Broadband for a mobile planet™

BGAN solutions guide

Using VPNs over BGAN

Version 01
15.05.06

www.inmarsat.com/bgan

bgan | inmarsat

Contents

1.0.   Introduction

1.1.   About this guide

This document introduces the VPN protocols and VPN clients that have been tested on the BGAN network, explains how to configure a VPN connection using BGAN LaunchPad, and gives advice on how to optimize your VPN client for use over BGAN.

It is intended for first time end-users, Distribution Partners, Service Providers and anyone who wants to use a BGAN terminal to connect to the BGAN network and use network services. A previous knowledge VPNs and VPN client software, and of the BGAN LaunchPad application is required. A previous knowledge of satellite communications is useful, but not essential.

This document assumes that the VPN client is connected to the BGAN terminal via the Ethernet interface.

The sections include:

- Introduction to VPNs – including the protocols and VPN clients tested over BGAN.

- Configuring a VPN connection using BGAN LaunchPad – explains how to configure a VPN for use over split tunnels and inclusive tunnels.

- VPN Scenarios – single-user, multi-user and workgroup solutions.

- Tests and Analysis – gives the results of comparative VPN client testing, and outlines some of the factors affecting performance.

- Troubleshooting – a small section on possible pitfalls.

1.2.   Other sources of information

- This is one of a series of PDF documents in the BGAN Solutions Guide. The Solutions Guide is designed to help you make the most of your BGAN terminal. Other documents in the series are available for download from **www.inmarsat.com/bgan**. Click on **BGAN support**, then click on **How to guides**.

    This Web site also gives further information on the BGAN service, including Industry solutions.

- Refer to "BGAN LaunchPad Help" for details on using BGAN LaunchPad.

- Refer to the documentation supplied with your VPN client for details on changing configuration and settings.

2.0.   Introduction to VPNs

The BGAN service enables remote offices or users to gain secure access their organization's network using Virtual Private Networks (VPNs) over the public telecommunications network. This provides the benefits of remote access without the expense of dedicated leased or owned lines. VPNs work by using tunnelling protocols, such as L2TP, to encrypt data at the sending end, and decrypt the data at the receiving end.

The following VPN client software has been formally tested over the BGAN network.

- Check Point VPN-1
- Cisco VPN Client
- Juniper Networks NetScreen
- Nortel VPN Client

In addition, the following VPN software has been informally tested:

- NetGear ProSafe™ VPN Client
- Microsoft PPTP VPN Client

2.1.   Protocols used

The VPNs tested use the following protocols (an overview of the protocols is given in section 2.2 "About the protocols"):

VPN	Supported protocols
Check Point VPN-1	PPTP
Cisco VPN Client	L2TP, IPSec
NetScreen	L2TP, IPSec
Nortel VPN Client	L2TP, L2F, PPTP, IPSec
NetGear ProSafe VPN Client	L2TP, IPSec
Microsoft PPTP VPN Client	PPTP

The above protocols use the following ports:

Service	Protocol number	Source port	Destination port
L2TP	17 (UDP)	1701	1701
PPTP tunnel connection	6 (TCP)	1023	1723
PPTP tunnel encapsulation	47 (GRE)	n/a	n/a
ISAKMP/IPSec key management	17 (UDP)	500	500
IPSec tunnel encapsulation	50 (ESP)	n/a	n/a
IPSec NAT transparency	17 (UDP)	1000 (default)	1000 (default)

2.2.   About the protocols

This section introduces the protocols used by VPN software over BGAN.

IPSec

IPSec (IP Security) is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec compliant device decrypts each packet.

PPTP/L2F

PPTP (Point-to-Point Tunnelling Protocol) was developed by the PPTP Forum (which includes Microsoft and US Robotics). The protocol encapsulates PPP packets by encrypting the data payload using MPPE (Microsoft Point to Point Encryption). Authentication is normally carried out using the MSCHAP method. L2F is similar to PPTP, and was developed by Cisco Systems.

L2TP

L2TP (Layer Two Tunnelling Protocol) merges the best features of two other tunnelling protocols: PPTP from Microsoft and L2F from Cisco Systems. The data is encrypted using IPSec, which includes both the data payload and some header information. Encryption uses DES or triple DES (3DES). Authentication is carried out using both username and password and the use of a certificate (or pre-shared key) for additional security over PPTP. In addition, the PPP authentication phase is encrypted (unlike PPTP).

NAT and NAT Traversal

NAT (Network Address Translation) enables routers or gateways to manage multiple devices behind a single device, and translate private IP addresses to public IP addresses on the border of the Internet.

- You can set the **Explorer 500** to operate in NAT mode, which allows multiple users to connect to the terminal and share a single IP data connection (or primary PDP context) over the BGAN network. The terminal uses NAT to allocate a unique private IP address to each connected device, even though the users share the public IP address on the network.

