NetCommWireless

IPSec VPN
Technical Support Guide

⚠ **Please note:** This document is subject to change without notice.

DOCUMENT VERSION	DATE
1.0 - Initial draft	19 August 2015

Table 1 - Document Revision History

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.

NetComm Wireless M2M routers support three types of Virtual Private Network (VPN) technologies:

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

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. NetComm Wireless M2M routers support IPsec end points and can be configured with Site to Site VPN tunnels with other NetComm Wireless M2M routers or third party VPN routers. Further configuration instructions for IPsec VPN tunnels on the M2M Series Router are provided in this document.

Applicable devices

This document is applicable to the following NetComm Wireless devices:

- NTC-6908
- NTC-6908-02
- NTC-6520
- NTC-6200
- NTC-30WV
- NTC-30WV-02
- NTC-40WV
- NTC-140W
- NWL-11
- NWL-15
- NWL-25

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.

i. Remote peer IP or hostname

ii. 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).

iii. Encryption Algorithm for confidentiality: DES, 3DES or AES, AES 128, 192, 256 bit key strength. AES is the strongest protocol.

iv. Hashing Algorithm for Data Integrity and authentication: SHA1 or MD5. SHA1 is the stronger authentication algorithm.

v. 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.

vi. 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.

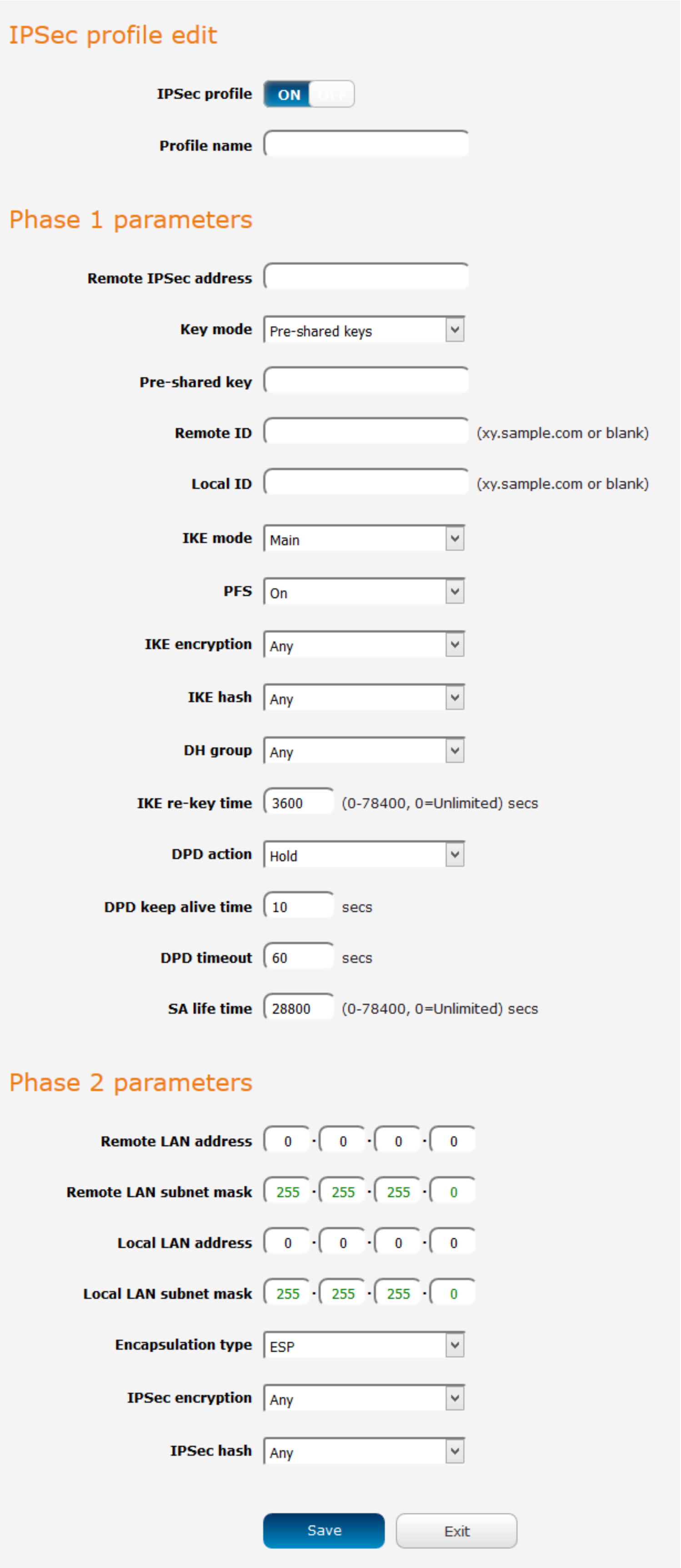
1. Transform set: This includes the encapsulation negotiation protocol to be used, either selecting Authentication Header (AH) or Encryption Security Payload (ESP). The Authentication Header only provides authentication and data integrity. The Encryption Security Payload provides authentication, data 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 router IPsec VPN web interface

On NetComm Wireless M2M routers, both the IKE phase 1 and phase 2 parameters are shown in one single configuration page (Figure 1). It can be found by selecting the **Networking** menu, then **VPN** and **IPSec**.



IPSec profile edit

IPSec profile	ON
Profile name	

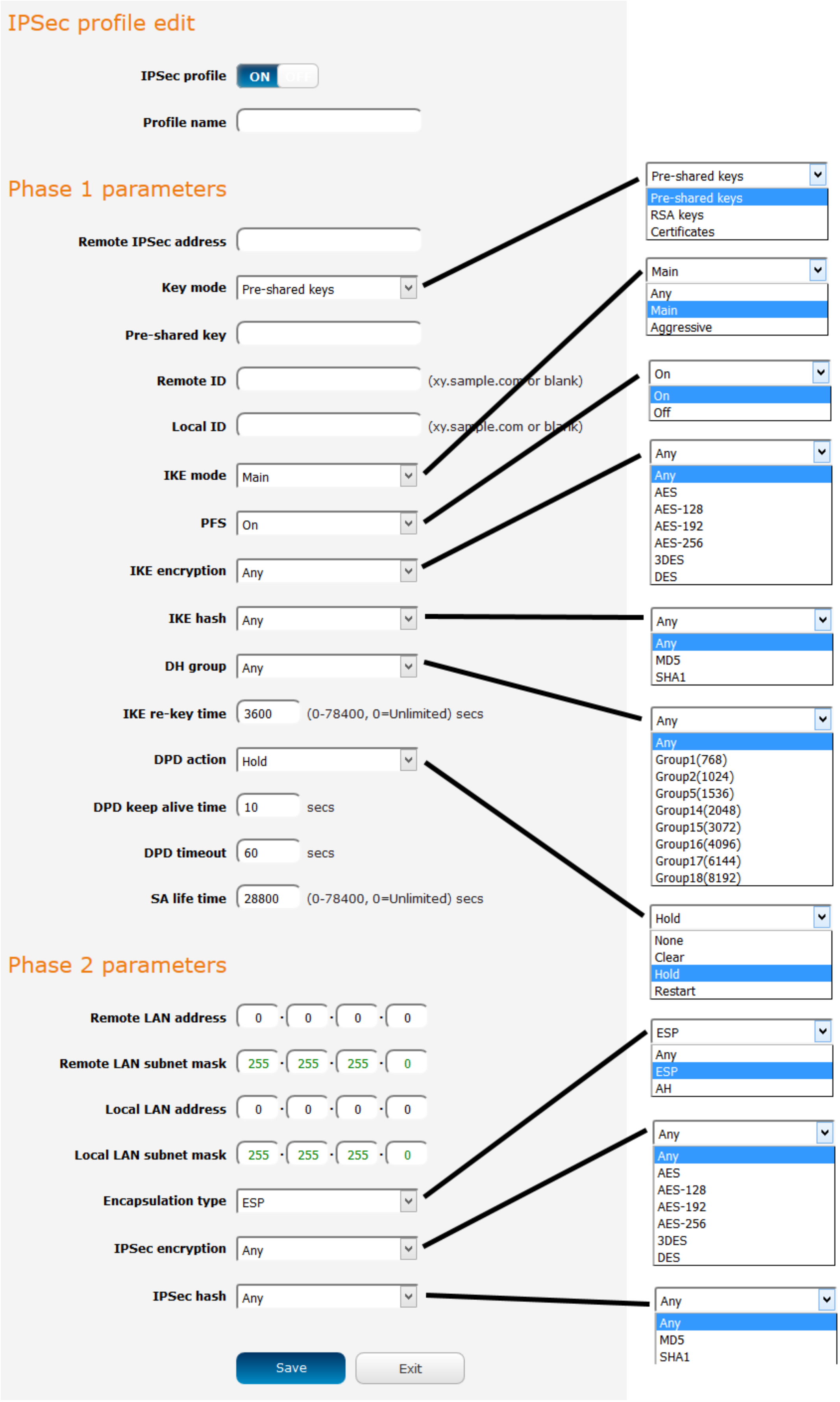
Phase 1 parameters

Remote IPSec address	
Key mode	Pre-shared keys
Pre-shared key	
Remote ID	(xy.sample.com or blank)
Local ID	(xy.sample.com or blank)
IKE mode	Main
PFS	On
IKE encryption	Any
IKE hash	Any
DH group	Any
IKE re-key time	3600 (0-78400, 0=Unlimited) secs
DPD action	Hold
DPD keep alive time	10 secs
DPD timeout	60 secs
SA life time	28800 (0-78400, 0=Unlimited) secs

