IPSec VPN Configuration Whitepaper

Table of Contents

DOCUMENT VERSION	DATE
- Initial document release	11/01/2012
- Added M2M Series Router Series IPsec VPN RSA Key Mode and Digital Certificate Mode Overview and their configuration examples	27/02/2012

Table 1 - Document Revision History

Note: Before performing the instructions in this guide, please ensure that you have the latest firmware version on your router. Visit http://www.netcommwireless.com/products/m2m-wireless to find your device and download the latest firmware.

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 a third party insecure network like the Internet.
In a remote access VPN scenario, a secure connection would be made from an individual computer to a VPN gateway. This would enable a user to access their e-mail, files and other resources at work from wherever they may be, providing they have an Internet connection.

The NetComm M2M Series Router Series Cellular Router running firmware version V1.9.42.x or later supports three types of Virtual Private Network (VPN) technologies:

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

PPTP works on a client server model. The M2M Series Router has a built-in PPTP client. Further details on how to set up the M2M Series Router PPTP VPN tunnel connection is described in a separate document.
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 M2M Series Router supports three different OpenVPN modes:

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

Further details on how to set up an M2M Series Router OpenVPN tunnel connection is also described in a separate document.
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 M2M Series Router Series Cellular routers support IPsec end points and can be configured with Site to Site VPN tunnels with other M2M Series 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 M2M Series Routers), the M2M Series 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 set to '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, ether:

- 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 provide a more scalable solution, suitable 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 M2M Series 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 aggressive mode. In Main mode, peers exchange identities with encryption whereas in Aggressive mode, peers exchanges 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.

1. Remote peer IP or hostname
2. 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).
3. Encryption Algorithm for confidentiality: DES, 3DES or AES, AES 128, 192, 256 bit key strength. AES is the strongest protocol.
4. Hashing Algorithm for Data Integrity and authentication: SHA1 or MD5. SHA1 is the stronger authentication algorithm.
5. 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 in the M2M Series Router Series.
6. IKE Security Association (SA) Lifetime in seconds: As a general rule, a shorter lifetime provides more secure IKE negotiations. In the M2M Series 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.

1. 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.
2. Peer information: the IP address of the VPN routers.
3. 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.
4. IPsec SA life time: The IPSec Security Association lifetime in the M2M Series 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.

The M2M Series Router IPsec VPN Web Interface

In the NetComm M2M Series Cellular Router, both the IKE phase 1 and phase 2 parameters are shown in one single configuration page (Figure 1). It is located in the following directory of its web management interface: Internet Settings > VPN > Add> IPsec.