- The **HNS 9201** automatically uses NAT, but works differently to the Explorer 500. Each computer connected to the terminal has its own IP data connection (or primary PDP context), and therefore each has a unique private IP address allocated by the terminal and a unique public IP address on the network. If required, you can configure the HNS 9201 to operate in the same way as the Explorer 500; that is all connected users share one public IP address. To do this, connect a router to the terminal, and connect the computers to the router.

NAT traversal is a technique used by VPNs to establish connections between hosts in private TCP/IP networks that use NAT devices. Both VPN client and server must support NAT Traversal for it to be effective. Nearly all recent versions of VPN software support NAT traversal.

Also, some NAT devices can operate in a VPN pass-through mode. This mode simply allows the device to recognise VPN traffic, and let it pass through the devices firewall.

2.3.   General Principles

Inmarsat recommends that you set up a VPN connection on a standard TCP/IP data connection. The standard IP data connection should operate effectively with VPN protocols and equipment. However it is possible that limitations of end-user equipment or firewalls installed at your BGAN Service Provider, your corporate firewall or the local firewall on your computer may interfere with the use of VPN over BGAN.

NOTE: VPNs operate effectively on a streaming IP data connection, assuming that the VPN server is located at the other end of the dedicated connection.

VPNs are generally set-up in one of three ways:

- **Client to Server (inclusive tunnel)** – All network traffic from the VPN client computer is directed through the VPN tunnel. Therefore, in order to access the Internet, traffic would first go through the VPN tunnel and then get routed to the Internet via the corporate Internet connection.
- **Client to Server (split tunnel)** – All network traffic that is destined for a particular address range will go through the tunnel. Other traffic will be sent directly to the Internet
- **Workgroup to Server** – A workgroup router is connected to the BGAN terminal, which creates a VPN tunnel over the Internet to the corporate VPN server. All traffic generated by clients connected to the router is passed directly over the VPN.

3.0.   Configuring a VPN connection using BGAN LaunchPad

This section explains how to set up VPN connections using BGAN LaunchPad, and how to optimize your VPN connections and software over the BGAN network.

3.1.   BGAN LaunchPad and VPNs

Both the Client to Server (inclusive tunnel) and Workgroup to Server methods disable communications between BGAN LaunchPad and the BGAN terminal whilst the VPN is open. Therefore, BGAN LaunchPad cannot be used for monitoring terminal signal strength, battery levels and so on. In addition, you cannot close the IP data connection using BGAN LaunchPad until the VPN has been disconnected.

If you want to continue to use BGAN LaunchPad whilst the VPN is open, you must use the Client to Server (split tunnel) method.

TIP: If you use the Client to Server (split tunnel) method, ensure that you use a personal firewall on the client computer.
Your firewall will need to allow access to and from the terminal's IP address, and to and from the following port numbers:
- **HNS 9201 – Telnet port 1829**
- **Explorer 500 – Telnet port 5454**

Using BGAN LaunchPad, it is possible to configure a VPN data connection, and to open your VPN client software automatically using the data connection. The configuration method differs depending on whether you are using an inclusive tunnel or split tunnel.

NOTE: If required, you can configure BGAN LaunchPad to open a VPN automatically after registration.

### 3.2.   Configuring a split tunnel VPN connection using BGAN LaunchPad

This section explains how to configure a VPN connection in BGAN LaunchPad, and, if required, open your VPN client software automatically when you open the connection. This procedure applies to split tunnel VPNs, which enables you to continue to use BGAN LaunchPad whilst the VPN is open.

To configure the VPN:

1. Open BGAN LaunchPad, and select the **Data** icon. The Data Connections screen is displayed, as shown below:
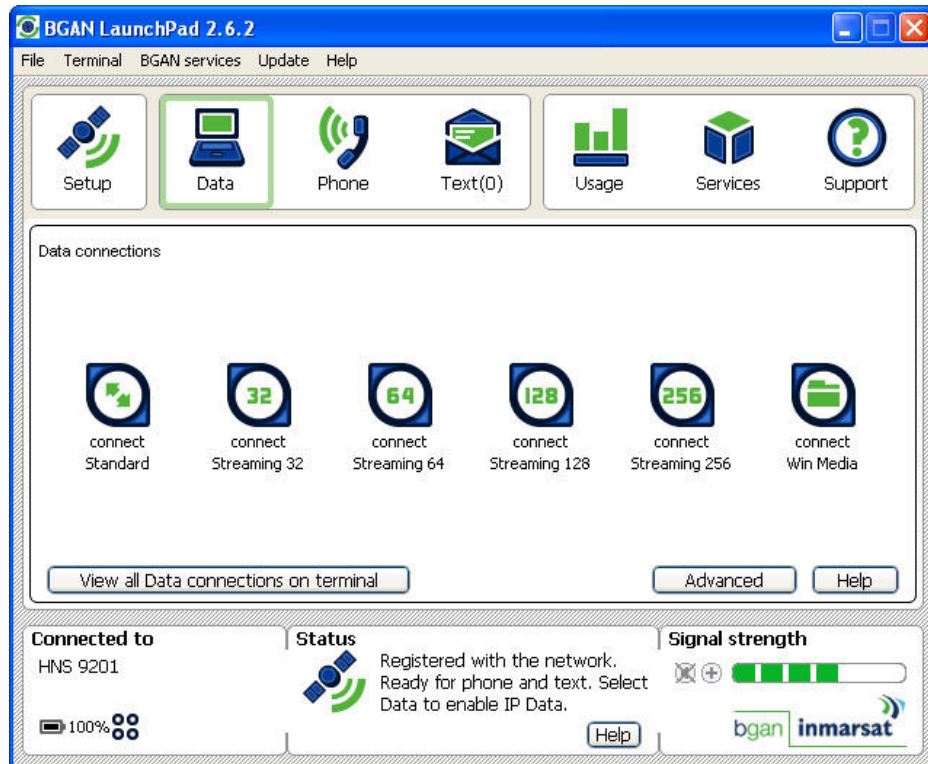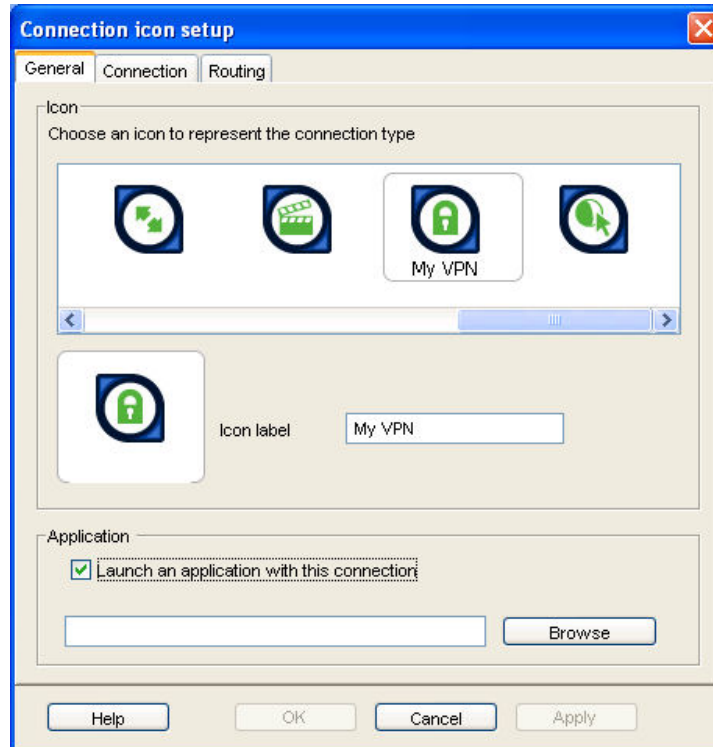

2. Click on **Advanced**. The Connection icon setup window is displayed, as shown below:
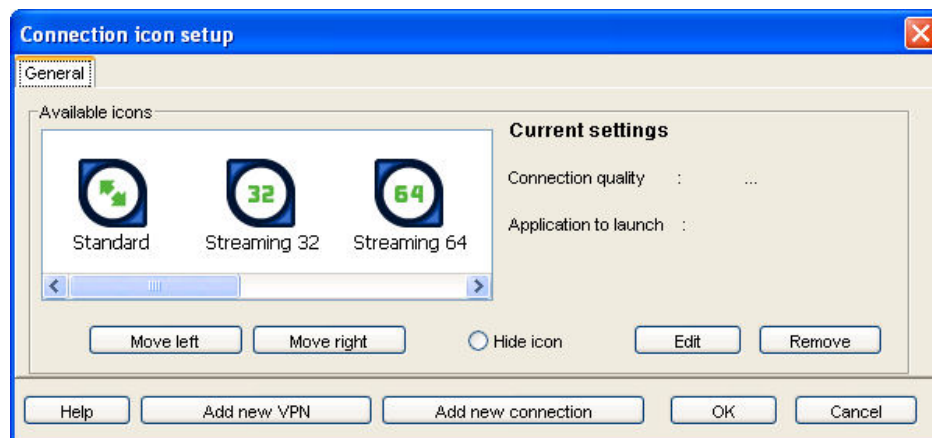
3. Click on **Add new connection** (<u>not</u> Add new VPN). The **Connection icon setup –
    General** tab is displayed, as shown below:

4. Select an icon to associate with the VPN connection, and enter a name for the connection
    in the Icon label field.

5. If you want to configure BGAN LaunchPad to automatically open a specific VPN client with
    this connection, check the **Launch an application with this connection** check box, and
    click on **Browse** to display a search window. Search for the executable file for your VPN
    client, and click on **Open** to import the file into the Application text box.

    **NOTE: You do not have to check the application check box and enter a
              filename. If you only want to configure this data connection to open a
              VPN tunnel, and not a VPN client, leave the check box blank. You can
              then use BGAN LaunchPad to open a VPN tunnel, and open your VPN
              client separately.**

6. Use the **Connection** and **Routing** tabs to select the profile of the connection you want to
    use for your VPN. Refer to "BGAN LaunchPad Help" for details.

