital certificate mode.

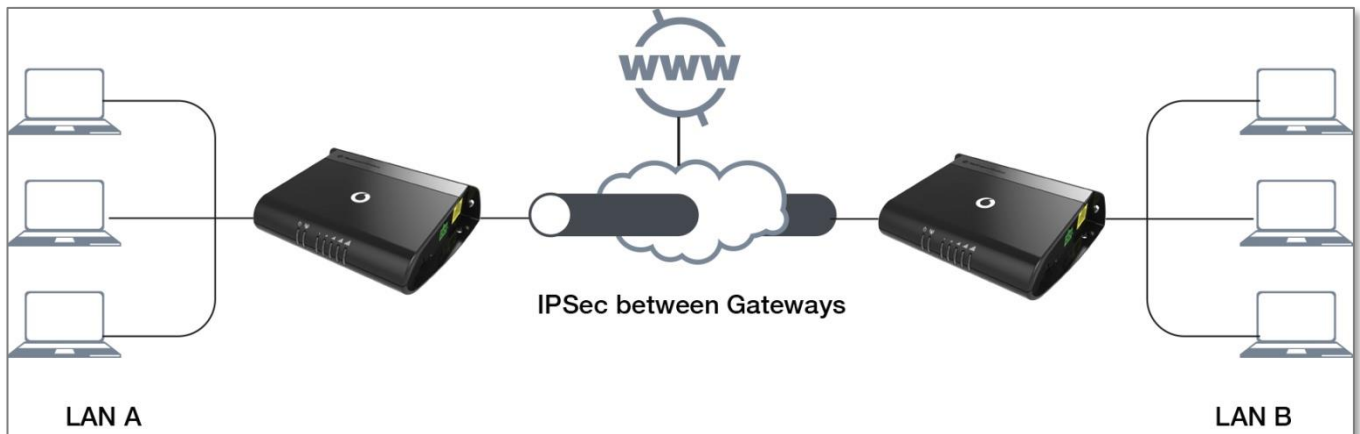


Figure 13 – MachineLink router to MachineLink router Digital Certificate Mode Site-to-site network diagram

	Local VPN Router (MachineLink 3G)	Remote VPN router (MachineLink 3g)
LAN IP Address	192.168.1.1	192.168.20.1
WAN IP Address	123.209.156.240	123.209.43.246
IPSec	Enabled	Enabled
Local Secure Group Network Address	192.168.1.0 / 255.255.255.0	192.168.20.0 / 255.255.255.0
Remote Secure Group Network Address	192.168.20.0 / 255.255.255.0	192.168.1.0 / 255.255.255.0
IPSec Gateway	123.209.156.240	123.209.43.246
IKE Mode	Main	Main
IKE Encryption	Any	Any
IKE Hash	Any	Any
IKE Reh		
IKE Rekey Time (sec)	3600	3600
IPSec Encapsulation Protocol	Any	Any
IPSec Encryption	Any	Any
IPSec Hash	Any	Any
SA Life Time (sec)	28800	28800
DH Group	Group 2 (1024)	Group 2 (1024)
PFS	ON	ON



	Local VPN Router (MachineLink 3G)	Remote VPN router (MachineLink 3g)
IKE Key Mode	Certificates	Certificates
Private key passphrase	test	test
Local private key	File named: device1.key	File named: device2.key
Local public certificate	File named: device1.crt	File named: device2.crt
Remote public certificate	File named: device2.crt	File named: device1.crt
CA Certificate	File named: root-ca.crt	File named: root-ca.crt
CRL Certificate	Not used	Not used
DPD Action	Hold	Hold
DPD Keep Alive Time (sec)	10	10
DPD Timeout (sec)	60	60

*Table 4 – MachineLink 3G to MachineLink 3G Digital Certificate Mode Site-to-site configuration details*



The 'Private Key Passphrase' of the router is the passphrase used when generating the router's private key using OpenSSL CA. It is important that you key this in correctly in the router's IPsec configuration page.



The router's system date and time is important as this will affect the validity period of the digital certificate. Therefore it is important to verify the routers have the current date and time.

## IPsec VPN Digital Certificate configuration for local router

**IPSec profile edit**

IPSec profile: 1

Profile name:

Remote IPSec address:

Remote LAN address:  ·  ·  ·

Remote LAN subnet mask:  ·  ·  ·

Local LAN address:  ·  ·  ·

Local LAN subnet mask:  ·  ·  ·

Encapsulation type:

IKE mode:

PFS:

IKE encryption:

IKE hash:

IPSec encryption:

IPSec hash:

DH group:

DPD action:

DPD keep alive time:  secs

DPD timeout:  secs

IKE re-key time:  (0-78400, 0=Unlimited) secs

SA life time:  (0-78400, 0=Unlimited) secs

Key mode:

Private key passphrase:

Key / Certificate:

Not uploaded

IPSec certificate upload:

Figure 14 – IPsec VPN Digital Certificate Mode Configuration in MachineLink routers (Local Router)