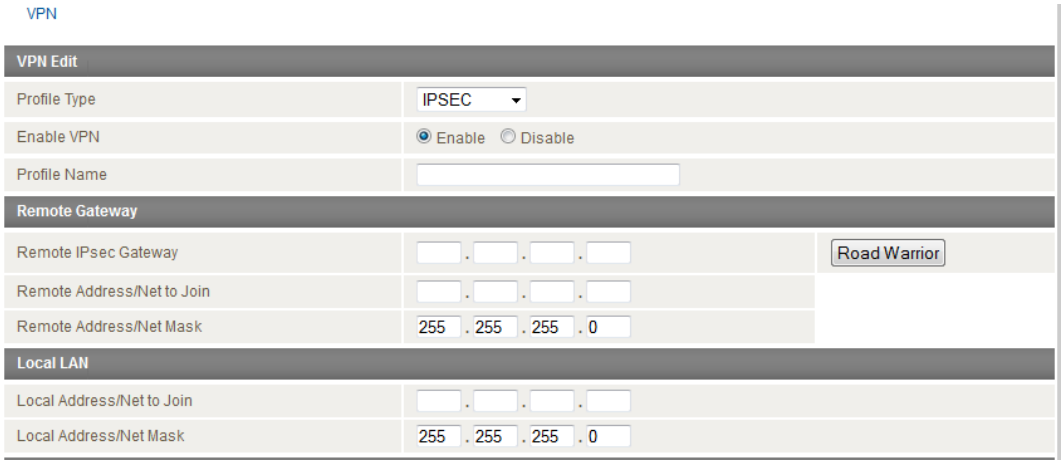


Figure 1 - IPSec Configuration Page of Web User Interface

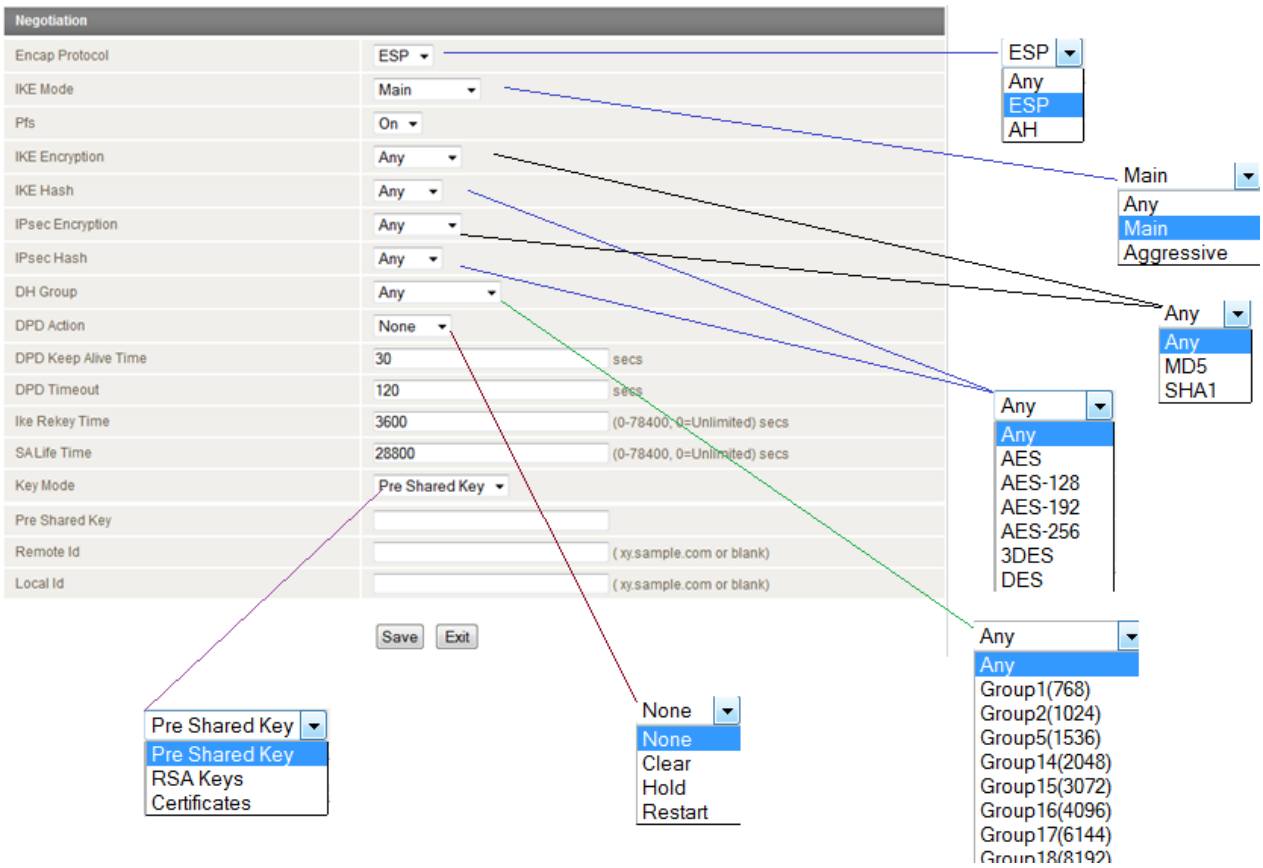


Figure 2 - Negotiation parameters for IPSec Configuration

Dead Peer Detection Mechanism in M2M Series Router

The M2M Series 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 havn’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 in M2M Series Router

RSA stands for the first letter in each of its inventors' (Ronald Rivest, Adi Shamir, and Leonard Adleman) last names. The RSA algorithm is a public-key cryptosystem that offers both encryption and digital signatures authentication. The M2M Series Router Series cellular router has a built-in RSA key generator. The RSA public key of your router can be genreated by clicking on the ‘Generate’ button under its web GUI interface: Internet Settings > 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 M2M Series Router Series cellular 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. Furher details can be found in the configuration examples section of this white paper.

Digital Certificate Mode in the M2M Series Router

The M2M Series Router Series Cellular 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 M2M Series 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 suceessful VPN connection.

IPsec VPN Configuration Examples

IPsec Site to Site VPN Tunnel with Cisco Router using Pre-shared key mode

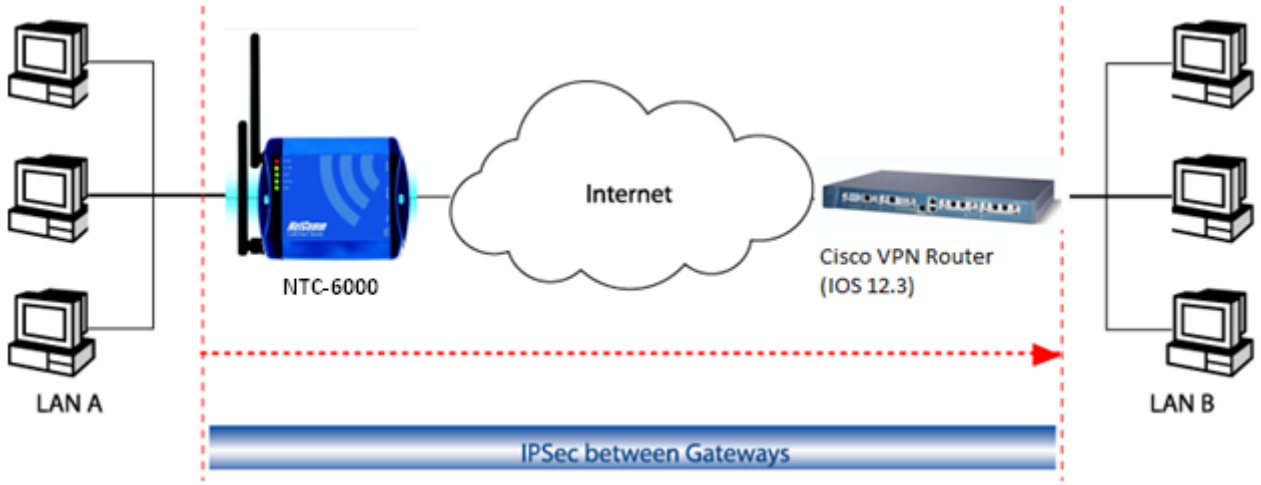


Figure 3 – M2M Series Router to Cisco VPN Router Site-to-Site Network Diagram and Policy Planning

	Local VPN Router (NTC-6900)		Remote VPN Router (Cisco VPN Router running IOS12.3)
LAN IP Address	192.168.20.1		192.168.1.80
WAN IP Address (Telstra IP WAN)	10.0.0.13		10.0.0.5
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	10.0.0.5		10.0.0.13
IKE Mode	Main		Main
IKE encryption	3DES		3DES
IKE Hash	MD5		MD5
IKE Rekey Time (sec)	3600		3600
Ipsec Encap 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
IKE Key Mode	Pre-Shared Key		Pre-Shared Key
Pre-Shared Key	myTESTkey		myTESTkey
DPD Action	Hold		
DPD Keep Alive Time (Sec)	10		
DPD Time Out (Sec)	60		

Figure 4 – M2M Series Router to Cisco VPN Router Site-to-Site Policy Planning Diagram