7. Click on **OK** to save your settings. The VPN icon displays in the Data Connections
    window.

To open the VPN connection from BGAN LaunchPad, click on the VPN icon that you created. If
you chose a VPN client in step 5, a Username and Password dialog box may be displayed by your
VPN client. Your VPN client confirms connection in the normal way.

To close the VPN client <u>and</u> the VPN data connection, click on the VPN icon in BGAN LaunchPad.

**NOTE: If you close your VPN client only, the BGAN data connection remains open.**

TIP: **Depending on the VPN client you are using, you may also need to configure your VPN client to start automatically on opening. This ensures that BGAN LaunchPad can successfully establish a VPN connection. Refer to section 3.4 "Configuring your VPN client to automatically open a VPN" for details on any further configuration required.**

3.3.   Configuring an inclusive tunnel VPN connection using BGAN LaunchPad

This section explains how to configure a VPN connection in BGAN LaunchPad, so that your VPN application opens automatically when you open the connection. This procedure applies to inclusive tunnel VPNs and workgroup VPNs, which disable the connection between BGAN LaunchPad and the terminal whilst the VPN is open.
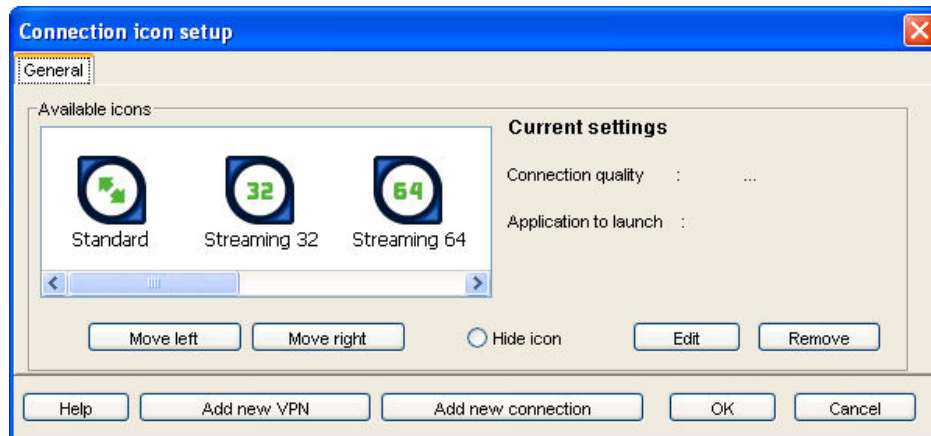
To configure the VPN:

1.   Open BGAN LaunchPad, and select the **Data** icon. The Data Connections screen is displayed, as shown below:
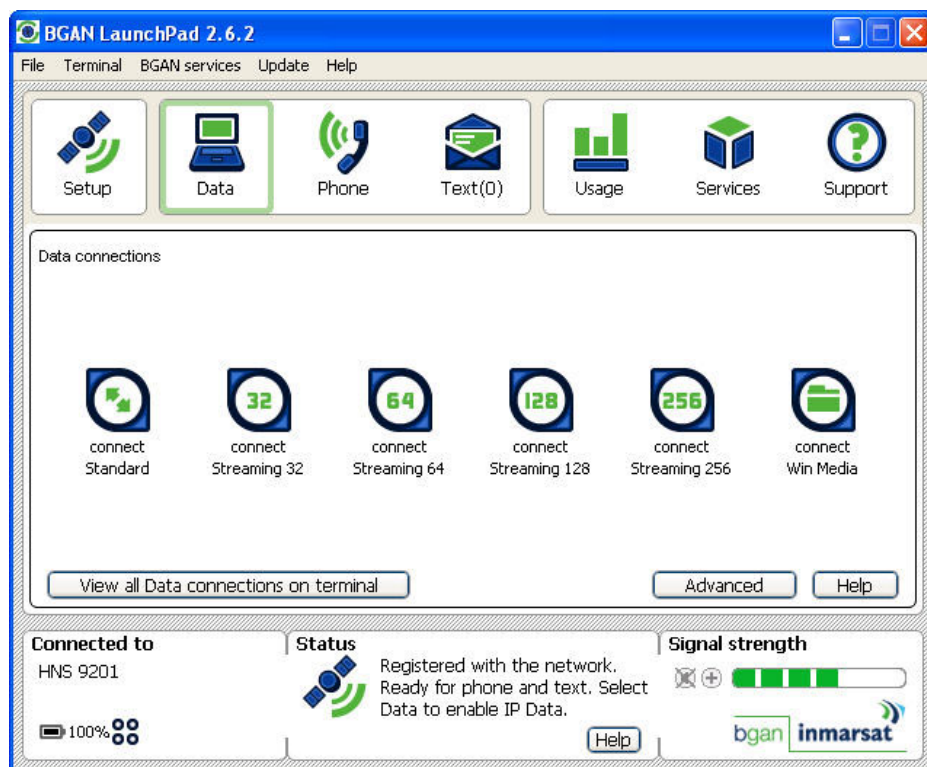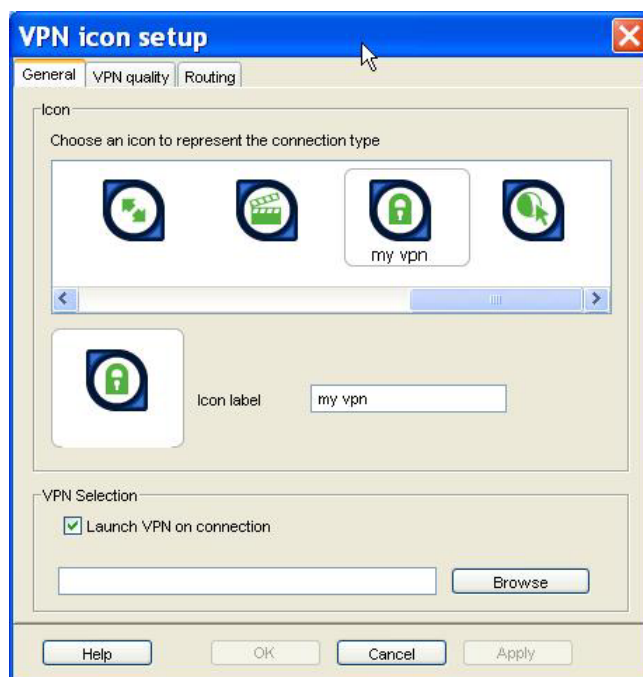
2. Click on **Advanced**. The Connection icon setup window is displayed, as shown below:

3. Click on **Add New VPN**. The **VPN icon setup – General** tab is displayed, as shown below

4. Select an icon to associate with the VPN connection, and enter a name for the connection in the icon label field. Then, check the **Launch VPN on connection** check box, and click **Browse**.

5. If you want to configure BGAN LaunchPad to automatically open a specific VPN client with this connection, check the **Launch an application with this connection** check box, and click on **Browse** to display a search window. Search for the executable file for your VPN client, and click on **Open** to import the file into the Application text box.

NOTE: You do not have to check the application check box and enter a filename. If you only want to configure this data connection to open a VPN tunnel, and not a VPN client, leave the check box blank. You can then use BGAN LaunchPad to open a VPN tunnel, and open your VPN client separately.

6. Use the **Quality** and **Routing** tabs to select the profile of the connection you want to use for your VPN. Refer to "BGAN LaunchPad Help" for details.

7. Click on **OK** to save your settings, and display the VPN icon in the Data Connections window.

To open the VPN connection from BGAN LaunchPad, click on the VPN icon that you created. If you chose a VPN client in step 5, a Username and Password dialog box may be displayed by your VPN client. Your VPN client confirms connection in the normal way.

Whilst the VPN connection is open, BGAN LaunchPad cannot view the terminal, and you cannot monitor the terminal or manage any terminal operations.

To close the VPN client <u>and</u> the VPN data connection, click on the VPN icon in BGAN LaunchPad.

NOTE: If you close your VPN client only, the BGAN data connection remains open.

TIP: Depending on the VPN client you are using, you may also need to configure your VPN client to start automatically on opening. This ensures that BGAN LaunchPad can successfully establish a VPN connection. Refer to section 3.4 "Configuring your VPN client to automatically open a VPN" for details on any further configuration required.

3.4.   Configuring your VPN client to automatically open a VPN

Depending on the VPN client you are using, you may need to configure your VPN client to automatically open a VPN connection. In particular, if you want to open your VPN client automatically from BGAN LaunchPad, you must configure your VPN client software are described below.

For Cisco VPN Client:

1. Choose your VPN connection, and select the **Set as Default Connection Entry** from the Connection menu.
2. Select **Option > Preferences**, and then check **Enable connect on open.**

For NetScreen:

1. Start the Security Policy Editor, and choose your connections from the **My Connections** folder.
2. Uncheck the option **Only Connect Manually**. Your VPN connection automatically starts when you attempt to connect to a host on the remote VPN subnet.

For Nortel VPN Client and Check Point VPN-1, no configuration is required.