Phase 2 parameters

Remote LAN address	0 . 0 . 0 . 0
Remote LAN subnet mask	255 . 255 . 255 . 0
Local LAN address	0 . 0 . 0 . 0
Local LAN subnet mask	255 . 255 . 255 . 0
Encapsulation type	ESP
IPSec encryption	Any
IPSec hash	Any

Figure 1 - IPSec configuration page



IPSec profile edit

IPSec profile: ON

Profile name:

Phase 1 parameters

Remote IPSec address:

Key mode: Pre-shared keys

Pre-shared key:

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

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

IKE mode: Main

PFS: On

IKE encryption: Any

IKE hash: Any

DH group: Any

IKE re-key time: 3600 (0-78400, 0=Unlimited) secs

DPD action: Hold

DPD keep alive time: 10 secs

DPD timeout: 60 secs

SA life time: 28800 (0-78400, 0=Unlimited) secs

Phase 2 parameters

Remote LAN address: 0 . 0 . 0 . 0

Remote LAN subnet mask: 255 . 255 . 255 . 0

Local LAN address: 0 . 0 . 0 . 0

Local LAN subnet mask: 255 . 255 . 255 . 0

Encapsulation type: ESP

IPSec encryption: Any

IPSec hash: Any

Figure 2 - Negotiation parameters for IPSec configuration

Dead peer detection mechanism

NetComm Wireless M2M routers support 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

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

NetComm Wireless M2M routers support 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

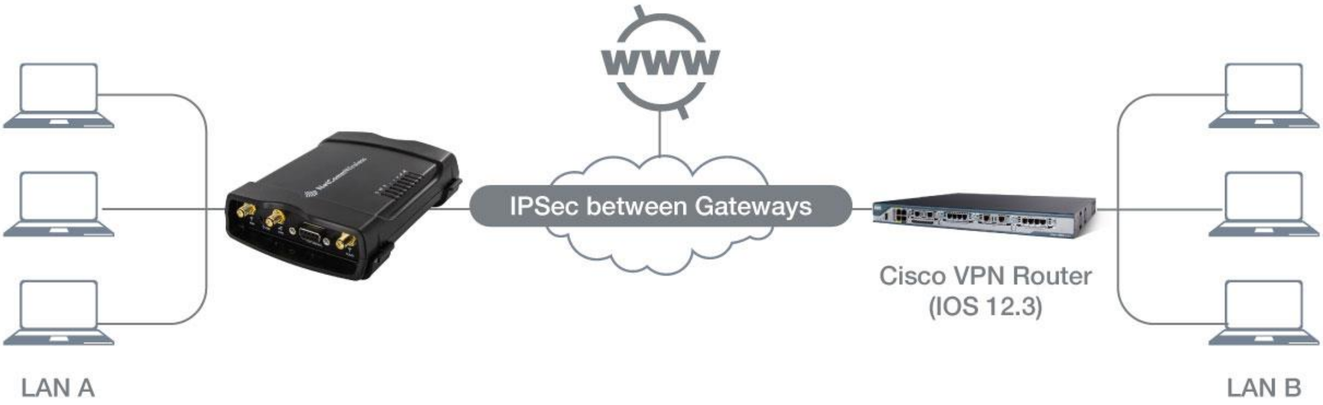
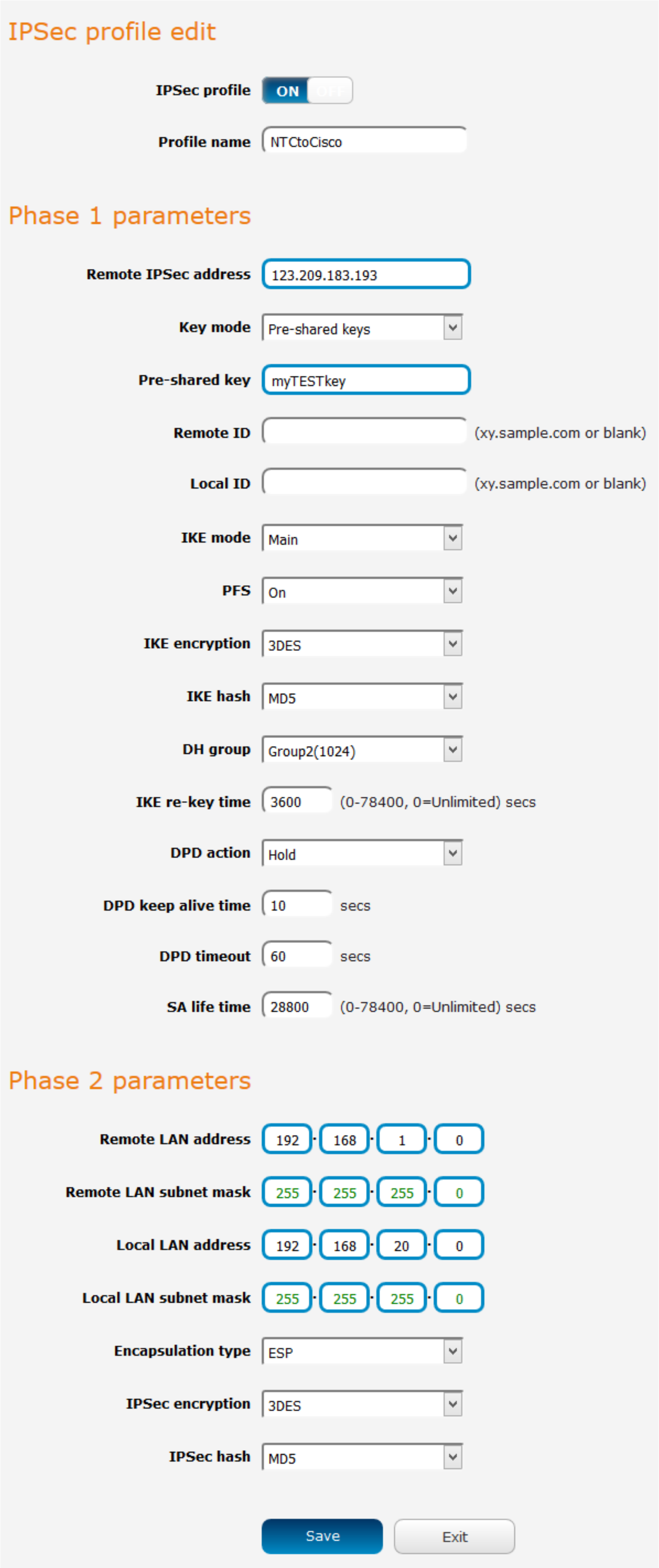


Figure 3 – M2M router to Cisco VPN router Site-to-Site network diagram and policy planning

	LOCAL VPN ROUTER	REMOTE VPN ROUTER (CISCO VPN ROUTER RUNNING IOS 12.3)
LAN IP Address	192.168.20.1	192.168.1.80
WAN IP Address	123.209.32.180	123.209.183.193
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	123.209.183.193	123.209.32.180
IKE Mode	Main	Main
IKE Encryption	3DES	3DES
IKE Hash	MD5	MD5
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	Group2(1024)	Group2(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 router to Cisco VPN router Site-to-Site policy planning diagram



IPSec profile edit

IPSec profile	ON
Profile name	NTCtoCisco

Phase 1 parameters

Remote IPSec address	123.209.183.193
Key mode	Pre-shared keys
Pre-shared key	myTESTkey
Remote ID	(xy.sample.com or blank)
Local ID	(xy.sample.com or blank)
IKE mode	Main
PFS	On
IKE encryption	3DES
IKE hash	MD5
DH group	Group2(1024)
IKE re-key time	3600 (0-78400, 0=Unlimited) secs
DPD action	Hold
DPD keep alive time	10 secs
DPD timeout	60 secs
SA life time	28800 (0-78400, 0=Unlimited) secs

Phase 2 parameters

Remote LAN address	192 . 168 . 1 . 0
Remote LAN subnet mask	255 . 255 . 255 . 0
Local LAN address	192 . 168 . 20 . 0
Local LAN subnet mask	255 . 255 . 255 . 0
Encapsulation type	ESP
IPSec encryption	3DES
IPSec hash	MD5