IPsec VPN Configuration in M2M Series Routers

Status | Internet Settings | Wireless Settings | Services | System

Internet Settings > VPN > IPSec

VPN IPSec Edit	
Enable This IPSec Profile	(•) Enable ( ) Disable
Profile Name	NTC-6000ToCisco
Remote Gateway	
Remote IPSec Gateway	10.0.0.5 Road Warrior
Remote Address/Net to Join	192 . 168 . 1 . 0
Remote Address/Net Mask	255 . 255 . 255 . 0
Local LAN	
Local Address/Net to Join	192 . 168 . 20 . 0
Local Address/Net Mask	255 . 255 . 255 . 0
Negotiation	
Encap Protocol	ESP
IKE Mode	Main
PFS	ON
ike encryption	3DES
IKE Hash	MD5
IPSec Encryption	3DES
IPSec Hash	MD5
DH Group	Group2(1024)
DPD Action	Hold
DPD Keep Alive Time	10 secs
DPD Timeout	60 secs
IKE Rekey Time	3600 (0-78400, 0=Unlimited) secs
SA Life Time	28800 (0-78400, 0=Unlimited) secs
Key Mode	Pre Shared Key
Pre Shared Key	myTESTkey
Remote Id	(xy.sample.com or blank)
Local Id	(xy.sample.com or blank)

Save Exit

Figure 5: IPsec Example VPN Configuration in M2M Series Router

IPsec VPN Configuration in Cisco Router Running IOS 12.3

NB: This configuration is provided as an example only, NetComm Wireless does not offer further assistance with Cisco configuration.

```
version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Router

!

boot-start-marker

boot-end-marker

!

no aaa new-model

ip subnet-zero

!

ip audit notify log

ip audit po max-events 100

ip ssh break-string

!

crypto isakmp policy 1

 encr 3des

 hash md5

 authentication pre-share

 group 2

 lifetime 28800

!

crypto isakmp key myTESTkey address 10.0.0.13

!

crypto ipsec transform-set 6908set esp-3des esp-md5-hmac

!

crypto dynamic-map dynmap6908 1
```

```
 description NTC6908
 set transform-set 6908set
 set pfs group2
 match address 101
 reverse-route
!
crypto map mymap 1 ipsec-isakmp dynamic dynmap6908
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 pppoe enable
 pppoe-client dial-pool-number 1
 no cdp enable
!
interface Serial0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.1.80 255.255.255.0
 no ip redirects
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
```

```
interface Dialer1
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname test@call-direct.com.au
 ppp chap password 0 test
 ppp ipcp dns request accept
 ppp ipcp address accept
 crypto map mymap
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.20.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login local
line aux 0
line vty 0 4
  login local
!
end
```

Verifying the IPSec VPN Connection Status on M2M Series Routers

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

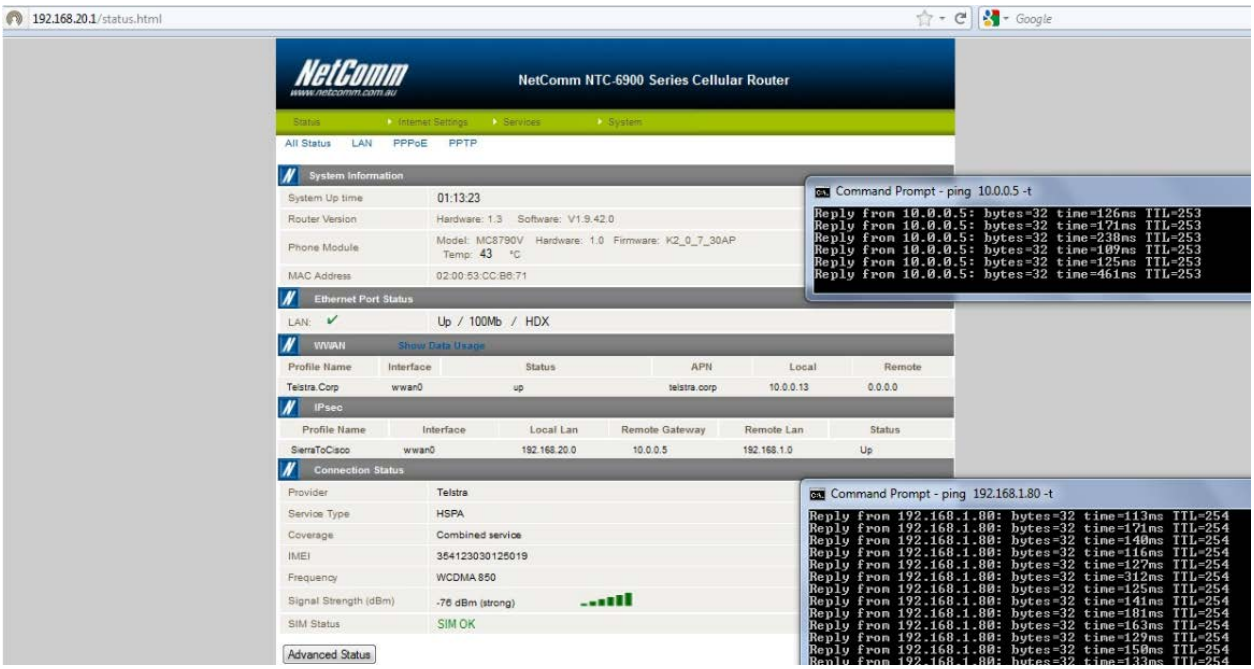


Figure 6: Testing the IPsec VPN Connection Status

The IPsec VPN tunnel between the M2M Series Router and the Cisco router is now up and running.