## IPsec VPN Digital Certificate configuration for remote router

### IPsec VPN Digital Certificate Mode Configuration (Remote Router)

**IPSec profile edit**

IPSec profile: I

Profile name:

Remote IPSec address:

Remote LAN address:  ·  ·  ·

Remote LAN subnet mask:  ·  ·  ·

Local LAN address:  ·  ·  ·

Local LAN subnet mask:  ·  ·  ·

Encapsulation type:

IKE mode:

PFS:

IKE encryption:

IKE hash:

IPSec encryption:

IPSec hash:

DH group:

DPD action:

DPD keep alive time:  secs

DPD timeout:  secs

IKE re-key time:  (0-78400, 0=Unlimited) secs

SA life time:  (0-78400, 0=Unlimited) secs

Key mode:

Private key passphrase:

Key / Certificate:

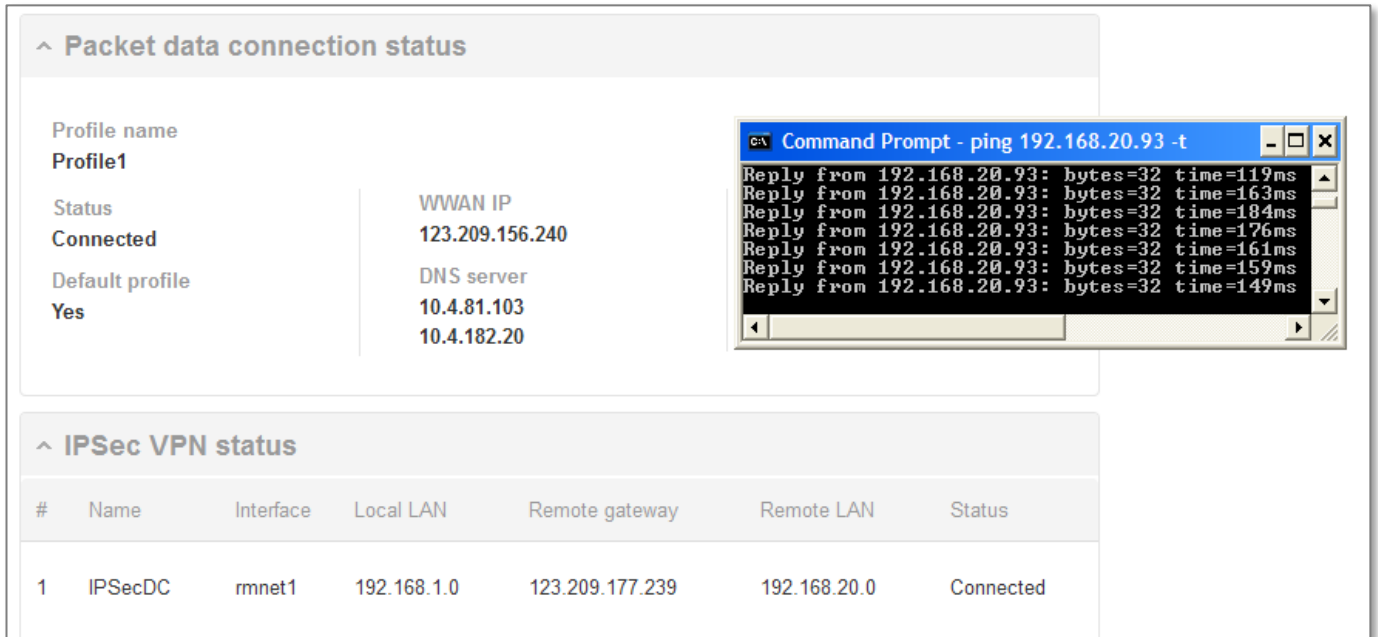
Not uploaded

IPSec certificate upload:

Figure 15 – IPsec VPN Digital Certificate Mode Configuration in MachineLink routers (Remote Router)

## Verify IPsec VPN connection status

To verify VPN tunnel connectivity, ping a device in the remote secure group. Refer to screen shot shown below.



**Packet data connection status**

Profile name  
**Profile1**

Status  
**Connected**

Default profile  
**Yes**

WWAN IP  
**123.209.156.240**

DNS server  
**10.4.81.103**  
**10.4.182.20**

**IPsec VPN status**

#	Name	Interface	Local LAN	Remote gateway	Remote LAN	Status
1	IPSecDC	rmnet1	192.168.1.0	123.209.177.239	192.168.20.0	Connected

```

C:\> Command Prompt - ping 192.168.20.93 -t
Reply from 192.168.20.93: bytes=32 time=119ms
Reply from 192.168.20.93: bytes=32 time=163ms
Reply from 192.168.20.93: bytes=32 time=184ms
Reply from 192.168.20.93: bytes=32 time=176ms
Reply from 192.168.20.93: bytes=32 time=161ms
Reply from 192.168.20.93: bytes=32 time=159ms
Reply from 192.168.20.93: bytes=32 time=149ms
    
```

Figure 16 – Verifying the IPsec VPN Connection Status on the MachineLink router

The IPsec VPN tunnel between the two MachineLink routers using Digital Certificates mode is now up and running.