Figure 5: IPsec Example VPN configuration on a NetComm Wireless M2M router

IPsec VPN configuration on a Cisco router running IOS 12.3

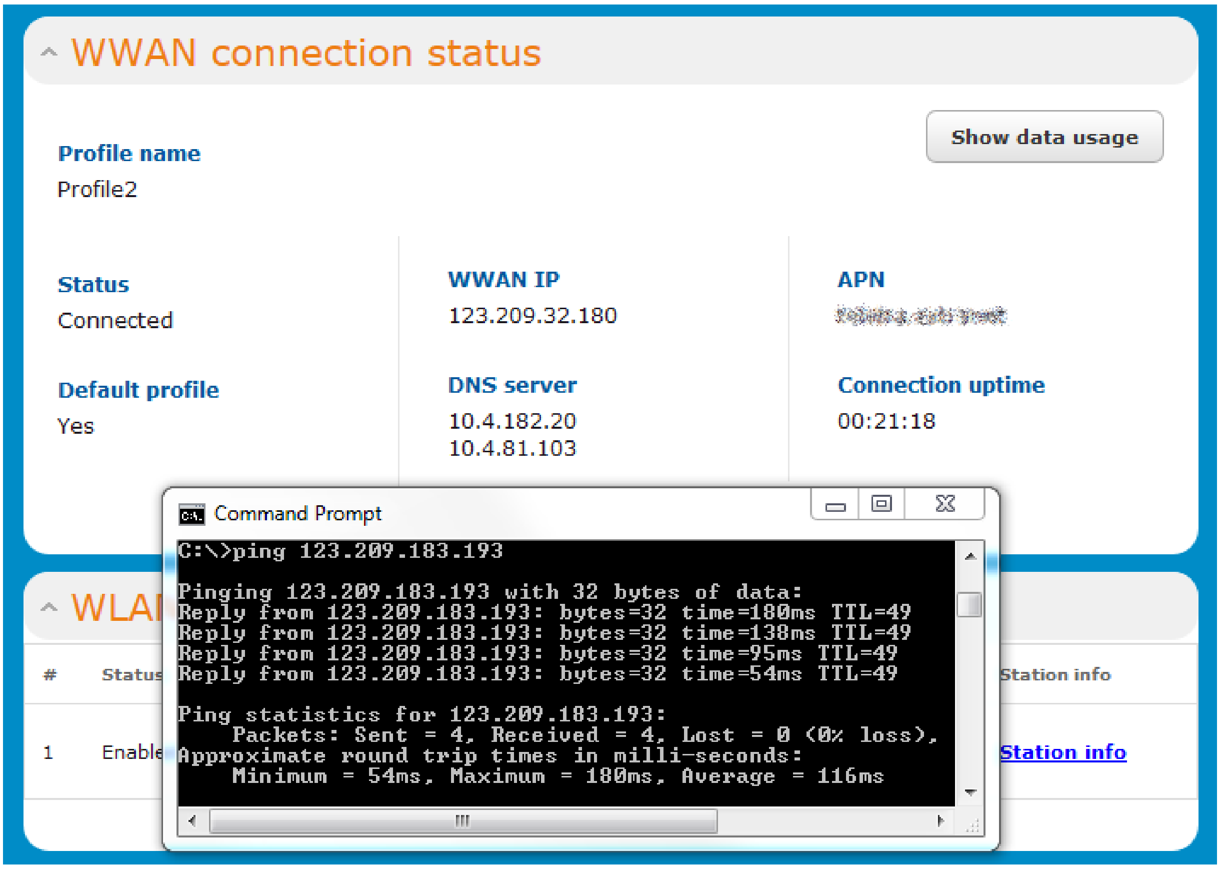
NB: This configuration is provided as an example only. NetComm Wireless does not offer further assistance with Cisco configuration.

```
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

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



Profile name
Profile2

Status
Connected

Default profile
Yes

WWAN IP
123.209.32.180

DNS server
10.4.182.20
10.4.81.103

APN
[redacted]

Connection uptime
00:21:18

#	Status	Station info
1	Enable	Station info

```
C:\>ping 123.209.183.193

Pinging 123.209.183.193 with 32 bytes of data:
Reply from 123.209.183.193: bytes=32 time=180ms TTL=49
Reply from 123.209.183.193: bytes=32 time=138ms TTL=49
Reply from 123.209.183.193: bytes=32 time=95ms TTL=49
Reply from 123.209.183.193: bytes=32 time=54ms TTL=49