IPsec Site to Site VPN Tunnel with another M2M Series Router using Pre-shared key mode

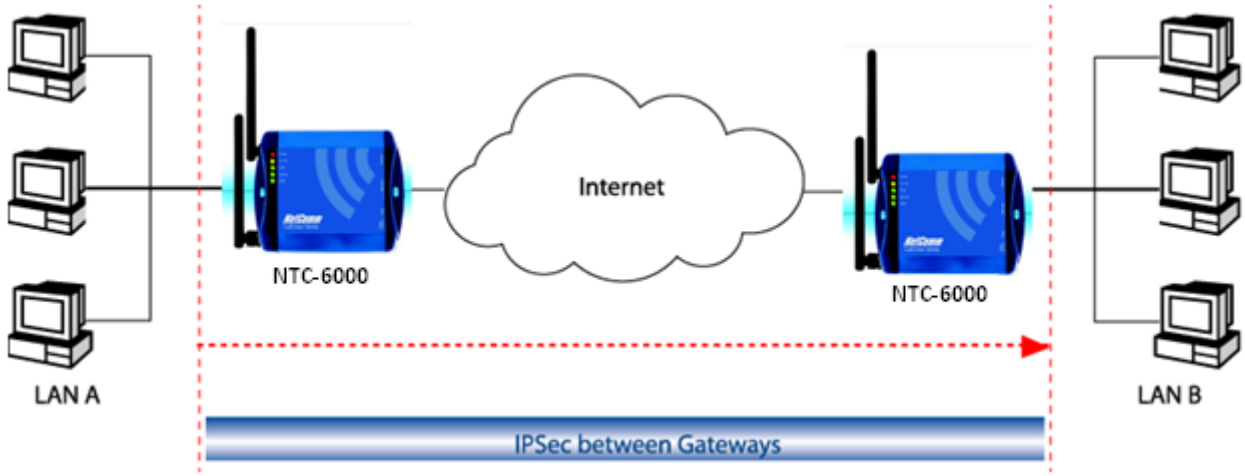


Figure 7 - M2M Series Router to M2M Series Router Site-to-Site Network Diagram and Policy Planning

	Local VPN Router (NTC-6000)		Remote VPN Router (NTC-6000)
LAN IP Address	192.168.20.1		192.168.30.1
WAN IP Address (Telstra IP WAN)	10.1.200.1		10.1.200.2
Ipsec	Enabled		Enabled
Local Secure Group Network Address	192.168.20.0 255.255.255.0		192.168.30.0 255.255.255.0
Remote Secure Group Network Address	192.168.30.0 255.255.255.0		192.168.20.0 255.255.255.0
Ipsec Gateway	10.1.200.2		10.1.200.1
IKE Mode	Main		Main
IKE encryption	AES		AES
IKE Hash	SHA1		SHA1
IKE Rekey Time (sec)	3600		3600
Ipsec Encap 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	myTESTkey		myTESTkey
DPD Action	Restart		
DPD Keep Alive Time (Sec)	10		
DPD Time Out (Sec)	60		

Figure 8 - M2M Series Router to M2M Series Router Site-to-Site Policy Planning Diagram

IPsec VPN Configuration in M2M Series Routers using Pre-Shared Key Mode (Local Router)

Status | Internet Settings | Wireless Settings | Services | System

Internet Settings > VPN > IPSec

VPN IPSec Edit	
Enable This IPSec Profile	(•) Enable ( ) Disable
Profile Name	NTC-6000ToNTC-6000
Remote Gateway	
Remote IPSec Gateway	10.1.200.2 [Road Warrior]
Remote Address/Net to Join	192 . 168 . 30 . 0
Remote Address/Net Mask	255 . 255 . 255 . 0
Local LAN	
Local Address/Net to Join	192 . 168 . 20 . 0
Local Address/Net Mask	255 . 255 . 255 . 0
Negotiation	
Encap Protocol	ESP
IKE Mode	Main
PFS	ON
ike encryption	AES
IKE Hash	SHA1
IPSec Encryption	AES
IPSec Hash	SHA1
DH Group	Group2(1024)
DPD Action	Restart
DPD Keep Alive Time	10 secs
DPD Timeout	60 secs
IKE Rekey Time	3600 (0-78400, 0=Unlimited) secs
SA Life Time	28800 (0-78400, 0=Unlimited) secs
Key Mode	Pre Shared Key
Pre Shared Key	myTESTkey
Remote Id	(xy.sample.com or blank)
Local Id	(xy.sample.com or blank)

[Save] [Exit]

Figure 9: IPsec VPN Configuration in M2M Series Router (Local Router)

IPsec VPN Configuration in M2M Series Routers using Pre-Shared Key Mode (Remote Router)

Status | Internet Settings | Wireless Settings | Services | System

Internet Settings > VPN > IPSec

VPN IPSec Edit	
Enable This IPSec Profile	(•) Enable ( ) Disable
Profile Name	NTC-6000ToNTC-6000
Remote Gateway	
Remote IPSec Gateway	10.1.200.1 [Road Warrior]
Remote Address/Net to Join	192 . 168 . 20 . 0
Remote Address/Net Mask	255 . 255 . 255 . 0
Local LAN	
Local Address/Net to Join	192 . 168 . 30 . 0
Local Address/Net Mask	255 . 255 . 255 . 0
Negotiation	
Encap Protocol	ESP
IKE Mode	Main
PFS	ON
ike encryption	AES
IKE Hash	SHA1
IPSec Encryption	AES
IPSec Hash	SHA1
DH Group	Group2(1024)
DPD Action	Restart
DPD Keep Alive Time	10 secs
DPD Timeout	60 secs
IKE Rekey Time	3600 (0-78400, 0=Unlimited) secs
SA Life Time	28800 (0-78400, 0=Unlimited) secs
Key Mode	Pre Shared Key
Pre Shared Key	myTESTkey
Remote Id	(xy.sample.com or blank)
Local Id	(xy.sample.com or blank)

[Save] [Exit]

Figure 10: IPsec VPN Configuration in M2M Series Router (Remote Router)

Verifying the IPSec VPN Connection Status on M2M Series Routers

Ping the remote M2M Series Router IPSec gateway and its secure group to verify VPN tunnel connectivity. Refer to screen shot shown below.