4.0.   VPN Scenarios

The following sections give an example of VPN scenarios that have been tested with BGAN.
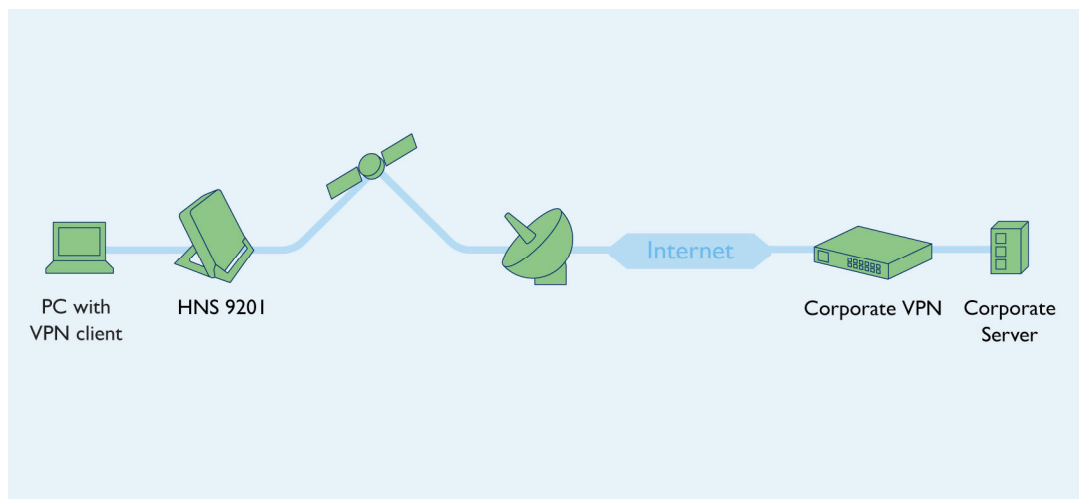
Recommendations

To maximize the efficiency of the VPN connection, Inmarsat recommends the following:

- **Explorer 500** – set up the terminal to open a standard IP data connection automatically. The Explorer 500 can be set up to exit pointing and open a connection automatically. Refer to "BGAN LaunchPad Help" for details.
- **HNS 9201** – set up the terminal to operate in Auto-start mode, and to allocate the static IP address 192.168.128.101 to the VPN gateway. Refer to "BGAN LaunchPad Help" for details on Auto-start mode.

4.1.   Single VPN client to corporate server

In this scenario, a single PC client is used to connect to a corporate server via BGAN. In all cases, the client can be connected via the USB or Ethernet interface, as required.

PC with   HNS 9201   Corporate VPN   Corporate
VPN client   Server
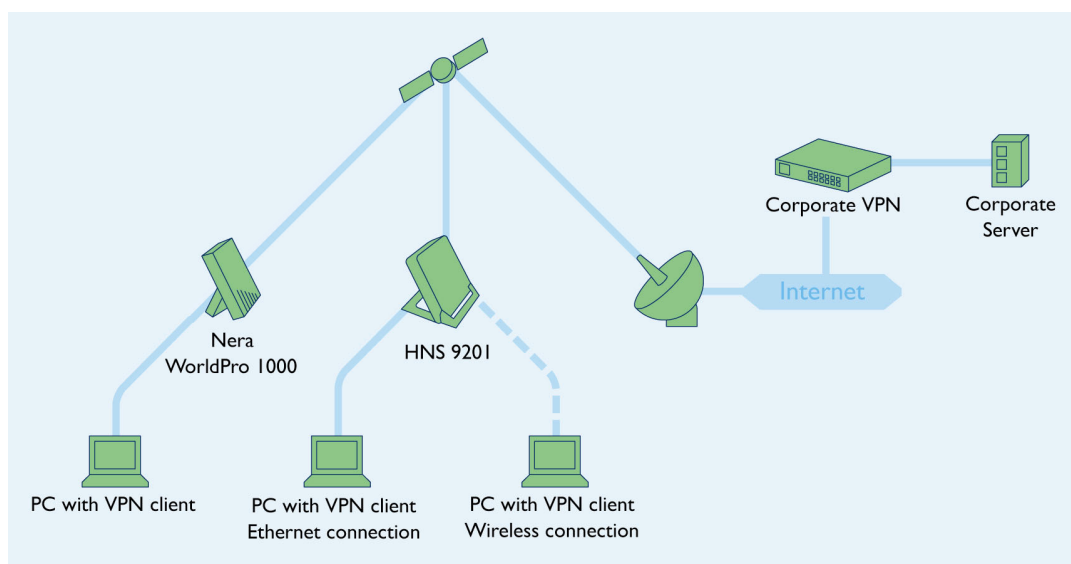
Recommendations

- When using Ethernet, configure the client computer to automatically obtain an IP address from the terminal.
- When using USB, configure the VPN client to use the BGAN terminal as a dial-up modem device.
- When using the Explorer 500, configure the terminal to operate in Modem mode. Some VPN clients do not work when the terminal is set to operate in NAT mode.

NOTE: The HNS 9201 presents a network adapter to the computer when connected via USB, so it operates in the same way as the Ethernet connection.

4.2.   Multiple VPN clients to corporate server

This scenario shows two different ways of using VPN clients with a BGAN terminal. The first client is connecting to the corporate VPN using a Nera WorldPro 1000, whilst the other two clients are connected via an HNS 9201. Note that the two clients using the HNS 9201 are allocated separate primary PDP contexts.