Ping statistics for 123.209.183.193:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 180ms, Average = 116ms
```

Figure 6: Testing the IPsec VPN connection status

The IPsec VPN tunnel between the NetComm Wireless router and the Cisco router is now up and running.

IPsec Site to Site VPN tunnel between two NetComm Wireless routers using Pre-shared key mode

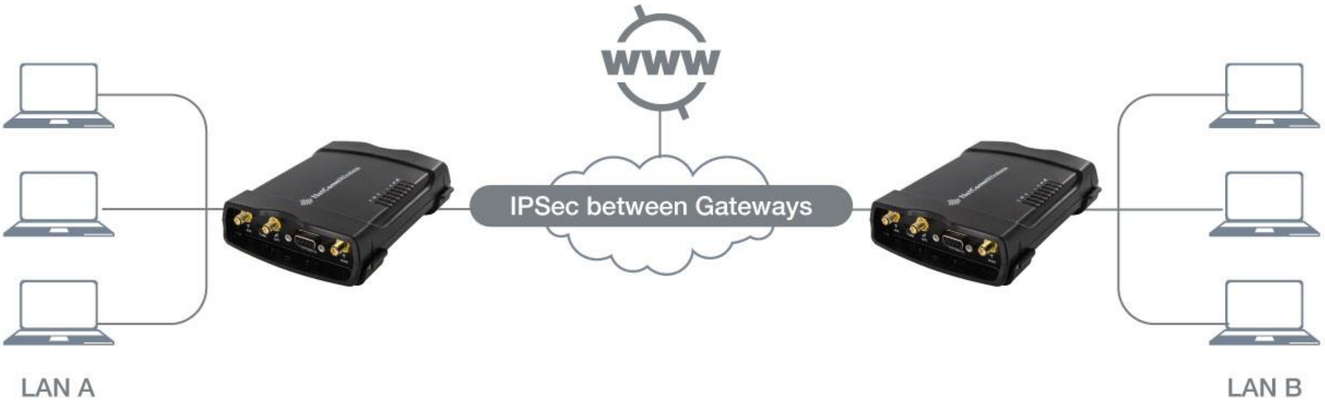
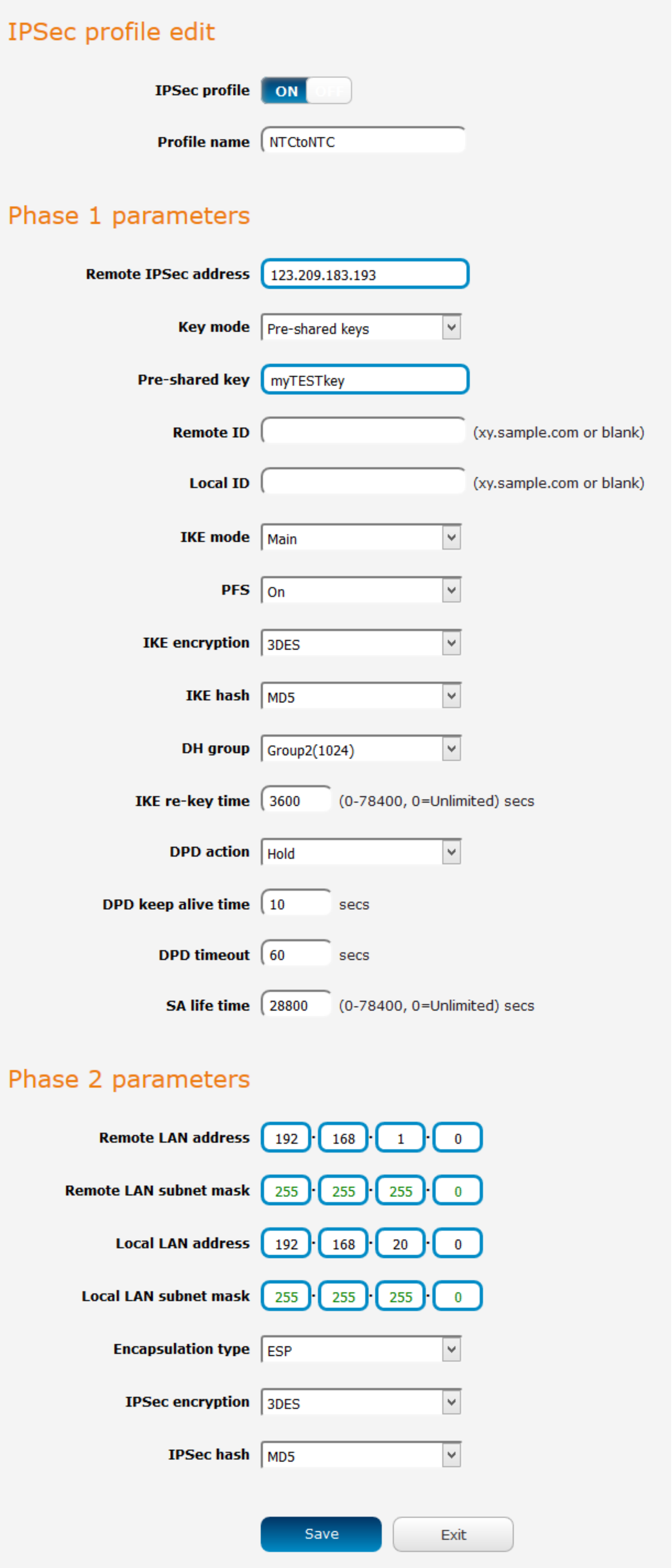


Figure 7 - IPsec Site to Site VPN tunnel between two NetComm Wireless routers network diagram and policy planning

	LOCAL VPN ROUTER	REMOTE VPN ROUTER
LAN IP Address	192.168.20.1	192.168.1.80
WAN IP Address	123.209.32.180	123.209.183.193
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	123.209.183.193	123.209.32.180
IKE Mode	Main	Main
IKE Encryption	3DES	3DES
IKE Hash	MD5	MD5
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	Group2(1024)	Group2(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 8 - IPsec Site to Site VPN tunnel between two NetComm Wireless routers policy planning diagram

IPsec VPN configuration on NetComm Wireless M2M routers using Pre-shared key mode (Local router)



IPSec profile edit

IPSec profile	ON
Profile name	NTCtoNTC

Phase 1 parameters

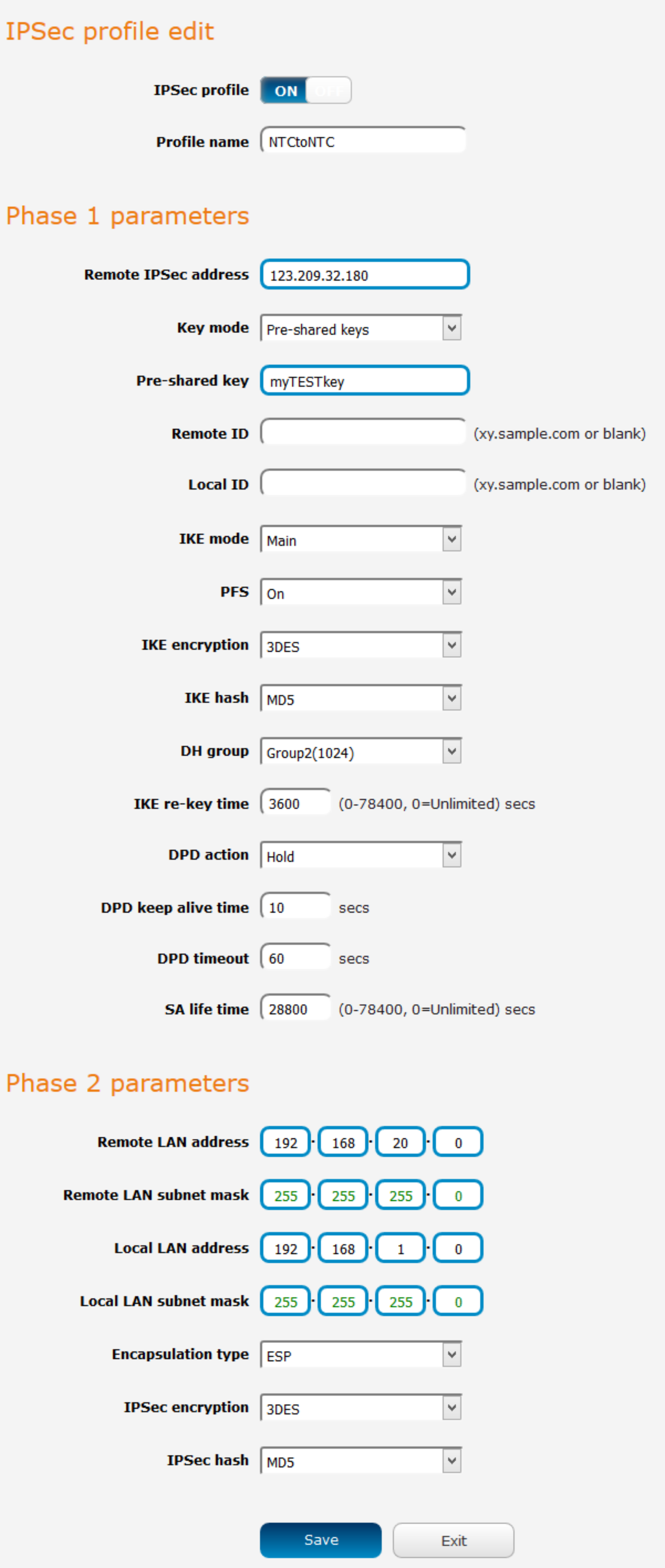
Remote IPSec address	123.209.183.193
Key mode	Pre-shared keys
Pre-shared key	myTESTkey
Remote ID	(xy.sample.com or blank)
Local ID	(xy.sample.com or blank)
IKE mode	Main
PFS	On
IKE encryption	3DES
IKE hash	MD5
DH group	Group2(1024)
IKE re-key time	3600 (0-78400, 0=Unlimited) secs
DPD action	Hold
DPD keep alive time	10 secs
DPD timeout	60 secs
SA life time	28800 (0-78400, 0=Unlimited) secs

Phase 2 parameters

Remote LAN address	192 . 168 . 1 . 0
Remote LAN subnet mask	255 . 255 . 255 . 0
Local LAN address	192 . 168 . 20 . 0
Local LAN subnet mask	255 . 255 . 255 . 0
Encapsulation type	ESP
IPSec encryption	3DES
IPSec hash	MD5

Figure 9: IPsec VPN configuration on Local router

IPsec VPN configuration on NetComm Wireless M2M routers using Pre-shared key mode (Remote router)



IPSec profile edit

IPSec profile	ON
Profile name	NTCtoNTC

Phase 1 parameters

Remote IPSec address	123.209.32.180
Key mode	Pre-shared keys
Pre-shared key	myTESTkey
Remote ID	(xy.sample.com or blank)
Local ID	(xy.sample.com or blank)
IKE mode	Main
PFS	On
IKE encryption	3DES
IKE hash	MD5
DH group	Group2(1024)
IKE re-key time	3600 (0-78400, 0=Unlimited) secs
DPD action	Hold
DPD keep alive time	10 secs
DPD timeout	60 secs
SA life time	28800 (0-78400, 0=Unlimited) secs

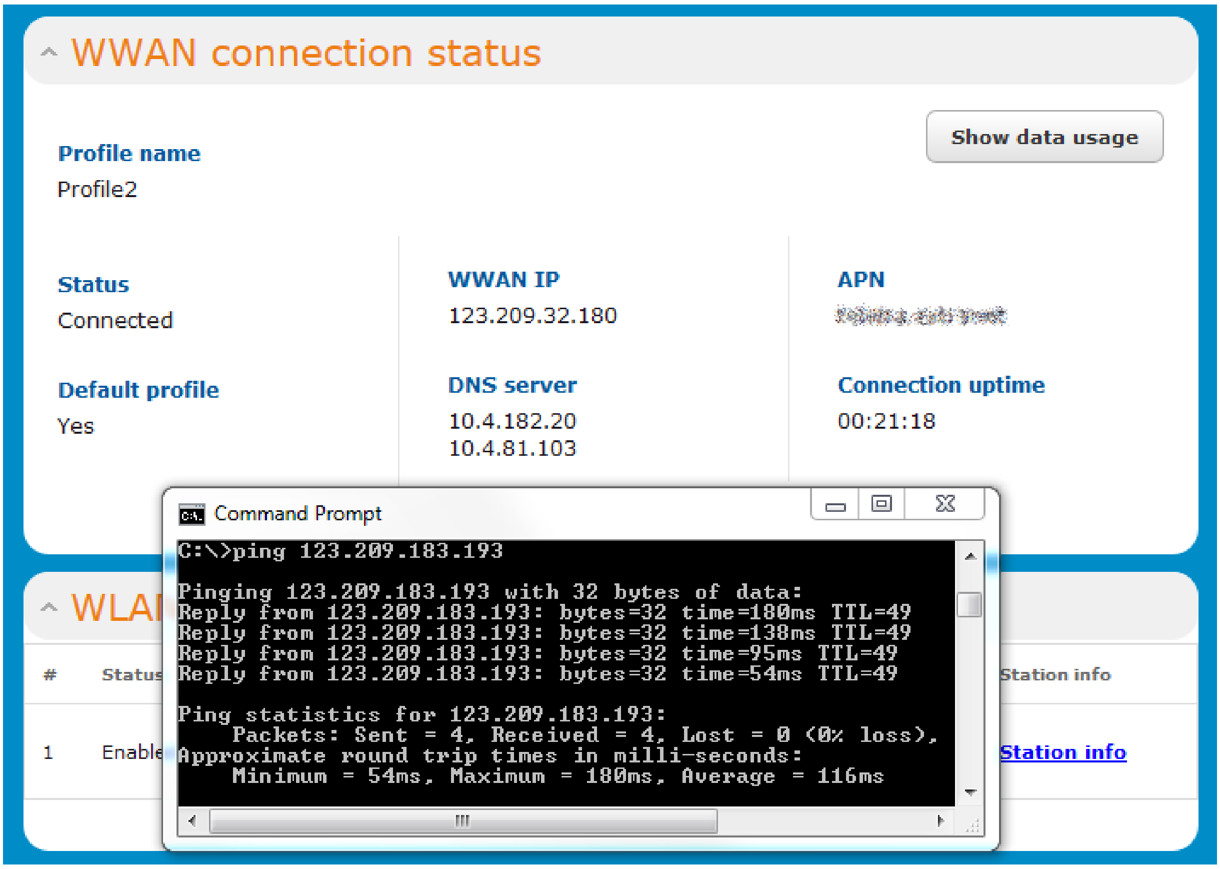
Phase 2 parameters

Remote LAN address	192 . 168 . 20 . 0
Remote LAN subnet mask	255 . 255 . 255 . 0
Local LAN address	192 . 168 . 1 . 0
Local LAN subnet mask	255 . 255 . 255 . 0
Encapsulation type	ESP
IPSec encryption	3DES
IPSec hash	MD5

Figure 10: IPsec VPN configuration on Remote router

Verifying the IPSec VPN Connection Status on M2M Series Routers

Ping the remote router IPSec gateway to verify VPN tunnel connectivity. Refer to screen shot shown below.



WWAN connection status

Profile name
Profile2

Status
Connected

WWAN IP
123.209.32.180

APN
[redacted]

Default profile
Yes

DNS server
10.4.182.20
10.4.81.103

Connection uptime
00:21:18