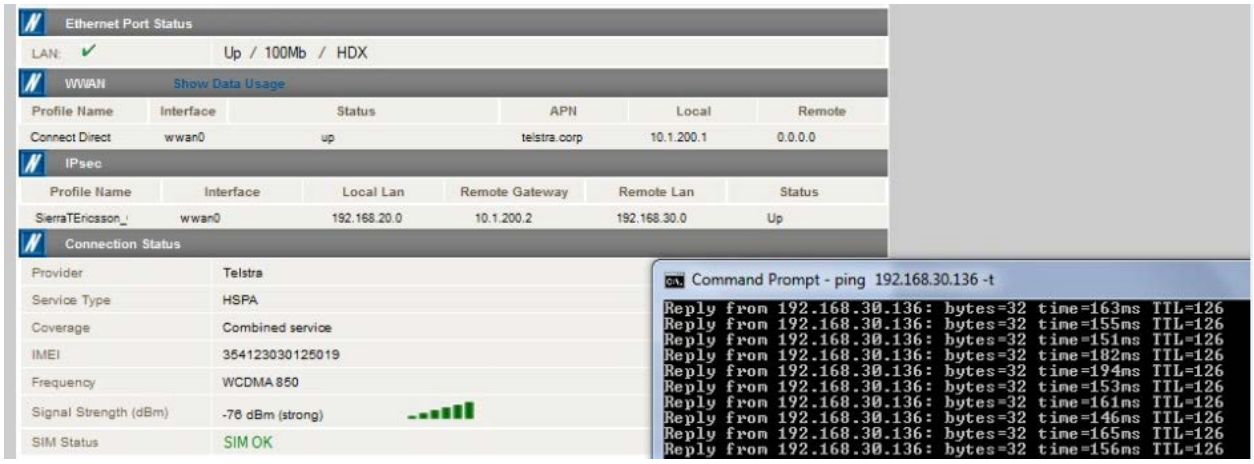


Figure 11: Verifying the IPSec VPN Connection Status

The IPsec VPN tunnel between the two M2M Series Router routers is now up and running.

IPsec Site to Site VPN Tunnel with another M2M Series Router using RSA key mode

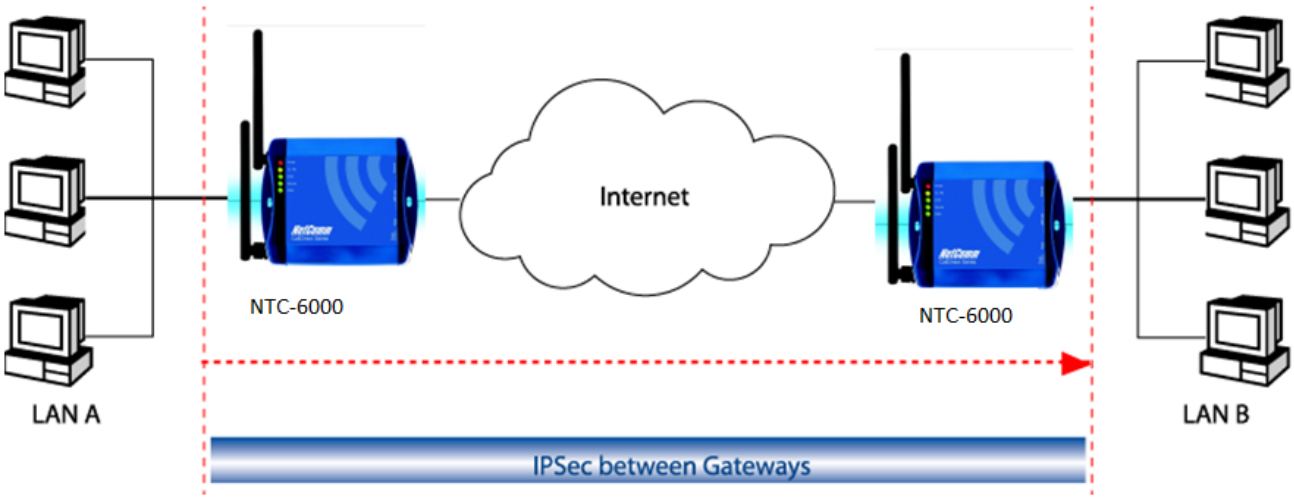


Figure 12 - M2M Series Router to M2M Series Router RSA Key Mode Site-to-Site Network Diagram and Policy Planning

	Local VPN Router (NTC-6000)		Remote VPN Router (NTC-6000)
LAN IP Address	192.168.30.1		192.168.20.1
WAN IP Address (Telstra IP WAN)	10.1.200.1		10.1.200.2
Ipsec	Enabled		Enabled
Local Secure Group Network Address	192.168.30.0 255.255.255.0		192.168.20.0 255.255.255.0
Remote Secure Group Network Address	192.168.20.0 255.255.255.0		192.168.30.0 255.255.255.0
Ipsec Gateway	10.1.200.2		10.1.200.1
IKE Mode	Main		Main
IKE encryption	3DES		3DES
IKE Hash	SHA1		SHA1
IKE Rekey Time (sec)	3600		3600
Ipsec Encap 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 RSA Key Upload	(No need to upload)*		(No need to upload)*
Remote RSA Key Upload	(Upload the peer's RSA key) **		(Upload the peer's RSA key) **
DPD Action	Hold		
DPD Keep Alive Time (Sec)	10		
DPD Time Out (Sec)	60		

Figure 13 - M2M Series Router to M2M Series Router RSA Key Mode Site-to-Site Policy Planning Diagram

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 M2M Series Router cellular router to this router. In other words, a M2M Series 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.