Corporate VPN   Corporate Server

Internet

Nera WorldPro 1000   HNS 9201

PC with VPN client   PC with VPN client Ethernet connection   PC with VPN client Wireless connection

4.3.   Workgroup VPN

Connecting a workgroup VPN requires the use of a VPN gateway or router, which is directly connected to the BGAN terminal. Client computers can then be connected to the VPN gateway via a network or wireless connection.

See the diagram on the next page for a possible scenario.

Recommendations

- The VPN gateway must be configured to have a public IP address that is on the same subnet as the BGAN terminal.
  - o   HNS 9201 – configure the terminal to operate in Auto-start mode. Auto-start mode activates the first PDP context automatically, and allocates uses the IP address 192.168.128.101 to the VPN gateway.
  - o   Explorer 500 – configure the terminal to operate in Modem mode. In Modem mode, the Explorer 500 transparently passes a public IP address to the VPN gateway when connected to the BGAN network.
  - o   Nera WorldPro 1000 – At the time of publication, the terminal does not support an Ethernet interface, and so requires a VPN router which is capable of activating the Nera terminal.
- Configure the terminal to automatically connect to the BGAN network, where possible. If you do not configure automatic connection, you must manually open a data connection using BGAN LaunchPad, before the VPN can be used. This requires that the VPN gateway allows traffic between the client network and the terminal.

HNS 9201

VPN
Gateway/Router

PC   PC   PC

Internet

Corporate VPN

Corporate
Server
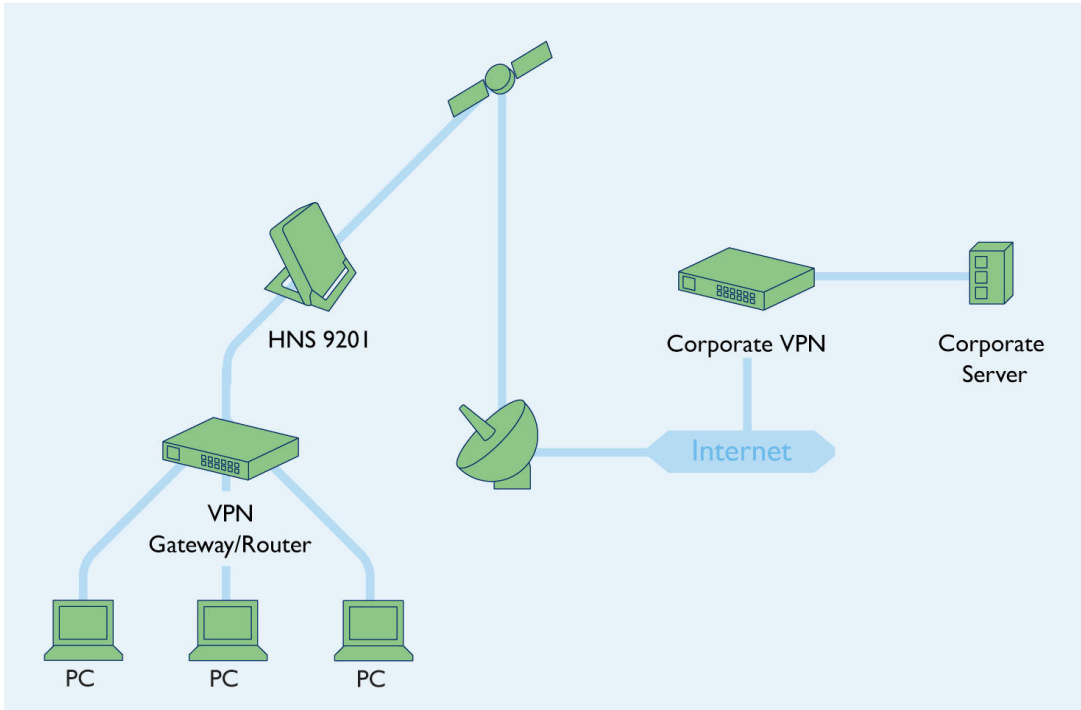
5.0.   VPN performance

Inmarsat has run a series of tests over BGAN using the four most commonly used VPN clients detailed in section 2.1 "Protocols used". In addition the set-up of the VPNs was checked to identify any changes required to make the protocols work more efficiently over BGAN.

5.1.   Tests carried out

The tests that were carried out involved the use of standard applications over a VPN connection. These were:

- FTP
- Email: SMTP, POP, IMAP

In addition, some ad-hoc tests were carried out with a number of other office applications, such as video conferencing.

The tests were also carried out without the VPN in place, to judge how much overhead, if any, the VPN added to the connection. VPNs provide compression, as encrypting data usually increases the size of transmitted data packets. However, it was found that if the data was compressed first, then encrypted, the resultant data stream was often smaller than one outside of a VPN. For this reason, it is not expected that VPNs will cause any issues with BGAN, and in most cases will not increase the amount of data sent and received by a significant amount, if at all.