```
C:\>ping 123.209.183.193

Pinging 123.209.183.193 with 32 bytes of data:
Reply from 123.209.183.193: bytes=32 time=180ms TTL=49
Reply from 123.209.183.193: bytes=32 time=138ms TTL=49
Reply from 123.209.183.193: bytes=32 time=95ms TTL=49
Reply from 123.209.183.193: bytes=32 time=54ms TTL=49

Ping statistics for 123.209.183.193:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 180ms, Average = 116ms
```

Figure 11: Verifying the IPSec VPN connection status

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

IPsec Site to Site VPN tunnel between two NetComm Wireless routers using RSA key mode

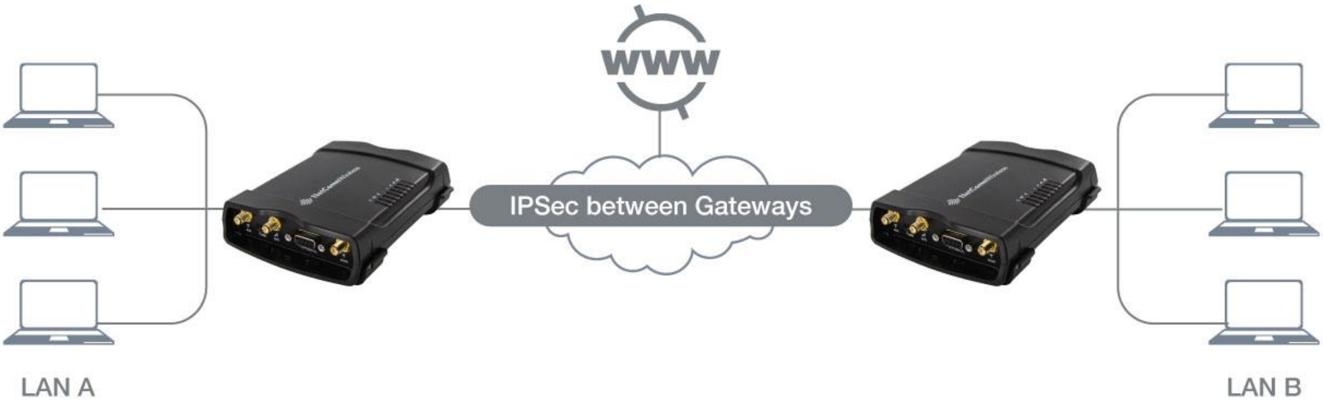


Figure 12 - IPsec Site to Site VPN tunnel between two NetComm Wireless routers using RSA key mode network diagram and policy planning

	LOCAL VPN ROUTER	REMOTE VPN ROUTER
LAN IP Address	192.168.20.1	192.168.1.80
WAN IP Address	123.209.32.180	123.209.183.193
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	123.209.183.193	123.209.32.180
IKE Mode	Main	Main
IKE Encryption	3DES	3DES
IKE Hash	MD5	MD5
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	Group2(1024)	Group2(1024)
PFS	ON	ON
IKE Key Mode	RSA keys	RSA keys
Local RSA Key Upload	Not required	Not required
Remote RSA Key Upload	Upload peer’s RSA key	Upload peer’s RSA key
DPD Action	Hold	
DPD Keep Alive Time (sec)	10	
DPD Time Out (sec)	60	

Figure 13 - IPsec Site to Site VPN tunnel between two NetComm Wireless routers using RSA key mode 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.

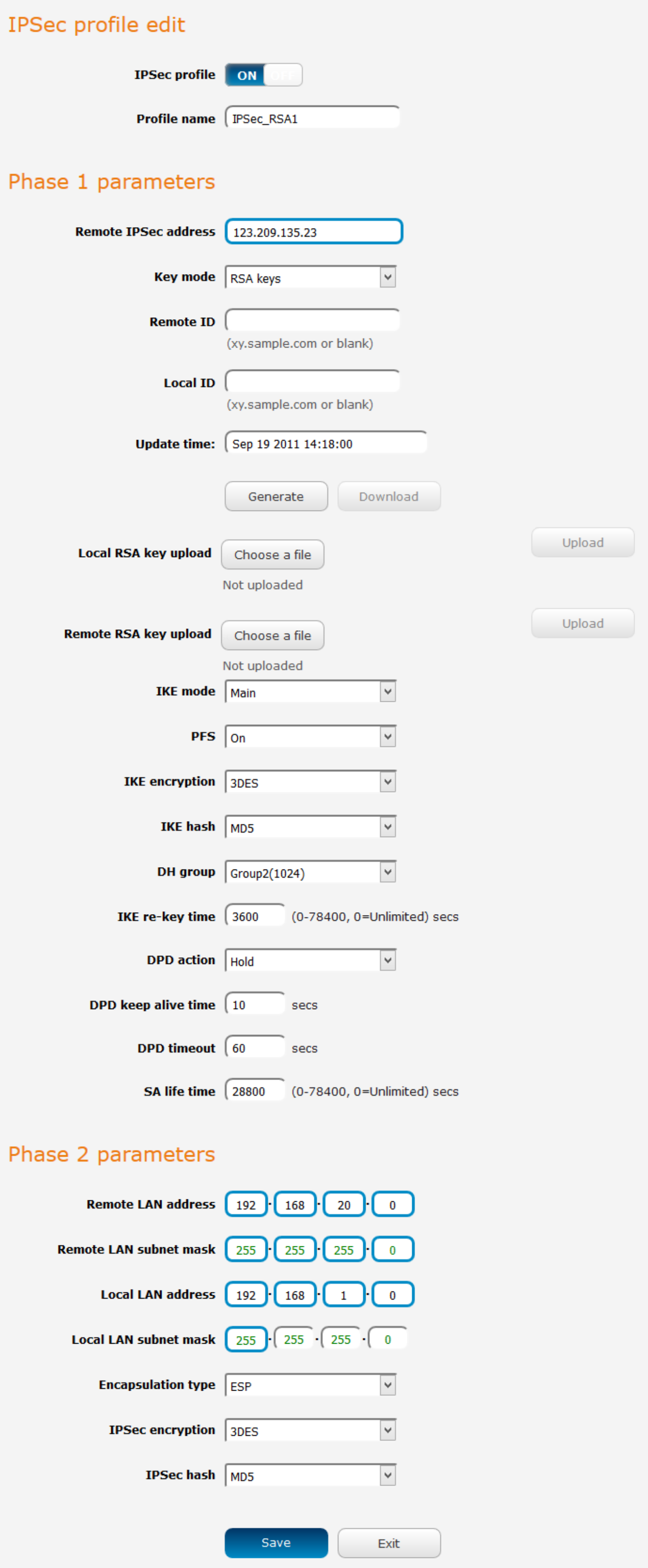
** “Remote RSA Key” refers to the peer’s RSA key in .key format. It is the RSA key file where you downloaded, saved and transferred from its peer M2M Series Router cellular router to this router. In other words, a M2M Series Router’s local RSA key is the remote RSA key for its peer VPN router.

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

	LOCAL VPN ROUTER	REMOTE VPN ROUTER
Local RSA Key file	left_rsa.key	right_rsa.key
Remote RSA Key file	right_rsa.key	left_rsa.key

Figure 14: Local and remote RSA key files

IPsec VPN RSA key mode configuration using RSA key mode (Local router)



IPSec profile edit