	NTC-6000 Local VPN Router		NTC-6000 Local VPN Router
Local RSA Key file	NTC-6000E_RSA.key		NTC-6000S_RSA.key
Remote RSA key file	NTC-6000S_RSA.key		NTC-6000E_RSA.key

Figure 14: Local and Remote RSA Key Files

IPsec VPN RSA Key Mode Configuration in M2M Series Routers using RSA Key Mode (Local Router)

Status | Internet Settings | Services | System

VPN

VPN Edit	
Profile Type	IPSEC
Enable VPN	Enable Disable
Profile Name	NTC-6000EToNTC-6000SIPsecRS
Remote Gateway	
Remote IPsec Gateway	10.1.200.2 Road Warrior
Remote Address/Net to Join	192 . 168 . 20 . 0
Remote Address/Net Mask	255 . 255 . 255 . 0
Local LAN	
Local Address/Net to Join	192 . 168 . 30 . 0
Local Address/Net Mask	255 . 255 . 255 . 0
Negotiation	
Encap Protocol	Any
IKE Mode	Main
Pfs	On
IKE Encryption	3DES
IKE Hash	SHA1
IPsec Encryption	3DES
IPsec Hash	SHA1
DH Group	Group2(1024)
DPD Action	Hold
DPD Keep Alive Time	10 secs
DPD Timeout	60 secs
Ike Rekey Time	3600 (0-78400, 0=Unlimited) secs
SA Life Time	28800 (0-78400, 0=Unlimited) secs
Key Mode	RSA Keys
Remote Id	(xy.sample.com or blank)
Local Id	(xy.sample.com or blank)
Local RSA Key	Update Time: Sep 19 2011 14:18:00 Generate Download...
Local Rsa Key Upload	Browse... Upload
Remote Rsa Key Upload	C:\Documents and Settings\Administrat Browse... Upload

Save Exit

Figure 15: IPsec VPN RSA Key Mode Configuration in M2M Series Router (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 M2M Series 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 Key Mode Configuration in M2M Series Routers using RSA Key Mode (Remote Router)

VPN Edit		
Profile Type	IPSEC	
Enable VPN	Enable Disable	
Profile Name	NTC-6000SToNTC-6000EIPsecRS	
Remote Gateway		
Remote IPsec Gateway	10 . 1 . 200 . 1	Road Warrior
Remote Address/Net to Join	192 . 168 . 30 . 0	
Remote Address/Net Mask	255 . 255 . 255 . 0	
Local LAN		
Local Address/Net to Join	192 . 168 . 20 . 0	
Local Address/Net Mask	255 . 255 . 255 . 0	
Negotiation		
Encap Protocol	Any	
IKE Mode	Main	
Pfs	On	
IKE Encryption	3DES	
IKE Hash	SHA1	
IPsec Encryption	3DES	
IPsec Hash	SHA1	
DH Group	Group2(1024)	
DPD Action	Hold	
DPD Keep Alive Time	10 secs	
DPD Timeout	60 secs	
Ike Rekey Time	3600 (0-78400, 0=Unlimited) secs	
SA Life Time	28800 (0-78400, 0=Unlimited) secs	
Key Mode	RSA Keys	
Remote Id	(xy.sample.com or blank)	
Local Id	(xy.sample.com or blank)	
Local RSA Key	Update Time Sep 19 2011 14:18:00 Generate Download...	
Local Rsa Key Upload	Browse... Upload	
Remote Rsa Key Upload	/PN Documents\NTC-6000E_RSA.key Browse... Upload	

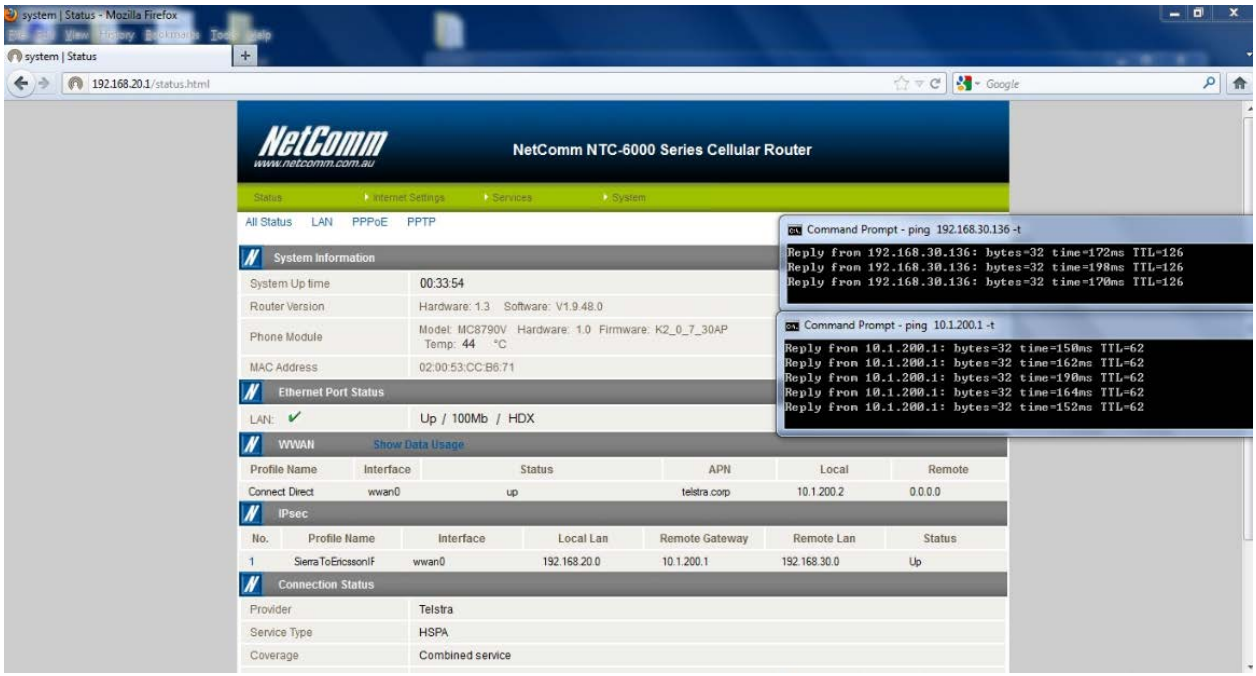
Save Exit

Figure 16: IPsec VPN RSA Key Mode Configuration (Remote Router)

It is important to 'Enable' and 'Save' the IPsec RSA key mode configuration profile before its own RSA key can be generated. This will ensure that the M2M Series 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.

