Using Innominate mGuard over BGAN

Version 2

6 June 2008

inmarsat.com/bgan

Contents

1 Overview

Innominate mGuard is a superior and easy to use mobile security solution, offering reliable firewall, VPN functionality and protection against viruses – all in a single small device. The mGuard technology is based on Innominate's innovative decentralized security concept, which eliminates the drawbacks associated with conventional security concepts in a simple, reliable and cost-effective manner.

mGuard smart is an independent platform about the size of the palm of your hand. It can be installed quickly and effortlessly by anyone, and requires no modifications to the BGAN satellite IP modem, the connected network or the computer configuration.

Moreover, it runs independently of the processor technology as well as the operating system of the connected PC, laptop or network. With "plug and protect" capability, mGuard can be installed and operated without requiring specific security know-how. It merely needs to be integrated externally between the computer or any other network system and the network connection provided via the BGAN satellite IP modem.

Power can be supplied via the free USB port of the connected computer, so that no separate power-socket is required.

The mGuard system is universally compatible. Other forms are available, such as the mGuard PCI – a PCI card for integration into a standard desktop PC – if required.

1.1 Single Stealth mode

mGuard features the unique Innominate "Single Stealth Mode". This allows the device to work completely transparently, requiring no IP address of its own. mGuard uses the same IP as the computer it is protecting and therefore cannot be recognized by invaders, making it resistant to attack.

To use the "Single Stealth Mode" setting, nothing needs to be reconfigured or modified on the mGuard. At the same time, it is possible to customize each individual mGuard device, even in Stealth Mode, to special security requirements.

1.2 Product range

Innominate offers mGuard in several forms, each providing identical functionality. The products are:

- mGuard smart - for mobile users.
- mGuard PCI - for integration into desktop PC or server.
- mGuard delta - for use in SOHO environments.

Single mGuard devices can be managed and configured via Web interface. For larger mGuard network installations, Innominate offers the IDM – Innominate Device Manager, a template based device management system supporting installations of up to several thousand devices.

2 Typical users

- Remote office workers.
- Military, government and surveillance personnel.
- Special interest groups.
- Anyone transferring confidential information over public networks.
- Companies that wish to cover satellite based communication with their security policy.

3 Key features

mGuard is a plug and protect, cost effective security appliance for mobile use. Key features include:

- VPN router for secure data transmission via satellite links and IP networks (hardware-based DES, 3DES and AES encryption, IPsec protocol).
- 1:1 NAT in VPN for simple management of VPN connections.
- Configurable firewall – protects the system from unauthorized access from “outside”.
- The Innominate Stealth Mode ensures the mGuard system is indiscernible for invaders and allows its instant integration in existent network configurations without reconfiguration.
- QoS (Quality of Service) features guarantee the required bandwidth allocation and support a prioritization of data-traffic.
- Integrated ClamAV virus protection (optional) supporting the protocols HTTP, SMTP and POP3.

4 Benefits to BGAN users

mGuard offers you the following main benefits:

- Mobile and lightweight solution.
- Power supply via USB interface of connected laptop / PC.
- Hardware security appliance with high performance (firewall up to 99 mbps, VPN up to 70mbps).
- Plug and protect - no interference with network topology and protected system.
- Compatible with IPsec compliant VPN gateways.

5 Setting up

This section describes how to set up BGAN and mGuard to be used together, and gives an example of an mGuard configuration.

As stated earlier, mGuard can be operated in several ways - stealth mode and router mode are explained here.

5.1 Stealth mode operation

The stealth mode is the factory default setting for mGuard devices. This mode provides security and VPN capabilities **for a single device** and is the easiest way to get secure communication setup and running:

- mGuard will operate with the static and dynamic BGAN IP settings , and also with public or private IP addresses
- Use an Ethernet cable to connect the BGAN terminal's Ethernet port to the Ethernet port of the mGuard. Then plug the mGuard's own Ethernet connector into the Ethernet port on your computer's network card.
- In order to automatically configure DNS, the mGuard stealth mode needs to receive ping replies from your local system, therefore make sure any installed local firewall allows ping requests/ replies.
- Connect the mGuard's USB connector to a free USB port on your computer and give the device 40 seconds to boot
- Make sure traffic has been initiated, so mGuard can test the network settings and setup automatically for you.
- Check for the mGuard availability by sending a ping to IP 1.1.1.1 or try to access **https://1.1.1.1** using your preferred web browser

The device will now provide basic security, allowing outgoing traffic and denying any kind of unrequested, incoming traffic

For additional firewall, anti virus protection, QoS and VPN configuration, consult the mGuard documentation.