IPSec profile	ON
Profile name	IPSec_RSA1

Phase 1 parameters

Remote IPSec address	123.209.135.23
Key mode	RSA keys
Remote ID	(xy.sample.com or blank)
Local ID	(xy.sample.com or blank)
Update time:	Sep 19 2011 14:18:00
	Generate Download
Local RSA key upload	Choose a file Upload Not uploaded
Remote RSA key upload	Choose a file Upload Not uploaded
IKE mode	Main
PFS	On
IKE encryption	3DES
IKE hash	MD5
DH group	Group2(1024)
IKE re-key time	3600 (0-78400, 0=Unlimited) secs
DPD action	Hold
DPD keep alive time	10 secs
DPD timeout	60 secs
SA life time	28800 (0-78400, 0=Unlimited) secs

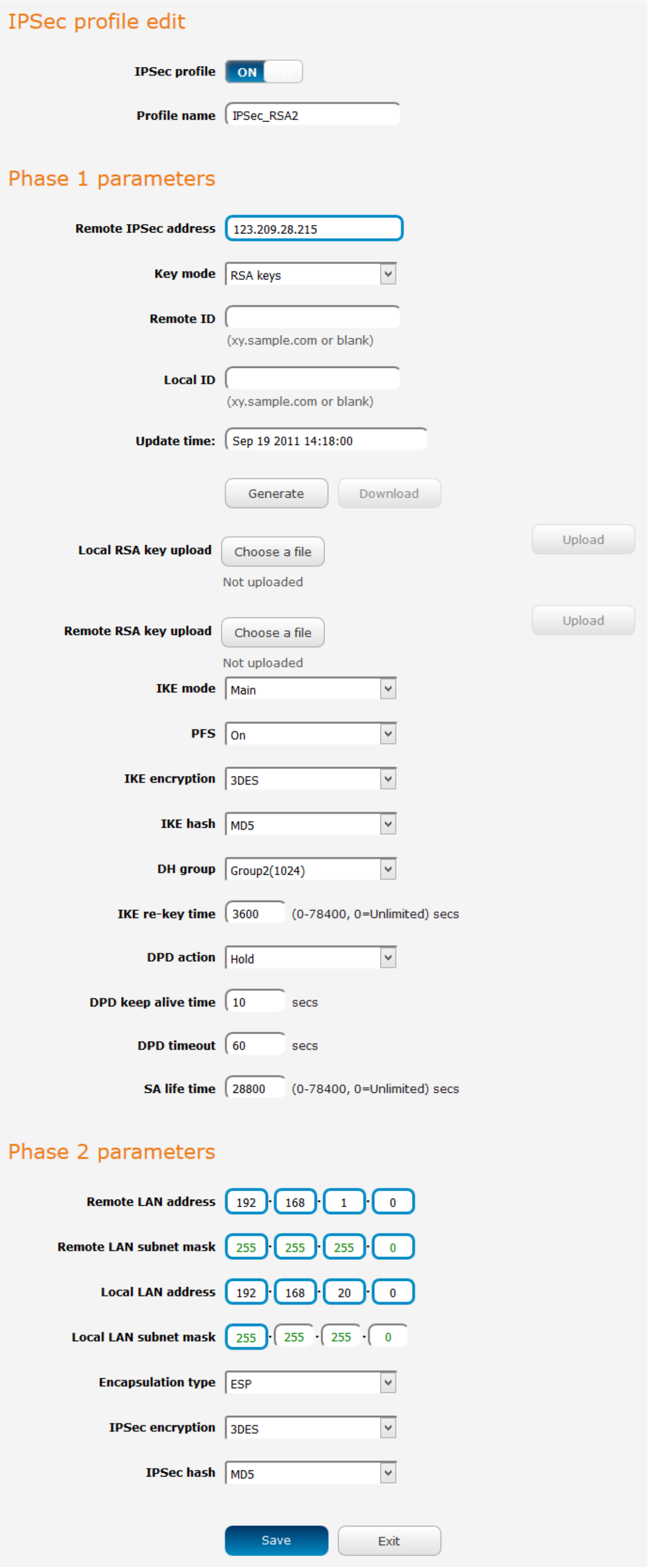
Phase 2 parameters

Remote LAN address	192 . 168 . 20 . 0
Remote LAN subnet mask	255 . 255 . 255 . 0
Local LAN address	192 . 168 . 1 . 0
Local LAN subnet mask	255 . 255 . 255 . 0
Encapsulation type	ESP
IPSec encryption	3DES
IPSec hash	MD5

Figure 15: IPsec VPN RSA key mode configuration on 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 using RSA key mode (Remote router)



IPSec profile edit

IPSec profile	ON
Profile name	IPSec_RSA2

Phase 1 parameters

Remote IPSec address	123.209.28.215
Key mode	RSA keys
Remote ID	(xy.sample.com or blank)
Local ID	(xy.sample.com or blank)
Update time:	Sep 19 2011 14:18:00
Local RSA key upload	Not uploaded
Remote RSA key upload	Not uploaded
IKE mode	Main
PFS	On
IKE encryption	3DES
IKE hash	MD5
DH group	Group2(1024)
IKE re-key time	3600 (0-78400, 0=Unlimited) secs
DPD action	Hold
DPD keep alive time	10 secs
DPD timeout	60 secs
SA life time	28800 (0-78400, 0=Unlimited) secs

Phase 2 parameters

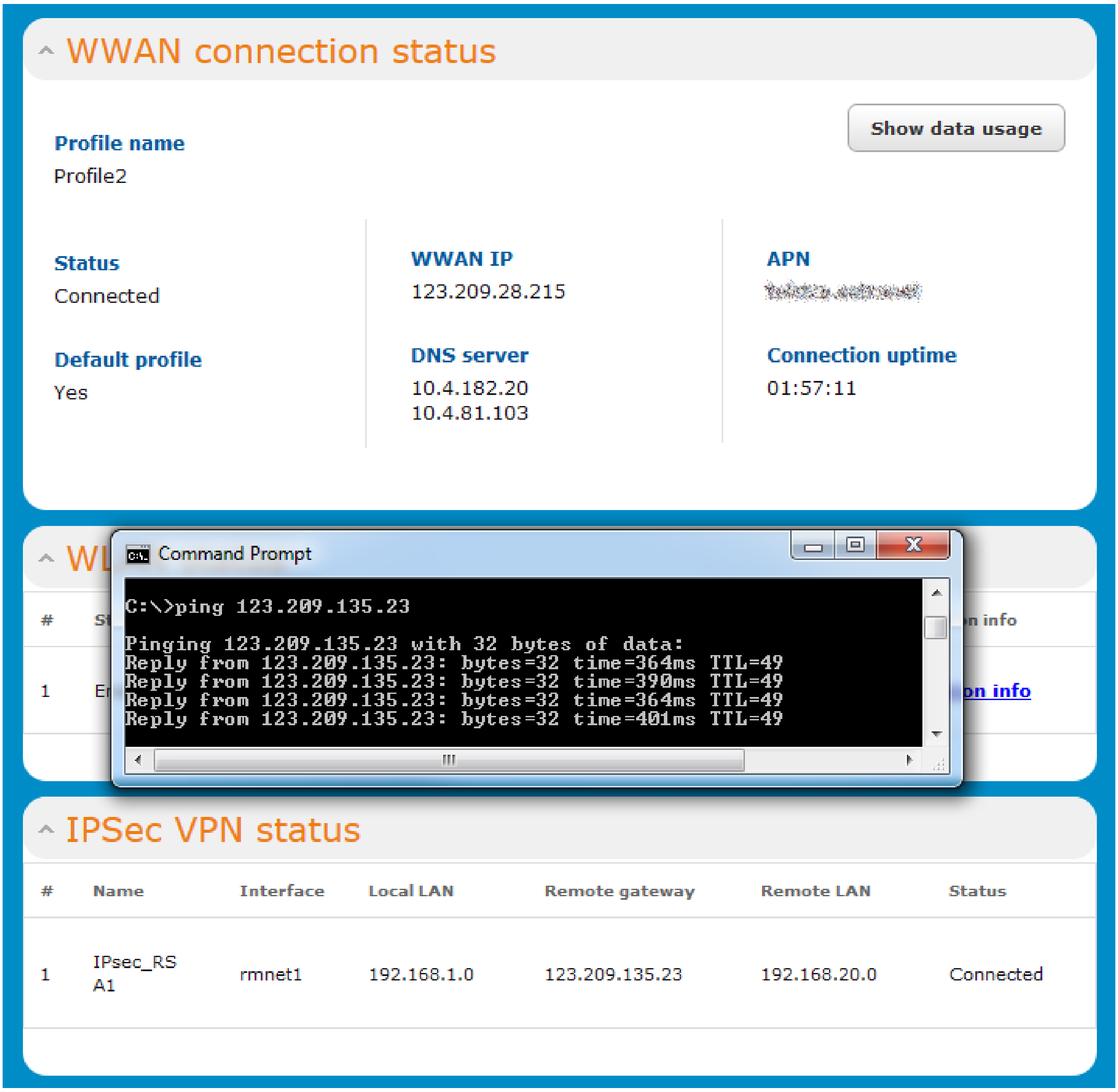
Remote LAN address	192 . 168 . 1 . 0
Remote LAN subnet mask	255 . 255 . 255 . 0
Local LAN address	192 . 168 . 20 . 0
Local LAN subnet mask	255 . 255 . 255 . 0
Encapsulation type	ESP
IPSec encryption	3DES
IPSec hash	MD5

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

Ping the remote gateway to verify VPN tunnel connectivity. Refer to screen shot shown below.



WWAN connection status

Profile name
Profile2

Status
Connected

Default profile
Yes

WWAN IP
123.209.28.215

DNS server
10.4.182.20
10.4.81.103

APN
[redacted]

Connection uptime
01:57:11