Verifying the IPsec VPN Connection Status on M2M Series Routers

Ping the remote M2M Series Router IPSec gateway and its secure group to verify VPN tunnel connectivity. Refer to screen shot shown below.



The IPsec VPN tunnel between the two M2M Series Router using RSA key mode is now up and running.

IPsec Site to Site VPN Tunnel with another M2M Series Router using Digital Certificate Mode

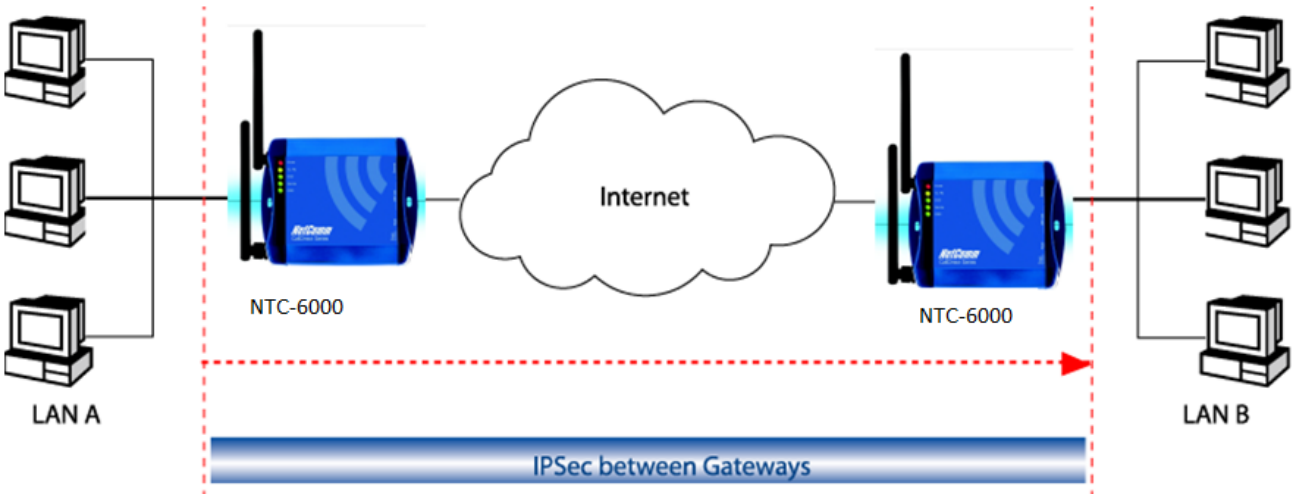


Figure 17 - M2M Series Router to M2M Series Router Digital Certificate Mode Site-to-Site Network Diagram and Policy Planning

	Local VPN Router (NTC-6000)		Remote VPN Router (NTC-6000)
LAN IP Address	192.168.30.1		192.168.20.1
WAN IP Address (Telstra IP WAN)	10.1.200.1		10.1.200.2
Ipsec	Enabled		Enabled
Local Secure Group Network Address	192.168.30.0 255.255.255.0		192.168.20.0 255.255.255.0
Remote Secure Group Network Address	192.168.20.0 255.255.255.0		192.168.30.0 255.255.255.0
Ipsec Gateway	10.1.200.2		10.1.200.1
IKE Mode	Main		Main
IKE encryption	DES		DES
IKE Hash	SHA1		SHA1
IKE Rekey Time (sec)	3600		3600
Ipsec Encap Protocol	ESP		ESP
Ipsec Encryption	DES		DES
Ipsec Hash	SHA1		SHA1
SA Life time (sec)	28800		28800
DH Group	Group 2 (1024)		Group 2 (1024)
PFS	ON		ON
IKE Key Mode	Certificates		Certificates
Private Key Passphrase	NTCNetCommE		NTCNetCommS
Local Private Key	File named: NTC6900EricssonKey.key		File named: NTC6900SierraKey.key
Local Public Certificate	File named: NTC6900EricssonCert.crt		File named: NTC6900SierraCert.crt
Remote Public Certificate	File named: NTC6900SierraCert.crt		File named: NTC6900EricssonCert.crt
CA Certificate	File named: NTCCaCert.crt		File named: NTCCaCert.crt
CRL Certificate	(Blank)		(Blank)
DPD Action	Restart		
DPD Keep Alive Time (Sec)	10		
DPD Time Out (Sec)	60		

Figure 18 - M2M Series Router to M2M Series Router Digital Certificate Mode Site-to-Site Policy Planning Diagram

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 M2M Series Router's system date and time matters as this will affect the validity period of the digital certificate. Therefore it is important to verify the M2M Series Routers have the current date and time.

IPsec VPN Digital Certificate Mode Configuration in M2M Series Routers (Local Router)

VPN Edit	
Profile Type	IPSEC
Enable VPN	(•) Enable ( ) Disable
Profile Name	EricssonToSierralPsecCertificate
Remote Gateway	
Remote IPsec Gateway	10 . 1 . 200 . 2 [Road Warrior]
Remote Address/Net to Join	192 . 168 . 20 . 0
Remote Address/Net Mask	255 . 255 . 255 . 0
Local LAN	
Local Address/Net to Join	192 . 168 . 30 . 0
Local Address/Net Mask	255 . 255 . 255 . 0
Negotiation	
Encap Protocol	Any
IKE Mode	Main
Pfs	On
IKE Encryption	DES
IKE Hash	SHA1
IPsec Encryption	DES
IPsec Hash	SHA1
DH Group	Group2(1024)
DPD Action	Restart
DPD Keep Alive Time	10 secs
DPD Timeout	60 secs
Ike Rekey Time	3600 (0-78400, 0=Unlimited) secs
SA Life Time	28800 (0-78400, 0=Unlimited) secs
Key Mode	Certificates
Private Key Pass Phrase	NTCNetCommE
Key or Certificate 2012-02-27 12:15:36	( ) Local Private Key Uploaded ( ) Local Public Certificate Uploaded ( ) Remote Public Certificate Uploaded ( ) CA Certificate ( ) CRL Certificate
Ipsec Certificate Upload	[Browse...] [Upload]