The following graph above shows a comparison of the throughput using all four VPNs with an HNS 9201, over a standard IP data connection.
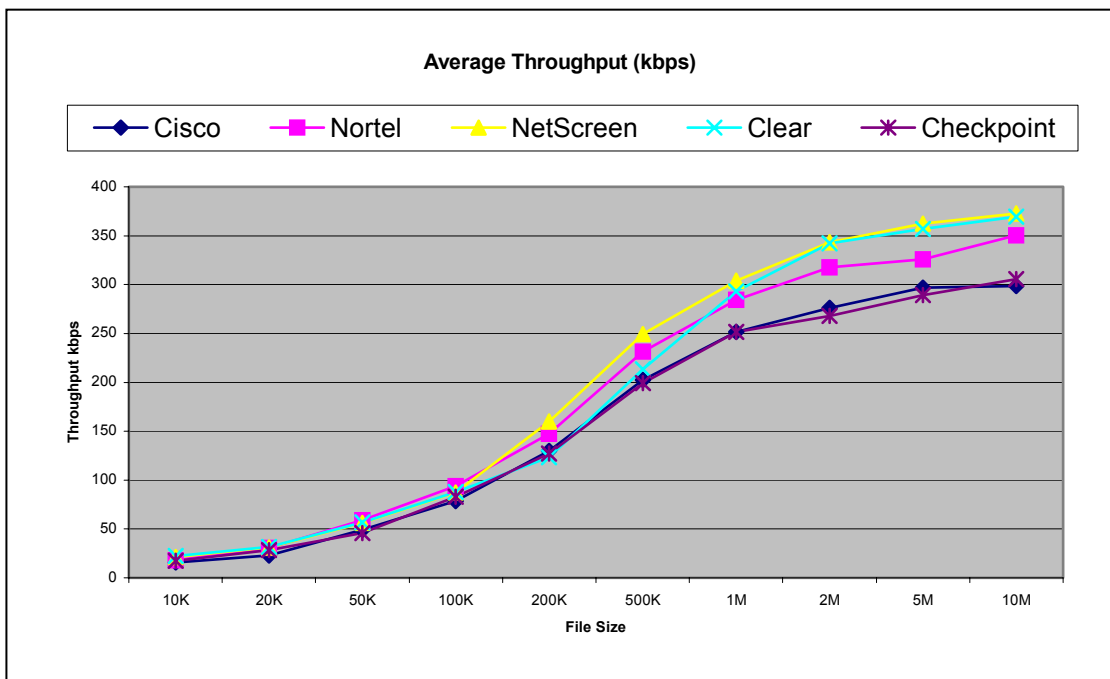
NOTE: Some of these differences in this graph are due to the variation in available bandwidth on the standard IP data connection. Thus, this graph alone cannot be used to determine which VPN is the most efficient over the BGAN network.

5.2.   Factors affecting VPN performance

VPN encapsulates network traffic destined for corporate servers by encrypting the data packets, and sending them as data in normal internet data packets. There are four main factors affecting the performance of VPNs. These are described in the table below:

Factor	Description
Signalling and Connection control	A VPN connection must be initiated by the exchange of secure password and/or certificate information between the client and server. This extra data send backwards and forwards may be in the order of 2-5KB both when connecting and disconnected the VPN. In addition, most VPNs send keep-alive packets to ensure that the VPN remains open. A typical IPSec based VPN will send between 2-3KB every 10 minutes or so. **NOTE: Do not leave a VPN connection running when not in use.**
Data Encapsulation	Taking a data packet and encapsulating it in another one will add an additional set of headers. Most VPNs use UDP encapsulation, so this adds another 7 bytes of information to each packet. Assuming a packet size of around 1200 bytes, this gives an overhead of about 0.5% **TIP: Use UDP encapsulation over TCP where configurable.**
Encryption method	All data send across a VPN is encrypted. The encryption algorithm used may increase the size of the data to be transmitted. The overhead depends on the algorithm used. In addition, a CPU overhead is added here, as the encryption algorithms are heavy on CPU usage. **TIP: Choose a 'lighter' encryption algorithm, if speed is more important than security.**
Compression method	Most VPNs attempt to compress the data as well as encrypt it. This is the one factor that decreases the overhead of a VPN. By using the correct encryption and encapsulation methods with a good compression algorithm may mean that using a VPN is more efficient than *not* using one. A CPU overhead is added when using compression. **TIP: Always ensure than compression is enabled.**

6.0.   Troubleshooting

- **You are having trouble initiating a VPN connection**. Make sure that your connection to the Internet is working correctly. If the Internet connection is not working, you cannot open a VPN.

- **You are configuring site-to-site VPNs on the HNS 9201**. Any site behind the HNS 9201 must use the address range of 192.168.128.0 to 192.168.128.24. Remember that the terminal's own address is 192.168.128.100.

- **You have connected a VPN router to the BGAN terminal but it does not have the same IP address as the previously connected device.** The terminal allocates IP addresses based on the MAC address of the connecting device. If you want the VPN router to have the same IP address as the previously connected computer, you must restart the terminal to clear the DHCP lease information.