```
C:\>ping 123.209.135.23

Pinging 123.209.135.23 with 32 bytes of data:
Reply from 123.209.135.23: bytes=32 time=364ms TTL=49
Reply from 123.209.135.23: bytes=32 time=390ms TTL=49
Reply from 123.209.135.23: bytes=32 time=364ms TTL=49
Reply from 123.209.135.23: bytes=32 time=401ms TTL=49
```

IPSec VPN status

#	Name	Interface	Local LAN	Remote gateway	Remote LAN	Status
1	IPsec_RSA1	rmnet1	192.168.1.0	123.209.135.23	192.168.20.0	Connected

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 between two NetComm Wireless routers using Digital Certificate mode

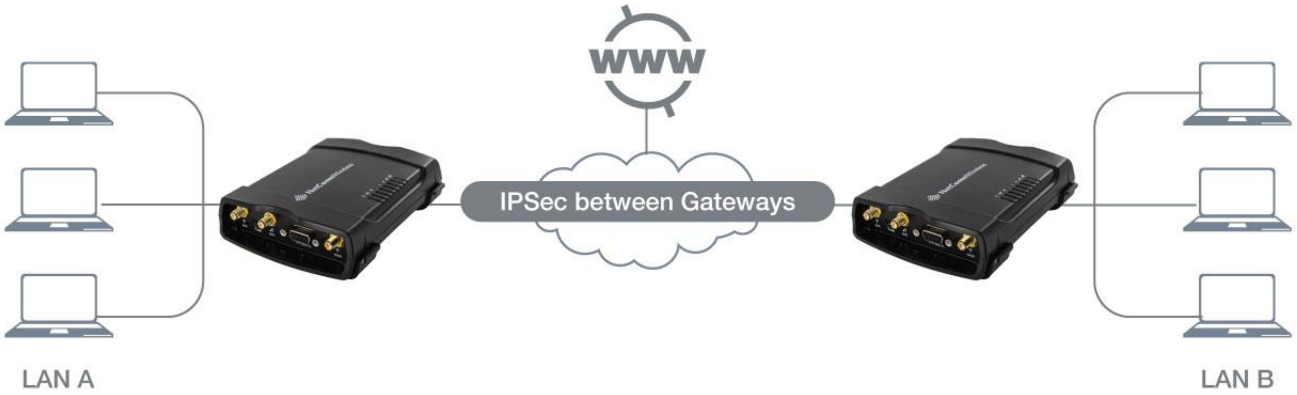


Figure 17 - IPsec Site to Site VPN tunnel between two NetComm Wireless routers using Digital Certificate mode network diagram and policy planning

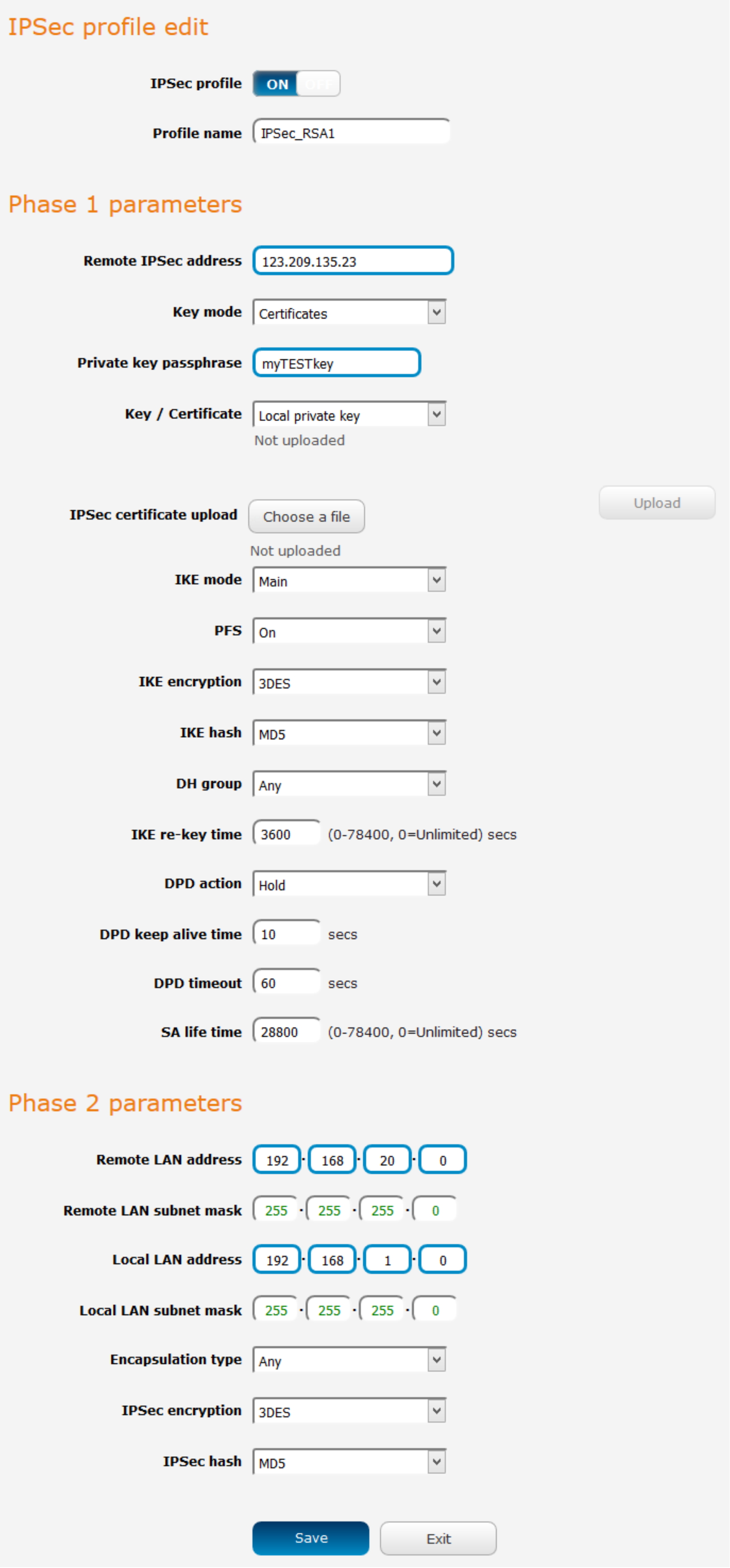
	LOCAL VPN ROUTER	REMOTE VPN ROUTER
LAN IP Address	192.168.20.1	192.168.1.80
WAN IP Address	123.209.32.180	123.209.183.193
IPsec	Enabled	Enabled
Local Secure Group Network Address	192.168.20.0 255.255.255.0	192.168.1.0 255.255.255.0
Remote Secure Group Network Address	192.168.1.0 255.255.255.0	192.168.20.0 255.255.255.0
IPsec Gateway	123.209.183.193	123.209.32.180
IKE Mode	Main	Main
IKE Encryption	3DES	3DES
IKE Hash	MD5	MD5
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	Group2(1024)	Group2(1024)
PFS	ON	ON
IKE Key Mode	Certificates	Certificates
Private Key Passphrase	myTESTkey	myTESTkey
Local Private Key	client1.key	client2.key
Local Public Certificate	client1.crt	client2.crt
Remote Public Certificate	client2.crt	client1.key
CA Certificate	ca.key	ca.key
CRL Certificate	*Blank*	*Blank*
DPD Action	Hold	
DPD Keep Alive Time (sec)	10	
DPD Time Out (sec)	60	

Figure 18 - IPsec Site to Site VPN tunnel between two NetComm Wireless routers using Digital Certificate mode network diagram and policy planning

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 NetComm Wireless M2M 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 routers have the current date and time.

IPsec VPN Digital Certificate mode configuration (Local router)



IPSec profile edit

IPSec profile: ON

Profile name: IPSec_RSA1

Phase 1 parameters

Remote IPSec address: 123.209.135.23

Key mode: Certificates

Private key passphrase: myTESTkey

Key / Certificate: Local private key
Not uploaded

IPSec certificate upload: Choose a file
Not uploaded

IKE mode: Main

PFS: On

IKE encryption: 3DES