[Save] [Exit]

Figure 19: IPsec VPN Digital Certificate Mode Configuration in M2M Series Routers (Local Router)

IPsec VPN Digital Certificate Mode Configuration in M2M Series Routers (Remote Router)

VPN Edit		
Profile Type	IPSEC	
Enable VPN	Enable Disable	
Profile Name	SierraToEricssonCertificate	
Remote Gateway		
Remote IPsec Gateway	10 . 1 . 200 . 1	Road Warrior
Remote Address/Net to Join	192 . 168 . 30 . 0	
Remote Address/Net Mask	255 . 255 . 255 . 0	
Local LAN		
Local Address/Net to Join	192 . 168 . 20 . 0	
Local Address/Net Mask	255 . 255 . 255 . 0	
Negotiation		
Encap Protocol	Any	
IKE Mode	Main	
Pfs	On	
IKE Encryption	DES	
IKE Hash	SHA1	
IPsec Encryption	DES	
IPsec Hash	SHA1	
DH Group	Group2(1024)	
DPD Action	Restart	
DPD Keep Alive Time	10	secs
DPD Timeout	60	secs
Ike Rekey Time	3600	(0-78400, 0=Unlimited) secs
SA Life Time	28800	(0-78400, 0=Unlimited) secs
Key Mode	Certificates	
Private Key Pass Phrase	NTCNetCommS	
Key or Certificate 2012-02-27 12:05:17	Local Private Key Local Public Certificate Remote Public Certificate CA Certificate CRL Certificate	Uploaded Uploaded Uploaded
Ipsec Certificate Upload	Browse... Upload	

Save Exit

Figure 20: IPsec VPN Digital Certificate Mode Configuration in M2M Series Router (Remote Router)

Verifying the IPSec VPN Connection Status on M2M Series Routers

Ping the remote M2M Series Router IPsec gateway and its secure group to verify VPN tunnel connectivity. Refer to the screenshot shown below.

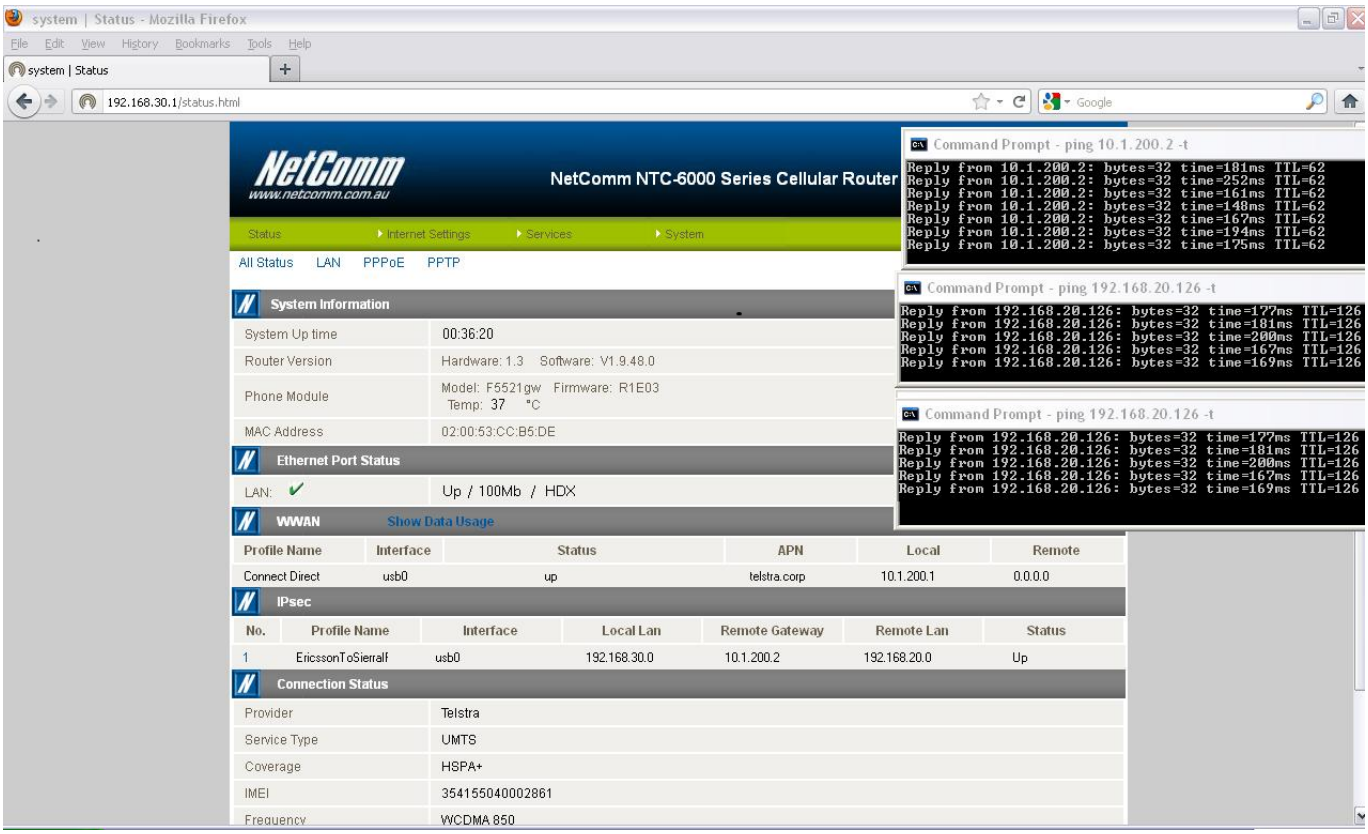


Figure 21: Verifying the IPSec VPN Connection Status on M2M Series Router

The IPsec VPN tunnel between the two M2M Series Router routers using Digital Certificates mode is now up and running.