Stealth mode operation

mGuard smart protects a single laptop computer connected to the BGAN terminal

5.2 Router mode operation

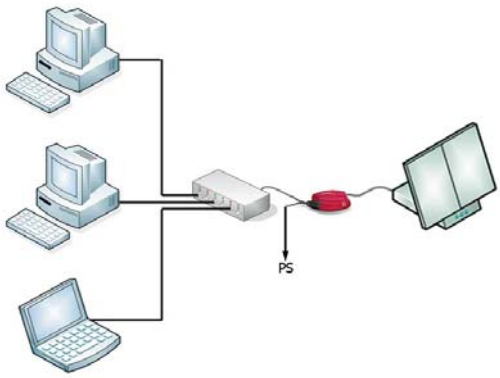
The router mode is the recommended configuration for mGuard devices, and provides security and VPN capabilities **for a series of devices.** This mode is the easiest way to get local network protection setup and running:

- mGuard will operate with static and dynamic BGAN IP settings , also with public or private IP addresses
- Use an Ethernet cable to connect the BGAN terminal's Ethernet port to the Ethernet port of the mGuard. Then plug the mGuard's own Ethernet connector into an Ethernet port on your router or switch.
- Connect the mGuard's USB connector to a free USB port and give the device 40 seconds to boot.
- If the mGuard was already configured as a router, connect to the correct IP address. If the mGuard is still in a factory default setting, access the mGuard's user interface as described in the supplied documentation.

- Set up the following initial settings:
  - Enable NAT for the IP range of 0.0.0.0/0
  - Enable DHCP for the internal interface of the mGuard
  - Enable or disable HTTPS access to the mGuard from the external interface. (From the internal interface access is allowed by default.)
  - Configure the mGuard to automatically receive its external IP via DHCP or set it up manually
  - Set up the internal interface IP address of the mGuard
  - Change the network mode to *router*
  - Write down the new IP address which you can use to access the device
  - Open a shell/DOS window, enter “arp –d” and press enter
  - Wait for the mGuard to finish it’s reboot
- In order to route traffic for more than one system, a Switch (or Hub) needs to be connected to the mGuard’s internal interface. Connect all systems you wish to protect to this switch (or hub).

The device will now provide basic security, allowing outgoing traffic and denying any kind of unrequested, incoming traffic

For additional firewall, anti virus protection, QoS and VPN configuration, consult the mGuard documentation



Router mode operation

mGuard smart in combination with an Ethernet switch can protect a network of computers connected to the BGAN terminal. Additional power supply for mGuard smart might be required (or USB of one of the connected PCs can be used)

5.3 Equipment needed

Minimum requirement:

- BGAN terminal
- Protected system (laptop, PC,..) with BGAN software and network adapter installed
- Unused USB port
- 2 pieces of twisted or untwisted Ethernet cable
- One mGuard device

6 Hints and tips

The following are best practice hints and tips to ensure you get the most from mGuard over BGAN:

- If setting up the mGuard for the first time, make sure, your communication works fine without the security device before plugging in the mGuard.
- For the most secure VPN setup, we recommend using X.509 certificates on both sides of the tunnel. Establish the VPN tunnel from the mGuard BGAN side and try to use smallest possible keysize by reducing the amount of key parameters to at least the common name while using 512bit keys.
- When accessing the mGuard it might be necessary to disable the proxy settings of your browser.

7 Technical summary

The mGuard technical feature sets are summarized below

	mGuard 266/VPN	mGuard 533/VPN
Firewall performance	99 mbps	
VPN performance	35 mbps	70 mbps
Anti Virus protection (requires additional licence)	Not recommended	Yes
BGAN addressing requirement	Static or dynamic	
Hardware solution	Yes	
Protocols supported	all IPv4 based protocols	
QoS, Bandwidth management	Yes	
Network modes	Stealth, router	

8 Further details and support

Inmarsat Contact:

Customer_care@inmarsat.com

Innominate contact details:

Innominate Security Technologies AG

Albert-Einstein Str. 14

12489 Berlin

Germany

Email: bgan@innominate.com

Tel.: +49 30 63923300

Internet:

http://www.innominate.com/content/view/96/144/lang,en/