IKE hash: MD5

DH group: Any

IKE re-key time: 3600 (0-78400, 0=Unlimited) secs

DPD action: Hold

DPD keep alive time: 10 secs

DPD timeout: 60 secs

SA life time: 28800 (0-78400, 0=Unlimited) secs

Phase 2 parameters

Remote LAN address: 192 . 168 . 20 . 0

Remote LAN subnet mask: 255 . 255 . 255 . 0

Local LAN address: 192 . 168 . 1 . 0

Local LAN subnet mask: 255 . 255 . 255 . 0

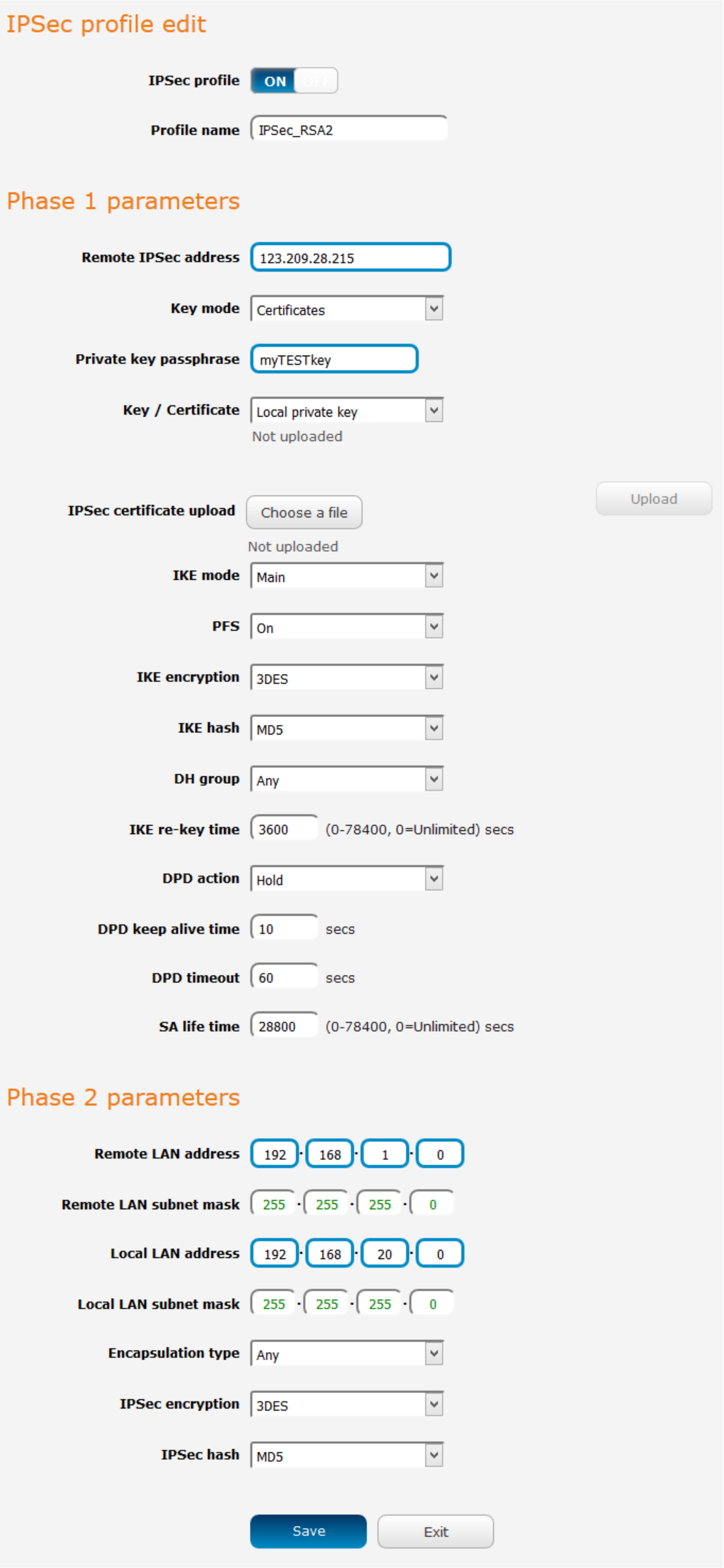
Encapsulation type: Any

IPSec encryption: 3DES

IPSec hash: MD5

Figure 19: IPsec VPN Digital Certificate mode configuration (Local router)

IPsec VPN Digital Certificate mode configuration (Remote router)



IPSec profile edit

IPSec profile: ON

Profile name: IPSec_RSA2

Phase 1 parameters

Remote IPSec address: 123.209.28.215

Key mode: Certificates

Private key passphrase: myTESTkey

Key / Certificate: Local private key

Not uploaded

IPSec certificate upload: Choose a file

Not uploaded

IKE mode: Main

PFS: On

IKE encryption: 3DES

IKE hash: MD5

DH group: Any

IKE re-key time: 3600 (0-78400, 0=Unlimited) secs

DPD action: Hold

DPD keep alive time: 10 secs

DPD timeout: 60 secs

SA life time: 28800 (0-78400, 0=Unlimited) secs

Phase 2 parameters

Remote LAN address: 192.168.1.0

Remote LAN subnet mask: 255.255.255.0

Local LAN address: 192.168.20.0

Local LAN subnet mask: 255.255.255.0

Encapsulation type: Any

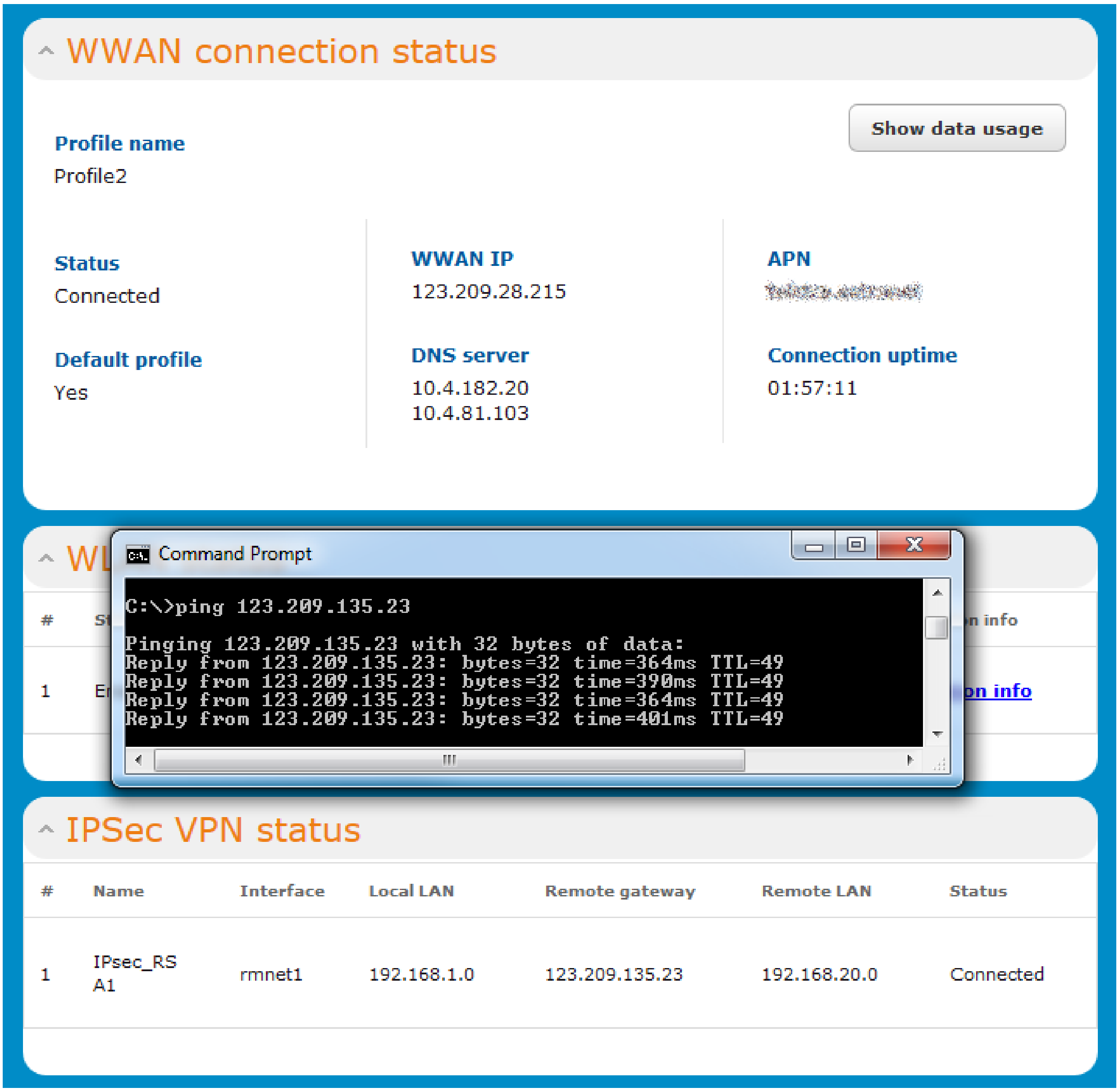
IPSec encryption: 3DES

IPSec hash: MD5

Figure 20: IPsec VPN Digital Certificate mode configuration (Remote router)

Verifying the IPSec VPN connection status

Ping the remote router’s IPsec gateway to verify VPN tunnel connectivity. Refer to the screenshot shown below.



Profile name
Profile2

Status	WWAN IP	APN
Connected	123.209.28.215	[redacted]

Default profile	DNS server	Connection uptime
Yes	10.4.182.20 10.4.81.103	01:57:11

```
C:\>ping 123.209.135.23

Pinging 123.209.135.23 with 32 bytes of data:
Reply from 123.209.135.23: bytes=32 time=364ms TTL=49
Reply from 123.209.135.23: bytes=32 time=390ms TTL=49
Reply from 123.209.135.23: bytes=32 time=364ms TTL=49
Reply from 123.209.135.23: bytes=32 time=401ms TTL=49
```

#	Name	Interface	Local LAN	Remote gateway	Remote LAN	Status
1	IPsec_RSA1	rmnet1	192.168.1.0	123.209.135.23	192.168.20.0	Connected

Figure 21: Verifying the IPSec VPN connection status

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